Spectrum Tomography Attacks: Inferring Spectrum Allocation Mechanisms in Multicarrier Systems

Shangqing Zhao[†], Zhe Qu[†], Zhuo Lu[†], Tao Wang[‡]
[†] Department of Electrical Engineering, College of Engineering, University of South Florida, Tampa, FL, 33620;
[‡]Department of Computer Science, New Mexico State University, Las Cruces, NM, 88003.

UNIVERSITY OF SOUTH FLORIDA

Abstract

Spectrum allocation algorithm is a vital process to improve the system throughput in a network. But in wireless networks, such an algorithm is vulnerable to leakage due to the broadcast nature of the wireless channel. By exploiting such vulnerability, we present a mechanism, called spectrum tomography, to obtain the allocation algorithm without direct access to the access point (AP) in an Orthogonal Frequency Division Multiple Access (OFDMA) network. Then, we propose an attack strategy, called spectrum tomography attack, which further takes advantage of the spectrum tomography to damage the network. Finally, we present three basic strategies for the spectrum tomography attack.

Objective

Multi-user communication system allows an access point (AP) serves multiple non-AP stations (or users) simultaneously. In this system, user selection is a very important procedure before sending packets. Therefore, user selection algorithm is usually unknown to public.

In this poster, we have two objectives

1) obtain the user selection algorithm without accessing to the system.

2) damage the network by injecting malicious users to interfere AP, such that it selects inappropriate users.

Background

1. OFDMA

One popular technique to support multi-user communication is Orthogonal Frequency Division Multiple Access (OFDMA), which assigns different and mutual exclusive subcarriers to different users.

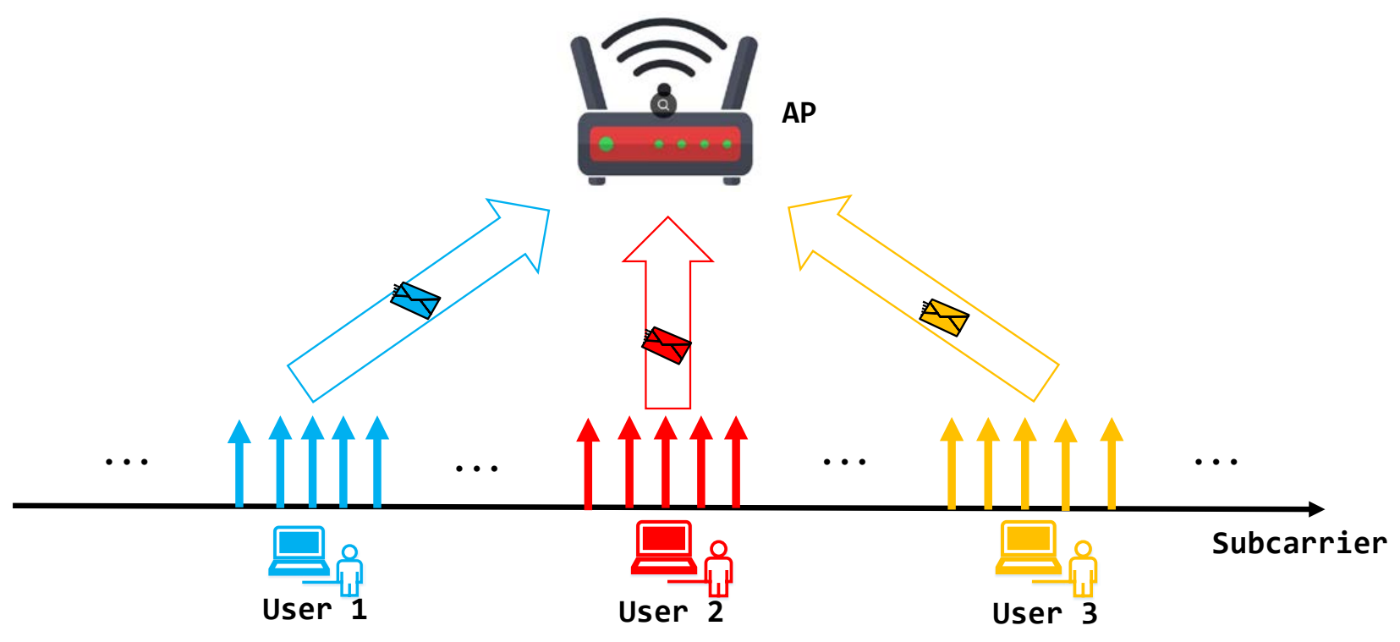


Figure: OFDMA system structure.

Two steps:
a) AP assigns subcarriers to users;
b) Users send packets through assigned subcarriers.

