# Stemming Downlink Leakage from Training Sequences in Multi-User MIMO Networks

**Yunlong Mao**, Yuan Zhang, Sheng Zhong

State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, China

*yl.mao09@gmail.com*

October 27, 2016

# Outline

1 Multi-User MIMO

2 Attack Model

3 Secure Estimation

4 Implementation and Experiments

# Channel State Information (CSI)

**Interference:**

- Multi-path propagation;
- Selective fading;
- Noise.
- ...

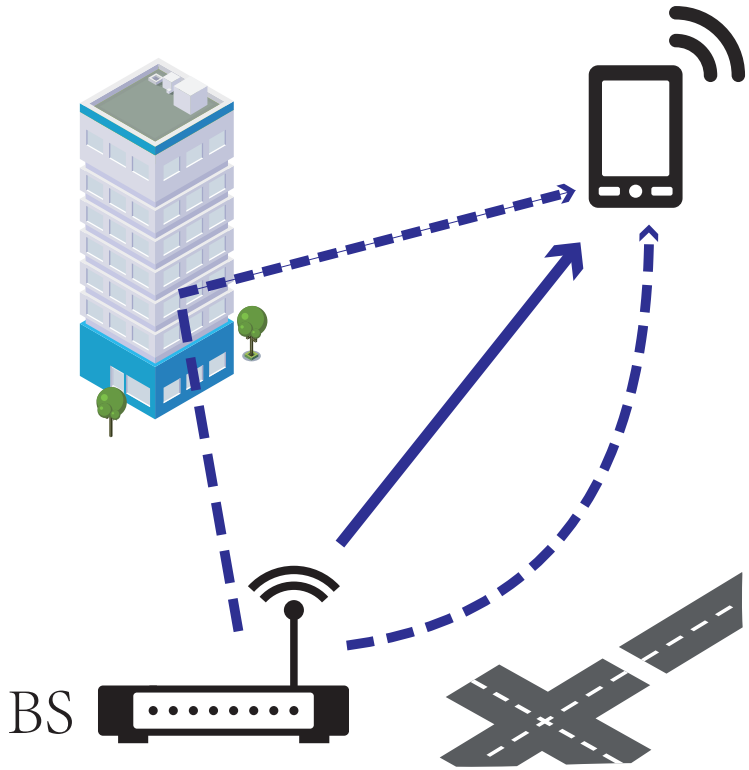



Figure: a situation of multi-path propagation

# Channel State Information (CSI)

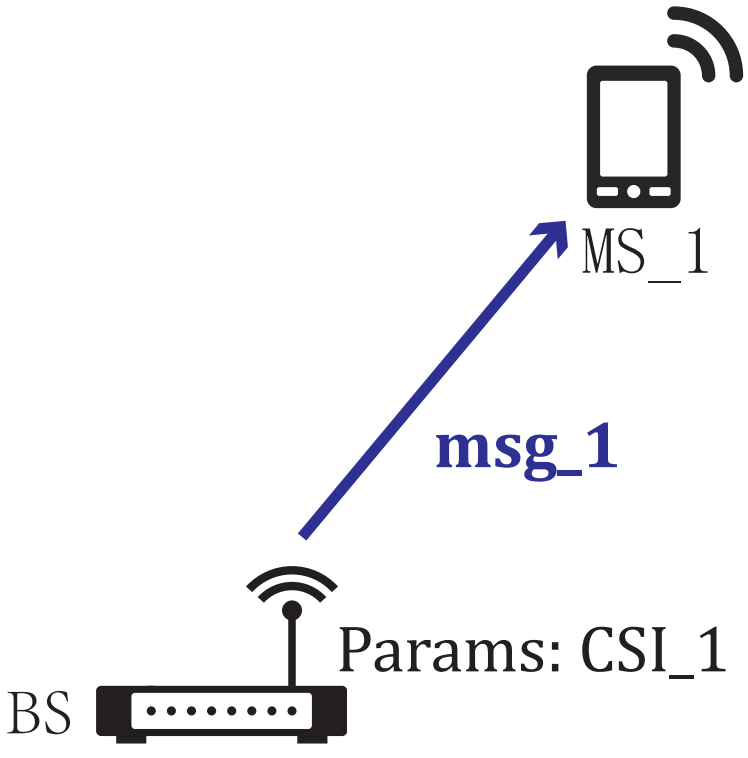



