RICE UNIVERSITY

New Security Threats in Multiple-Antenna Networks: Analysis and Experiments

by

Xu Zhang

A THESIS SUBMITTED
IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE
Doctor of Philosophy

APPROVED, THESIS COMMITTEE:

Edward W. Knightly, Chair
Sheafor-Lindsay Professor of Electrical and Computer Engineering and Computer Science

Behnaam Aazhang
J.S. Abercrombie Professor of Electrical and Computer Engineering

Lin Zhong
Professor of Electrical and Computer Engineering and Computer Science

Dan S. Wallach
Professor of Computer Science and Electrical and Computer Engineering

Houston, Texas
November, 2017
ABSTRACT

New Security Threats in Multiple-Antenna Networks: Analysis and Experiments

by

Xu Zhang

Due to the multiple to massive number of antennas at the Access Point (AP), the performance of wireless network has substantially improved over the last decade. However, new security threats also arise, mainly because of the redesign of wireless protocols that adapt to these many antennas, as well as the critical dependence of the multi-fold increases on Channel State Information (CSI), a key parameter in multiple-antenna networks. In this thesis, I study two security threats of CSI that are closely related to its core properties. First, I analyze the confidentiality of CSI with a passive adversary. I discover that CSI is no longer confidential in a multi-user MIMO network, because there is a fundamental conflict between using CSI to optimize PHY design and hiding CSI from malicious nodes. I present CSIsnoop, a framework by which a passive adversary can infer any client’s CSI, even when both channel sounding sequence from the AP and CSI measurement feedback from the clients are encrypted during downlink channel sounding, or when uplink channel sounding is employed. I implement CSIsnoop on a software defined radio and collect over 100,000 over-the-air transmissions in various indoor environments. CSIsnoop’s high estimation accuracy urges reconsideration of the use of CSI as a tool to enhance physical layer security in multi-user MIMO networks. Second, I analyze the integrity of CSI with an active adversary. I present and model the Pilot Distortion Attack, a highly efficient
yet devastating jamming strategy targeting the channel sounding process, in which the adversary distorts the AP’s CSI measurement of even a single client leading to denial-of-service for all clients associated with the AP. As a countermeasure, I propose MACE, which exploits the AP’s multiple antennas to detect Pilot Distortion Attack, as well as general jamming in wireless network, with zero startup cost, zero additional network overhead, and no coordination between the AP and the clients. I build a testbed with the Argos 72-antenna AP and collect over 3,000,000 over-the-air transmissions. My experiments demonstrate the devastating impacts of the Pilot Distortion Attack, as well as the superior detection performance of MACE.
Acknowledgments

First, I would like to express my gratitude to my advisor, Professor Edward Knightly, for your advice and guidance throughout my study at Rice. You always push me to go one step further and show me the possibilities when I am satisfied, and pull me forward at my difficult times. I have learned far beyond what can be included in this thesis from you.

Next, I would like to thank my committee members, Professor Behnaam Aazhang, Professor Lin Zhong, and Professor Dan Wallach, for their invaluable comments on my thesis and advice in these many years. Specifically, I would like to thank Professor Lin Zhong for those inspiring discussions. Furthermore, I would like to express my gratitude to my group mates Oscar, Ryan, Naren, Adriana, Sharan, Yasaman, Kumail, Peshal, Jonghun, Chia-Yi and Riccardo, for joining me in numerous discussions, providing valuable feedback, and helping me shape all my projects. It is really wonderful to be a member of the Rice Network Group. In addition, I would like to thank Ryan, Naren, Clay and Abeer for their support and help with my experiments. I am also very fortunate to have been surrounded by brilliant friends and colleagues Shuqiao Jia, Peiyu Chen, Xu Du, Xing Zhang, Kaipeng Li, Jian Ding, Boqiang Fan and Shi Su. They are always willing to discuss with me with great patience, help me review my initial ideas and provide valuable feedback.

I owe all my success to my parents, Guoliang Zhang and Weiwen Xu. They teach me how to be perseverance even at my hardest times. Their continuous and unconditional support encourage me to accomplish each of my milestones.

Last, I would like to thank the most important person, Fei Wang, for accompanying me throughout this tough yet exciting journey, for encouraging me to never give
up, and for supporting me to pursue each of my dreams. Without you, I would not have been able to achieve this.
Contents

Abstract ii
Acknowledgments iv
List of Illustrations ix
List of Tables xv

1 Introduction 1

2 Confidentiality of Channel State Information in Multiple-Antenna Networks 5
   2.1 Introduction . 5
   2.2 Threat Model . 9
   2.3 CSIsnoop . 11
      2.3.1 Base Case Analysis of $K \times K$ . 11
      2.3.2 Generalization to $M \times K$ with $M < K$ . 14
   2.4 Estimating $H_{AE}$ between Alice and Eve . 16
      2.4.1 Estimating $H_{AE}$ with Encrypted Downlink Channel Sounding . 16
      2.4.2 Estimating $H_{AE}$ with Uplink Channel Sounding . 18
   2.5 CSIsnoop+a . 22
   2.6 Implementation . 25
   2.7 Experimental Evaluation . 27
      2.7.1 Experimental Setup . 28
      2.7.2 Accuracy of CSIsnoop . 29
      2.7.3 Impact of $H_{AE}$ . 31
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.7.4</td>
<td>Number of Known Symbols and Overheard Packets</td>
<td>33</td>
</tr>
<tr>
<td>2.7.5</td>
<td>Number of Clients and Data Streams</td>
<td>37</td>
</tr>
<tr>
<td>2.7.6</td>
<td>Computation of $H_{AE}$ with Encrypted Downlink Sounding Sequence</td>
<td>38</td>
</tr>
<tr>
<td>2.7.7</td>
<td>Computation of $H_{AE}$ with Uplink Sounding Sequence</td>
<td>40</td>
</tr>
<tr>
<td>2.8</td>
<td>CSI-based Attacks</td>
<td>44</td>
</tr>
<tr>
<td>2.8.1</td>
<td>Computing CSI-Based Password</td>
<td>44</td>
</tr>
<tr>
<td>2.8.2</td>
<td>Removing Artificial Noise</td>
<td>46</td>
</tr>
<tr>
<td>2.8.3</td>
<td>Decreasing Network Throughput</td>
<td>47</td>
</tr>
<tr>
<td>2.9</td>
<td>Counter Mechanisms</td>
<td>51</td>
</tr>
<tr>
<td>2.10</td>
<td>Conclusion</td>
<td>51</td>
</tr>
<tr>
<td>3</td>
<td>Integrity of Channel State Information in Multiple-Antenna Networks</td>
<td>53</td>
</tr>
<tr>
<td>3.1</td>
<td>Introduction</td>
<td>53</td>
</tr>
<tr>
<td>3.2</td>
<td>Threat Model</td>
<td>57</td>
</tr>
<tr>
<td>3.3</td>
<td>Pilot Distortion Attacks</td>
<td>58</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Thwart Concurrent Uplink Transmission by Distorting CSI of a Single Bob</td>
<td>59</td>
</tr>
<tr>
<td>3.3.2</td>
<td>CSI Distortion of Multiple Bobs</td>
<td>62</td>
</tr>
<tr>
<td>3.4</td>
<td>Jamming Detection with $MACE$</td>
<td>64</td>
</tr>
<tr>
<td>3.4.1</td>
<td>CFO Estimation with a Single Receiving Antenna</td>
<td>64</td>
</tr>
<tr>
<td>3.4.2</td>
<td>System Architecture of $MACE$</td>
<td>65</td>
</tr>
<tr>
<td>3.4.3</td>
<td>Variance of CFO Estimates without Jamming</td>
<td>67</td>
</tr>
<tr>
<td>3.4.4</td>
<td>Variance of CFO Estimates with Jamming</td>
<td>69</td>
</tr>
<tr>
<td>3.4.5</td>
<td>Per-Frame Random CFO Injection by Bobs</td>
<td>71</td>
</tr>
<tr>
<td>3.4.6</td>
<td>Discussions</td>
<td>73</td>
</tr>
<tr>
<td>3.5</td>
<td>Experimental Evaluation</td>
<td>74</td>
</tr>
</tbody>
</table>
3.5.1 Experimental Setup ................................................ 74
3.5.2 Achievable Rate Reduction due to Pilot Distortion Attacks .. 76
3.5.3 Validation of the Two Assumptions of CFO Estimates ........ 79
3.5.4 Variance of Normalized CFO Estimates without Jamming ... 81
3.5.5 Variance of Normalized CFO Estimates with Jamming ....... 84
3.5.6 ROC Curves of MACE .............................................. 85
3.5.7 Impact of Number of Antennas and Repeated Symbols ....... 90
3.6 Conclusion ................................................................. 94

4 Related Work .............................................................. 95
    4.1 Confidentiality of Channel State Information in Multiple-Antenna Networks ......................................................... 95
    4.2 Integrity of Channel State Information in Multiple-Antenna Networks ................................................................. 97

5 Conclusion ................................................................. 99

Bibliography ................................................................. 100
Illustrations

2.1 Threat model of CSIsnoop. ................................. 9
2.2 Base case analysis of CSIsnoop, where Bobs’ data stream number
equals the number of antennas at Alice in one downlink transmission. 11
2.3 CSIsnoop combines the computation of multiple downlink
transmissions to compute the CSI of a target Bob. ............... 15
2.4 VHT PPDU format of IEEE 802.11ac [1] and IEEE 802.11af [2] (with
different length of each field). The Null Data Packet for downlink
channel sounding has the same format except that there is no data field. 17
2.5 Absolute normalized correlation between the dynamic cyclic shift
beamforming weights with different values of the sub-carrier gap r. 21
2.6 For CSIsnoop+a, Eve becomes active and joins in the downlink
transmission, which enables Eve to compute $H_{AB}$ more quickly in
certain scenarios. .................................................. 24
2.7 Fractional timing offset due to ADC sampling. .................. 27
2.8 Experiment timeline. ........................................... 28
2.9 CCDF of the absolute value of normalized correlation between
$H_{AB,meas}$ and $H_{AB,comp}$, and $H_{AB,meas}$ and $H_{AE}$. (b) is the zoomed-in
upper-right portion of (a). ...................................... 30
2.10 The variation of $C$ (median with 25th/75th percentile) over (a) the
average signal SNR at Eve and (b) the average condition number of
$H_{AE}$. Alice has 4 antennas. ................................. 32
2.11 Variation of $C$ over the number of known symbols by Eve. ....... 34
2.12 (a) and (b) plot the variation of $C$ over the number of overheard transmissions by Eve (20 known symbols per transmission). In particular, for (a) Eve’s average signal SNR is 30 dB and the average condition number of $H_{AE}$ is 5; for (b) Eve’s average signal SNR is 20 dB and the average condition number of $H_{AE}$ is 30. I only show the results for 4-antenna Alice.

2.13 The median of $C$ (with 25th/75th percentile) of the 3 cases of $CSIsnoop$ Base, $CSIsnoop$ Multi, and $CSIsnoop+a$ (defined in Table 2.1). The average signal SNR at Eve is 30 dB and the average condition number of $H_{AE}$ is 5.

2.14 The median (with 25th/75th percentile) of the absolute normalized correlation between $H_{AE,comp}$ and $H_{AE,meas}$ for 4-antenna Alice over (a) Eve’s average signal SNR and (b) the average condition number of $H_{AE}$.

2.15 CCDF of the absolute value of normalized correlation between $H_{AE,comp}$ and $H_{AE,meas}$ when the $EqualChannel$ algorithm is employed. The average signal SNR at Eve is 30 dB and the average condition number of $H_{AE}$ is 5.

2.16 CCDF of the absolute value of normalized correlation between $H_{AE,comp}$ and $H_{AE,meas}$ when the $PhaseCompensation$ algorithm is employed. The average signal SNR at Eve is 30 dB and the average condition number of $H_{AE}$ is 5.

2.17 CCDF of the absolute value of normalized correlation between $H_{AE,comp}$ and $H_{AE,meas}$ when the $GeneralizedPhaseCompensation$ algorithm is employed. The average signal SNR at Eve is 30 dB and the average condition number of $H_{AE}$ is 5. For each transmission, the sub-carrier gaps take a fixed value from 1 to 10.
2.18 CDF of the selected sub-carrier gap (number of sub-carriers) that
leads to highest correlation between $H_{AE,comp}$ and $H_{AE,meas}$ for the
*GeneralizedPhaseCompensation* algorithm in Fig. 2.17............... 44

2.19 The average bit mis-match rate (with standard deviation) between
the password computed by Eve and the password generated by Bob. .... 45

2.20 The CDF of SINR increase when Eve employs the computed CSI to
remove the artificial noise. ................................................................. 47

2.21 CDF of downlink SNR reduction of $Bob_j$ and $Bob_{i\neq j}$ when an active
Eve sends $H_{AB,comp}$ instead of $H_{AE,meas}$ as her CSI feedback to Alice. 48

2.22 CDF of interference difference between $Bob_j$ and $Bob_{i\neq j}$ when Eve
selectively jams $Bob_j$ in the uplink. ............................................. 50

3.1 Threat model: A single-antenna malicious node Mallory distorts CSI
measurement of a legitimate client Bob by jamming his channel
sounding. ................................................................. 57

3.2 System architecture of *MACE*: the variance of CFO estimates at
Alice greatly increases with jamming signals, which is used by *MACE*
for detection. ................................................................. 66

3.3 Per-frame random CFO injection, with which each Bob injects a
random CFO in the digital domain before sending his channel
sounding pilots. ................................................................. 72

3.4 (a) Experimental setup with the location of the massive MIMO AP
Alice, and part of the locations of the legitimate clients Bobs and the
adversary Mallory. (b) The Argos massive MIMO AP (Alice) and the
format of signals from Bob/Mallory to Alice. .................................. 75
3.5 Average per-client uplink achievable rate of un-distorted Bobs when Alice has different number of antennas. All 4 Bobs’ SNR before receive beamforming are around 20 dB (18 ~ 22 dB). And a single Bob’s CSI is distorted by around 0 dB SIR (−2 ~ 2 dB) jamming signals. NPS and PS stand for Non-Protocol-Specific and Protocol-Specific jamming, respectively. 

3.6 Average per-client uplink achievable rate of un-distorted Bobs when Alice has 72 antennas but the number of Bobs increases from 4 to 9. All Bobs’ SNR before receive beamforming are around 20 dB (18 ~ 22 dB). And a single Bob’s CSI is distorted by around 0 dB SIR (−2 ~ 2 dB) jamming signals. NPS and PS stand for Non-Protocol-Specific and Protocol-Specific jamming, respectively.

3.7 CDF of CFO estimation error in the experiments and that of a Gaussian distribution with same average and variance when signal SNR is around 20 dB (19.5 ~ 20.5 dB).

3.8 p-value of Kolmogorov-Smirnov test of whether the experimental data can be fitted by a Gaussian distribution when signal SNR ranges from 5 to 35 dB.

3.9 CDF of absolute correlation between CFO estimates at different antennas of Alice with different signal SNR.

3.10 (a) and (b) display the variance of normalized CFO estimates with noise strength measured by the (a) Non-Signal-Aided and (b) Signal-Aided method, respectively, when there are no jamming signals. Alice has 72 antennas.

3.11 CDF of the range of SNR difference (largest SNR minus smallest SNR) across Alice’s 72 antennas in experiments.
3.12 Variance of normalized CFO estimates (with noise strength measured by the Non-Signal-Aided method) when there are non-protocol-specific jamming ($\sim 20 \text{ dB SNR}$). Alice has 72 antennas.

3.13 Variance of normalized CFO estimates (with noise strength measured by the Non-Signal-Aided method) when there are protocol-specific jamming signals with (a) $\sim 20 \text{ dB SNR}, \sim 0.4 \text{ rad between } \theta \text{ and } \eta$, different SIR and (b) $\sim 20 \text{ dB SNR}, \sim 10 \text{ dB SIR}$, different rad between $\theta$ and $\eta$, respectively. Alice has 72 antennas.

3.14 ROC curves of non-protocol-specific jamming signals. The range of SNR and SIR are $5 \sim 35 \text{ dB and } -5 \sim 35 \text{ dB}$, respectively, with SNR–SIR$\geq 5 \text{ dB}$. Alice has 72 antennas.

3.15 ROC curves (average over different CFO between Bob and Mallory) of protocol-specific jamming signals. The range of SNR and SIR are $5 \sim 35 \text{ dB and } -5 \sim 35 \text{ dB}$, respectively, with SNR–SIR$\geq 5 \text{ dB}$. Alice has 72 antennas.

3.16 ROC curves for protocol-specific jamming signals, and with different CFO between Bob and Mallory for (a) MACE and (b) MSE-Abs-Value detector, respectively. The range of SNR and SIR are $5 \sim 35 \text{ dB and } -5 \sim 35 \text{ dB}$, respectively, with SNR–SIR$\geq 5 \text{ dB}$. Alice has 72 antennas.

3.17 True positive at 0.03 false positive when Alice has different number of antennas (with 64 repeated symbols). The SNR and the SIR is within $5 \sim 35 \text{ dB and } -5 \sim 35 \text{ dB}$, respectively, with SNR–SIR$\geq 5 \text{ dB}$. NPS and PS stand for Non-Protocol-Specific and Protocol-Specific jamming, respectively.
3.18 True positive at 0.03 false positive when different number of repeated symbols are input into MACE (with 16 or 72 antennas). The SNR and the SIR is within 5 ~ 35 dB and −5 ~ 35 dB, respectively, with SNR−SIR≥5 dB. NPS and PS stand for Non-Protocol-Specific and Protocol-Specific jamming, respectively.
Tables

2.1 Definition of CSIsnoop Base, CSIsnoop Multi, and CSIsnoop+a in Fig. 2.13. 37

2.2 Median of the absolute value of normalized correlation between $H_{AE,comp}$ and $H_{AE,meas}$ for the EqualChannel, the PhaseCompensation, and the GeneralizedPhaseCompensation algorithm. 42

3.1 Non-Protocol-Specific Distortion 87

3.2 Protocol-Specific Distortion 89
Chapter 1

Introduction

Over the last decade, Access Points (AP) equipped with multiple antennas have brought substantial performance improvement to wireless network. For example, in WLAN, the datarate greatly increases from IEEE 802.11a/b/g where a single-antenna AP is employed, to IEEE 802.11n where multiple-antenna AP first appears, and to state-of-art IEEE 802.11ac where the AP can have as many as 8 antennas. There are hot discussions that in the near future, hundreds of antennas will be connected to a single AP, which is named massive MIMO [3, 4] or networked MIMO system [5–7]. Besides increasing throughput, the multiple-antenna AP also provides new opportunities to redesign the spectrum sharing model [8], to scale the secrecy rate [9], and to enable more accurate indoor localization [10].

However, these various improvements depend critically on the Channel State Information (CSI) in wireless network, which characterizes the channel between the multiple antennas at the AP and those at different clients. Specifically, CSI has two fundamental properties in rich-scattering indoor environments:

- **Uncorrelation.** CSI becomes uncorrelated over half a wavelength distance, which is just several centimeters in 2.4/5 GHz WiFi network. This lays the foundation for the AP to differentiate different clients, and to transmit/receive multiple data streams to/from them simultaneously [11,12]. This is also a main reason why CSI was proposed to function as a shared secret between the AP
and the client in order to enhance network security [13–15].

- **On-the-fly Measurement.** In order to obtain accurate CSI, the AP and the client need to keep measuring it on-the-fly. In other words, CSI cannot be predicted or computed based on the location of the transmitter and the receiver. Therefore, in multi-user MIMO networks, there is always a channel sounding process prepended to the following data transmission. According to IEEE 802.11ac [1], a known channel sounding sequence is broadcasted by the AP, from which different clients compute and feedback their measurement results of CSI. Such a process is called downlink channel sounding. Similarly, the channel sounding sequence can be transmitted by different clients for the AP to directly measure their CSI, which is called uplink channel sounding.