2. User Selection

Restricted by the bandwidth, an AP can only simultaneously serve a limited number of users. For example, in 802.11ax, an AP can support up to 9 users for a 20MHz system.

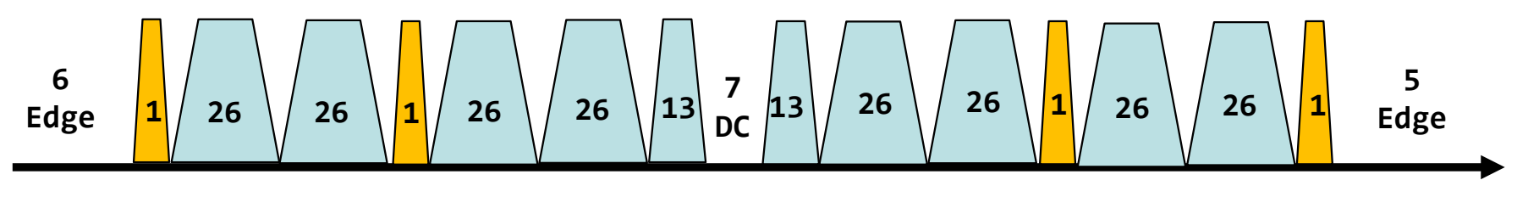


Figure: Subcarrier Allocation of 802.11ax system with 20MHz bandwidth.

Therefore, user selection is necessary before assigning subcarriers. Generally, the user selection process is based on the instantaneous channel state information (CSI) of each user. In order to improve the throughput, AP often select users with better CSI for the immediate data transmissions. Therefore, there are two steps for the user selection

i) Sounding: AP first sends sounding packets to all users, who are connected with it. The sounding packet indicates how users feedback their CSIs.

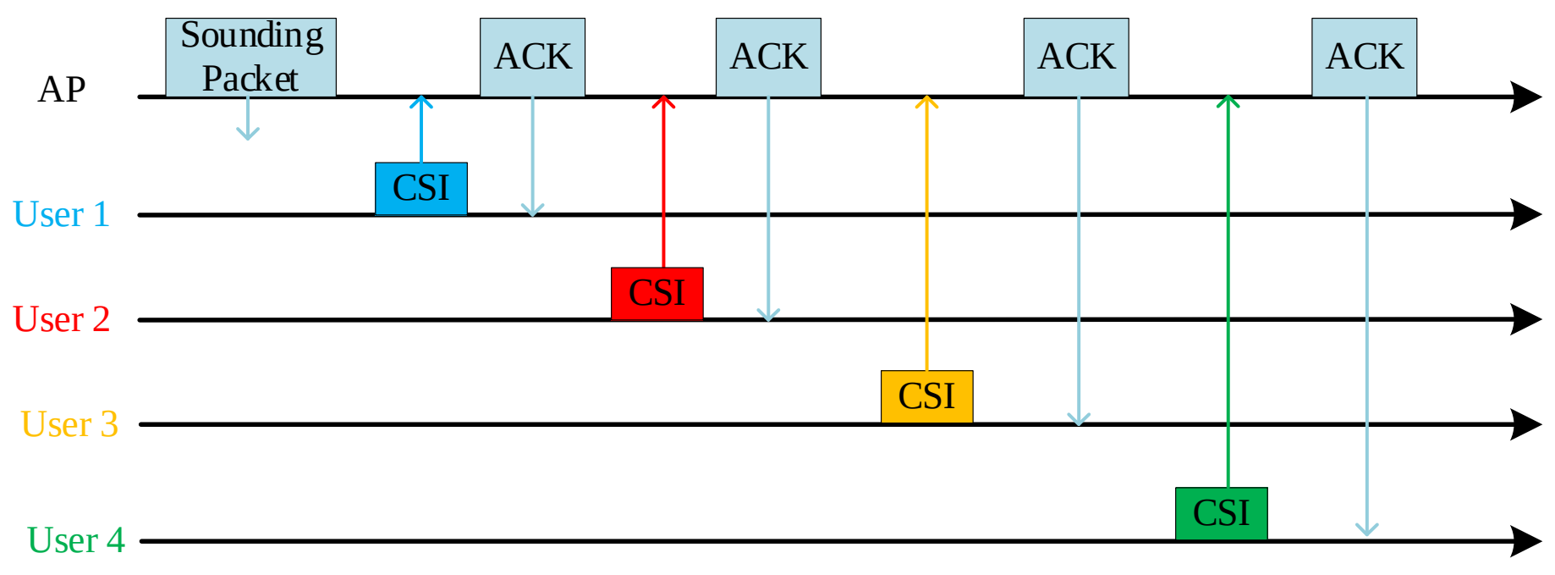


Figure: OFDMA sounding process.

ii) Acknowledgement: AP compares collected CSIs and selects those who have better CSI than others. Then AP assigns subcarriers to the selected users, and sends trigger frames to selected users to ask them prepare for the following data transmission.