Figure: use $CSI_1$ to enhance the communication of $MS_1$

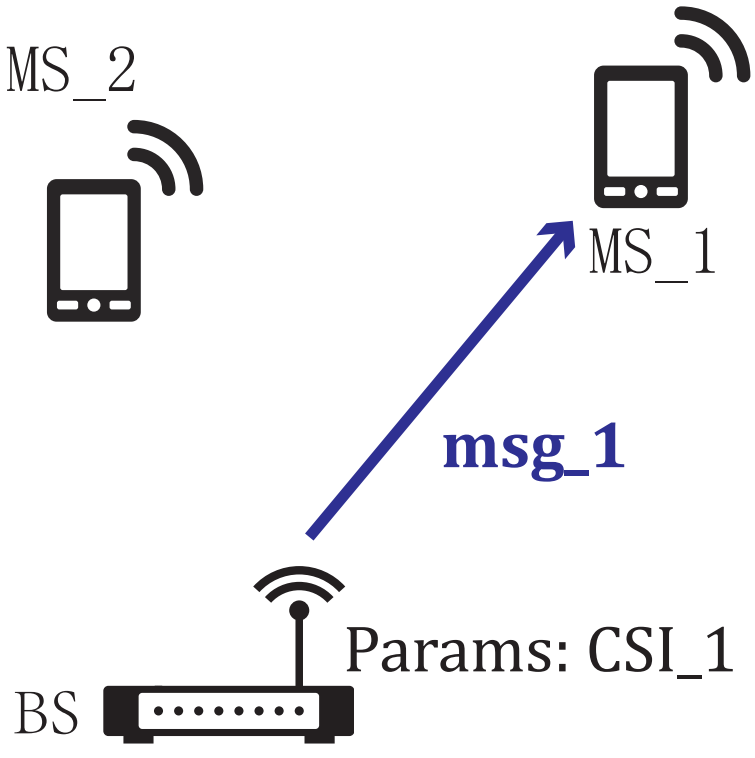



Figure: when there is another user to serve

# Channel State Information (CSI)

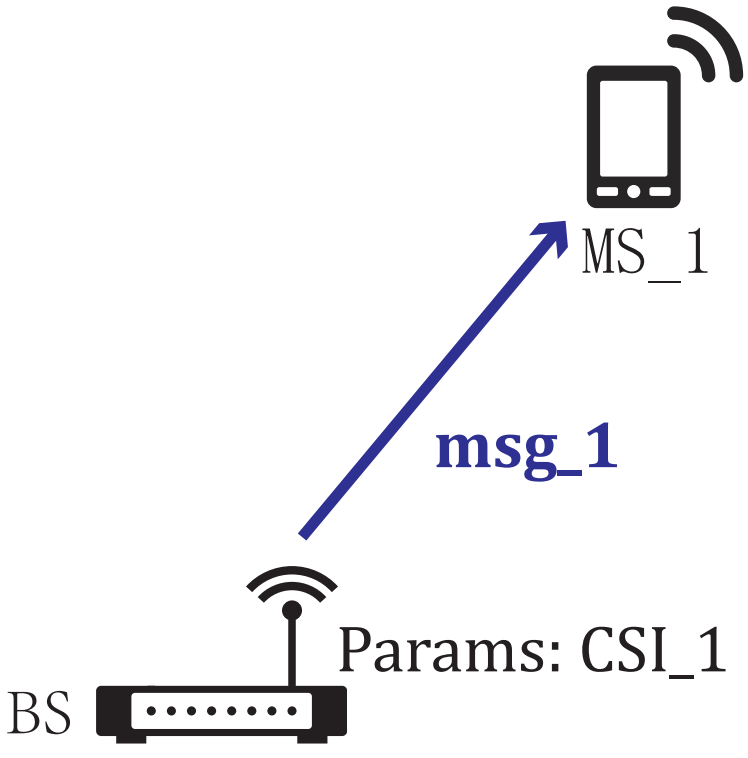



Figure: use $CSI_1$ to enhance the communication of $MS_1$

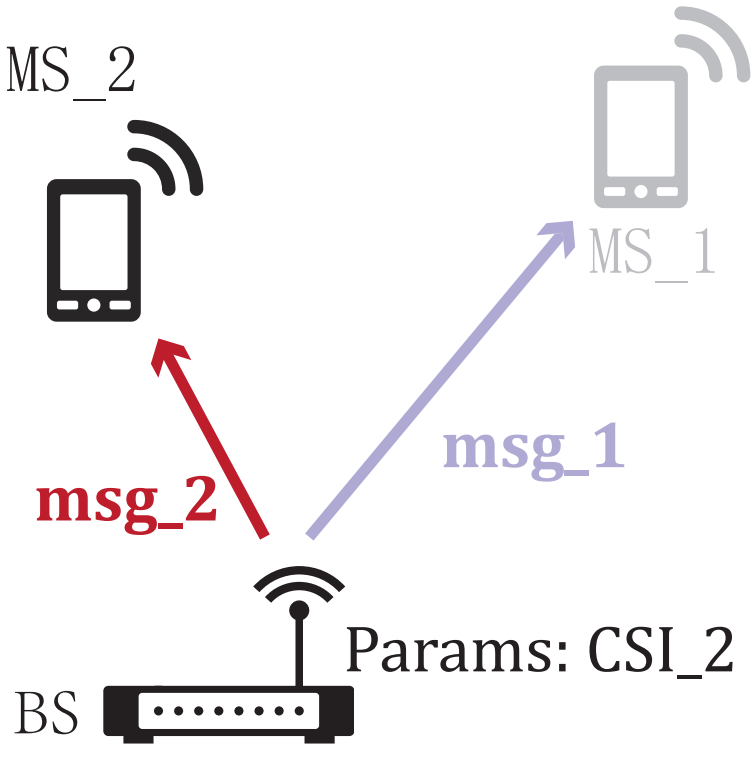
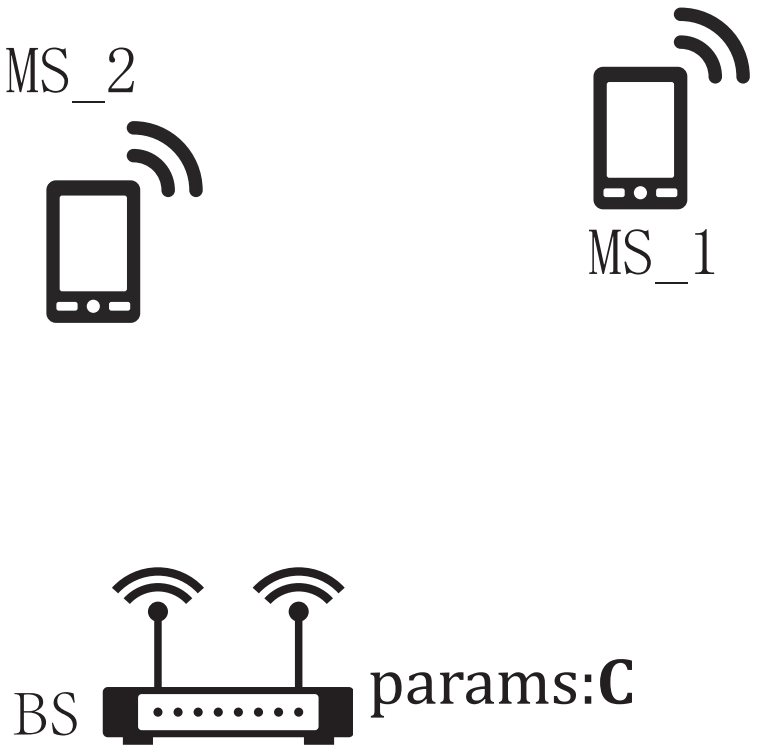



Figure: change parameters and use $CSI_2$ to serve $MS_2$

# Multi-User MIMO

**Serve them simultaneously?**

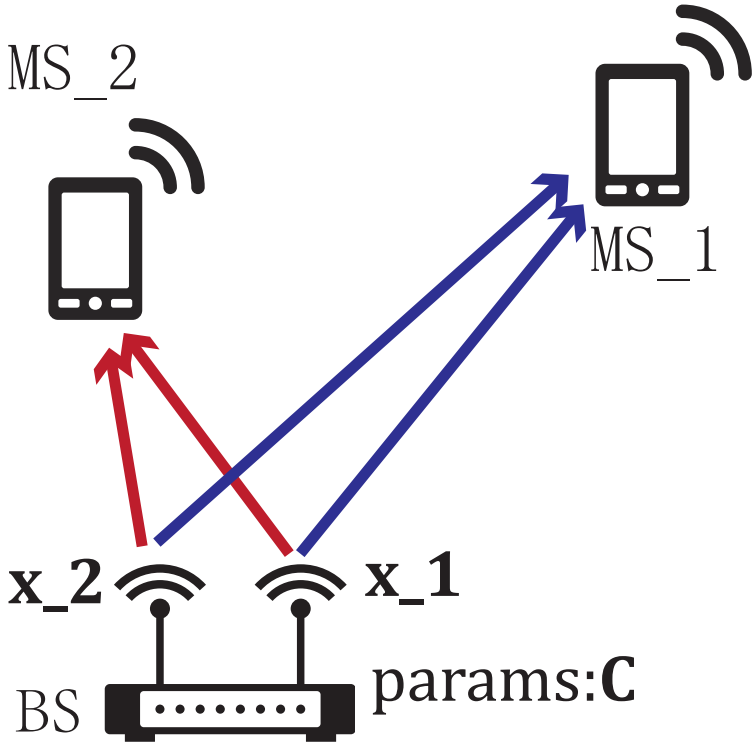
- Another antenna is needed.
- Parameters of transmitting should be corresponding to both $CSI_1$ and $CSI_2$.