Because of the critical dependence on CSI, as well as the requirement to redesign wireless protocols to adapt to the AP’s multiple antennas, new security threats arise in the meantime when the network performance improves. In this thesis, I analyze the security issues around CSI. More specifically, I study the confidentiality and integrity of CSI that are directly related to its above two core properties.

First, I study the confidentiality of CSI in multi-user MIMO networks with passive adversary [16]. While different previous works employed the uncorrelation property of CSI to enhance network security [13–15], I discover that CSI is no longer confidential in multi-user MIMO networks, because even a passive malicious node can infer the CSI of any client. The key finding is that there is a fundamental conflict between using CSI to optimize PHY design by beamforming and hiding CSI from malicious nodes: on one hand, the AP can use the multiple antennas to support concurrent transmission of multiple data streams, but this process opens a backdoor for the malicious nodes
to obtain the clients’ CSI; on the other hand, the AP can only do omni-directional transmission, which limits the throughput, but also prevents the malicious nodes from inferring the CSI. I describe a framework call *CSIsnoop*, which reveals how a passive malicious node overhearing the downlink multi-user transmission can estimate the transmit beamforming weights that the AP must have used, and further use these transmit beamforming weights to infer the CSI of different clients. By analyzing the limiting factors of *CSIsnoop*, I further discuss several counter mechanisms to prevent such an attack.

Second, I study the integrity of CSI in multi-user MIMO networks with active adversary [17]. The dependence of network performance on accurate CSI measurement makes the channel sounding process an ideal target from the attacker’s point of view. Unfortunately, the channel sounding process is vulnerable to jamming attacks. I first present and model the *Pilot Distortion Attack*, a highly efficient and devastating jamming strategy targeting the channel sounding process: a malicious node active during only channel sounding of even a single client can lead to denial-of-service of all clients associated with the AP. As a counter mechanism, I further propose a detector called _Multipl-Antenna Carrier frequency offset Estimate (MACE)_ , which exploits the variance scaling of carrier frequency offset measurements across the AP’s multiple antennas to detect *Pilot Distortion Attack*, as well as general wireless jamming, with no startup cost, no additional network overhead and no coordination between the AP and the clients. After detection by _MACE_, different methods can be further taken to reduce the impact of the inaccurate CSI measurement.

Finally, I build testbeds to experimentally study the confidentiality and integrity of CSI in practical multiple-antenna and massive MIMO wireless networks. I first implement *CSIsnoop* on WARP v3 [18] and collect measurements from over 100,000
over-the-air transmissions. The experimental results show that *CSIsnoop* can infer the target client’s CSI with an absolute normalized correlation of over 0.99 when the AP has 2 to 4 antennas. Then I employ the Rice Argos massive MIMO AP [19] to evaluate the impact of the Pilot Distortion Attack and the detection performance of *MACE* for both state-of-art IEEE 802.11ac and massive MIMO network. In total I collect over 3,000,000 packet measurements. And I demonstrate that by setting a single detection threshold, *MACE* can achieve 0.97 true positive at 0.01 false positive.

The remainder of this thesis is organized as follows. Chapt. 2 focuses on the confidentiality of CSI, and presents the design of *CSIsnoop*. Chapt. 3 focuses on the integrity of CSI. It analyzes the Pilot Distortion Attack and presents the design of *MACE*. Chapt. 4 discusses related work. Finally Chapt. 5 concludes the thesis.
Chapter 2

Confidentiality of Channel State Information in Multiple-Antenna Networks

2.1 Introduction

Channel State Information (CSI) plays a key role in multi-user beamforming systems, because it enables an Access Point (AP) to increase throughput by concurrently sending multiple data streams to multiple clients. According to IEEE 802.11ac/af [1, 2], a known channel sounding sequence is broadcasted by the AP, from which clients compute and feedback their measurement results of the channel’s effect on the known sequence. Based on the collected CSI, the AP can compute transmit beamforming weights and, for example, zero-force the signals of one client at other clients in order to eliminate inter-client interference [11,12]. Moreover, CSI can be also used to increase network throughput by grouping clients with orthogonal channels [11,20].

Besides data transmission, CSI has also been proposed to enhance network security. In particular, CSI can be used as a shared secret between a transmitter and a receiver, because it decorrelates over half a wavelength (several centimeters in 2.4/5 GHz WiFi) in rich scattering environments. Therefore, wireless devices can employ CSI for secret key establishment [13], which appears especially promising when there are limited resources or lacking key management infrastructure. In addition, CSI can be used as a signature to authenticate the source of packets, as each client in the network will have a unique CSI signature [14,15]. Finally, CSI can be used to in-
ject artificial noise orthogonal to the intended recipient to degrade an eavesdropper’s channel [21, 22]. Such artificial noise is nulled at the clients by the AP so that the signal SINR at the clients will not be reduced.

Because of the importance of CSI, it has been proposed to encrypt CSI during the standard-defined downlink (explicit) channel sounding process: either by encrypting the measurement feedback from the clients, or by encrypting the channel sounding sequence from the AP [23]. It was also discussed to replace downlink channel sounding by uplink (implicit) channel sounding, which is based on channel reciprocity and requires each client to transmit the sounding sequences for CSI measurement at the AP. Therefore, a malicious node within range of the network cannot learn clients’ CSI by overhearing their measurement process.

However, I discover that the above methods cannot ensure the confidentiality of CSI in multi-user MIMO WLANs. In particular, in this chapter I describe CSIsnoop, a framework by which a passive attacker can infer the CSI of clients by overhearing their downlink beamforming transmission. The first step of CSIsnoop is to employ the knowledge of part of the transmitted symbols (e.g., the MAC header) and trains an adaptive filter to separate the different data streams at the multiple-antenna malicious node (Eve), which I term as a known-transmitted-symbol attack (a PHY analogy of the known-plaintext attack). The malicious node subsequently estimates her channel from the AP and combines it with the adaptive filter to compute the transmit beamforming weights that the AP must have used. Finally, CSIsnoop uses the estimated beamforming weights to compute the CSI of clients. I analyze CSIsnoop with various number of clients within the network, and also show that even if the AP encrypts the channel sounding sequence [23], or only employs uplink channel sounding, it is still possible for the multiple-antenna malicious node to estimate CSI for both herself
and the target client. Moreover, I discuss how an active adversary can accelerate the computing process by using a variant of CSIsnoop which I name CSIsnoop+a.

My results reveal a fundamental conflict between using CSI to optimize PHY design and hiding CSI from malicious nodes, which urges reconsideration of the use of CSI as a shared secret in WLANs that have advanced PHY capabilities by making use of CSI for transmission optimization. In particular, with CSIsnoop, I demonstrate that a malicious node can now break the following security schemes in multi-user WLANs:

- The malicious node can compute CSI of clients even if the AP encrypts the channel sounding sequence and the clients encrypt their CSI measurement feedback [23).
- The malicious node can compute CSI of clients even if the AP employs only uplink channel sounding.
- With the computed CSI, the malicious node can further estimate the CSI-based password [13].
- With the computed CSI, the malicious node can fake CSI-based signatures [14, 15].
- With the computed CSI, the malicious node can remove most of the artificial noise and decode the overheard packets [21, 22].

In addition, I show that CSIsnoop can be also employed to degrade downlink and uplink throughput in the network. Specifically, I identify a new threat, which I term selective jamming, to the uplink multi-user transmission in next generation wireless standards [24–26]: once the malicious node obtains the CSI of a target client, she
can selectively jam the client’s data stream in uplink multi-user transmission, while not interfering with the data streams from all other clients. This is fundamentally different from current jamming techniques [27,28], which treat all the concurrent data streams identically.

Finally, I implement CSIsnoop on WARP v3 [18], deploy a testbed, and conduct experiments in various indoor environments. Specifically, I consider that the AP has 2, 3, or 4 antennas and collect measurements from over 100,000 over-the-air transmissions. My main experimental results can be summarized as follows:

- With the adversary’s average signal SNR being 30 dB and the average condition number of the channel matrix between the AP and the adversary being 5, CSIsnoop can infer the target client’s CSI with an absolute normalized correlation of over 0.99.

- The accuracy of CSIsnoop is related to the attacker’s channel: if Eve is able to move to a location with high signal strength but small condition number of her CSI matrix from the AP, she can perform better by observing just a single frame than if she were able to observe multiple frames but in a less favorable location. This also provides hints of how attacks based on CSIsnoop can be mitigated.

- CSIsnoop enables the malicious node to compute over 85% of the CSI-based password.

- CSIsnoop enables the malicious node to increase her SINR for eavesdropping by 20.7 dB when the AP injects artificial noise.

- For selective jamming, CSIsnoop creates a 20 dB average increase in interference.
to the uplink data stream of the target client compared to other clients.

The rest of this chapter is organized as follows. Sec. 2.2 introduces the threat model. Sec. 2.3, Sec. 2.4 and Sec. 2.5 describe the principles of $CSIsnoop$ and its variant $CSIsnoop+a$. I discuss implementation in Sec. 2.6 and experimental evaluations in Sec. 2.7. Several attack applications of $CSIsnoop$ are explored in Sec. 2.8. Sec. 2.9 discusses countermeasures and Sec. 2.10 concludes the chapter.

2.2 Threat Model

In this chapter, I consider the threat model illustrated in Fig. 2.1. Alice is a multiple-antenna multi-user AP and each Bob is a legitimate single-antenna client. The network has multiple clients, i.e., multiple “Bobs”. Different channel sounding configurations are considered within the network. For downlink (explicit) channel sounding, I consider that a process as the case with IEEE 802.11ac/af [1, 2] is employed. That is Alice transmits sounding sequences such that the Bobs can measure CSI and send the results back to Alice. However, each Bob can encrypt his CSI feedback in order to prevent malicious nodes from directly overhearing his CSI measure-
ments. I also consider the case that Alice encrypts her broadcasted channel sounding sequence [23] (i.e., the sounding sequence is only known to Alice within the network). For uplink (implicit) channel sounding, each Bob transmits sounding sequences such that Alice measure the CSI. There are no sounding sequences broadcasted by Alice or CSI measurement feedback sent by the Bobs under this configuration.

After acquiring Bobs’ CSI $H_{AB}$, Alice uses zero-forcing beamforming (ZF-BF) to compute her transmit beamforming weights, which is

$$ W_A = H_{AB}^\dagger = (H_{AB}^H H_{AB})^{-1} H_{AB}. \quad (2.1) $$

ZF-BF has been widely used because it can asymptotically achieve network capacity with relatively low computational complexity [11, 12, 23, 29]. Nonetheless, the CSI\textit{snoop} framework can be extended to other different beamforming algorithms, e.g., conjugate beamforming. Moreover, I assume that Alice uses all of her antennas to transmit no matter what the number of data streams is. In other words, Alice will fully utilize her antenna resources to boost the downlink network throughput.

There is a malicious node, Eve, within range of Alice. I consider a rich scattering environment typical of an indoor WLAN so that Eve can overhear signals of Alice’s downlink transmission to all Bobs. And Eve has the same number of antennas as Alice (Alice’s antenna number can be known from the network control signals).

I further assume that Eve knows a subsequence of the symbols that are transmitted by Alice for each Bob’s downlink data packet. These known symbols can be portions of the MAC packet header that follow a pre-defined format in the standards [1, 2]. Finally, I assume that Eve knows which Bobs are included in a specific downlink transmission. This can be done by Eve overhearing the control signals broadcasted by Alice before the data transmission, or the ACK packets sent from the Bobs after the data transmission.
2.3 CSIsnoop

In this section, I describe CSIsnoop, a technique by which a passive adversary can infer the CSI of different clients by overhearing downlink multi-user transmission. I begin by analyzing the base case where the number of data streams from Alice to the Bobs equals the number of antennas at Alice. Then I generalize to scenarios where the number of data streams is smaller.

2.3.1 Base Case Analysis of $K \times K$

![Diagram of CSIsnoop](image)

Figure 2.2: Base case analysis of CSIsnoop, where Bobs’ data stream number equals the number of antennas at Alice in one downlink transmission.

To begin with, I first consider the base case of CSIsnoop as shown in Fig. 2.2, where Alice has $K$ antennas and beamforms $K$ data streams to $K$ Bobs in one downlink transmission. In this case, the pseudo-inverse computation of ZF-BF is simplified to matrix inversion. Thus $H_{AB}$ and $W_A$ uniquely determine each other.

Denote the channel between Alice and $Bob_j$ to be $H_{AB_j}$, and the channel between Alice and Bobs to be $H_{AB} = [H_{AB_1}^T, H_{AB_2}^T, \ldots]^T$. Eve also has $K$ antennas, and the channel between Alice and Eve is $H_{AE}$. $X_j$ is a $1 \times L$ vector that contains $L$ symbols of $Bob_j$’s data stream. Therefore, for all $K$ Bobs, $X = [X_1^T, \ldots, X_K^T]^T$ represents
the $K \times L$ transmitted symbols from Alice. Similarly, I denote $Y_j$ as the $L$ symbols received by the $j^{th}$ antenna of Eve, and $Y = [Y_1^T, \ldots, Y_K^T]^T$ as the $K \times L$ symbols overheard by Eve. Therefore, $Y$ can be represented as

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

where $W_A$ is Alice’s transmit beamforming weights, $P$ is the transmit power scaling matrix and $P = \text{diag}(\{\sqrt{p_1}, \ldots, \sqrt{p_K}\})$, and $N$ is random noise.

In order to compute $H_{AB}$ between Alice and the Bobs, Eve needs to first estimate $W_A$ used by Alice. I identify the known-transmitted-symbol attack that can be employed by CSIsnoop to accomplish this. After that, Eve computes $H_{AB}$ based on the relationship between $H_{AB}$ and $W_A$. I divide the whole process into 4 steps and discuss each of them as follows.

(1) **Known-Transmitted-Symbol Attack.** CSIsnoop employs known-transmitted-symbol attack to compute an adaptive filter based on only $X$ and $Y$, and uses this filter to further compute $H_{AE}W_A P$. Specifically, if Eve knows the $1 \times L$ vector $X_j$ of Bob$_j$ (as discussed in Sec. 2.2, these known symbols can be part of the MAC header that follow a pre-defined format in the standards [1, 2]), she can compute a $1 \times K$ receive beamforming vector $W_{E,j}^{(1)}$ such that

$$E\{\|e_j^{(1)}\|\} = E\{\|X_j - W_{E,j}^{(1)}Y\|\}$$

is minimized. By taking the derivative of $E\{\|e_j^{(1)}\|\}$ over $W_{E,j}^{(1)}$ and setting it to zero, Eve obtains

$$W_{E,j}^{(1)} = X_j Y^\dagger,$$

where $Y^\dagger$ is the Moore-Penrose pseudo-inverse of $Y$.

Therefore, if Eve launches known-transmitted-symbol attack targeting Bobs’ $K$
data streams, she can compute
\[ W_E^{(1)} = XY^\dagger, \] (2.5)
where \( W_E^{(1)} = [W_{E,1}^{(1)} \ldots W_{E,K}^{(1)}]^T \). By ignoring the random noise \( N \), Eve can estimate
\[ H_{AE}W_AP = W_E^{(1)-1}. \] (2.6)
Here \( W_E^{(1)} \) is a \( K \times K \) square matrix because of the \( K \) data streams. So Eve can directly compute its inverse.

However, the above process will amplify the random noise \( N \) when calculating \( Y^\dagger \), which degrades the accuracy of the estimation of \( H_{AE}W_AP \). Therefore, instead of Eq. (2.3), \textit{CSIsnoop} minimizes
\[ E\{\|e^{(2)}\|\} = E\{\|Y - W_E^{(2)}X\|\}, \] (2.7)
which leads to
\[ W_E^{(2)} = YX^\dagger, \] (2.8)
and
\[ H_{AE}W_AP = W_E^{(2)}. \] (2.9)
In the following, I use \( W_E \) to represent \( W_E^{(2)} \).

(2) \textbf{Estimation of} \( H_{AE} \). It can be observed from Eq. (2.9) that in order to compute \( W_AP \), Eve needs to estimate \( H_{AE} \) first. If downlink channel sounding is employed within the network and the sounding sequences broadcasted from Alice are not encrypted, Eve can use them to estimate \( H_{AE} \) directly (even though these sequences are designed for the Bobs to measure their CSI). The computation of \( H_{AE} \) at Eve under encrypted downlink channel sounding and uplink channel sounding are discussed in Sec. 2.4.
(3) **Computation of** $W_A P$. With $W_E$ and $H_{AE}$, Eve can compute

$$W_A P = H_{AE}^{-1} W_E.$$  

(2.10)

This is because Eve has the same number of antennas as Alice and $H_{AE}$ is a $K \times K$ square matrix. Thus its inverse can be directly computed.

(4) **Computation of** $H_{AB}$. ZF-BF computes the transmit beamforming weights as the pseudo-inverse of the CSI matrix. For the base case, because the number of data streams equals the number of antennas at Alice, the pseudo-inverse computation is matrix inversion. As a result, Eve can compute

$$P^{-1} H_{AB} = P^{-1} W_A^{-1} = W_E^{-1} H_{AE}.$$  

(2.11)

It should be noted that the $j^{th}$ row of $P^{-1} H_{AB}$ (which is $\frac{1}{\sqrt{P_j}} H_{AB_j}$) and the $j^{th}$ row of $H_{AB}$ are in the same sub-space. Therefore, even though Eve does not know $P$, she can still locate the signal sub-space from Alice to Bob$_j$. This already provides enough information for Eve to learn the relative relationship among the CSI of different Bobs, and to further break various CSI-based security mechanisms and decrease network throughput as discussed in Sec. 2.8.

### 2.3.2 Generalization to $M \times K$ with $M < K$

In the above base case analysis, I assume that the number of data streams from Alice to the Bobs in one downlink transmission equals the number of antennas at Alice. Therefore, Eve can directly compute the inverse of $W_A P$ in Eq. (2.11). However, in practice, it is possible that the number of data streams in one downlink transmission is smaller, e.g., not all Bobs are backlogged. Under such circumstances, while Eve can still compute Alice’s transmit beamforming weights $W_A$, $H_{AB}$ is no longer a square matrix and the sub-space spanned by each of its rows can be no longer uniquely
determined by its pseudo-inverse. In the following, I discuss how CSIsnoop addresses this problem by overhearing multiple downlink transmissions.

Figure 2.3: CSIsnoop combines the computation of multiple downlink transmissions to compute the CSI of a target Bob.

I first use an example in Fig. 2.3 to illustrate Eve’s computing process. Suppose that there are $M_s$ and $M_s+1$ Bobs involved in transmission $s$ and $s+1$, respectively. And both $M_s$ and $M_s+1$ are smaller than $K$. Because Eve has the same number of antennas as Alice, she can always compute $W_A P$ from Eq. (2.10). And I denote $W_{A,s} P_s = [V_{s,1}, \ldots, V_{s,M_s}]$ and $W_{A,s+1} P_{s+1} = [V_{s+1,1}, \ldots, V_{s+1,M_{s+1}}]$ to be the multiplication of transmit beamforming weights and transmit power scaling matrix at Alice for downlink multi-user frame $s$ and $s+1$, respectively.

If $Bob_1$ is included in both transmissions, because ZF-BF transmits the data of all other Bobs into the null space of $H_{AB_1}$ of $Bob_1$, Eve can obtain

$$H_{AB_1} V_{s,i} = H_{AB_1} V_{s+1,i} = 0, \forall i \geq 2.$$  \hspace{1cm} (2.12)

Consequently, when the total number of different Bobs that are included in these 2 transmissions is no smaller than $K$, Eve can have at least $K - 1$ uncorrelated vectors $V$ from Eq. (2.12) such that $H_{AB_1} V = 0$, which enables Eve to locate the sub-space
spanned by the $1 \times K$ vector $H_{AB_i}$.