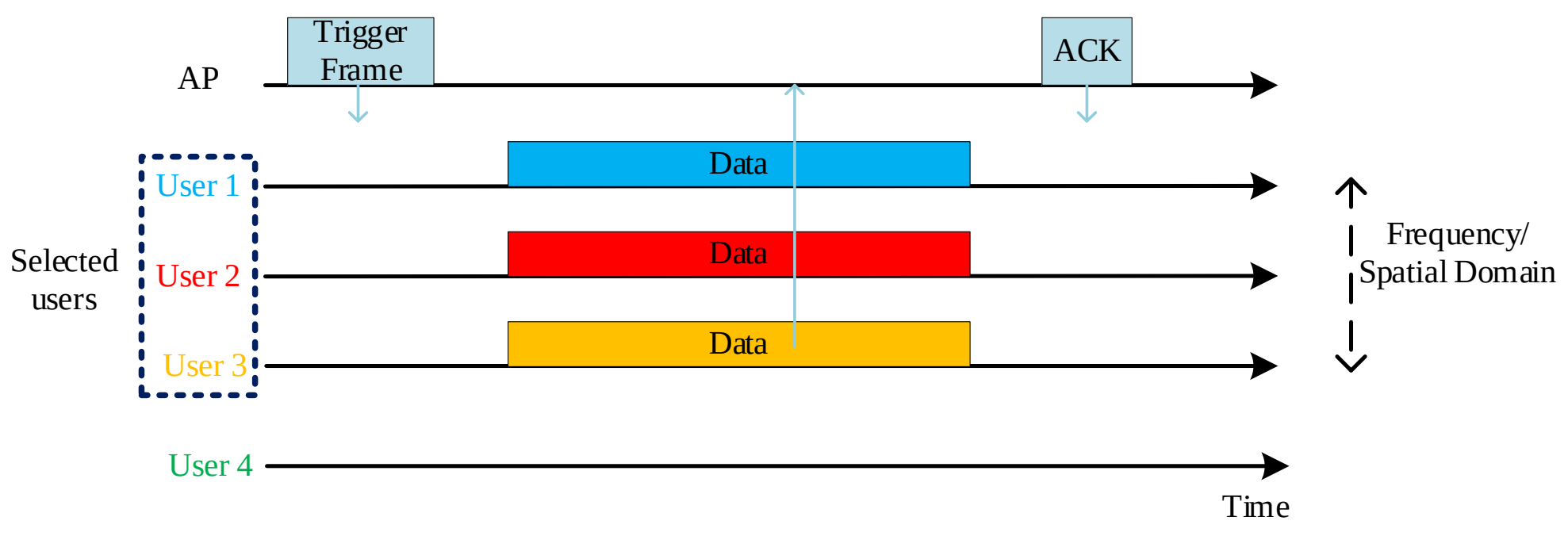


Figure: OFDMA acknowledgement and data transmission.