# Multi-User MIMO

**Serve them simultaneously?**

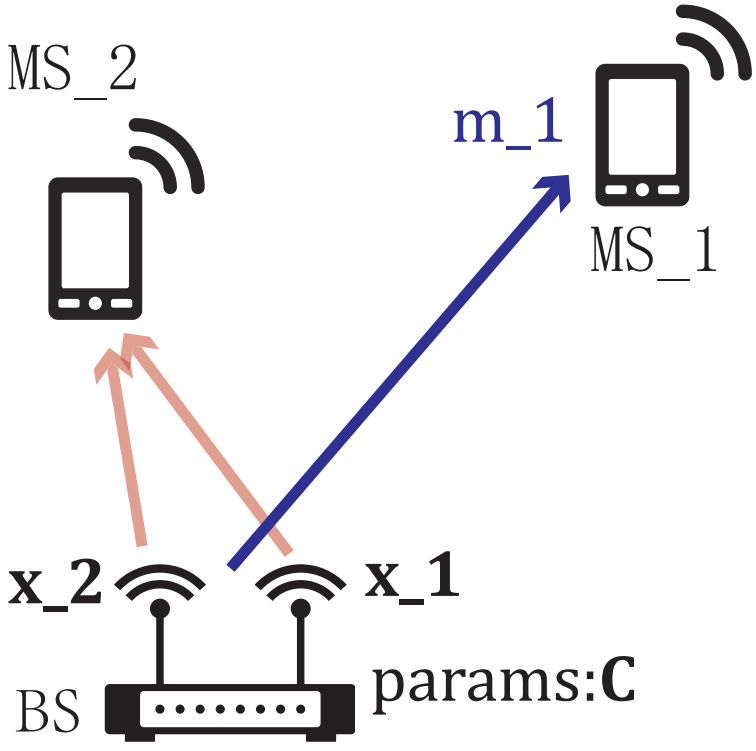
- Another antenna is needed.
- Parameters of transmitting should be corresponding to both $CSI_1$ and $CSI_2$.



# Multi-User MIMO

## Serve them simultaneously?

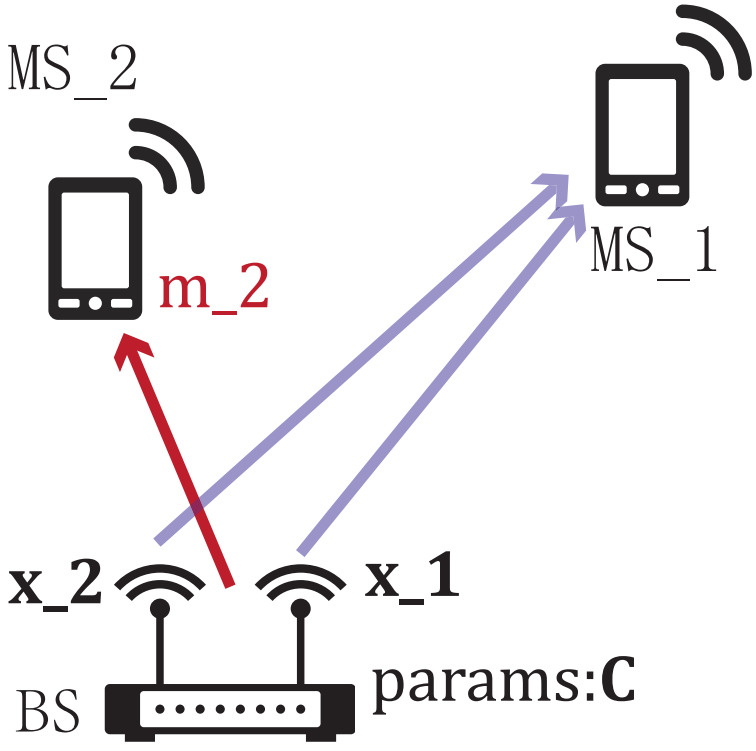
- Another antenna is needed.
- Parameters of transmitting should be corresponding to both $CSI_1$ and $CSI_2$.
- Ideal situation.



# Multi-User MIMO

## Serve them simultaneously?

- Another antenna is needed.
- Parameters of transmitting should be corresponding to both $CSI_1$ and $CSI_2$.
- Ideal situation.



# Training Sequence

What is **Training Sequence**?

## How to encode signal for antennas?

Zero-Forcing Beamforming, CSI needed.

## How to acquire accurate CSI?

Learn from the change of commonly known sequence.

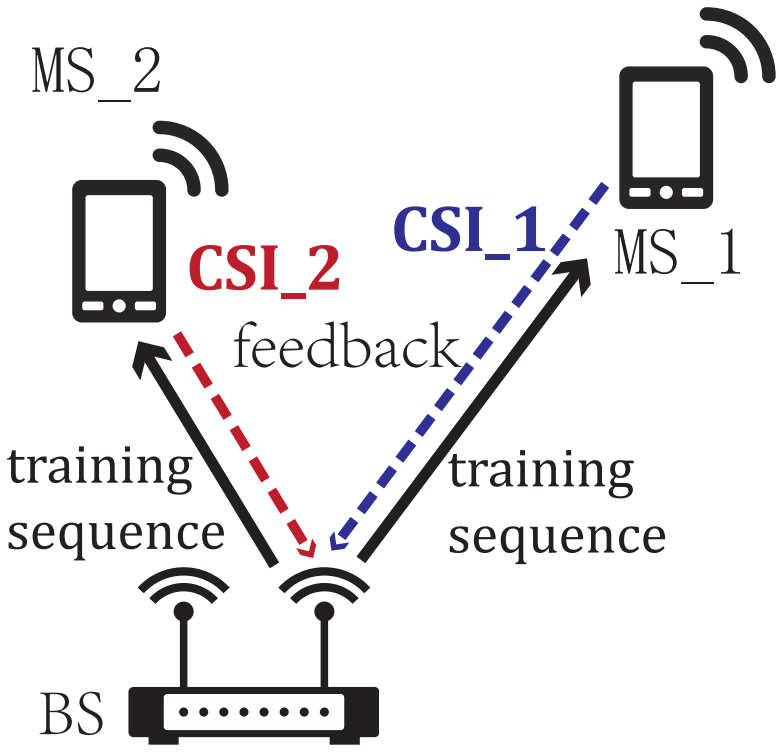
## How to implement this?