Therefore, when the number of data streams in one downlink transmission is smaller than $K$, for Eve to compute $H_{AB_i}$, she needs to overhear multiple downlink multi-user transmissions that (1) each includes $Bob_j$, and that (2) the total number of different Bobs that are involved should be no smaller than $K$. However, these multiple transmissions need not be consecutive as long as $H_{AB_j}$ remains stable. In comparison, $H_{AB_{i\neq j}}$ of other Bobs can even vary during the transmissions. In fact, as can be observed from Eq. (2.12), a changing $H_{AB_{i\neq j}}$ will only increase the number of different $V$’s that Eve can have and thereby enable Eve to locate the sub-space of $H_{AB_j}$ more quickly. $H_{AE}$ can also change as long as its variation can be detected by Eve so that Eq. (2.10) remains accurate.

2.4 Estimating $H_{AE}$ between Alice and Eve

In this section, I discuss how Eve is able to estimate her channel $H_{AE}$ under various channel sounding configurations. When Alice broadcasts unencrypted channel sounding sequences in the downlink, Eve can directly use them to estimate $H_{AE}$. However, I will show in the following that, even when Alice encrypts her downlink channel sounding sequences, or employs only uplink channel sounding, Eve can still estimate her channel.

2.4.1 Estimating $H_{AE}$ with Encrypted Downlink Channel Sounding

To encrypt the downlink channel sounding sequences, I consider that Alice uses the CSI$sec$ scheme [23]. Particularly, in the $l^{th}$ sub-carrier, Alice broadcasts a random symbol $R_l$ instead of the known symbol $D_l$. Therefore, $Bob_j$ and Eve measure their channel as $(R_l/D_l)H_{AB_{j,l}}$ and $(R_l/D_l)H_{AE,l}$, respectively. Because Alice knows $R_l/D_l$,
she can remove it from Bob’s measurement feedback. In contrast, Eve does not know $R_l/D_l$ and thereby cannot obtain $H_{AE,l}$.

The key reason that Eve can estimate $H_{AE,l}$ in CSIsnoop is because she now has multiple antennas instead of only a single antenna as in the discussion of [23]. In particular, Eve can combine the measured $(R_l/D_l)H_{AE,l}$ with the L-LTF field defined in IEEE 802.11ac/af to compute $H_{AE,l}$. Fig. 2.4 shows the standard-defined packet format. The L-LTF field contains the long training sequence of IEEE 802.11a/b/g, and is designed to make IEEE 802.11ac compatible with IEEE 802.11a/b/g. However, to avoid un-intentional beamforming, the L-LTF field is sent with dynamic cyclic shift, i.e., a different phase shift is added to the signals sent by each of Alice’s antennas. Such phase shifts are pre-defined in the standard and publicly known. Moreover, the L-LTF field is used by all nearby 802.11 devices to decode the following L-SIG field and thereby cannot be encrypted by Alice.

I still consider that both Alice and Eve have $K$ antennas. In addition, I denote the known channel sounding symbol and its encrypted version from the $i^{th}$ antenna of Alice in sub-carrier $l$ to be $D_{i,l}$ and $R_{i,l}$, respectively. Therefore, for the $l^{th}$ sub-carrier
and from the channel sounding process between Alice and the Bobs, Eve can compute

\[ G_{AE,l} = H_{AE,l} \Gamma_l, \tag{2.13} \]

where \( \Gamma_l = diag(\{R_{1,l}/D_{1,l}, \ldots, R_{K,l}/D_{K,l}\}) \). Suppose that the dynamic cyclic shift added to the \( i^{th} \) antenna of Alice in sub-carrier \( l \) is \( \beta_{i,l} \). Thus from the L-LTF field of the same channel sounding packet, Eve can estimate

\[ F_{AE,l} = H_{AE,l} B_l = H_{AE,l} [\beta_{1,l}, \ldots, \beta_{K,l}]^T. \tag{2.14} \]

Combining Eq. (2.13) and Eq. (2.14), Eve can obtain

\[ G_{AE,l}^{-1} F_{AE,l} = \Gamma_l^{-1} B_l = \left[ \frac{D_{1,l}}{R_{1,l}} \beta_{1,l}, \ldots, \frac{D_{K,l}}{R_{K,l}} \beta_{K,l} \right]^T. \tag{2.15} \]

Since Eve knows the dynamic cyclic shift beamforming weights \( B_l = [\beta_{1,l}, \ldots, \beta_{K,l}]^T \), she can solve \( \Gamma_l^{-1} \) from Eq. (2.15) and thereby compute \( H_{AE,l} = G_{AE,l} \Gamma_l^{-1} \).

Therefore, for downlink channel sounding, whether or not Alice encrypts her channel sounding sequences, Eve can always estimate \( H_{AE} \) in different sub-carriers and further compute \( H_{AB} \) based on \( \text{CSInoop} \).

### 2.4.2 Estimating \( H_{AE} \) with Uplink Channel Sounding

When uplink channel sounding is employed within the network, there are no longer channel sounding sequences, either unencrypted or encrypted, broadcasted in the downlink. However, under such circumstances, it is still possible for Eve to estimate her channel \( H_{AE} \) by solely relying on the L-LTF field included in every downlink packet.

As shown in Eq. (2.14), for the \( l^{th} \) sub-carrier, there are \( K^2 \) unknowns in \( H_{AE,l} \) but only \( K \) equations at Eve. Because the number of equations is \( K \) times the number of unknowns, to obtain \( H_{AE,l} \), a simple method that Eve can take is to group \( K \)
continuous sub-carriers by assuming that their channels are similar between Alice and Eve. Eve can thus have $K^2$ equations and thereby solve $H_{AE,l}$. This method is summarized as the EqualChannel algorithm.

**Algorithm 1: EqualChannel**

1. Assume that the $K$ continuous sub-carriers have the same channel, which is $H_{AE,1} = H_{AE,2} = \cdots = H_{AE,K}$. Therefore, Eve can compute

   $H_{AE,1} = [F_{AE,1}, F_{AE,2}, \ldots, F_{AE,K}][B_1, B_2, \ldots, B_K]^{-1}$.

2. Apply the same calculation to sub-carrier 2 to $K + 1$, 3 to $k + 2$, and etc.

3. For sub-carrier $l$, combine all the calculation results that include this sub-carrier to obtain the estimated $H_{AE,l}$.

However, as evaluated in Sec. 2.7.7, EqualChannel leads to inaccurate estimation in practical environments. In other words, assuming that the $K$ continuous sub-carriers have almost the same channel introduces large estimation error. In the following, I discuss a more accurate approximation based on the signal propagation between a transmitter and a receiver.

When there are multiple paths between the transmitter and the receiver, the channel $H_t$ in sub-carrier $l$ with central frequency $f_t$ can be computed as [30]

$$H_t = \sum \alpha_q e^{-j2\pi f_t \frac{\bar{d} + \Delta d_q}{c} + j\Phi_q}, \quad (2.16)$$

where $\alpha_q$ is the pathloss of the $q^{th}$ path, $\bar{d}$ is the average length of all paths, and $\Delta d_q$ is the difference between the length of the $q^{th}$ path and $\bar{d}$. $\Phi_q$ is a frequency-independent phase that captures whether the path is direct or reflected.

Similarly, for sub-carrier $l+1$, which has central frequency $f_t + \Delta f$, we can compute
Algorithm 2: PhaseCompensation

1: Assume that for the $K + 1$ continuous sub-carriers, $H_{AE,1} = H_{AE,2} e^{\Delta f \delta} = \cdots = H_{AE,K+1} e^{K \Delta f \delta}$. Therefore, Eve has

$$[F_{AE,1}, F_{AE,2}, \ldots, F_{AE,K+1}] = H_{AE,1}[B_1, B_2 e^{\Delta f \delta}, \ldots, B_{K+1} e^{K \Delta f \delta}] + N.$$ 

2: To solve the above multiple times multivariate equations, Eve can employ the following method:

(a) For a fixed step size, compute $C_t$ for all $\delta_t$ ($0 \leq \delta_t < 2\pi$) such that $[B_1, B_2 e^{\Delta f \delta_1}, \ldots, B_{K+1} e^{K \Delta f \delta_1}] \cdot C_t = 0$;

(b) Determine $\delta_t$ and $C_t$ that minimize $\| [F_{AE,1}, F_{AE,2}, \ldots, F_{AE,K+1}] \cdot C_t \|$;

(c) Eve computes $H_{AE,1}$ as

$$H_{AE,1} = [F_{AE,1}, F_{AE,2}, \ldots, F_{AE,K+1}] \cdot \text{pinv}([B_1, B_2 e^{\Delta f \delta_1}, \ldots, B_{K+1} e^{K \Delta f \delta_1}]).$$

3: Apply the same calculation to sub-carrier 2 to $K + 2$, 3 to $k + 3$, and etc.

4: For sub-carrier $l$, combine all the calculation results that include this sub-carrier to obtain the estimated $H_{AE,l}$.

that

$$H_{l+1} = \sum \alpha_q e^{-j2\pi(f_l + \Delta f) \frac{\tilde{d} + \Delta d_q}{c} + j\Phi_q}$$

$$= \sum \alpha_q e^{-j2\pi(f_l \frac{\tilde{d} + \Delta d_q}{c} + \Delta f \frac{\tilde{d} + \Delta d_q}{c} + j\Phi_q).} \quad (2.17)$$

Compared to $f_l$ which is usually on the order of hundreds of MHz or even several GHz, $\Delta f$ in IEEE 802.11ac standard is only 312.5 KHz. Therefore, if we further assume that $\Delta d_q$ is much smaller than $\tilde{d}$, which is when the delay spread of the channel between Alice and Eve is relatively small, or when there is strong LOS path,
we can compute a new approximation such that

$$H_{t+1} = H_t e^{-j2\pi\Delta f \delta_c}.$$  \hspace{1cm} (2.18)

It should be noted that the above assumption is not contradicted with the rich-scattering indoor environment, because Eve can very easily move to places where there is a strong LOS path from Alice.

Therefore, instead of assuming that $H_{AE,1} = H_{AE,2} = \cdots = H_{AE,K}$, we can derive the new approximation that $H_{AE,1} = H_{AE,2} e^{\Delta f \delta} = \cdots = H_{AE,K} e^{(K-1)\Delta f \delta}$, where $\delta = j2\pi \frac{\delta}{c}$. Because $\delta$ depends on the distance between Alice and Eve, which is usually unknown or hard to measure by Eve, Eve now needs to group $K+1$ instead of $K$ sub-carriers. This leads to a new algorithm summarized as the PhaseCompensation.

However, because the PhaseCompensation algorithm includes matrix pseudo-inverse, its accuracy is limited by the condition number of $[B_1, B_2 e^{\Delta f \delta}, \ldots, B_{K+1} e^{K\Delta f \delta}]$, which equals to the condition number of $[B_1, B_2, \ldots, B_{K+1}]$. Nonetheless, $B_t$ is highly

![Figure 2.5](image.png)

**Figure 2.5**: Absolute normalized correlation between the dynamic cyclic shift beamforming weights with different values of the sub-carrier gap $r$. 


correlated with $B_{t+r}$ when $r$ is small. This leads to a large condition number of the matrix and thereby large numerical error during pseudo-inverse computation.

Fig. 2.5 shows the absolute value of normalized correlation between $B_l$ and $B_{t+r}$ with different values of $r$ when Alice has 2, 3, and 4 antennas, respectively. It can be observed that when $r = 1$, the normalized correlation is very close to 1. And to decorrelate the dynamic cyclic shift beamforming weights, a larger sub-carrier gap is needed when Alice has more antennas. The following GeneralizedPhaseCompensation algorithm generalizes the above PhaseCompensation algorithm and allows the sub-carrier gap $r$ to take values larger than 1.

However, there is a trade-off in determining the value for the sub-carrier gap $r$: if it increases, the error of the approximation $H_{AE,l} = H_{AE,l+r}e^{r\Delta f\delta}$ becomes larger; if it decreases, the correlation between $B_l$ and $B_{t+r}$ becomes larger. Both of them will lead to inaccurate estimation of $H_{AE}$ between Alice and Eve. The value of $r$ is also different in various environments.

Finally, while the above analysis employs the packet format of IEEE 802.11ac, the methods can be applied to general scenarios. This is because the fundamental reason that dynamic cyclic shift is used is to avoid un-intentional beamforming when the same or similar signals (e.g., some control signals) are transmitted from a device’s multiple antennas. Therefore, dynamic cyclic shift is employed in various multiple-antenna systems.

### 2.5 CSIsnoop+a

In the discussion in Sec. 2.3 and Sec. 2.4, Eve is completely passive and computes $H_{AB}$ by only overhearing the downlink transmission from Alice to the Bobs. In this section, I describe a variant of CSIsnoop which I name CSIsnoop+a. For CSIsnoop+a,
Algorithm 3: GeneralizedPhaseCompensation

1: Assume that for the $K + 1$ continuous sub-carriers, $H_{AE,r_1}e^{r_1\Delta f\delta} = \ldots = H_{AE,r_{K+1}}e^{r_{K+1}\Delta f\delta}$. Therefore, Eve has

$$[F_{AE,r_1}, \ldots, F_{AE,r_{K+1}}] = H_{AE,r_1}[B_{r_1}e^{r_1\Delta f\delta}, \ldots, B_{r_{K+1}}e^{r_{K+1}\Delta f\delta}] + N.$$

2: To solve the above multiple times multivariate equations, Eve can employ the following method:

(a) For a fixed step size, compute $C_t$ for all $\delta_t$ ($0 \leq \delta_t < 2\pi$) such that

$$[B_{r_1}e^{r_1\Delta f\delta_t}, \ldots, B_{r_{K+1}}e^{r_{K+1}\Delta f\delta_t}] \cdot C_t = 0;$$

(b) Determine $\delta_t$ and $C_t$ that minimize $\| [F_{AE,r_1}, \ldots, F_{AE,r_{K+1}}] \cdot C_t \|$;

(c) Eve computes $H_{AE,1}$ as

$$H_{AE,r_1} = [F_{AE,r_1}, \ldots, F_{AE,r_{K+1}}] \cdot \text{pinv}([B_{r_1}e^{r_1\Delta f\delta_t}, \ldots, B_{r_{K+1}}e^{r_{K+1}\Delta f\delta_t}]).$$

3: Apply the same calculation to different groups of sub-carriers.

4: For sub-carrier $l$, combine all the calculation results that include this sub-carrier to obtain the estimated $H_{AE,l}$.

Eve becomes active and joins in the downlink multi-user transmission, which enables Eve to compute $H_{AB}$ more quickly in certain scenarios.

One of the examples is shown in Fig. 2.6, where there are $K - 1$ single-antenna Bobs within the network. As a result, the maximum number of different Bobs that are included in multiple transmissions can only be $K - 1$. If Eve uses CSIsnoop to compute $H_{AB_j}$ of $Bob_j$, at least one $H_{AB_i \neq j}$ of $Bob_i$ need to change during the overheard multiple transmissions, so that Eve still has at least $K - 1$ uncorrelated
Figure 2.6: For CSIsnoop+a, Eve becomes active and joins in the downlink transmission, which enables Eve to compute $H_{AB}$ more quickly in certain scenarios.

vectors $V$ for Eq. (2.12).

In comparison, if CSIsnoop+a is employed, Eve can locate $H_{AB_j}$ much more quickly. As shown in Fig. 2.6, Eve now fakes the legitimate client $Bob_K$ by using her first antenna and participates in the downlink multi-user transmission, i.e., she participates in the channel sounding process and asks Alice to beamform downlink data to the faked $Bob_K$ (e.g., Eve can setup a remote server and ask the server to send data to the faked $Bob_K$). After that, Eve still uses her $K$ antennas to overhear the $K$ data streams, except that now she only needs to launch $K - 1$ known-transmitted-symbol attacks, because the first row of $W_E$ in Eq. (2.8) can be directly set to $[0, \ldots, 0, 1/\sqrt{p_K}]$. Then Eve can obtain $P^{-1}H_{AB}$ by following step 2 to step 4 in Sec. 2.3.1.

In general, if there are $N$ Bobs in the network and $N < K$, Eve can use her $K - N$ antennas to pretend to be $K - N$ clients and join in the downlink multi-user transmission. However, Eve still only needs to have $K$ antennas in total. What is more, Eve can pretend to be legitimate clients using a subset of her antennas while
at the same time overhear multiple downlink transmissions. Therefore, Eve does not need to have precise timing control of when her downlink data of the faked clients should arrive at the AP.

2.6 Implementation

**Access Point (Alice) and Legitimate Clients (Bobs).** I implement the functions of beamforming transmission of Alice and the Bobs in the software defined radio WARP v3 [18]. In particular, Alice broadcasts the channel sounding sequence defined in IEEE 802.11ac [1] from each of her antennas, which is used by the Bobs to measure their channel. After Alice receives the measurement feedback from the Bobs, she uses ZF-BF to calculate her transmit beamforming weights and beamforms Bobs’ downlink data packet. I also implement the *CSIsec* scheme [23], with which Alice encrypts the channel sounding sequence by multiplying it with a random complex number in each sub-carrier and for each of her antennas.

The transmission has a bandwidth of 20 MHz and includes 64 OFDM sub-carriers (based on IEEE 802.11ac). Bobs’ data are modulated by BPSK or 4-QAM. And I use different WARP v3 boards to implement Alice and the Bobs so they are not clock-synchronized.

**CSI$_{snoop}$ and CSI$_{snoop+a}$.** I also implement all steps and calculations of *CSI$_{snoop}$* and *CSI$_{snoop+a}$* as described above in WARP v3. Specifically, when Eve overhears the downlink transmission, she first uses the normal method [31] to correct the timing and carrier frequency offset (due to the different oscillator frequencies between devices) based on the L-STF and the L-LTF field of each packet. After that, even though Eve has not computed the transmit beamforming weights $W_A$ at Alice yet, she can still track and correct the residue carrier frequency offset with the
aid of the pilot sub-carriers (these are reserved sub-carriers with pre-defined pilots throughout the entire packet [1, 2]). Suppose that the pilot is $\alpha$. According to the standards, it is the same for all data streams. Therefore, what Eve overhears can be represented as

$$[Y_1, \ldots, Y_k]^T = H_{AEWA}P \left( [\alpha, \ldots, \alpha]_{1 \times \text{data stream \#}} \right)^T. \quad (2.19)$$

Even if $H_{AEWA}P$ is not known by Eve, for her $j^{th}$ antenna, $Y_j/\alpha$ should have a fixed phase over time if there is no residue carrier frequency offset (but it can have different values across Eve’s antennas). Therefore, by tracking the phase of every $Y_j/\alpha$, Eve can detect and correct the residue carrier frequency offset.

Eve can subsequently begin to compute $H_{AEWA}P$ by known-transmitted-symbol attack (Eq. (2.8)). In my implementation, I directly minimize the mean square error for this computation. While this has computational complexity of $O(n^3)$ ($n$ is the size of the matrix $X$), it is optimal. Alternatively, we can use the iterative Least Mean Square algorithm to reduce computational complexity [32].

Finally, after Eve overhears multiple packets within channel coherence time of $H_{ABj}$ (during which $H_{ABj}$ stays stable), she can combine her estimates together to increase accuracy. However, Eve cannot simply compute the average value, because different packets will have different (1) transmit power scaling factors and (2) fractional timing offsets. The impacts of the scaling factors have already been discussed in Sec. 2.3.1. In the following, I analyze the impact of the fractional timing offset.

Fractional timing offset is mainly due to the ADC sampling at the receiver. Particularly, in wireless networks the correlation computation of the training sequences in the L-STF and the L-LTF field is used to determine the start of a packet among a series of sampling points [31]. Because this computation occurs in the digital domain, the actual start of the packet may deviate from the computed point with a maximum
error of $\frac{\Delta}{2}$, where $\Delta$ is the ADC sampling interval (as shown in Fig. 2.7). Therefore, even if the physical channel stays unchanged, the actual channel that the packets go through will be different. According to the Fourier transform, delay in the time domain translates into rotation over sub-carriers in the frequency domain. As a result, each estimated $H_{AB}$ at Eve will also have an additional unknown phase rotation.