Insert commonly known sequence into transmitting. Then estimate CSI by the changing of sequence. This process can be repeated for many times to train more accurate CSI. The commonly known sequence is called **training sequence**.

# Eavesdropping Attack Based on CSI Feedback

## Previous work

- [Y.-C. Tung, S. Han, D. Chen, and K. G. Shin. CCS '14]
- Sniffing attack based on CSI feedback.

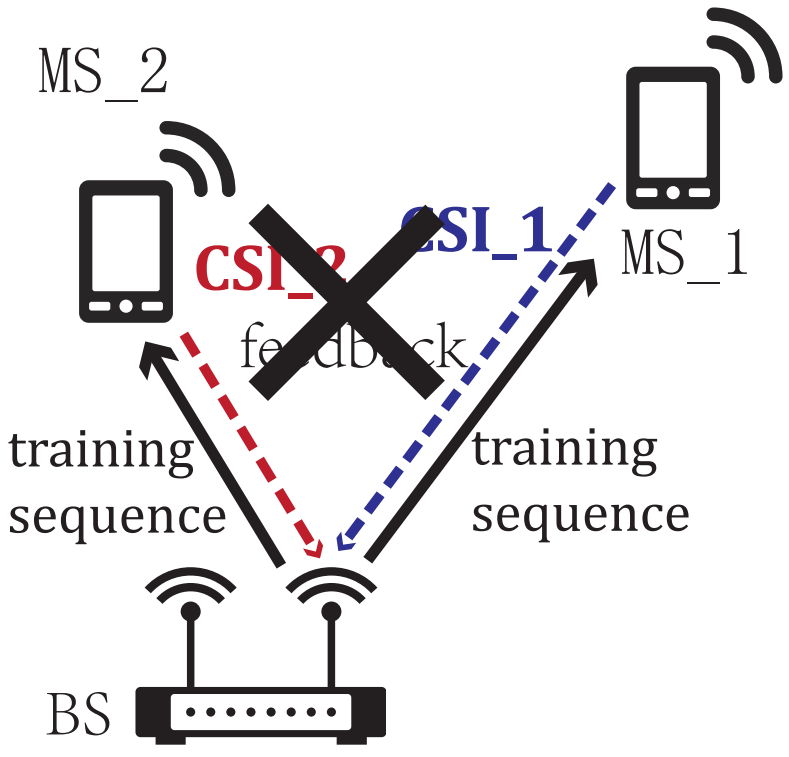


# Eavesdropping Attack Based on CSI Feedback

## Previous work

- [Y.-C. Tung, S. Han, D. Chen, and K. G. Shin. CCS '14]
- Sniffing attack based on CSI feedback.

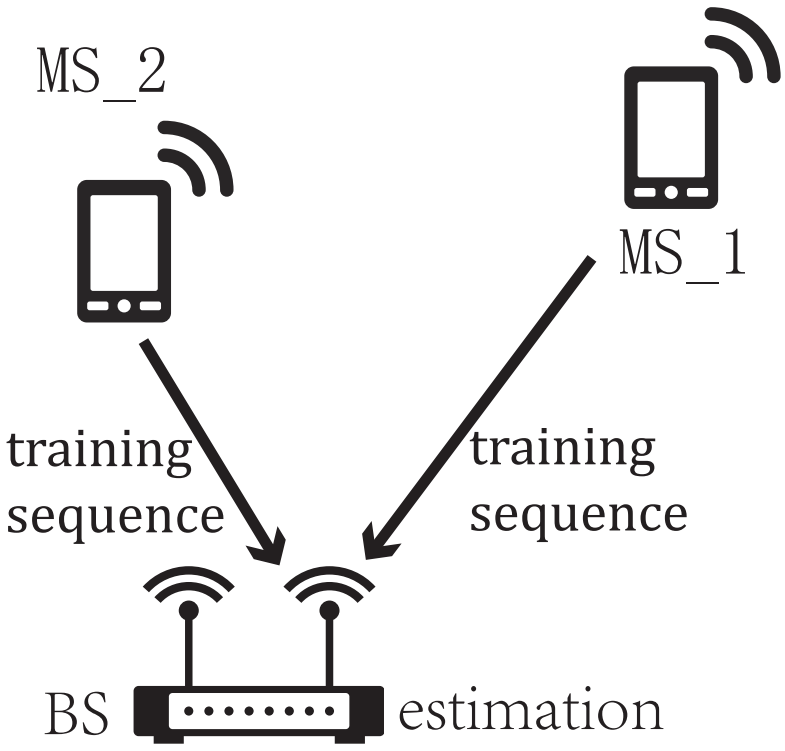
What if there is no feedback?



# Implicit CSI Estimation

**Advantages**

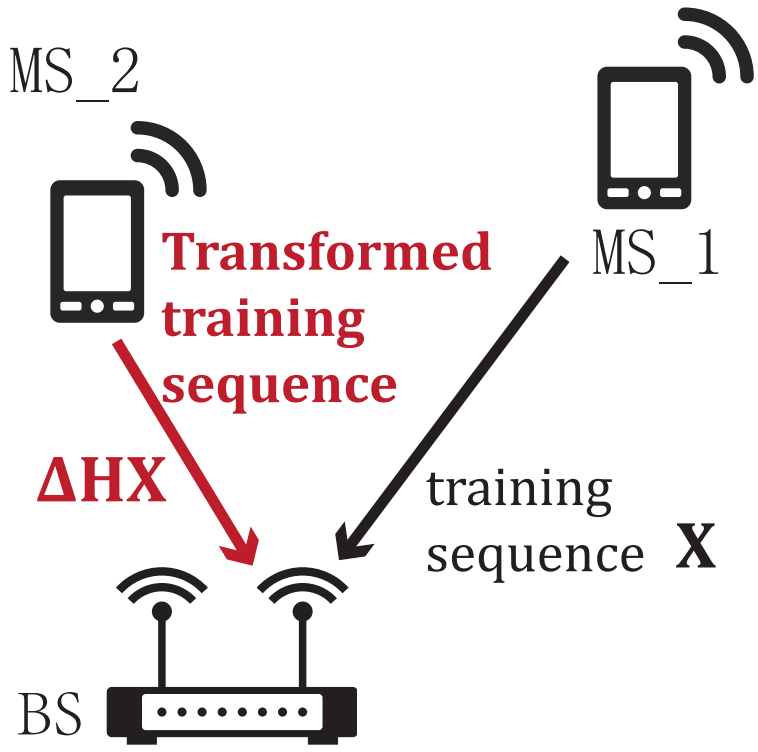
- Communication complexity is low;
- Base station performs estimation. Energy is saved for mobile users;
- No delay from estimating CSI to using CSI.



# Transformed Training Sequence

**How to transform training sequence**

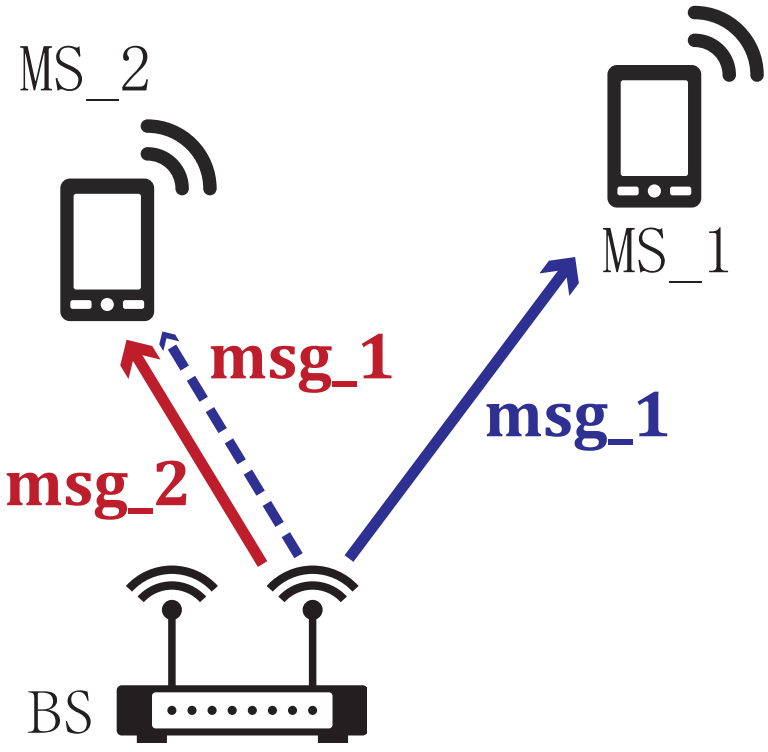
1. Malicious user calculates expected CSI;
2. Calculate the difference $\Delta H$ between expected CSI and his own CSI;
3. Transform commonly known training sequence with $\Delta H$;



# Eavesdropping Attack

**Two steps for eavesdropping attack**

1. Transform training sequence to lead the base station send other user's message to malicious user;
2. Use cancellation method to cancel the interference caused by download of malicious user himself;



# Challenges

This attack is easy to perform:

- Plain text of training sequence;
- Linear system.

This attack is hard to be identified and prevented:

- Base station has no evidence to tell who is lying;
- Original training procedure is based on cooperation;
- Estimation is time sensitive. Complex protocols cannot be used.

# Secure Estimation of CSI

## First Phase: Generating Commitments

Mobile users generate commitments about their own training sequence that the base station should use for estimation.

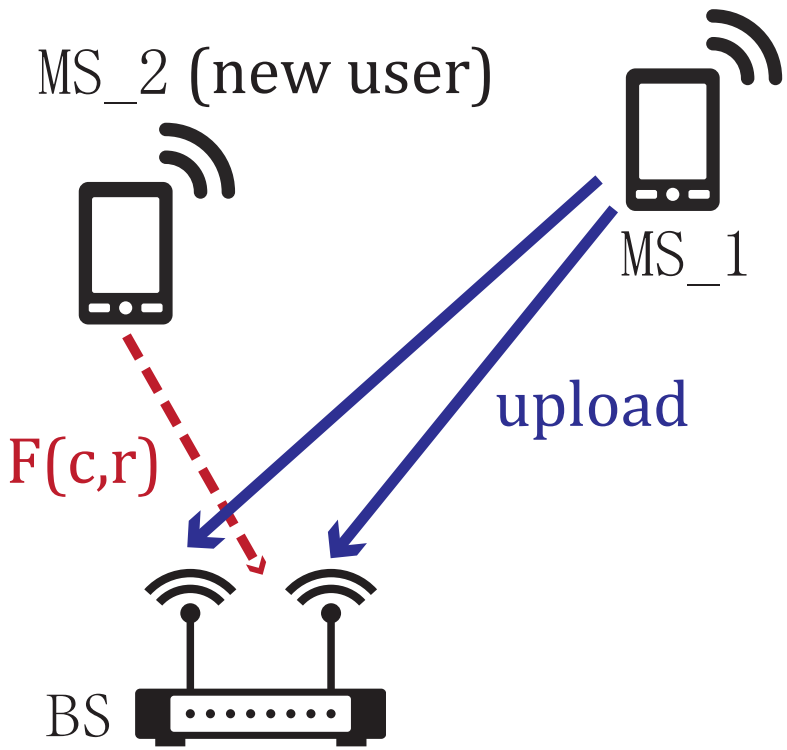
## Second Phase: Revealing Commitments

After the base station has held commitments for one coherence interval, mobile users will reveal their commitments to the base station. The base station will do CSI estimation with training sequences that mobile users have committed about.

# First Phase: Generating Commitments

**Two steps:**

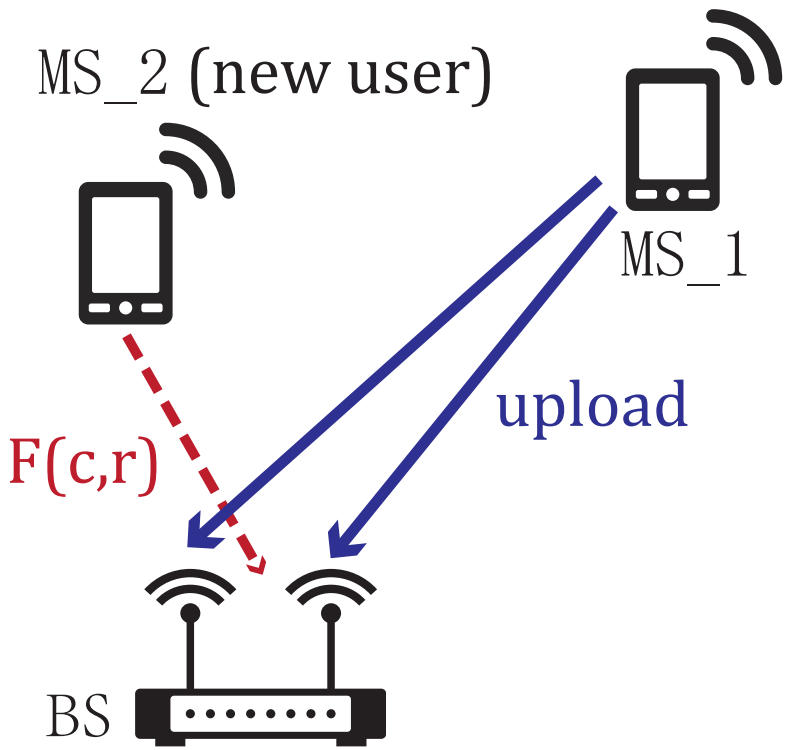
1. Generate commitment $F(c_i, r_i)$;
   Fuzzy Commitment Scheme [by A. Juels and M. Wattenberg, CCS '99];
   Linear Error Correcting Code.