To address the different transmit power scaling factors and fractional timing offsets, when Eve has a set of observations $\mathcal{H}_{ABj} = [H_{ABj}^{(1)T}, H_{ABj}^{(2)T}, \ldots]^{T}$, she searches $\hat{H}_{ABj}$ that maximizes

$$\sum_{i} \left\| H_{ABj}^{(i)} \hat{H}_{ABj}^{H} \right\|$$

with constraint $\|\hat{H}_{ABj}\| = 1$. The evaluation in Sec. 2.7.4 shows that this will lead to a significantly more accurate result compared to simply calculating the average.

## 2.7 Experimental Evaluation

In this section, I conduct experiments in various indoor environments to evaluate the performance of $CSI_{snoop}$ and $CSI_{snoop+a}$. I first describe my experimental setup.
Then I discuss the accuracy of the estimated $H_{AB}$ as well as the impacts of various factors, beginning with the base case, followed by the generalized scenarios. Finally, I study how accurately Eve can estimate $H_{AE}$ when Alice encrypts her downlink channel sounding sequence, or employs only uplink channel sounding.

### 2.7.1 Experimental Setup

I use my WARP v3 implementation to conduct experiments in typical lab, office, and apartment environments. Alice is configured to have 2, 3, or 4 antennas and beamform data to up to 4 single-antenna Bobs. Eve has the same number of antennas as Alice and stays within Alice’s transmitting range. Therefore, Eve can overhear Bobs’ downlink packets and use CSIsnoop to compute $H_{AB}$. During the experiments, I collect more than 100,000 over-the-air packets.

![Figure 2.8: Experiment timeline.](image)

Due to the extra delay of the WARPLab framework [33], in order to ensure that each experiment is finished within channel coherence time (during which the channel stays stable), I divide it into 2 phases. In the first phase, I continuously measure...
$H_{AB,\text{meas}}$ for over 100 ms. In the second phase, I first ask Alice to broadcast the channel sounding sequence (to emulate the downlink channel sounding process), by which Eve can estimate $H_{AE}$. After that, Alice sends the pre-computed downlink beamforming data packets to the Bobs, which are based on the previously collected $H_{AB,\text{meas}}$. Eve launches known-transmitted-symbol attack targeting these downlink packets and uses $\text{CSI}_\text{snoop}$ to compute $H_{AB,\text{comp}}$. The timeline of the experiment is shown in Fig. 2.8.

### 2.7.2 Accuracy of $\text{CSI}_\text{snoop}$

I first define a metric for estimation accuracy. As discussed in Sec. 2.3.1, Eve only needs to compute the sub-space spanned by $H_{ABj}$ instead of its exact value. Therefore, it is natural to use the degree of correlation as the evaluating metric. In particular, I use the absolute value of the normalized correlation, which is defined as

$$C = \frac{|H_{ABj,\text{comp}} \cdot H_{ABj,\text{meas}}^H|}{\|H_{ABj,\text{comp}}\| \cdot \|H_{ABj,\text{meas}}\|}$$  \hspace{1cm} (2.21)

for $H_{ABj}$ of $Bob_j$. $C$ ranges from 0 to 1. $C = 0$ indicates that $H_{ABj,\text{comp}}$ and $H_{ABj,\text{meas}}$ are orthogonal, while $C = 1$ indicates that $H_{ABj,\text{comp}}$ and $H_{ABj,\text{meas}}$ are perfectly correlated. Therefore, the closer to 1 is $C$, the more accurate the estimation is by Eve.

I assume that Eve uses 20 known symbols for the known-transmitted-symbol attack according to [32]. And Fig. 2.9(a) displays the Complementary Cumulative Distribution Function (CCDF) of $C$ when Eve’s average signal SNR is 30 dB and when the average condition number of $H_{AE}$ is 5 (the influence of signal SNR and condition number are discussed later in Sec. 2.7.3). As a baseline for comparison, I also plot the CCDF of correlation between $H_{ABj,\text{meas}}$ and $H_{AE}$: if $\text{CSI}_\text{snoop}$ is not
employed, I suppose that Eve uses $H_{AE}$ to infer $H_{AB,j}$. The results indicate that \textit{CSI}snoop enables Eve to locate the sub-space spanned by $H_{AB,j}$ with very high accuracy. For all 2-, 3-, and 4-antenna Alice, the average value of $C$ largely increases.
from 0.46 to over 0.99.

I further zoom in the upper-right portion of Fig. 2.9(a) and show the details in Fig. 2.9(b). For 2-antenna Alice, it can be seen that over 99% of Eve’s CSI inferences yield $C$ larger than 0.99. However, the estimation accuracy decreases with the number of antennas at Alice. The main reason is that more noise will be included into the computation when Alice has more antennas.

2.7.3 Impact of $H_{AE}$

In the following, I study the influence of Eve’s relative position to Alice via $H_{AE}$ on CSIsnoop’s accuracy. $H_{AE}$ is important because (1) if Eve is mobile or there are multiple Eves, CSIsnoop can search for places with favorable $H_{AE}$ to reduce the estimation error; and (2) Alice can also use the connection between $H_{AE}$ and CSIsnoop’s accuracy to design schemes to prevent $H_{AB}$ from being computed.

**Strength of $H_{AE}$**. On average, the strength of $H_{AE}$ determines the signal SNR at Eve (while for each overheard packet, the SNR is also related to Alice’s transmit beamforming weights). To examine how SNR impacts Eve’s CSI inference accuracy, I consider measurements only from scenarios in which the average condition number of $H_{AE}$ is 5, and plot the median of $C$ (with 25th and 75th percentile) under different SNR in Fig. 2.10(a). I do not use the mean and standard deviation here because the distribution of $C$ is highly non-normal (as shown in Fig. 2.9). It can be observed from the blue solid curve that (when $W_E = W_E^{(2)}$ is employed by CSIsnoop), the median of $C$ decreases to below 0.96 when the SNR becomes smaller than 15 dB. On the other side, when the SNR is over 25 dB, increasing the SNR further does not lead to a large increase of $C$.

Moreover, as discussed in Sec. 2.3.1, there are 2 ways for Eve to compute the
Figure 2.10 : The variation of $C$ (median with 25th/75th percentile) over (a) the average signal SNR at Eve and (b) the average condition number of $H_{AE}$. Alice has 4 antennas.

Adaptive filter based on known-transmitted-symbol attack. Therefore, Fig. 2.10(a) also depicts the median of $C$ when $W_E = W_E^{(1)}$ is employed. It can be seen that $W_E^{(2)}$ consistently outperforms $W_E^{(1)}$ in accuracy. Moreover, the difference between $W_E^{(2)}$
and $W_E^{(1)}$ increases when the signal SNR becomes smaller: from 30 dB to 15 dB, the difference between their median increases from 0.001 to 0.05; and at 15 dB, the 25th percentile of $C$ further reduces to below 0.8 when $W_E^{(1)}$ is used. The main reason is that during the computation of $W_E^{(1)}$, the random noise in the signals are amplified. Thus the reduction in estimation accuracy increases with larger noise strength (or equivalently, smaller signal SNR).

Condition Number of $H_{AE}$. After $W_E = W_E^{(2)}$ (Eq. (2.8)) is estimated from known-transmitted-symbol attack, CSIsnoop computes Alice’s transmit beamforming weights as $W_A \cdot P = H_{AE}^{-1}W_E$. Therefore, the accuracy of $W_A$ is also related to the condition number of $H_{AE}$. To analyze this factor, I consider measurements only from scenarios in which the average signal SNR is 30 dB, and plot the median of $C$ with different condition number of $H_{AE}$ in Fig. 2.10(b). In our experiments, I use the 2-norm condition number of $H_{AE}$, which is defined as the ratio of the largest singular value of $H_{AE}$ to the smallest. It can be seen that $C$ decreases when $H_{AE}$ has a larger condition number. In particular, the estimation accuracy becomes worse than the 15 dB SNR point in Fig. 2.10(a) when the average condition number of $H_{AE}$ exceeds 35.

Therefore, if Eve wants to increase her accuracy, she needs to search for favorable places where the signal SNR is large but the condition number of $H_{AE}$ is small. Given that Alice is often fixed, one of the best strategies for Eve is to find a favorable place near Alice. Moreover, when Eve is near Alice, the change of $H_{AE}$ due to environmental mobility also tends to be smaller.

2.7.4 Number of Known Symbols and Overheard Packets

Here, I evaluate whether the CSIsnoop’s inference accuracy is improved when Eve has more observations. Specifically, Eve can (1) still overhear just one transmission
but have more known symbols, or (2) overhear multiple packets within the channel coherence time of $H_{ABj}$ and combine the observations. In the following, I study each of them separately.

![Graph showing variation of $C$ over the number of known symbols by Eve.](image)

**Figure 2.11:** Variation of $C$ over the number of known symbols by Eve.

**More Known Symbols.** When Eve overhears just one transmission but has more known symbols, she can calculate $W_E$ in Eq. (2.8) with smaller error and thereby increase her estimation accuracy. To study this, I suppose that Eve knows from 10 to 50 symbols and plot the change of $C$ in Fig. 2.11.

It can be observed that when Eve is in a favorable location (where the signal SNR is high while the condition number of $H_{AE}$ is small), having more known symbols does not lead to a large increase of $C$, especially when the number of known symbols is over 20. This is because CSIsnoop already achieves a very accurate estimation with as few as only 10 known symbols (median of $C$ is 0.993). In contrast, when Eve is restricted to a non-favorable location, the estimation accuracy keeps improving when Eve has more known symbols: from 10 to 50 known symbols, the median of $C$ increases from 0.95 to 0.98. Nonetheless, even with 50 known symbols, the estimation is still less
accurate compared to the results when Eve is in a favorable place but has only 10 known symbols.

**Overhearing Multiple Packets.** When Eve overhears multiple transmissions, she can combine them to improve accuracy. Fig. 2.12(a) and Fig. 2.12(b) depict $C$ when the number of overheard packets increases from 1 to 5. Specifically, $SubSpaceSearch$ indicates that Eve maximizes Eq. (2.20) when combining the multiple observations, while $SimpAvg$ indicates that Eve simply calculates the average.

Similar to Fig. 2.11, it can be observed that when Eve is in a favorable location, the computation based on 1 overheard transmission is already very accurate, and repeated observations do not lead to a large increase in $C$. In comparison, when Eve is in a non-favorable location, accuracy significantly improves with more overheard transmissions. Yet again, even with 5 transmissions, the accuracy is still worse than when Eve is in a favorable place but overhears just 1 transmission. Therefore, compared to increasing the number of known symbols or overhearing multiple transmissions, it is more important for Eve to have a favorable $H_{AE}$.

Furthermore, it can be observed from Fig. 2.12(a) and Fig. 2.12(b) that simply averaging the results of multiple overheard packets can actually lead to worse estimation accuracy. This is mainly due to the random phase rotation from fractional timing offset that is added to every single observation. For example, if for 2 overheard packets, the computed channel are $H_{AB}$ and $e^{j\pi}H_{AB}$, $SimpAvg$ computes the average value to be $H_{est} = 0$, while $SubSpaceSearch$ maximizes $\|H_{est}H_{AB}^H\| + \|H_{est}(e^{j\pi}H_{AB})^H\|$ and obtains $H_{est} = H_{AB}$. 
Figure 2.12: (a) and (b) plot the variation of $C$ over the number of overheard transmissions by Eve (20 known symbols per transmission). In particular, for (a) Eve’s average signal SNR is 30 dB and the average condition number of $H_{AE}$ is 5; for (b) Eve’s average signal SNR is 20 dB and the average condition number of $H_{AE}$ is 30. I only show the results for 4-antenna Alice.
2.7.5 Number of Clients and Data Streams

In the following, I evaluate the performance of CSIsnoop in the generalized scenario of Sec. 2.3.2 and CSIsnoop+a of Sec. 2.5. Table 2.1 lists the detailed description and Fig. 2.13 plots the results.

Table 2.1: Definition of CSIsnoop Base, CSIsnoop Multi, and CSIsnoop+a in Fig. 2.13.

<table>
<thead>
<tr>
<th>Case</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSIsnoop Base</td>
<td>The number of data streams from Alice to the Bobs equals the number of antennas at Alice.</td>
</tr>
<tr>
<td>CSIsnoop Multi</td>
<td>Alice has ( K ) antennas and there are ( K ) Bobs. The 1st packet is to Bob(_1) and Bob(_2). The 2nd packet is to Bob(_1) and Bob(_3) ((K = 3)), or Bob(_1), Bob(_3) and Bob(<em>4) ((K = 4)). Eve computes ( H</em>{AB1} ).</td>
</tr>
<tr>
<td>CSIsnoop+a</td>
<td>Alice has ( K ) antennas but there are ( K - 1 ) Bobs. Eve fakes Bob(_K) by using her first antenna. So Alice still sends ( K ) data streams.</td>
</tr>
</tbody>
</table>

It can be observed in Fig. 2.13 that the estimation accuracy of the 3 cases of Table 2.1 are very similar, with the difference among the median of \( C \) within 0.001. But CSIsnoop+a has a smaller variance than CSIsnoop. This is because when Eve joins in the downlink transmission, part of \( W_E \) become known to Eve. As a result, Eve can obtain a more accurate \( W_A \) and thereby \( H_{AB} \). It should also be noted that there is a significant difference between the “Multi” case here and the discussion in Fig. 2.12: in Fig. 2.12, each overheard transmission contains \( k \) data streams, whereas
Figure 2.13: The median of $C$ (with 25th/75th percentile) of the 3 cases of CSIsnoop Base, CSIsnoop Multi, and CSIsnoop+a (defined in Table 2.1). The average signal SNR at Eve is 30 dB and the average condition number of $H_{AE}$ is 5.

in the “Multi” case each overheard transmission contains fewer than $k$ data streams. Therefore, even if Eve overhears more than one transmission in the “Multi” case, she may not obtain more information compared to the base case. Thus estimation accuracy may not be improved.

2.7.6 Computation of $H_{AE}$ with Encrypted Downlink Sounding Sequence

Next, I examine how accurately Eve can estimate $H_{AE}$ when Alice encrypts her channel sounding sequence [23]. Similar to the analysis of $H_{AB}$, it is equivalent that Eve estimates $H_{AE}$ and $a \cdot H_{AE}$, where $a$ is an unknown complex number. Therefore, I still use the absolute normalized correlation defined in Eq. (2.21) to evaluate the estimation accuracy of $H_{AE}$, which here is computed as ($H_{AE,comp}$ and $H_{AE,meas}$ are
first expanded into 1-dimensional vectors)

\[ C_{AE} = \frac{|H_{AE,comp} \cdot H_{AE,meas}^H|}{\|H_{AE,comp}\| \cdot \|H_{AE,meas}\|}. \]  

(2.22)

Figure 2.14: The median (with 25th/75th percentile) of the absolute normalized correlation between \( H_{AE,comp} \) and \( H_{AE,meas} \) for 4-antenna Alice over (a) Eve’s average signal SNR and (b) the average condition number of \( H_{AE} \).

- (a) Signal SNR (dB)
- (b) Average cond\( (H_{AE}) \)
I first fix the average condition number of $H_{AE}$ to be 5 and plot the variation of $C_{AE}$ over signal SNR in Fig. 2.14(a). It can be seen that under the same channel condition (in terms of $H_{AE}$), the computation of $H_{AE}$ is more accurate than that of $H_{AB}$ (by comparing with Fig. 2.10(a)). Moreover, it can also be observed that, while the accuracy of $H_{AE}$ reduces when the SNR becomes smaller, the impact of noise strength is very small from 20 dB to 30 dB, and the median of $C_{AE}$ is constantly above 0.996.

In comparison, the average condition number of $H_{AE}$ has a larger impact on the estimation accuracy. Specifically, in Fig. 2.14(b), median of $C_{AE}$ decreases to 0.96 when the condition number increases to 40. The 25th percentile also reduces to below 0.94. Nonetheless, compared to Fig. 2.10(b), the change of $C_{AE}$ is still small. In other words, the estimation of $H_{AE}$ is more robust to the channel condition between Alice and Eve than the estimation of $H_{AB}$. This is mainly because that the latter computation includes more steps. With the estimated $H_{AE}$, Eve can further use CSIsnoop to compute $H_{AB}$, even if Alice encrypts the downlink channel sounding sequence.

### 2.7.7 Computation of $H_{AE}$ with Uplink Sounding Sequence

Finally, I evaluate the estimation accuracy of the 3 algorithms discussed in Sec. 2.4.2 when Alice employs uplink channel sounding. The same metric as calculated in Eq. (2.22) is used. Eve’s average signal SNR is 30 dB and the average condition number of $H_{AE}$ is 5.

From Fig. 2.15 and Fig. 2.16, it can be observed that the PhaseCompensation algorithm significantly improves the estimation accuracy compared to the EqualChannel algorithm. In particular, when Alice has 2 antennas, the median of the absolute nor-
Figure 2.15 : CCDF of the absolute value of normalized correlation between $H_{AE, \text{comp}}$ and $H_{AE, \text{meas}}$ when the EqualChannel algorithm is employed. The average signal SNR at Eve is 30 dB and the average condition number of $H_{AE}$ is 5.

Figure 2.16 : CCDF of the absolute value of normalized correlation between $H_{AE, \text{comp}}$ and $H_{AE, \text{meas}}$ when the PhaseCompensation algorithm is employed. The average signal SNR at Eve is 30 dB and the average condition number of $H_{AE}$ is 5.
Figure 2.17: CCDF of the absolute value of normalized correlation between $H_{AE,comp}$ and $H_{AE,meas}$ when the GeneralizedPhaseCompensation algorithm is employed. The average signal SNR at Eve is 30 dB and the average condition number of $H_{AE}$ is 5. For each transmission, the sub-carrier gaps take a fixed value from 1 to 10.

Table 2.2: Median of the absolute value of normalized correlation between $H_{AE,comp}$ and $H_{AE,meas}$ for the EqualChannel, the PhaseCompensation, and the Generalized-PhaseCompensation algorithm.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>2 ants</th>
<th>3 ants</th>
<th>4 ants</th>
</tr>
</thead>
<tbody>
<tr>
<td>EqualChannel</td>
<td>0.588</td>
<td>0.281</td>
<td>0.206</td>
</tr>
<tr>
<td>PhaseCompensation</td>
<td>0.987</td>
<td>0.383</td>
<td>0.196</td>
</tr>
<tr>
<td>GeneralizedPhaseCompensation</td>
<td>0.997</td>
<td>0.968</td>
<td>0.795</td>
</tr>
</tbody>
</table>

Normalized correlation increases from 0.588 to 0.987. This is mainly because the PhaseCompensation algorithm essentially employs a first-order approximation of Eq. (2.17) while the EqualChannel algorithm employs a zeroth-order approximation. However,
when Alice has 3 or 4 antennas, the estimation accuracy barely increases. This is due to the increasing correlation between the dynamic cyclic shift beamforming weights of adjacent sub-carriers when Alice has more antennas, which is shown in Fig. 2.5. The resulting numerical error reduces Eve’s estimation accuracy.

To reduce the correlation between the dynamic cyclic shift beamforming weights, larger sub-carrier gaps are used in the GeneralizedPhaseCompensation algorithm. And the corresponding experimental results are shown in Fig. 2.17. Particularly, while the GeneralizedPhaseCompensation algorithm as discussed in Sec. 2.7.7 supports varied sub-carrier gaps, in the experiments a fixed sub-carrier gap is used. And because the total number of non-silent sub-carriers is 52, I further limit the largest sub-carrier gap to be 10. By comparing Fig. 2.17 and Fig. 2.15, it can be seen that the GeneralizedPhaseCompensation algorithm significantly increases the estimation accuracy for all 2-, 3-, and 4-antenna Alice. However, for 4-antenna Alice, because the correlation between the dynamic cyclic shift beamforming weights is around 0.5 even when the sub-carrier gap is as large as 10 (as shown in Fig. 2.5), the median of the absolute normalized correlation is only around 0.795.