# First Phase: Generating Commitments

**Two steps:**

1. Generate commitment $F(c_i, r_i)$;
2. Insert commitments to upload.
   Time Division Multiplexing in the very beginning;
   Spatial Multiple Uplink Access scheme after initialization.



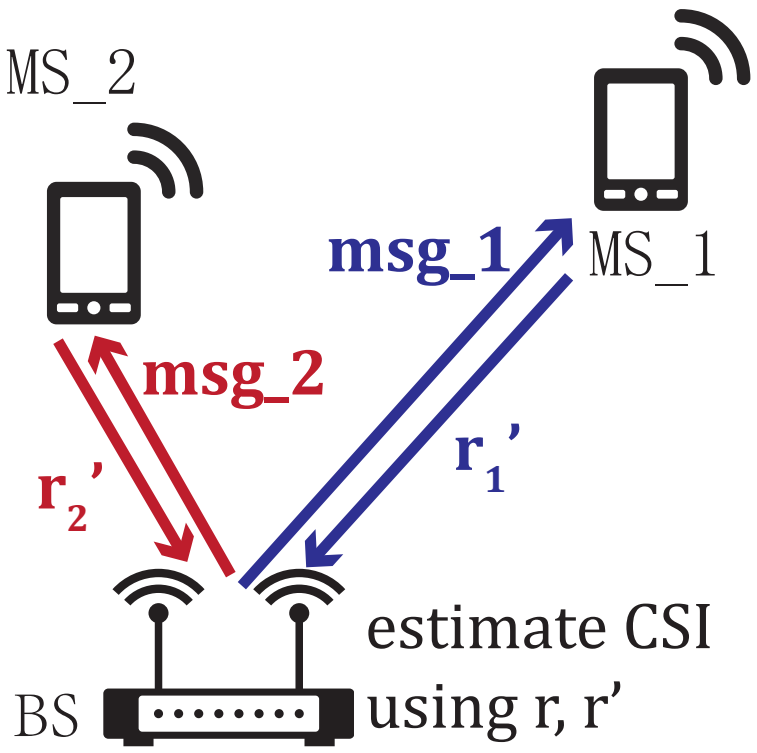
# Second Phase: Revealing Commitments

**Mobile User:**

1. Reveal commitment by sending $r'$.

**Base Station:**

1. Verify commitment by checking whether $r$ can be recovered from $r'$.
2. Estimate CSI by linear estimator using $r$ and $r'$.



# Phase 1 and Phase 2

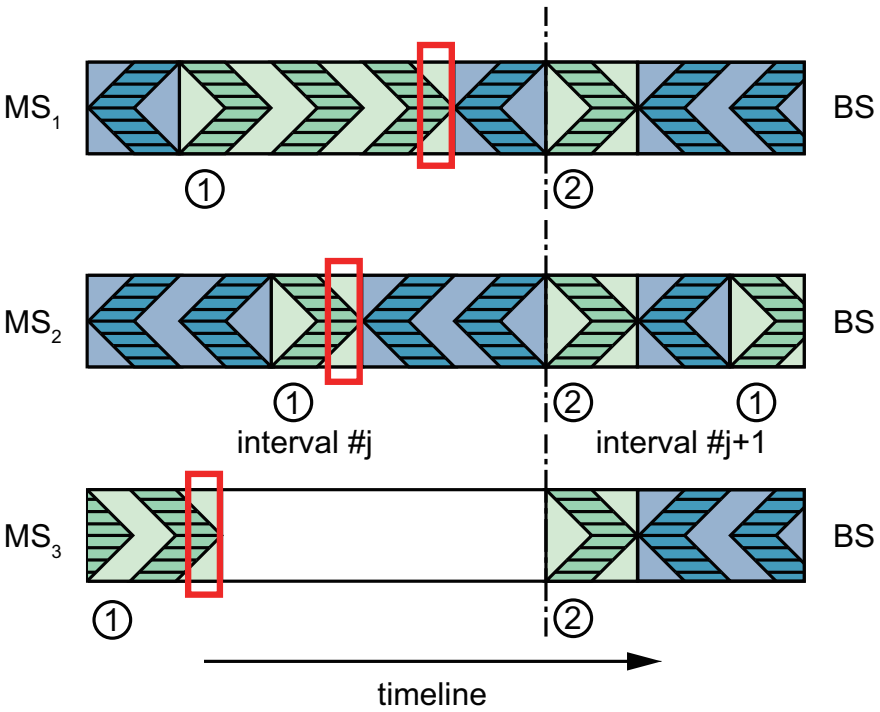



Figure: Commitments inserted.

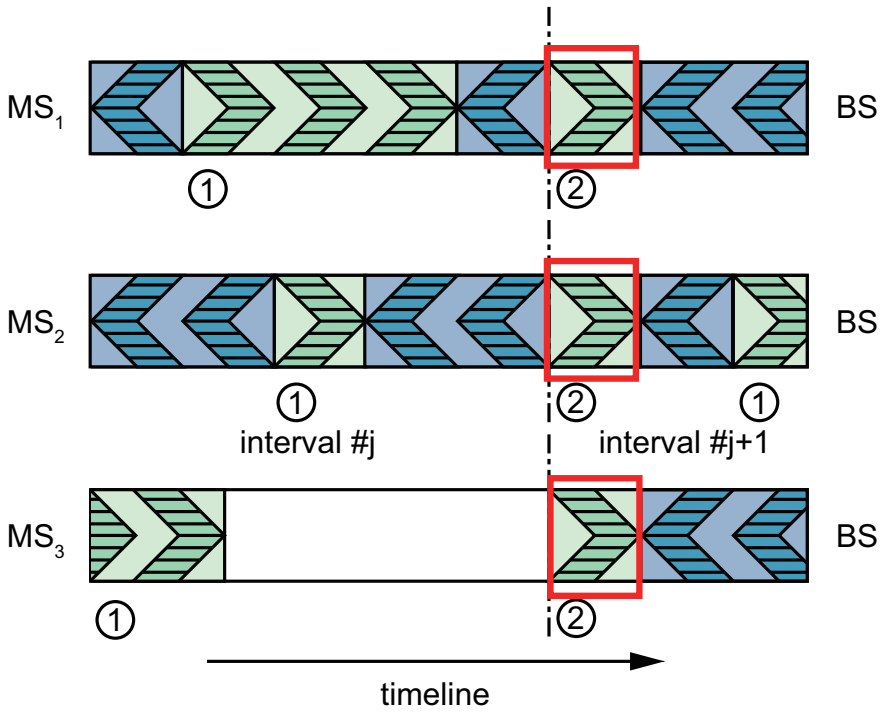



Figure: Revealing commitments.