Fig. 2.18 further displays the CDF of the selected sub-carrier gap that leads to the most accurate estimation for the GeneralizedPhaseCompensation algorithm when Alice has different number of antennas. It can be first observed that there is no single optimal sub-carrier gap that fits all environments. What is more, when Alice has 4 antennas, over 43% of the optimal sub-carrier gap takes the largest possible value 10 in the experiments. Thus it can be predicted that when the signal bandwidth is larger than 20 MHz (thereby there are more sub-carriers and a larger sub-carrier gap can be used), the estimation accuracy of $H_{AE}$ at Eve for 4-antenna Alice will further increase.
Figure 2.18: CDF of the selected sub-carrier gap (number of sub-carriers) that leads to highest correlation between $H_{AE,comp}$ and $H_{AE,meas}$ for the Generalized Phase Compensation algorithm in Fig. 2.17.

2.8 CSI-based Attacks

In this section, I study how Eve can use the computed $H_{AB,comp}$ to attack the network, including computing the CSI-based password, reversing the effects of “orthogonal blinding” to thwart eavesdroppers, and reducing the downlink and uplink throughput of a target Bob.

2.8.1 Computing CSI-Based Password

Because CSI decorrelates over half a wavelength in rich scattering environments, which is several centimeters in 2.4/5 GHz WiFi, schemes were proposed to generate a password between a transmitter and a receiver based on the CSI. It was assumed that such a password cannot be estimated by Eve even if Eve is close to Alice or Bob. However, by using CSISnoop, Eve can compute CSI between Alice and Bob and use
it to further compute the CSI-based password.

To evaluate how much Eve can estimate about the password, I consider the password generating scheme proposed in [13]: Alice and Bob quantify the relative amplitude of each sub-carrier of the downlink channel to generate password bits. Therefore, for q-bit quantization, the total bits of the password will be \( k \cdot n \cdot q \), where \( k \) is the number of antennas at Alice and \( n \) is the number of sub-carriers that are used. Moreover, I assume that Eve’s average SNR is 30 dB and the average condition number of \( H_{AE} \) is 5. After estimating the CSI from Alice to Bob, Eve uses the same method to compute the password.

![Image of bar chart]

**Figure 2.19:** The average bit mis-match rate (with standard deviation) between the password computed by Eve and the password generated by Bob.

Fig. 2.19 depicts experimental results for the bit mis-match rate between the password computed by Eve and the password generated by Bob. The blue and red bars represent the cases when 2 and 3 bits are used to quantify the amplitude of each sub-carrier, respectively. As discussed in Fig. 2.9, when Alice has more antennas, Eve’s estimation accuracy of \( H_{AB} \) decreases. Consequently, the bit mis-match rate
increases with the number of antennas at Alice, ranging from 7.5% to 9.5% for 2-bit quantization, and from 10.2% to 13.1% for 3-bit quantization.

However, Alice and Bob will also have bit mis-match between them. According to [13], in an indoor environment, the 2-bit scheme has bit mis-match rate between 3.5% and 5%, and the 3-bit scheme has bit mismatch rate between 5.6% and 7.9%. Suppose that the bit mis-match rate between Alice and Bob and between Eve and Bob is $x\%$ and $y\%$, respectively. It can be calculated that Eve can estimate at least $(100-x-y)/(100-x)$ of the common bits between Alice and Bob. Therefore, for 2-bit and 3-bit quantization, CSIsnoop enables Eve to estimate over 90% and 85% of the password, respectively. For a practical system, there is still a step called “Information Reconciliation” for Alice and Bob to correct their bit mis-match by exchanging some packets over the air [13]. Eve may overhear these packets to further improve her computation of the password.

### 2.8.2 Removing Artificial Noise

Besides the CSI-based password, it was also proposed that CSI can be used to inject artificial noise into the network [22] in order to thwart eavesdroppers. In particular, the AP null-beamforms the artificial noise at the legitimate client. But other locations, and hence the eavesdroppers, will have significantly reduced SINR.

However, with CSIsnoop, Eve can project the overheard signals onto the subspace spanned by $H_{AB}$ (after multiplying with $H_{AE}^{-1}$ first to reverse the effect of $H_{AE}$) and thereby remove the artificial noise. Fig. 2.20 shows the CDF of SINR increase when Eve employs CSIsnoop compared to when Eve only chooses one of her antennas that has the largest SINR. The channel condition between Alice and Eve is the same as Fig. 2.19. It can be seen that on average, CSIsnoop enables Eve to increase her
Figure 2.20: The CDF of SINR increase when Eve employs the computed CSI to remove the artificial noise.

SINR by 20.7 dB. In comparison, in STROBE [22] the authors show that the artificial noise causes a 15-22 dB decrease in SINR at the eavesdroppers. Therefore, CSIsnoop is able to remove most of the artificial noise thereby reversing the effects of Alice’s anti-eavesdropping technique.

### 2.8.3 Decreasing Network Throughput

In beamforming systems, CSI is used to remove inter-stream interference for both downlink and uplink transmission. Thus if Eve computes $H_{AB}$ with CSIsnoop, she can use it to decrease the throughput of Bob.

**Downlink.** According to current multi-user beamforming standards (IEEE 802.11 ac/af [1, 2]), the AP needs to explicitly measure the channel to clients and compute transmit beamforming weights based on their CSI feedback. A recent study points out that some APs do not check channel orthogonality when grouping clients for beamforming transmission, mainly because of the limited computing resources [34].
Under such circumstances, Eve can modify her CSI feedback to be $H_{AB,\text{comp}}$ to reduce the downlink throughput of Bobs.

![CDF of downlink SNR reduction of Bob$^j$ and Bob$^{i\neq j}$ when an active Eve sends $H_{AB,\text{comp}}$ instead of $H_{AE,\text{meas}}$ as her CSI feedback to Alice.](image)

Figure 2.21: CDF of downlink SNR reduction of Bob$^j$ and Bob$^{i\neq j}$ when an active Eve sends $H_{AB,\text{comp}}$ instead of $H_{AE,\text{meas}}$ as her CSI feedback to Alice.

In particular, I consider a scenario where a 4-antenna Alice beamforms 4 data streams in each downlink transmission. Eve pretends to be a client in the network: when $\text{CSI}_{\text{snoop}}$ is not employed, Eve sends $H_{AE,\text{meas}}$ as her CSI feedback, whereas when $\text{CSI}_{\text{snoop}}$ is employed, Eve sends $H_{AB,\text{comp}}$ as her CSI feedback, with Bob$^j$ being 1 of the 3 Bobs that are included in the same client group as Eve. Fig. 2.21 depicts the CDF of SNR decrease of Bob$^j$ and Bob$^{i\neq j}$ when $\text{CSI}_{\text{snoop}}$ is used. Alice uses ZF-BF with equal transmit power allocated to each data stream. It can be observed that on average, the SNR reduces by 17.7 dB for Bob$^j$ and 8.1 dB for Bob$^{i\neq j}$. This is mainly because the high correlation between $H_{AB,\text{comp}}$ from Eve and $H_{AB,\text{meas}}$ from Bob$^j$ will waste Alice much transmit power to null the signals of Bob$^j$ at Eve, as well as the signals of Bob$^{i\neq j}$ at both Bob$^j$ and Eve. Such a large drop of SNR will result in a high packet error rate especially for Bob$^j$. 
On the other side, even if Alice takes channel orthogonality into account, the high correlation between $H_{AB,j,\text{comp}}$ from Eve and $H_{AB,j,\text{meas}}$ from Bob$_j$ will restrict that Alice can only take turns at transmitting data to Eve and Bob$_j$, which will reduce the air time of Bob$_j$.

**Uplink.** Concurrent *uplink* transmission of multiple data streams has been regarded as an important feature in the next generation wireless standard [24–26]. Receiver-based ZF-BF can be used to remove the inter-stream interference by projecting the desired signals onto the sub-space orthogonal to the interference. Nonetheless, this same property can be exploited by Eve to *selectively jam* the uplink transmission of Bob$_j$. In particular, once Eve knows the downlink CSI of Bob$_j$, she can send interference only in the sub-space of Bob$_j$’s uplink signals. This is fundamentally different from current jamming techniques [27,28], which treat all the concurrent data streams as the same.

In above analysis in this chapter, I only consider the downlink CSI of Bob$_j$, which I denote as $H_{AB,j}^d$ in the following. **CSI** snoops computes $H_{AB,j}^d$ from Alice’s downlink multi-user beamforming transmission. However, the uplink CSI of Bob$_j$, $H_{AB,j}^u$, will be different from $H_{AB,j}^d$, mainly because of the difference between the receiving and the transmitting chain. Such difference has been shown to be stable over time and can be calibrated [4, 35]. Specifically, I denote $\alpha_{\text{Alice},i}$ and $\alpha_{\text{Eve},i}$ as the calibration coefficient between the receiving and the transmitting chain of Alice’s and Eve’s $i$th antenna, respectively, and $Q_{\text{Alice}} = \text{diag}(\{\alpha_{\text{Alice},1}, \ldots, \alpha_{\text{Alice},k}\})$ and $Q_{\text{Eve}} = \text{diag}(\{\alpha_{\text{Eve},1}, \ldots, \alpha_{\text{Eve},k}\})$. For Bob$_j$, $\alpha_{\text{Bob},j}$ has the same definition. Therefore, it can be computed that

$$H_{AB,j}^u = Q_{\text{Alice}} (H_{AB,j}^d)^T \alpha_{\text{Bob},j}. \quad (2.23)$$
If Eve sends her jamming signals with beamforming weights

\[ Q_{Eve}^{-1} \left( (H_{AE}^d)^T \right)^{-1} \left( H_{ABj}^d \right)^T, \]

it can be calculated that at Alice, the jamming signals will be in the sub-space spanned by \((1/\alpha_{Bob,j})H_{ABj}^u\), which is exactly the same signal sub-space of Bob\(_j\)'s uplink transmission.

Figure 2.22: CDF of interference difference between Bob\(_j\) and Bob\(_i\neq j\) when Eve selectively jams Bob\(_j\) in the uplink.

To evaluate this attack, I assume that both Alice and Eve have 4 antennas. I also suppose that Eve already computes her calibration coefficients. Fig. 2.22 shows the CDF of the interference difference between Bob\(_j\) and Bob\(_i\neq j\) when selective jamming or normal jamming (for which Eve broadcasts her jamming signals) is used. It can be seen that with selective jamming, Eve is able to direct most of her jamming signal energy towards the uplink transmission of Bob\(_j\). On average, there is a 20 dB difference between the interference at Bob\(_j\) and Bob\(_i\neq j\), which indicates that this selective attack is highly effective.
2.9 Counter Mechanisms

In this section, I discuss some countermeasures that Alice and the Bobs can take to prevent Eve from using CSIsnoop to infer their CSI.

From the antenna point of view, Alice can increase the number of antennas that she has. This not only requires Eve to have more antennas, as Eve’s antenna number should be no smaller than Alice’s antenna number in CSIsnoop, but also reduces Eve’s estimation accuracy, as shown in both Fig. 2.9 and Fig. 2.17. Moreover, Alice can dedicate a group of antennas only for security purposes while another group for data transmission. Because Eve is only able to compute the CSI of Alice’s antennas that are used to send downlink data, the CSI of the antennas that are used for security purposes cannot be inferred.

From the network management point of view, Alice can determine a period of time during which beamforming transmission to certain Bobs is disabled. Such period should be extended to at least $T_{ch}$ before and after the instant when CSI-based security mechanisms are employed, where $T_{ch}$ is the channel coherent time.

From the beamforming algorithm point of view, Alice can design novel beamforming algorithms that prevent Eve from using the inferred transmit beamforming weights to reverse engineer and obtain Bobs’ CSI.

2.10 Conclusion

In this chapter, I study the confidentiality of CSI. I describe CSIsnoop, a framework by which the malicious node can infer CSI between the AP and clients by overhearing downlink multi-user transmission. I implement CSIsnoop in the software defined radio WARP v3 and show that the absolute normalized correlation between the computed
CSI by CSIsnoop and the measured CSI by clients has an average of over 0.99. I also demonstrate that the malicious node can now use the computed CSI to break CSI-based security schemes, which urges reconsideration of the use of CSI as a shared secret in multi-user MIMO WLANs. Finally, I discuss some countermeasures that can be taken to prevent attacks of CSIsnoop.
3.1 Introduction

Access Points (APs) employing multiple to a massive number of antennas provide new opportunities to scale both throughput and secrecy rate. However, in both conventional multiple-antenna networks such as IEEE 802.11ac, and the latest massive MIMO networks, the gain depends critically on whether the AP can accurately estimate the Channel State Information (CSI) of different clients [36, 37]. Current methods of CSI estimation can be divided into downlink and uplink channel sounding: downlink channel sounding requires the AP to broadcast pre-defined channel sounding pilots, which enables clients to measure their CSI and send back to the AP, while uplink channel sounding requires clients to transmit sounding pilots to the AP, which enables the AP to measure the uplink CSI from different clients, and further obtain the downlink CSI by using channel reciprocity. Even though IEEE 802.11ac employs downlink channel sounding, the CSI feedback of downlink channel sounding was shown to take too much network overhead when the number of antennas at the AP increases [4]. In comparison, uplink channel sounding consumes much less overhead, which also does not scale with the antenna number at the AP.

However, previous work has shown that the uplink channel sounding process is vulnerable to jamming attacks: If an adversary transmits jamming signals during
both pilot transmission and the subsequent data transmission, network throughput will collapse even when the AP has unlimited antennas [38, 39]. The secrecy rate of clients also rapidly decreases when there is jamming during channel sounding [40–42].

In this chapter, I analytically and experimentally study the impact and detection of jamming during channel sounding in multiple antenna networks. I first present and model the Pilot Distortion Attack, a simple but devastating jamming strategy that can lead to denial-of-service of all clients associated with the AP. Different from previous attacks in which the adversary is active during both channel sounding and data transmission, pilot distortion attacks only require the adversary to transmit jamming signals during channel sounding, while keeping silent afterwards. In particular, I study both non-protocol-specific jamming via Gaussian white noise spread over the entire channel as well as protocol-specific jamming, in which jamming signals have the same format as client channel sounding pilots. I show that in both multiple-antenna networks (such as IEEE 802.11ac) and practical massive MIMO networks, the distorted CSI of even a single client can thwart concurrent uplink MMSE reception at the AP, thereby vastly degrading aggregate throughput.

As a counter mechanism, I propose Multiple-Antenna Carrier frequency offset Estimate (MACE), a system that exploits variance scaling of Carrier Frequency Offset (CFO) measurements at the AP’s different antennas to detect jamming with zero startup cost and zero additional network overhead. In other words, MACE can detect jamming for even the first packet received by the AP and is compatible with current WiFi and LTE standards. A key insight of MACE is that when there are no jamming signals, the CFO estimated by different antennas at the AP are very close to each other, because all estimates share the same true value and are also based on signals in the same carriers. Thus, I develop a model of the variance of CFO estimates and
show that without jamming, the normalized variance is independent of the wireless channel, the signal SNR, and the CFO between the AP and the client. In comparison, when there are jamming signals, I show that even if they are sent in exactly the same format as the channel sounding pilots, the normalized variance estimator significantly increases. As this difference increases with the size of the AP’s antenna array, MACE can detect jamming with zero startup cost, i.e., without a priori statistical training. This further enables MACE to support highly mobile clients, and prevents the adversary from escaping detection by affecting statistical training. Moreover, because repeated symbols already exist in various wireless standards for CFO estimation, MACE does not introduce any additional network overhead. MACE also does not require any shared secrets. Consequently, after detection via MACE, the AP can use different scheduling and beamforming algorithms to minimize the impact of distorted CSI (e.g., exclude the distorted clients for concurrent uplink transmission).

Furthermore, to prevent the adversary who is aware of the MACE mechanism and may foil the detection by imitating the client’s CFO when transmitting protocol-specific jamming signals [43], I propose client-side Per-Frame Random CFO Injection. In particular, before sending the channel sounding pilots, each client will inject a random CFO in the digital domain. The range of this random CFO is computed by the client, such that it does not lead to decoding error at the AP. Moreover, by changing the random CFO per transmission, the adversary cannot estimate its value.

Finally, I build a massive MIMO testbed to evaluate the impact of pilot distortion attacks and the detection performance of MACE when the AP has different number of antennas. This is also the first experimental study of massive MIMO from a security point of view. In particular, I use WARP v3 [18] and the Argos massive MIMO AP [4,19] that has a 72-antenna array, and collect over 3,000,000 packet measurements.
in the 5 GHz WiFi band. My main experimental results can be summarized as follows:

- For the pilot distortion attack, even with 72 antennas at the AP, a single adversary jamming no more than \( \frac{1}{60} \) of the overall airtime and having no more transmit power than any client can lead to 38% to 23% reduction of achievable rate when 4 to 9 clients are grouped for concurrent uplink transmission. In practice, the damage will be even more severe, as limiting throughput reduction to 38% and 23% requires the clients to perfectly adapt their Modulation and Coding Scheme (MCS) to the maximum achievable rate given the attack properties. Otherwise, the attack can degrade throughput to zero due to unrecoverable decoding errors.

- With 72 antennas at the AP, because the variance of the normalized CFO estimates is independent of the wireless channel and the signal SNR, by setting a single detection threshold, MACE can achieve 0.97 true positive at 0.01 false positive for various client/adversary locations, and for a wide range of SNR (5 \( \sim \) 35 dB) and SIR (\( -5 \sim 35 \) dB) with SNR–SIR\( \geq 5 \) dB.

- Even with only 16 antennas at the AP and 32 repeated symbols, MACE can achieve 0.97 true positive at 0.03 false positive with the same client/adversary locations and SNR/SIR range; consequently, MACE can also be used for general-purpose jamming detection, even with a moderate number of antennas and repeated symbols (e.g., cyclic prefix of OFDM symbol).

The rest of this chapter is organized as follows. Sec. 3.2 describes the threat model. I analyze pilot distortion attacks in Sec. 3.3 and present my design of MACE in Sec. 3.4. Experimental evaluations are studied in Sec. 3.5. Sec. 3.6 concludes this chapter.


3.2 Threat Model

As shown in Fig. 3.1, I consider a threat model with a WLAN setup, which includes a multiple-antenna AP (Alice) that has $M$ antennas, and $K$ single-antenna clients (Bobs). OFDM transmission is employed along with uplink channel sounding with time division to measure CSI between Alice and the $K$ different Bobs. That is, pre-defined channel sounding pilots are transmitted from different Bobs to Alice in orthogonal time slots (sending pilots from Alice to Bobs and feeding back the CSI measurements becomes infeasible when the AP has more and more antennas [4]). However, because there are no standards defining the channel sounding pilots originated from clients, I use the signal format of IEEE 802.11ac, where two identical Long Training Sequences (LTS) are concatenated and broadcasted by Al-
ice for downlink CSI measurement. After Alice receives Bobs’ LTS and estimates Bobs’ CSI, linear beamforming algorithms like ZF/MMSE are used for concurrent uplink/downlink transmissions. Recent developments have shown that ZF/MMSE can be implemented even for massive MIMO \cite{44} and lead to higher throughput than conjugate beamforming \cite{4,36}.

I further consider that there is a single-antenna malicious node Mallory in range of Alice. Mallory is a reactive jammer and can transmit jamming signals during channel sounding (the timing of channel sounding can be estimated by overhearing network control signals). In particular, I consider the following two types of jamming signals:

1. \textit{Non-Protocol-Specific Jamming}: Mallory knows the carriers in which the channel sounding pilots are transmitted, but is unaware of the detailed protocol used between Alice and Bobs. In this case, Mallory transmits white Gaussian noise in the carriers.

2. \textit{Protocol-Specific Jamming}: Mallory knows that each Bob transmits two repeated LTS for CFO/CSI measurement, and is also able to strictly time-synchronize with Bob \cite{28}. Therefore, Mallory can also send repeated jamming signals (in this chapter I consider the same repeated LTS as Bob) to distort Bob’s CSI measurement at Alice.

\section{3.3 Pilot Distortion Attacks}

In this section, I analyze the impact of the pilot distortion attacks. Particularly, I focus on uplink throughput, because distorting CSI of as few as a single Bob can already thwart concurrent uplink transmission in multiple-antenna networks. I begin by considering that only a single Bob’s CSI is distorted, followed by the analysis of
multi-CSI distortion.

3.3.1 Thwart Concurrent Uplink Transmission by Distorting CSI of a Single Bob

A multi-antenna AP can realize concurrent uplink and downlink transmissions to multiple clients. However, with a Pilot Distortion Attack, an adversary transmits jamming signals during channel sounding, targeting that the distorted CSI measurement at the AP, will result in large reduction of network throughput. Not only is such an attack difficult to detect due to its small energy and time footprint, it is also powerful because distorting the CSI of a single Bob can lead to denial-of-service for all Bobs associated with the AP.

Distorted CSI can have different influences on uplink and downlink due to properties of beamforming algorithms. Consider ZF beamforming as an example. Denote the channel between an $M$-antenna Alice and $K$ single-antenna Bobs to be an $M \times K$ matrix $H$. Thus the beamforming weights are computed by $W = (H^*H)^{-1}H^*$ ($H^*$ is the conjugate transpose of $H$). In the uplink, inter-client interference is removed by Alice computing $W \cdot H$, while in the downlink, interference is removed by Alice computing $H^T \cdot W^T$ ($H^T$ is the transpose of $H$). As a result, if Mallory distorts the CSI of Bob$_i$, which is the $i^{th}$ column of $H$, only Bob$_i$ receives extra interference in the downlink, while all clients but Bob$_i$ receive extra interference in the uplink. In other words, by distorting the CSI of a single Bob, all concurrent uplink transmission can be thwarted. This also reduces downlink throughput for closed-loop traffic (e.g., TCP) [45].

To further quantify the reduction of uplink throughput when Bob$_i$’s CSI is distorted (the generalization to multi-CSI distortion is discussed in Sec. 3.3.2), I denote
the channel from Bob \(_i\) and Mallory to Alice to be \(H_{Bi} \sim CN(0,1)\) and \(H_{Mal} \sim CN(0,1)\), respectively. During channel sounding, Bob’s sounding pilot is \(X_{Bi,p}\) while Mallory’s jamming signal is \(X_{Mal,p} (|X_{Bi,p}| = |X_{Mal,p}| = 1)\). What Alice receives can thus be written as

\[
Y_{i,p} = \sqrt{P_{Bi,p}}H_{Bi}X_{Bi,p} + \sqrt{P_{Mal,p}}H_{Mal}X_{Mal,p} + Z, \tag{3.1}
\]

where \(P_{Bi,p}\) and \(P_{Mal,p}\) are the signal strength of Bob \(_i\) and Mallory at Alice during channel sounding, respectively. \(Z\) is random noise with strength \(N\). Here I assume that Bob \(_i\) only transmits the channel sounding pilot once without loss of generality. When Bob \(_i\) transmits repeated channel sounding pilots, \(P_{Mal,p}\) will become the effective jamming strength and may have different values for protocol-specific and non-protocol-specific jamming. \(N\) will also become the effective noise strength. The MMSE estimate of \(H_{Bi}\) given \(Y_{i,p}\) is

\[
\hat{H}_{Bi} = E\{H_{Bi}X_{Bi,p}Y_{i,p}^*\}E\{Y_{i,p}Y_{i,p}^*\}^{-1}Y_{i,p}, \tag{3.2}
\]

with error \(\epsilon_{Bi} = H_{Bi} - \hat{H}_{Bi}\) being Gaussian with variance \(\sigma^2_{\epsilon_{Bi}} I\) where

\[
\sigma^2_{\epsilon_{Bi}} = \frac{P_{Mal,p} + N}{P_{Bi,p} + P_{Mal,p} + N}. \tag{3.3}
\]

During concurrent uplink transmission, I denote \(W_j\) to be the beamforming weights of Bob \(_j\) \((j \neq i)\). Mallory keeps silent during data transmission. Therefore, after receive beamforming, Alice obtains

\[
Y_{j,d} = W_j\sqrt{P_{Bj,d}}H_{Bj}X_{Bj,d} + W_j\sum_{k \neq i,j} \sqrt{P_{Bk,d}}H_{Bk}X_{Bk,d} + W_j\sqrt{P_{Bi,d}} \left(\hat{H}_{Bi} - \epsilon_{Bi}\right) X_{Bi,d} + W_jZ, \tag{3.4}
\]

where \(P_{Bk,d}\) is the signal strength of Bob \(_k\) at Alice during data transmission, and \(|X_{Bk,d}| = 1, \forall k\). It can be observed in Eq. (3.4) that, due to Bob \(_i\)’s distorted
CSI, extra interference to Bob \(_j\) can be computed as \(W_j \sqrt{P_{Bi,d} \epsilon_{Bi} X_{Bi,d}}\). For MMSE estimate, \(\epsilon_{Bi}\) is independent of \(\hat{H}_{Bi}\) and thereby the computed beamforming weights \(W_j\). Therefore, the expected strength of the extra interference with normalized \(W_j\) is

\[
E\{|W_j \sqrt{P_{Bi,d} \epsilon_{Bi} X_{Bi,d}}|^2\} = E\{|W_j|^2\} P_{Bi,d} \sigma^2_{\epsilon_{Bi}} E\{|X_{Bi,d}|^2\} = \frac{(P_{Mal,p} + N) P_{Bi,d}}{P_{Bi,p} + P_{Mal,p} + N}. \tag{3.5}
\]

Two observations can be obtained from Eq. (3.5). First, the extra interference does not decrease when Alice has an increasing number of antennas. However, because of the beamforming gain, when Alice has more antennas, Bob’s signal strength after receive beamforming increases. This makes the impact of the extra interference diminish when Alice’s antenna number tends to infinity. Nonetheless, for practical massive MIMO networks, Alice’s antenna number is limited. It is shown in Sec. 3.5.2 that even if Mallory has no more transmit power than any Bob, pilot distortion attack can still lead to \(38\%\) to \(23\%\) reduction of per-client achievable rate for concurrent uplink transmission of 4 to 9 Bobs.

Second, if the noise strength \(N\) is ignored in Eq. (3.5), we can further compute that the pilot distortion attack is \(\Delta\) times more efficient than attacks with the same strength \(P_{Mal,p}\) but directly jamming the data transmission, where

\[
\Delta = \beta \cdot \frac{P_{Bi,d}}{P_{Bi,p} + P_{Mal,p}}. \tag{3.6}
\]

Here \(\beta\) is the ratio of duration of data transmission over channel sounding. For 20 MHz bandwidth and 2 LTS as channel sounding pilots, each Bob’s channel sounding takes \(8\mu s\) (including cyclic prefix of the LTS). In comparison, data transmission can be extended within channel coherence time that ranges from 500\(\mu s\) to more than 1\(ms\) \([4]\). This leads to a \(\beta\) no smaller than 60. Consequently, if Mallory has similar power to Bob, pilot distortion attack will be over 30 times more efficient than directly
jamming the data transmission. In other words, the pilot distortion attack has high efficiency with small energy and time footprint.

3.3.2 CSI Distortion of Multiple Bobs

When CSI of multiple Bobs are distorted, say both Bobi1 and Bobi2, we need to re-examine whether the MMSE estimation error \( \epsilon_{B_1} \) of Bobi1 is still uncorrelated with \( \hat{H}_{B_2} \) of Bobi2, which lays the foundation for the analysis in Eq. (3.5). Denote \( P_{Mal,i_1,p} \) as the jamming strength at Alice during Bobi1’s channel sounding, \( X_{Mal,i_1,p} \) as Mallory’s jamming signal during Bobi1’s channel sounding, and \( H_{Mal,i_1} \) as the channel between Mallory and Alice during Bobi1’s channel sounding. Therefore, we can compute that

\[
E\{\epsilon_{B_1} \hat{H}_{B_2}^H\} = E\{(H_{B_1} - \hat{H}_{B_1}) \hat{H}_{B_2}^H\} = E \left\{ \frac{\sqrt{P_{B_1,p} P_{Mal,i_1,p}} \sqrt{P_{B_2,p} P_{Mal,i_2,p}}}{(P_{B_1,p} + P_{Mal,i_1,p} + N)(P_{B_2,p} + P_{Mal,i_2,p} + N)} \right\} 
\cdot E\{X_{B_1,p}^H X_{B_2,p}\} \cdot E\{X_{Mal,i_1,p} X_{Mal,i_2,p}^H\} \cdot E\{H_{Mal,i_1} H_{Mal,i_2}^H\}.
\]

(3.7)

It can be observed that when \( E\{X_{Mal,i_1,p} X_{Mal,i_2,p}^H\} = 0 \) or \( E\{H_{Mal,i_1} H_{Mal,i_2}^H\} = 0 \), \( \epsilon_{B_1} \) will still be uncorrelated with \( \hat{H}_{B_2}^H \). In other words, if we assume that Mallory transmits uncorrelated jamming signals during the channel sounding of Bobi1 and Bobi2, we can keep employing Eq. (3.5) to analyze multi-CSI distortion.

In the following, I further assume that \( H_{Mal,i_1} = H_{Mal,i_2} \), and that the total jamming strength of Mallory is fixed. In other words, we can rewrite \( P_{Mal,i_1,p} = \beta_{i_1} P_{Mal,p} \) and \( P_{Mal,i_2,p} = \beta_{i_2} P_{Mal,p} \), with \( \beta_{i_1} + \beta_{i_2} = 1 \). In this case, Bob’s \((j \neq i_1, i_2)\) receive beamforming weight \( W_j \) at Alice, which depends on \( \hat{H}_{B_1} \) and \( \hat{H}_{B_2} \), will be uncorrelated with \( \epsilon_{B_1} \) and \( \epsilon_{B_2} \). Therefore, the expected strength of the extra
interference with normalized $W_j$ is

$$E\{ |W_j\sqrt{P_{Bi1,d}\epsilon_{Bi1}X_{Bi1,d}} + W_j\sqrt{P_{Bi2,d}\epsilon_{Bi2}X_{Bi2,d}}|^2 \}$$

$$= E\{ |W_j\sqrt{P_{Bi1,d}\epsilon_{Bi1}X_{Bi1,d}}|^2 \} + E\{ |W_j\sqrt{P_{Bi2,d}\epsilon_{Bi2}X_{Bi2,d}}|^2 \}$$

$$= \frac{\beta_{i1}P_{Mal,p} + N}{P_{Bi1,p} + \beta_{i1}P_{Mal,p} + N} P_{Bi1,d} + \frac{\beta_{i2}P_{Mal,p} + N}{P_{Bi2,p} + \beta_{i2}P_{Mal,p} + N} P_{Bi2,d}.$$ (3.8)

From Mallory’s point of view, in order to maximize the extra interference to Bob$_j$ (the objective function will be the same if Mallory tries to maximize the total extra interference to all the Bobs, both distorted and un-distorted), Mallory can use the Lagrangian methods to determine the optimal value for $\beta_{i1}$ and $\beta_{i2}$, which can be computed to satisfy

$$\frac{P_{Bi1,p}P_{Bi1,d}}{(P_{Bi1,p} + \beta_{i1}P_{Mal,p} + N)^2} = \frac{P_{Bi2,p}P_{Bi2,d}}{(P_{Bi2,p} + \beta_{i2}P_{Mal,p} + N)^2}.$$ (3.9)

Two observations can be obtained from Eq. (3.9). First, when $P_{Bi1,p} = P_{Bi2,p}$ during channel sounding, $\beta_{i1}$ increases with $P_{Bi1,d}$. It indicates that in order to maximize the attacking performance, Mallory tends to allocate more jamming strength to the clients that have stronger signal strength at Alice during data transmission.

In comparison, when $P_{Bi1,d} = P_{Bi2,d}$ during data transmission, $\beta_{i1}$ decreases with $P_{Bi1,p}$. It indicates that in order to maximize the attacking performance, Mallory tends to allocate more jamming strength to the clients that have weaker signal strength at Alice during channel sounding.

Finally, different from distorting CSI of a single Bob, now both Bob$_{i1}$ and Bob$_{i2}$ receive extra interference that is introduced by the other one. Moreover, while the above analysis considers CSI distortion of only 2 Bobs, the results can be directly generalized to scenarios where CSI of more than 2 Bobs are distorted.
3.4 Jamming Detection with MACE

In this section, I present MACE, a system that can detect jamming with zero startup cost and zero additional network overhead. I introduce the background of CFO estimation, present the architecture of MACE, and analyze the variance of CFO estimates without and with jamming signals, respectively. I further study the countermeasure of per-frame random CFO injection, as well as how Alice can use MACE to reduce the impact of pilot distortion attacks.

3.4.1 CFO Estimation with a Single Receiving Antenna

CFO commonly exists due to hardware discrepancies between the transmitter and the receiver, and it needs to be estimated and corrected in the early stage of the decoding chain. In current wireless networks, CFO is estimated through repeated training sequences. Denote $Y = \{Y_1|Y_2\}$ to be the signals at the receiver ($Y_1$ and $Y_2$ are the first and the second half of $Y$, respectively). We can thus obtain

$$Y_1 = R + Z_1,$$

$$Y_2 = R e^{j\theta} + Z_2,$$

where $R$ is the received copy of the training sequence, $Z_1$ and $Z_2$ are random noise with strength $N$, and $\theta = 2\pi ft \cdot \text{len}(R)$ is the phase rotation due to CFO $f$ and sampling interval $t$. I define $\text{len}(\cdot)$ as the function that returns the length a vector.

The Maximum Likelihood (ML) estimate of $\theta$ given $Y_1$ and $Y_2$ was derived by Moose in [46], which computes

$$\hat{\theta} = \arg(Y_2 Y_1^*).$$
It was also computed that in high SNR regime,

\[ E\{\hat{\theta}|\theta, R\} = \theta, \]
\[ Var\{\hat{\theta}|\theta, R\} = \frac{N}{RR^*}. \quad (3.12) \]

### 3.4.2 System Architecture of MACE

The architecture of MACE is illustrated in Fig. 3.2. MACE employs the CFO estimates of Alice’s many antennas to detect jamming signals, because the existence of jamming signals will rapidly increase the variance of CFO estimates, thus enabling detection (since MACE targets jamming detection, this is not the optimal CFO estimation for packet decoding). Since CFO estimation is supported by various wireless standards, MACE does not introduce any additional network overhead.

As a stand alone module at Alice, there are four steps of computation after MACE receives the raw signals from each Bob and before it determines whether jamming signals are present. The four steps are summarized as follows:

1. **SNR Estimation.** MACE first measures the SNR of each antenna. Particularly, the noise strength is measured when there are no incoming signals.

2. **CFO Estimation.** Subsequently, the repeated symbols received by each antenna are used to compute a CFO estimate. I employ the ML estimator discussed in Sec. 3.4.1.

3. **CFO Normalization.** MACE then computes the average of these \( M \) CFO estimates, and normalizes each CFO estimate by subtracting the average and scaling with the corresponding SNR. Without jamming signals, each normalized CFO estimate can be approximated by a standard Gaussian random variable. The details are discussed in Sec. 3.4.3.
Figure 3.2: System architecture of MACE: the variance of CFO estimates at Alice greatly increases with jamming signals, which is used by MACE for detection.

4. Jamming Detection. Finally, MACE computes the variance of these normalized CFO estimates, which is close to 1 without jamming, but much larger than 1 with jamming. Therefore, a threshold can be set for jamming detection.
The details are discussed in Sec. 3.4.3 and Sec. 3.4.4.

### 3.4.3 Variance of CFO Estimates without Jamming

Because the multiple CFO estimates at Alice share the same true value and are also based on signals in the same carriers, when there is no jamming, the variance of these CFO estimates should be small (in high SNR regime). In the following, I derive an analytical form of this variance.

Denote the multiple CFO estimates when Alice has $M$ antennas as $\{\hat{\theta}_1, \hat{\theta}_2, \ldots, \hat{\theta}_M\}$. Therefore, we can compute the average $\phi$ and the variance $s$ as

$$
\phi = \frac{1}{M} \sum_{i=1}^{M} \hat{\theta}_i,
$$

$$
s = \frac{1}{M} \sum_{i=1}^{M} (\hat{\theta}_i - \phi)^2.
$$

However, it can be observed that, without the knowledge of the distribution of each $\hat{\theta}_i$, the statistics of $s$ can hardly be computed. Therefore, I further make the following 2 assumptions about the CFO estimates at Alice, with their validation based on experimental data are discussed in Sec. 3.5.3:

1. **Normal Distribution.** Given $\theta$ and $R_i$ (which is the the training sequence received by Alice’s $i^{th}$ antenna), $\hat{\theta}_i$ is a Gaussian random variable with average $\theta$ and variance $N_i/(R_iR_i^*)$.

2. **Uncorrelated Noises.** I assume that the random noises are uncorrelated among Alice’s different antennas. Therefore, $\hat{\theta}_i$ is uncorrelated with $\hat{\theta}_j$ if $i \neq j$.

With the assumption of uncorrelated noises, I can first compute the statistics of
the average $\phi$, which are

$$E\{\phi|\theta, R_1, \ldots, R_M\} = \frac{1}{M} \sum_{i=1}^{M} E\{\hat{\theta}_i|\theta, R_i\} = \theta,$$

$$Var\{\phi|\theta, R_1, \ldots, R_M\} = \frac{1}{M^2} \sum_{i=1}^{M} Var\{\hat{\theta}_i|\theta, R_i\}. \quad (3.14)$$

Therefore, $\phi$ is a conditionally unbiased estimate of $\theta$, and has a small conditional variance (due to the $1/M^2$ factor) when Alice has many antennas. Consequently, I can use $\phi$ to approximate the true CFO $\theta$. This allows us, together with the assumption of normal distribution, to normalize each CFO estimate $\hat{\theta}_i$ into a standard Gaussian random variable $\hat{\theta}'_i$ by

$$\hat{\theta}'_i = \frac{\hat{\theta}_i - \phi}{\sqrt{Var\{\hat{\theta}_i|\theta, R_i\}}} = (\hat{\theta}_i - \phi) \sqrt{\frac{S_i}{N_i} \cdot \text{len}(R_i)}, \quad (3.15)$$

where $S_i$ and $N_i$ are the signal and noise strength measured by Alice’s $i^{th}$ antenna, respectively. Moreover, it is known that the summation of the square of $M$ standard Gaussian random variables is subjected to chi-squared distribution with $M$ degrees of freedom. Therefore, if I denote $s'$ to be the variance of these $M$ normalized CFO estimates, I can compute that

$$E\{s'|\theta, R_1, \ldots, R_M\} = 1,$$

$$Var\{s'|\theta, R_1, \ldots, R_M\} = \frac{2}{M}. \quad (3.16)$$

It can be observed in Eq. (3.16) that, when Alice has more antennas, $s'$ becomes increasingly concentrated around 1. This makes it possible to set a threshold to separate those channel sounding pilots without jamming signals. Furthermore, the conditional statistics of $s'$ is independent of the wireless channel, the signal SNR (as long as in high SNR regime), and the CFO between Alice and Bob. This is the main reason why MACE can detect jamming with zero startup cost. Moreover, each detection is independent of (and thereby will not be impacted by) previous detections.
3.4.4 Variance of CFO Estimates with Jamming

CFO estimate at each Alice’s antenna becomes less accurate in the presence of jamming signals. As a result, the variance of CFO estimates increases, which makes $s'$ larger than 1. In the following, I characterize $s'$ for both non-protocol-specific and protocol-specific jamming.