# Secure Estimation of Statistical CSI

## Statistical CSI

- As opposed to instantaneous CSI;
- Can be described by statistics;
- CSI keeps unchanged or,
- CSI changes slowly.

## Tradeoff between security and transmitting rate

- Stable CSI contributes to high communication rate;
- Relatively statistical CSI is easy to predict.

# Secure Estimation of Statistical CSI

**Two steps for eavesdropping:**

1. Lead the base station transmit partial download content of other users to malicious user (by transforming training sequence)
2. Cancel the interference caused by channels and malicious user's own downloading content, to reveal target's download.

# Adaptive Security With Statistical CSI

1. The base station calculates how much higher the SNR of changing CSI is than threshold.
2. The base station solves how many bit error are needed.
3. The base station adds artificial bit errors into transmitting queue.

Integrate adaptive security scheme into secure CSI estimation.

# Implementation

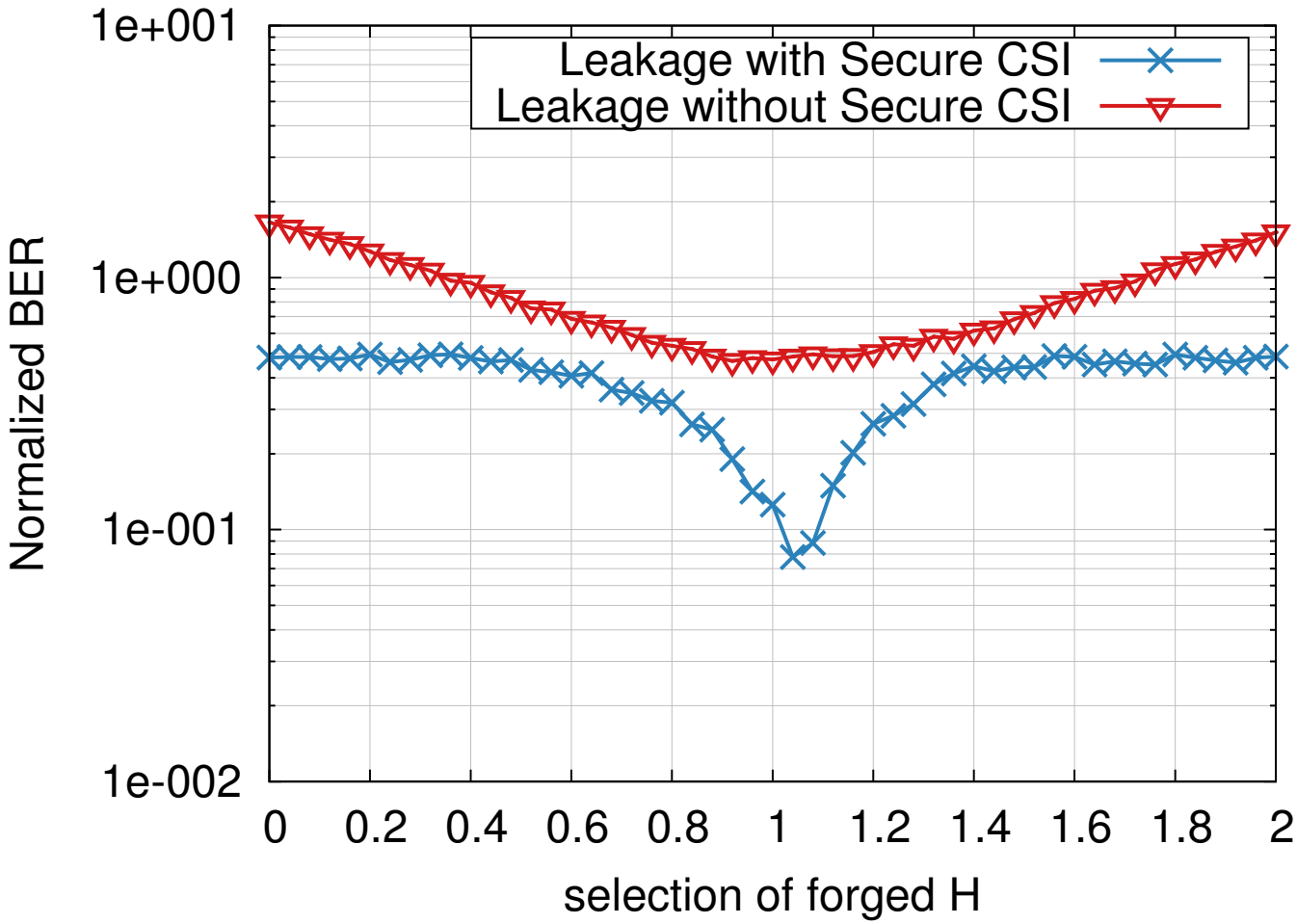
Hardware:

- Universal Software Radio Peripheral (USRP) N210;
- OctoClock-G;
- Switch and cable for Gigabyte.