**Non-Protocol-Specific Jamming.** Since Mallory transmits white Gaussian noise during channel sounding, if the signal SINR at Alice is not very small, according to Eq. (3.12), $\hat{\theta}_i$ should have conditional variance $((N_i + J_i)/(S_i \cdot \text{len}(R_i)))$, where $J_i$ is the jamming signal strength at Alice’s $i^{th}$ antenna. As a result, the correct normalization of $\hat{\theta}_i$ should be

$$\hat{\theta}_i' = (\hat{\theta}_i - \phi) \sqrt{\frac{S_i}{N_i + J_i}} \cdot \text{len}(R_i).$$  \hspace{1cm} (3.17)

However, Alice does not know the existence of jamming signals, and thereby treats $S_i + J_i$ as the legitimate signal strength. Assume that the average $\phi$ keeps unchanged. Alice will now mistakenly compute

$$\hat{\theta}_i^{(err)} = (\hat{\theta}_i - \phi) \sqrt{\frac{S_i + J_i}{N_i}} \cdot \text{len}(R_i).$$  \hspace{1cm} (3.18)

Therefore, as long as $J_i > N_i$, we can obtain

$$\frac{\hat{\theta}_i^{(err)}}{\hat{\theta}_i'} = \sqrt{1 + \frac{S_iJ_i + J_iJ_i + J_iN_i}{S_iN_i}} > 1.$$  \hspace{1cm} (3.19)

Consequently, the variance of $\hat{\theta}_i^{(err)}$ also increases.

One may question that if the jamming signal is very strong, will MACE mistakenly treat the jamming signal as the legitimate signal, while the legitimate signal as the jamming signal, and fail to detect? In order to analyze it, I consider the following 2 cases: (1) $S_i = U$ and $J_i = \frac{1}{\alpha} U$; and (2) $S_i = U$ and $J_i = \alpha U$. In the first case, we
can compute that
\[
\frac{\hat{\theta}_i^{(err)}}{\hat{\theta}_i^\prime} = \sqrt{\frac{1 + \alpha U^2 + U^2 + \alpha UN_i}{\alpha^2 UN_i}}. \tag{3.20}
\]
In the second case, if we switch the role between the jamming signal and the legitimate signal, we can compute that
\[
\frac{\hat{\theta}_i^{(err)}}{\hat{\theta}_i^\prime} = \sqrt{1 + \frac{\alpha^2 U^2 + \alpha U^2 + \alpha UN_i}{\alpha^2 UN_i}}. \tag{3.21}
\]
It can be observed that Eq. (3.21) differs from Eq. (3.20), in that it contains \(\alpha^2 U^2\) in its numerator instead of \(U^2\). Therefore, with \(\alpha > 1\), the variance of \(\hat{\theta}_i^{(err)}\) will actually increase when the jamming signal becomes stronger than the legitimate signal, which makes it easier to be detected by MACE.

**Protocol-Specific Jamming.** When Mallory uses protocol-specific jamming, the jamming signals received by Alice’s \(i^{th}\) antenna can be written as \(\{Q_i|Q_i e^{j\eta}\}\), where \(\eta\) is the phase rotation due to CFO between Alice and Mallory. Similarly, because Alice is not aware of the jamming signals, she uses Eq. (3.11) to compute a mistaken CFO estimate \(\hat{\theta}_i^{(err)}\), which has conditional average
\[
E\{\hat{\theta}_i^{(err)}|\theta, R_i, \eta, Q_i\} = \arg \left( (R_i e^{j\theta} + Q_i e^{j\eta})(R_i + Q_i)^* \right) \tag{3.22}
\]
\[
= \arg \left( e^{j\theta}(|R_i|^2 + R_i Q_i^*) + e^{j\eta}(|Q_i|^2 + Q_i R_i^*) \right) .
\]
While \(\theta\) and \(\eta\) are fixed for all of Alice’s \(M\) antennas, \(R_i\) and \(Q_i\) will be different. However, when Alice is equipped with more and more antennas, it will become harder and harder for Mallory to estimate or control the channel between Alice and herself, or the channel between Alice and Bob (even if Mallory uses \(CSI_{snoop}\), as discussed in Chap. 2, the estimation accuracy decreases when Alice’s antenna number increases), and thereby the values of \(R_i\) and \(Q_i\). Consequently, the only parameter in Eq. (3.22)
that Mallory can control is $\eta$. And as long as $\theta \neq \eta$, the conditional average of $\hat{\theta}_i(\text{err})$ will no longer be the same for Alice’s different antennas.

In addition, we can also compute the conditional variance of $\hat{\theta}_i(\text{err})$ when there are protocol-specific jamming signals, which is

$$Var(\hat{\theta}_i^{(\text{err})}|\theta, R_i, \eta, Q_i) = \frac{N_i}{(R_i + Q_i)(\bar{R}_i + \bar{Q}_i)}.$$  \hspace{1cm} (3.23)

Combining Eq. (3.22) and Eq. (3.23), it can be observed that when Alice normalizes $\hat{\theta}_i^{(\text{err})}$ to $\hat{\theta}_i^{(\text{err})}$ by using Eq. (3.15), each $\hat{\theta}_i^{(\text{err})}$ will have unit variance but non-zero average. This again makes $s'$ larger than 1.

### 3.4.5 Per-Frame Random CFO Injection by Bobs

As discussed in Sec. 3.4.4, for protocol-specific jamming, as long as $\theta \neq \eta$, the value of $s'$ will be larger than 1. Thus jamming can be detected by MACE. In contrast, if $\theta \approx \eta$, $s'$ gets close to 1, which makes the jamming signals hard to be detected. However, it was shown in previous work that it is possible for Mallory to set $\eta$ close to $\theta$ [43] (which may then foil the MACE detection). In particular, oscillator frequency remains stable within short durations. By overhearing Bob’s packets, Mallory can estimate the CFO between Bob and herself, and thereby compensate for such CFO in the digital domain before sending the jamming signals.

To address this problem, I further propose a countermeasure called **Per-Frame Random CFO Injection**, with which each Bob injects a random CFO in the digital domain before sending his channel sounding pilots. Such random CFO cannot be predicted and thereby imitated by Mallory. Mallory also cannot estimate its value before completely receiving the 2 LTS, because Bob can actually inject the random CFO only to the LTS but not the prepended short training sequences. In the meantime, this random CFO should not lead to decoding error at Alice (exceeds Alice’s
correcting range, which is defined in standards like IEEE 802.11ac) when there are no jamming signals, which further makes it fully compatible with current WiFi and LTE standards.

![Diagram of per-frame random CFO injection]

**Figure 3.3**: Per-frame random CFO injection, with which each Bob injects a random CFO in the digital domain before sending his channel sounding pilots.

The detailed process of per-frame random CFO injection is illustrated in Fig. 3.3, where $f_{\text{Alice}}$, $f_{\text{Bob}}$, and $f_{\text{Mal}}$ are the actual oscillator frequencies of Alice, Bob, and Mallory, respectively. $f(\delta)$ denotes the frequency offset that causes $\delta$ phase rotation. First, when Bob overhears packets from Alice, he can estimate $f_{\text{Alice}} - f_{\text{Bob}}$. Since Bob knows that Alice can correct CFO within $[f(-\pi), f(\pi)]$, he can then compute a range $[f(\delta_{\text{Bob},\text{min}}), f(\delta_{\text{Bob},\text{max}})]$ in which the additional random CFO will not lead to decoding error at Alice.

Similar to Bob, Mallory can also estimate $f_{\text{Alice}} - f_{\text{Mal}}$ and thereby compute $[f(\delta_{\text{Mal},\text{min}}), f(\delta_{\text{Mal},\text{max}})]$. As a result, at Alice both $\theta$ of Bob and $\eta$ of Mallory are between $-\pi$ and $\pi$. If Bob uniformly chooses his additional random CFO within $[f(\delta_{\text{Bob},\text{min}}), f(\delta_{\text{Bob},\text{max}})]$, the best strategy for Mallory is to also uniformly select an additional CFO within $[f(\delta_{\text{Mal},\text{min}}), f(\delta_{\text{Mal},\text{max}})]$, or to just fix her CFO. In this case,
if MACE cannot detect protocol-specific jamming signals when $|\theta - \eta| < \omega$, we can computed that

$$P(|\theta - \eta| < \omega) = \frac{\omega}{\pi}. \quad (3.24)$$

As evaluated in Sec. 3.5.5, $\omega$ has a small value in practice.

### 3.4.6 Discussions

In the above analysis, MACE employs the repeated symbols received by Alice to estimate CFO and detect jamming. Because CFO represents the phase information of these repeated symbols, a direct question following it is whether the amplitude of these symbols can be also used. I evaluate the idea of using the difference of the amplitude of these repeated symbols to detect jamming in Sec. 3.5.6, and show that the detection performance actually becomes worse. One of the reasons is that the variance of CFO estimate is related to signal SINR (Eq. (3.12)), while the difference of the amplitude is mostly determined by the noise strength. In addition, MACE is also more sensitive to protocol-specific jamming signals when CFO between Mallory and Bob is relatively small (but cannot be too small, as discussed in Fig. 3.16).

What is more, while MACE targets pilot distortion attack, it can also be used as a general-purpose jamming detector in various wireless networks. The repeated symbols are not limited to repeated training sequences, but can also be cyclic prefix of OFDM symbols, repeated bits in packet headers, or even intentionally added repeated data symbols within data packets. MACE can also be used to detect the recently proposed analog man-in-the-middle attack [47], and the frequency offset estimation attack discussed in [28, 48].

Finally, after MACE detects distorted CSI, Alice can employ different methods to reduce the impact of pilot distortion attack, including re-sounding the channel
of the distorted Bobs, excluding the distorted Bobs from concurrent transmission, or proactively lowering the MCS of various Bobs. Furthermore, as can be observed in Eq. (3.5), the expected strength of the extra interference is proportional to the signal strength of the distorted Bobs during data transmission. Therefore, Alice can ask the distorted Bobs to reduce their transmitting power in order to limit the extra interference.

3.5 Experimental Evaluation

In this section, I build a testbed and use experiments to evaluate the impact of pilot distortion attacks and to study the detection performance of MACE for both multiple-antenna networks like IEEE 802.11ac and practical massive MIMO systems.

3.5.1 Experimental Setup

I build a testbed for experimental evaluation by using the WARP v3 [18] and the Argos massive MIMO AP [4, 19], and use the topology shown in Fig. 3.4(a). It emulates a network with one multiple-antenna/massive MIMO AP and multiple clients, and a malicious node jams the channel sounding process to reduce the network throughput. In particular, the Argos massive MIMO AP has a 72-antenna array spaced by 6.35 cm (Fig. 3.4(b)). During each experiment, a single Bob and a single Mallory are selected to transmit signals to Alice, which emulates the channel sounding with time division and with/without jamming signals. Moreover, to emulate different CFO between Bob and Mallory, I add additional CFO to the signals in the digital domain before each transmission. This is because the inherent CFO between Bob and Mallory due to hardware discrepancies is relatively stable over time. I also change the transmit power of Bob and Mallory to explore various combinations of SNR and SIR. All experiments
Figure 3.4: (a) Experimental setup with the location of the massive MIMO AP Alice, and part of the locations of the legitimate clients Bobs and the adversary Mallory. (b) The Argos massive MIMO AP (Alice) and the format of signals from Bob/Mallory to Alice.

are conducted in the 5 GHz WiFi band with 20 MHz bandwidth. In total, I collect measurements for over 3,000,000 packets.

The detailed format of each transmission from Bob/Mallory to Alice is shown in Fig. 3.4(b). The first part contains only LTS (defined in IEEE 802.11ac) from the selected Bob, which is used to estimate Bob’s CSI/CFO (to Alice) and to compute MACE’s output without jamming. In comparison, the second part contains only jamming signals from the selected Mallory: for non-protocol-specific jamming, they are white Gaussian noise within the 20 MHz channel, while for protocol-specific jamming,
they are the same LTS that are transmitted by Bob. I use the second part to measure
the jamming signal strength and Mallory’s CFO (to Alice). Finally, the third part
contains signals from both Bob and Mallory, which is used to measure Bob’s distorted
CSI and MACE’s output with jamming.

In addition, to study the impact of pilot distortion attacks and the detection
performance of MACE when Alice has fewer antennas, I randomly select \( M \) antennas
out of the 72 if \( M < 72 \). For every \( M \), this process is repeated several times to obtain
the average results.

### 3.5.2 Achievable Rate Reduction due to Pilot Distortion Attacks

![Figure 3.5: Average per-client uplink achievable rate of un-distorted Bobs when Alice
has different number of antennas. All 4 Bobs’ SNR before receive beamforming are
around 20 dB (18 \( \sim \) 22 dB). And a single Bob’s CSI is distorted by around 0 dB
SIR (\(-2 \sim 2 \) dB) jamming signals. NPS and PS stand for Non-Protocol-Specific and
Protocol-Specific jamming, respectively.](image)
To study the impact of the Pilot Distortion Attacks, I use the Shannon equation \( \log_2(1 + SINR) \) to compute the achievable rate of Bobs’ concurrent uplink transmissions, and compare their values without and with different jamming signals. Particularly, for protocol-specific jamming signals, \( \theta - \eta \) is uniformly distributed within \([-0.2, 0.2]\), where \( \theta \) is the phase rotation due to CFO between Alice and Bob, while \( \eta \) is the phase rotation due to CFO between Alice and Mallory. This leads to about the largest impact of pilot distortion attacks with protocol-specific jamming. The results with Alice having different number of antennas and using MMSE receive beamforming are shown in Fig. 3.5.

It can be observed that, even if only a single Bob’s CSI is distorted, the achievable rate significantly decreases, ranging from 49% to 38% reduction for protocol-specific jamming, and from 36% to 29% for non-protocol-specific jamming, when Alice’s antenna number increases from 8 to 72. The main reason that non-protocol-specific jamming leads to a smaller reduction is because its effective jamming strength reduces to half of its original value when 2 repeated LTS are used for CSI measurement. In contrast, for protocol-specific jamming, because between Mallory and Bob \( \theta - \eta \) is uniformly distributed within \([-0.2, 0.2]\), its effective jamming strength is almost unchanged. In particular, the resulting average increase of inter-client interference is measured to be 16.2 dB and 13.7 dB for protocol-specific and non-protocol-specific jamming, respectively. In comparison, substituting the experimental parameters into Eq. (3.5), we can compute the increase to be 15.3 dB and 13.6 dB, respectively.

Fig. 3.6 further displays the achievable rate when Alice has 72 antennas but the number of Bobs increases from 4 to 9. Because only a single Bob’s CSI is distorted, the achievable rates under the pilot distortion attacks do not change much, while the achievable rates without the attack decrease with the number of Bobs. The main
Figure 3.6: Average per-client uplink achievable rate of un-distorted Bobs when Alice has 72 antennas but the number of Bobs increases from 4 to 9. All Bobs’ SNR before receive beamforming are around 20 dB (18 ~ 22 dB). And a single Bob’s CSI is distorted by around 0 dB SIR (−2 ~ 2 dB) jamming signals. NPS and PS stand for Non-Protocol-Specific and Protocol-Specific jamming, respectively.

reason is the increasing inter-client interference due to random noise during channel sounding (even when there are no jamming signals). Nonetheless, when there are 9 Bobs transmitting concurrently, we can still observe that the pilot distortion attacks with protocol-specific and non-protocol-specific jamming leads to 31% and 23% decrease of achievable rate, respectively. In practice, the damage will be even more severe, as limiting throughput reduction to 31% or 23% requires the clients to perfectly adapt their MCS to the maximum achievable rate given the attack properties. Otherwise, the attack can degrade throughput to zero due to unrecoverable decoding errors. Meanwhile, Mallory can also distort multiple CSI to further reduce the clients’ achievable rate. And as more clients tend to be included in concurrent transmissions
when Alice has more antennas, the network-wide impact of pilot distortion attack actually increases.

Therefore, for the pilot distortion attacks, a single adversary jamming no more than $\frac{1}{60}$ of the time (8$\mu$s over > 500$\mu$s as discussed in Sec. 3.3.1) and having no more transmit power than any client can lead to 38% to 23% reduction of achievable rate when 4 to 9 clients are grouped for concurrent uplink transmission.

3.5.3 Validation of the Two Assumptions of CFO Estimates

In the following, I use experiments to validate the two assumptions of CFO estimates in Sec. 3.4.3. The first assumption is that the CFO estimate at each antenna of Alice is subjected to Gaussian distribution. During the experiments, I synchronize the clock of two WARP v3 boards and program one of them to transmit repeated LTS to the other one. The ML CFO estimates at the receiver, which are now also the CFO estimation error because of the clock-synchronization, are recorded for evaluation.

The CDF of the CFO estimation error with around 20 dB SNR at the receiver is shown in Fig. 3.7, which also includes the CDF of Gaussian distribution that has the same average and variance as the experimental data. It can be observed that these two CDF curves match each other very well. I use the Kolmogorov-Smirnov (KS) test to check the normality of the experimental data and calculate the p-value to be 0.40 (the probability of observing a larger maximum absolute difference between the two CDF curves). In other words, the null hypothesis is true at the 40% significance level. Fig. 3.8 further shows the p-value of the KS test with SNR ranging from 5 to 35 dB. We can calculate that on average it is 0.73.

The second assumption is that the CFO estimates at Alice’s different antennas are independent of each other. Because each of them is subjected to Gaussian dis-
Figure 3.7: CDF of CFO estimation error in the experiments and that of a Gaussian distribution with same average and variance when signal SNR is around 20 dB (19.5 \sim 20.5 \text{ dB}).

Figure 3.8: p-value of Kolmogorov-Smirnov test of whether the experimental data can be fitted by a Gaussian distribution when signal SNR ranges from 5 to 35 dB.
Figure 3.9: CDF of absolute correlation between CFO estimates at different antennas of Alice with different signal SNR.

Absolute Value of Correlation

CDF

0 0.2 0.4 0.6 0.8 1

10 dB SNR
15 dB SNR
20 dB SNR

Figure 3.9: CDF of absolute correlation between CFO estimates at different antennas of Alice with different signal SNR.

distribution, independence is equivalent to uncorrelation. The CDF of the absolute correlation between CFO estimates at different antennas are shown in Fig. 3.9. If we set a threshold at 0.05, over 95% of absolute correlation will be smaller than this threshold with 10 dB and 15 dB SNR. However, when SNR increases to 20 dB, only 80% of absolute correlation are smaller than 0.05. This is mainly because when SNR increases, noise introduced by the transmitter begins to have a larger impact. And such noise is correlated at the different antennas at the receiver. Nonetheless, even at 20 dB, over 99% of absolute correlation are smaller than 0.1.

Therefore, both assumptions can be validated by experimental data.

3.5.4 Variance of Normalized CFO Estimates without Jamming

To evaluate the detection performance of MACE, in the following, I first discuss the CDF of the variance of normalized CFO estimates without jamming signals.
Figure 3.10: (a) and (b) display the variance of normalized CFO estimates with noise strength measured by the (a) Non-Signal-Aided and (b) Signal-Aided method, respectively, when there are no jamming signals. Alice has 72 antennas.
Particularly, I compare 2 methods for noise strength estimation at Alice:

1. **Non-Signal-Aided.** Alice measures noise strength when there are no incoming signals. This method only allows Alice to measure the noise strength generated by the receiver.

2. **Signal-Aided.** Alice knows that for her $i^{th}$ antenna, the incoming signals have a structure of $\{Y_{1i}|Y_{2i}\}$, where $Y_{1i} = R_i + W_{1i}$ and $Y_{2i} = R_i e^{j\theta} + W_{2i}$. Therefore, Alice can first estimate $\hat{\theta}$ and then compute the noise strength as $E\{|Y_{2i}e^{-j\hat{\theta}} - Y_{1i}|^2\}/2$. This method requires an accurate estimation of $\theta$, yet it does not include the noise correlated with signal $R_i$.