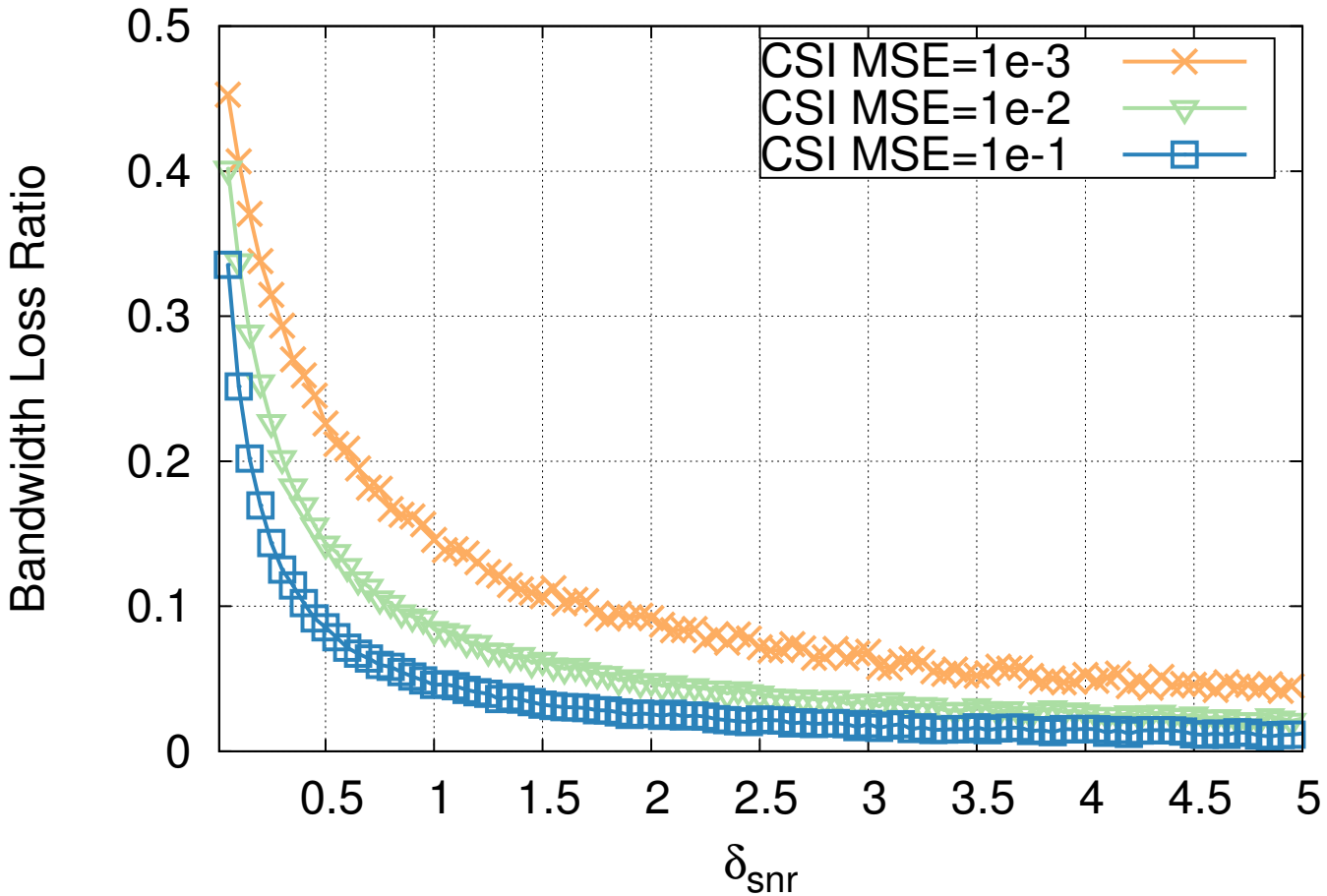
Software:

- GNU Radio development kit.

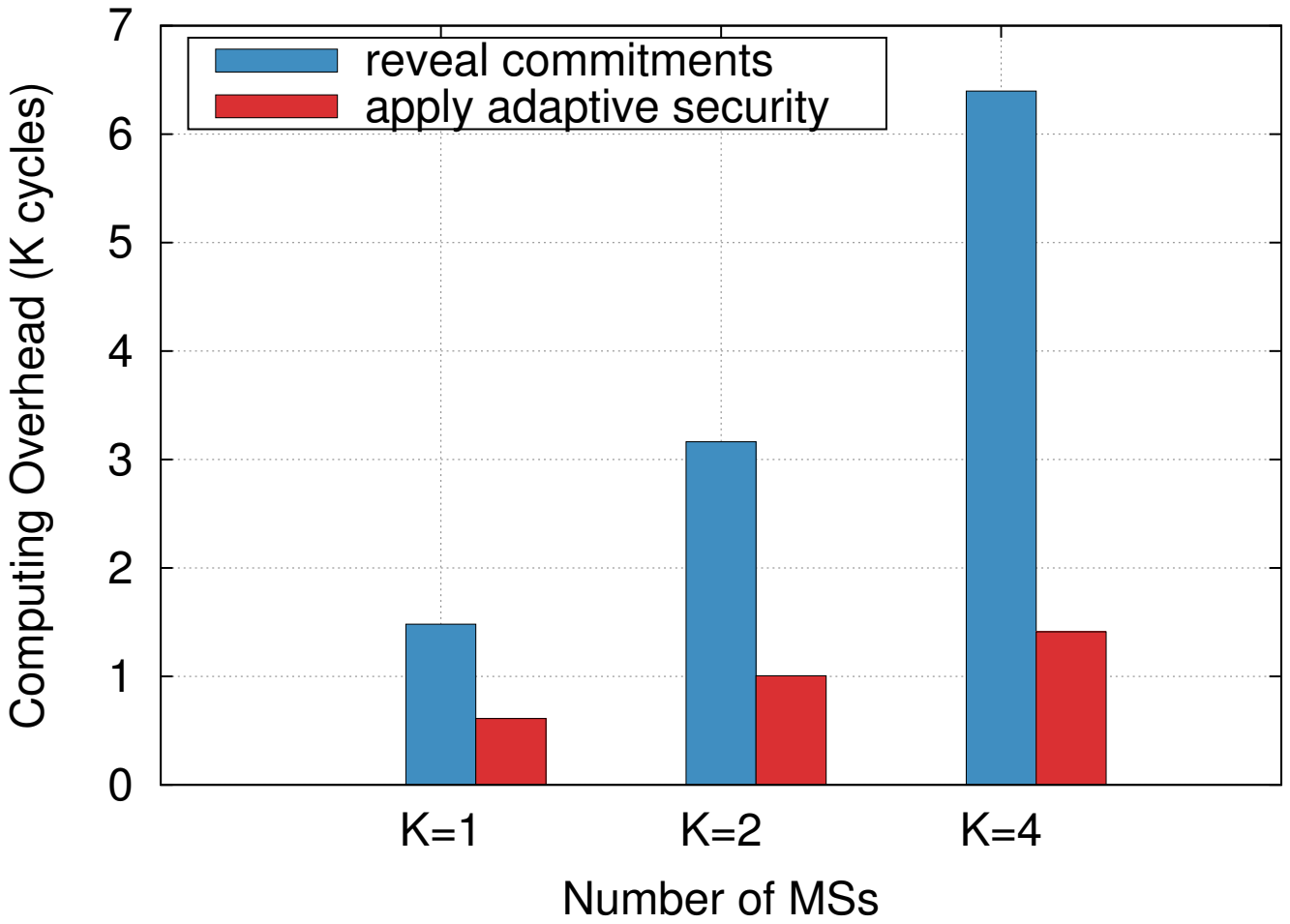
# Leakage


Leakage with Secure CSI
Leakage without Secure CSI
Normalized BER
1e+001
1e+000
1e-001
1e-002
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2
selection of forged H

# Loss of bandwidth



# Overhead


reveal commitments
apply adaptive security
Computing Overhead (K cycles)
0
1
2
3
4
5
6
7
K=1
K=2
K=4
Number of MSs

# Summary

1. Malicious user in MU-MIMO networks can eavesdrop on other users download by transforming his own training sequence, even there is no explicit CSI feedback.
2. We propose a secure CSI estimation to stop malicious user from downloading messages of other user.
3. When CSI changes slowly or keeps unchanged, we will use adaptive security scheme to prevent malicious user from decoding other user's messages.

# Thank You