It can be first observed in Fig. 3.10(a) that, for the Non-Signal-Aided method, the experimental results with high/low SNR deviate from the theoretical calculation. The main reasons are that: when SNR is high, noise strength introduced by the transmitter begins to surpass that generated by the receiver, which results in large normalization error in Eq. (3.15); when SNR is low, the error in Eq. (3.12) becomes large. In comparison, when SNR is within $5 \sim 25$ dB, the experimental results are close to the theoretical calculation. The main reason for the long tail is that the SNR of Alice’s different antennas vary significantly. As shown in Fig. 3.11, in experiments the average range of SNR difference is 22 dB.

In contrast, as can be observed in Fig. 3.10(b), the difference between the experimental results and the theoretical calculation decrease when the Signal-Aided method is used to measure the noise strength. In particular, when the transmitter side noise is included, the experimental results at high SNR become much closer to the theoretical calculation. However, the Signal-Aided method cannot be employed by MACE, because it will mistakenly include the white Gaussian jamming signals
when computing the noise strength. Therefore, all of the following figures are based on the Non-Signal-Aided method.

### 3.5.5 Variance of Normalized CFO Estimates with Jamming

When there are non-protocol-specific white Gaussian jamming signals, the variance of the normalized CFO estimates significantly increases. In Fig. 3.12, the x-axis now extends to 200 instead of 10 as in Fig. 3.10(a) and 3.10(b). It can be also seen that, when the jamming signals become stronger, the ratio of $\frac{\hat{\theta}_i^{(err)}}{\hat{\theta}_i}$ computed in Eq. (3.19) increases, and therefore the variance of the normalized CFO estimates also increases.

For protocol-specific jamming, a similar trend that the variance of the normalized CFO estimates increases with stronger jamming signals is observed in Fig. 3.13(a). Moreover, in Fig. 3.13(b), I display the variance of the normalized CFO estimates...
when the CFO between Mallory and Bob changes: $\theta$ is the phase rotation due to CFO between Alice and Bob, while $\eta$ is the phase rotation due to CFO between Alice and Mallory. It can be seen that when $|\theta - \eta|$ is small, the variance of CFO estimates is also small, which makes the jamming signals hard to be detected. This is the main reason why per-frame random CFO needs to be injected by Bobs before sending the channel sounding pilots (as discussed in Sec. 3.4.5). Nevertheless, when $|\theta - \eta|$ increases, the variance also quickly increases.

3.5.6 ROC Curves of MACE

To characterize the performance of MACE, I plot its ROC curves for both non-protocol-specific and protocol-specific jamming: the false positive is the mistaken detection rate when there are no jamming signals, while the true positive is the
Figure 3.13: Variance of normalized CFO estimates (with noise strength measured by the Non-Signal-Aided method) when there are protocol-specific jamming signals with (a) $\sim 20$ dB SNR, $\sim 0.4$ rad between $\theta$ and $\eta$, different SIR and (b) $\sim 20$ dB SNR, $\sim 10$ dB SIR, different rad between $\theta$ and $\eta$, respectively. Alice has 72 antennas.
correct detection rate when there are jamming signals. For performance evaluation baselines, I also consider the following 3 detectors that employ the repeated symbols received by Alice, and compare their performance to $MACE$:

1. **Raw-CFO.** As discussed in Sec. 3.4.3, $MACE$ normalizes the CFO estimates by the corresponding SNR. In contrast, Raw-CFO does not normalize the CFO estimates and directly compute their variance.

2. **MSE-Abs-Value.** Without jamming signals, Alice’s $i^{th}$ antenna receives $\{Y_{1i}, Y_{2i}\}$, where $Y_{1i} = R_i + W_{1i}$ and $Y_{2i} = R_i e^{j\theta} + W_{2i}$. Therefore, $E\{|Y_{1i} - Y_{2i}|^2\}$ should be small and is only related to the noise strength. MSE-Abs-Value normalizes $E\{|Y_{1i} - Y_{2i}|^2\}$ by the noise strength of each antenna and computes the average over all antennas.

3. **MSE-Raw-Value.** Different from MSE-Abs-Value, MSE-Raw-Value computes $E\{|Y_{1i} - Y_{2i}|^2\}$ instead of $E\{|Y_{1i} - Y_{2i}|^2\}$.

<table>
<thead>
<tr>
<th>TP,FP=0.003</th>
<th>MACE</th>
<th>Raw-CFO</th>
<th>MSE-Abs-Value</th>
<th>MSE-Raw-Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.93</td>
<td>0.39</td>
<td>0.39</td>
<td>0.01</td>
<td></td>
</tr>
<tr>
<td>0.97</td>
<td>0.50</td>
<td>0.93</td>
<td>0.02</td>
<td></td>
</tr>
<tr>
<td>1.00</td>
<td>0.67</td>
<td>1.00</td>
<td>0.08</td>
<td></td>
</tr>
</tbody>
</table>

**Non-Protocol-Specific Jamming.** Fig. 3.14 plots the ROC curves of the 4 detectors with white Gaussian jamming signals, where a single detection threshold is set for a wide range of SNR (5 $\sim$ 35 dB) and SIR ($-5 \sim 35$ dB) with SNR–SIR$\geq$5
Figure 3.14: ROC curves of non-protocol-specific jamming signals. The range of SNR and SIR are $5 \sim 35$ dB and $-5 \sim 35$ dB, respectively, with $\text{SNR} - \text{SIR} \geq 5$ dB. Alice has 72 antennas.

dB. It can be observed that $MACE$ achieves 0.97 true positive at 0.01 false positive (as listed in Table 3.1). In contrast, Raw-CFO only achieves 0.50 true positive at the same false positive. This is mainly because the large variance of SNR at Alice’s different antennas leads to a relatively large variance of raw CFO estimates (compared to $MACE$) even without jamming signals.

In comparison, MSE-Raw-Value has even worse detection performance than Raw-CFO, while MSE-Abs-Value has similar detection performance to $MACE$. The main reason is the CFO between Alice and Bob, which makes $E\{|Y_{i_1} - Y_{i_2}|^2\}$ have a large value even without jamming signals. However, MSE-Abs-Value addresses this problem by taking the absolute value of the received signals (i.e., $E\{||Y_{i_1}| - |Y_{i_2}||^2\}$).

**Protocol-Specific Jamming.** As discussed in Fig. 3.13(b), the detection performance of $MACE$ when there is protocol-specific jamming is closely related to the
Figure 3.15: ROC curves (average over different CFO between Bob and Mallory) of protocol-specific jamming signals. The range of SNR and SIR are $5 \sim 35$ dB and $-5 \sim 35$ dB, respectively, with $\text{SNR} - \text{SIR} \geq 5$ dB. Alice has 72 antennas.

### Table 3.2: Protocol-Specific Distortion

| TP,FP = 0.003 | 0.96 | 0.68 | 0.44 | 0.01 |
| TP,FP = 0.01 | 0.97 | 0.75 | 0.78 | 0.04 |
| TP,FP = 0.03 | 0.98 | 0.85 | 0.89 | 0.15 |

CFO between Bob and Mallory. Therefore, in order to plot the expected ROC curves, I vary $|\theta - \eta|$ between $0 \sim \pi$ in the experiments, where $\theta$ is the phase rotation due to CFO between Alice and Bob, while $\eta$ is the phase rotation due to CFO between Alice and Mallory. After that, I group the data based on $|\theta - \eta|$ by dividing $0 \sim \pi$ into bins with 0.1 rad width. ROC curves of each bin is computed first and then the
expected ROC curves over all bins are obtained. The results are shown in Fig. 3.15.

It can be observed that, similar to non-protocol-specific jamming, Raw-CFO and MSE-Raw-Value have relatively poor detection performance. Contrarily, while MACE still achieves 0.97 true positive at 0.01 false positive, the true positive of MSE-Abs-Value quickly decreases to 0.78. A main reason is shown in Fig. 3.16(a) and 3.16(b), which demonstrate that when $|\theta - \eta|$ is relatively small, MACE has a much better detection performance than MSE-Abs-Value. As discussed in Sec. 3.4.6, this is because for MSE-Abs-Value, the result of $E\{|\|Y_{i1}\| - |Y_{i2}|\|^2\}$ mainly depends on the noise strength (the difference between $Y_{i1}$ and $Y_{i2}$), while for MACE, the variance of the CFO estimates is related to the SINR (both the difference between and strength of $Y_{i1}$ and $Y_{i2}$ as in Eq. (3.12)). Therefore, even if $|\theta - \eta|$ is small, the change of SINR (mainly the signal strength) can still be detected by MACE.

Finally, as can be seen in Table 3.2, the true positive of MACE with protocol-specific jamming converges more slowly to 1 (with increasing false positive) when compared to non-protocol-specific jamming. This is mainly because there is still a chance that $|\theta - \eta|$ is small even if Bob injects per-frame random CFO before sending his channel sounding pilots.

Therefore, for both non-protocol-specific and protocol-specific jamming, by setting a single threshold, MACE can achieve 0.97 true positive at 0.01 false positive for various client/adversary locations, and for a wide range of SNR ($5 \sim 35 \text{ dB}$) and SIR ($-5 \sim 35 \text{ dB}$) with $\text{SNR} - \text{SIR} \geq 5 \text{ dB}$.

### 3.5.7 Impact of Number of Antennas and Repeated Symbols

As shown in Fig. 3.5, pilot distortion attacks lead to larger reduction of per-client achievable rate when Alice has fewer antennas. In the following, I explore whether
Figure 3.16: ROC curves for protocol-specific jamming signals, and with different CFO between Bob and Mallory for (a) MACE and (b) MSE-Abs-Value detector, respectively. The range of SNR and SIR are $5 \sim 35$ dB and $-5 \sim 35$ dB, respectively, with SNR–SIR$\geq5$ dB. Alice has 72 antennas.
Figure 3.17: True positive at 0.03 false positive when Alice has different number of antennas (with 64 repeated symbols). The SNR and the SIR is within $5 \sim 35$ dB and $-5 \sim 35$ dB, respectively, with $\text{SNR} - \text{SIR} \geq 5$ dB. NPS and PS stand for Non-Protocol-Specific and Protocol-Specific jamming, respectively.

*MACE* can still detect jamming when Alice’s antenna number reduces.

Fig. 3.17 shows the true positive (at 0.03 false positive) for both non-protocol-specific and protocol-specific jamming when Alice’s antenna number increases from 2 to 72. When the number of antennas increases, the true positives for both types of jamming increase. This is mainly because with fewer antennas, the variance of both $\phi$ in Eq. (3.14) and $s'$ in Eq. (3.16) increases, thereby leading to a larger variance of normalized CFO estimates even without jamming signals. However, for protocol-specific jamming, because there is always a chance that $|\theta - \eta|$ (Eq. (3.22)) is small, its true positive quickly saturates, and becomes smaller than that of non-protocol-specific jamming afterwards. Nevertheless, for both types of jamming, *MACE* can achieve 0.97 true positive at 0.03 false positive with only 16 antennas. For stronger
jamming signals, an even smaller number of antennas are required at the AP.

Figure 3.18: True positive at 0.03 false positive when different number of repeated symbols are input into MACE (with 16 or 72 antennas). The SNR and the SIR is within $5 \sim 35$ dB and $-5 \sim 35$ dB, respectively, with SNR–SIR\geq5 dB. NPS and PS stand for Non-Protocol-Specific and Protocol-Specific jamming, respectively.

Furthermore, I also study the detection performance of MACE when fewer than 64 (which is the length of one LTS) repeated symbols are employed. In particular, I reduce the number to as few as 1, and the results with Alice having 72 antennas are shown in Fig. 3.18. Compared to Fig. 3.17, it can be seen that, while the true positive decreases with the number of repeated symbols, the operational limit of MACE is primarily from the number of antennas at Alice. If I set a same threshold with 0.97 true positive at 0.03 false positive, I can observe that MACE needs to use at least 16 repeated symbols for a 72-antenna array, or 32 repeated symbols for a 16-antenna array.

Therefore, even with only 16 antennas at the AP and 32 repeated symbols, MACE
can achieve 0.97 true positive at 0.03 false positive with the same client/adversary locations and SNR/SIR range; consequently, \textit{MACE} can also be used for general-purpose jamming detection, even with a moderate number of antennas and repeated symbols (e.g., cyclic prefix of OFDM symbol).

### 3.6 Conclusion

In this chapter, I study the integrity of CSI. I present the Pilot Distortion Attack, and show that an adversary jamming only the channel sounding of even a single client can lead to all-client denial-of-service in both multiple-antenna networks like IEEE 802.11ac and practical massive MIMO networks. As a counter mechanism, I propose \textit{MACE}, which detects jamming with zero startup cost and zero additional network overhead, and requires no shared secrets. My experiments show that \textit{MACE} can achieve 0.97 true positive at 0.01 false positive when the AP has 72 antennas.
Chapter 4

Related Work

4.1 Confidentiality of Channel State Information in Multiple-Antenna Networks

CSI-based security schemes. Because CSI decorrelates over half a wavelength, it has been proposed as a security mechanism. One technique is artificial noise, which degrades the eavesdropper’s channel by sending artificial noise in the null-space of the desired signals. The secrecy rate achieved by this scheme was analyzed in [21]. Experiments further demonstrated that the eavesdropper consistently has an SINR 15 dB smaller than the desired receiver [22]. Besides artificial noise, the transmitter and the receiver can also use CSI to generate a password between them. The generating framework as well as the secret key extraction speed were studied both theoretically [49] and experimentally [13]. What is more, the AP can also use CSI to authenticate the source of packets: if the packets are from the same client, they should have similar CSI within channel coherence time. Both averaged CSI magnitudes [14] and angle-of-arrival information [15] were proposed as a signature.

However, these schemes assume that the malicious node does not know the CSI between the transmitter and the receiver. Otherwise, they will be no longer safe. Indeed, artificial noise was demonstrated to be removable once CSI is known [32]. Likewise, link signatures based on CSI can be spoofed as long as the attacker has information about the uplink CSI of the client [50]. Furthermore, I demonstrate in
this thesis that once the attacker knows the CSI, a password generated out of it can also be predicted. Thus, because a malicious node with CSIsnoop is able to compute the CSI of any client by overhearing their downlink data transmission, the above designs need to be reconsidered for multi-user WLANs.

**Encrypted CSI measurement.** Even though CSI quickly decorrelates over distance, the downlink (explicit) channel sounding process in current beamforming standards [1, 2] provides an opportunity for a malicious node to learn the CSI of clients by overhearing their CSI measurement feedback. One solution is to encrypt the feedback, but it results in additional overhead for the clients and the AP to establish the encryption and decryption key [23]. Consequently, a multi-stage discriminatory channel estimation scheme was proposed in [51]. The key idea is to exploit channel estimation from the previous training stage to inject artificial noise into the next training stage. In comparison, CSIsec uses a random sequence unknown to Eve instead of the pre-defined one to sound the channel by the AP [23]. The AP can also use uplink (implicit) channel sounding which removes the CSI measurement feedback.

In contrast, CSIsnoop uses the downlink data transmission instead of the channel sounding process to compute the CSI of clients. Moreover, while it was discussed in [23] that an encrypted channel sounding sequence can prevent the malicious node from estimating her channel (which is an important pre-filtering step in [32]), I show that the malicious node can still do so by employing her multiple antennas and the L-LTF field prepended to every packet [1,2]. I also show that the malicious node can actually employ only the L-LTF field to estimate her channel, which does not require the encrypted channel sounding sequence and enables the malicious node to obtain her CSI even with uplink (implicit) channel sounding.
4.2 Integrity of Channel State Information in Multiple-Antenna Networks

**Pilot Distortion Attacks.** Because the improvements brought by multiple-antenna or massive MIMO networks are closely related to the accuracy of clients’ CSI at the AP, a smart adversary can significantly degrade network performance by reducing accuracy of CSI measurements. For small-scale MIMO network, optimal jamming strategies were researched for a multiple-antenna transmitter and a multiple-antenna receiver with Singular Value Decomposition (SVD) beamforming [52,53]. For massive MIMO, if the adversary jams both channel sounding and data transmission, clients’ achievable rates were shown to quickly saturate even with unlimited antennas at the AP [38,39]. Moreover, jamming during channel sounding to aid active eavesdropping in massive MIMO networks was studied in [40–42]. Due to the channel sounding pilots from the eavesdropper, the AP now measures a combination of the client’s and the eavesdropper’s channel, which will significantly reduce the client’s secrecy rate.

In comparison, I present pilot distortion attacks, and show that even if the adversary is active only during channel sounding, which takes no more than 1/60 of the time, concurrent uplink transmission in both multiple-antenna networks like IEEE 802.11ac and practical massive MIMO networks can be thwarted. I further demonstrate by experiments that an adversary having no more transmit power than any client can lead to large reduction of achievable rate of all clients.

**Jamming Detection.** Various techniques have been proposed to detect jamming in wireless networks. However, when they are applied to channel sounding in multiple-antenna networks, a first problem will be the excessively high startup cost (training time). Because concurrent uplink transmission is employed, much longer time (or
more strictly, relatively more network overhead) is needed for the AP to collect enough single-user transmissions from a specific client in order to compute a priori statistics of the packet delivery ratio [27], the received signal strength [54], or the angle-of-arrival information [41]. Moreover, the concurrent transmission also makes the AP hard to differentiate packet decoding error due to incorrect CSI from that due to expired CSI, which renders jamming detection based on packet decoding error less effective [55].

Another problem lies in the network efficiency. Different from data packets, channel sounding pilots are management frames that have lengths as short as several training sequences. Consequently, jamming detection should only introduce minimum network overhead. Techniques that are based on embedded secret keys [52], specially designed random PSK symbols [56], and information exchange between AP and clients [57, 58] all add to network overhead.

In comparison, I propose MACE, which employs the capabilities of the many antennas at the AP to detect jamming with zero startup cost, zero additional network overhead, and no shared secrets between the AP and the clients. I also implement MACE in my testbed and show that it achieves superior detection performance for a wide range of SNR and SIR.

Lastly, CFO has been employed to enhance network security, especially for device fingerprinting, e.g., [59, 60]. MACE differs from them in that MACE does not need to estimate the value of the CFO. Instead, MACE uses the variance of the CFO estimates of a single frame at the AP for jamming detection.
Chapter 5

Conclusion

In this thesis, I study the confidentiality and integrity of CSI in multiple-antenna networks. I first reveal the fundamental conflict between using CSI to optimize PHY design and ensuring the confidentiality of CSI. Specifically, I describe a framework call *CSIsnoop*, and demonstrate how a passive malicious node can employ the overheard downlink multi-user transmission to infer the CSI of any client within the network. As a counter mechanism, the AP can use dedicated antennas for security purposes or redesign beamforming algorithms to prevent reverse engineering by *CSIsnoop*.

Second, I analyze the jamming attacks during channel sounding in multiple-antenna networks, by presenting the highly efficient yet devastating Pilot Distortion Attack. As a counter mechanism, I propose *MACE*, which employs the variance of CFO estimates across the multiple antennas at the AP to detect Pilot Distortion Attack, as well as general wireless jamming, with zero start-up cost and zero additional network overhead.

Finally, I build testbeds by using the WARP v3 software defined radio and the Argos massive MIMO AP to experimentally study both the confidentiality and integrity of CSI in various indoor environments. I show that *CSIsnoop* achieves an average correlation of over 0.99 in inferring clients’ CSI, and can be further employed to break various CSI-based security schemes. Moreover, while Pilot Distortion Attack can lead to all-client denial-of-service in practical multiple-antenna and massive MIMO networks, *MACE* can detect it with 0.97 true positive at 0.01 false positive.
Bibliography