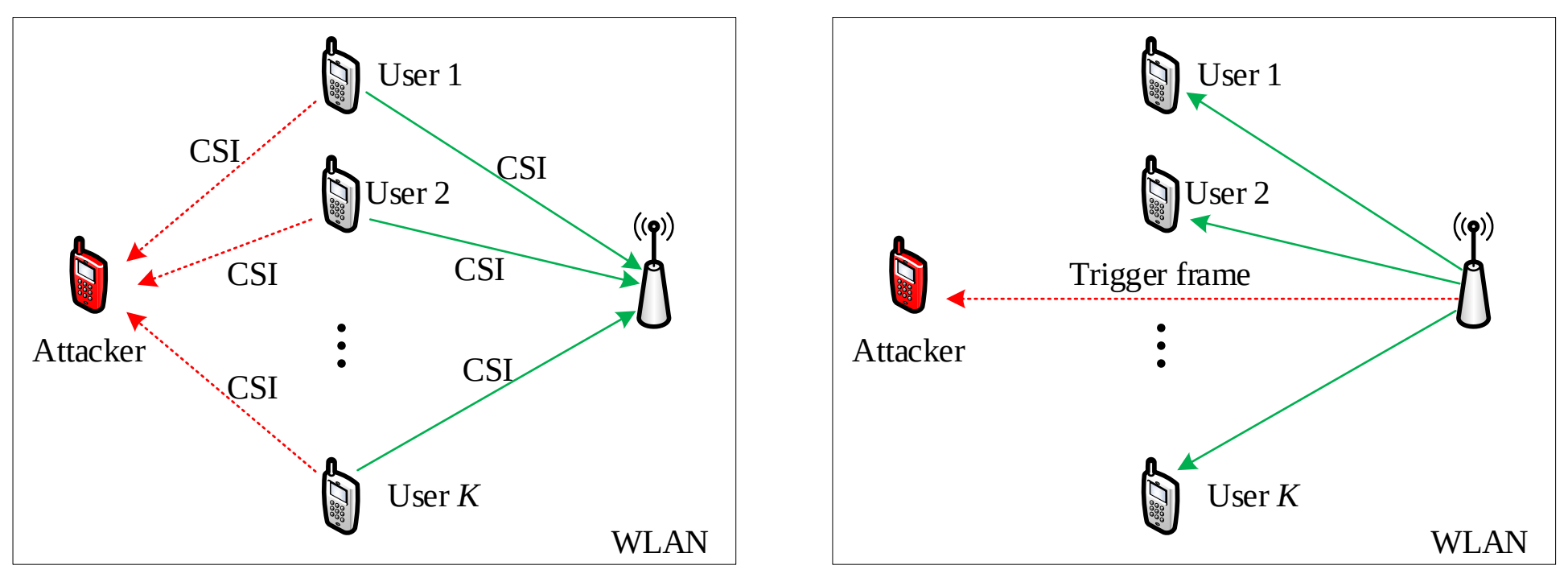
Vulnerability

There are two facts in the user selection process:

1) CSI and trigger frames are transmitted in plaintext.

2) Broadcast nature of the wireless channel.

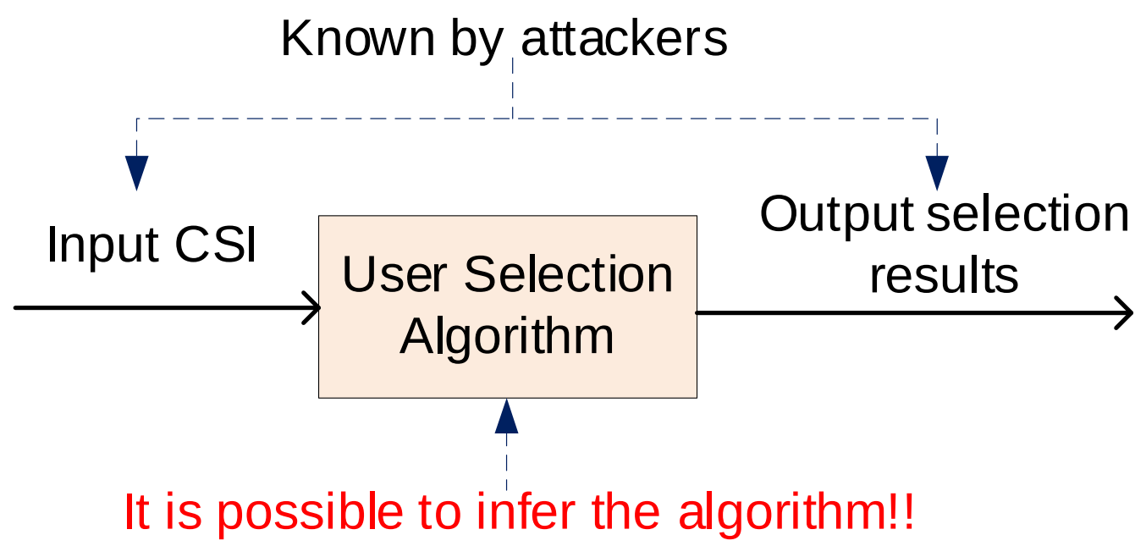
These two facts enable the attacker to know both CSI (from sounding phase) and the selection results (from acknowledgement phase).



Sounding

Acknowledgement

After obtaining CSI and results of user selection (from the trigger frame), the attacker is possible to get the user selection algorithm indirectly.


Known by attackers

Input CSI

User Selection Algorithm

Output selection results

It is possible to infer the algorithm!!

We propose a method ***spectrum tomography*** to infer the user selection algorithm:

1) we first collect the CSI feedback from each user, as well as the final selection decision from the AP,

2) then build a statistic model to infer the algorithm.

Attack Strategy

Leveraging spectrum tomography, in this poster, we propose an attack, called ***spectrum tomography attack***, to mislead the AP to select inappropriate users. It consists of two steps: (i) the spectrum tomography step, and (ii) the damage step.

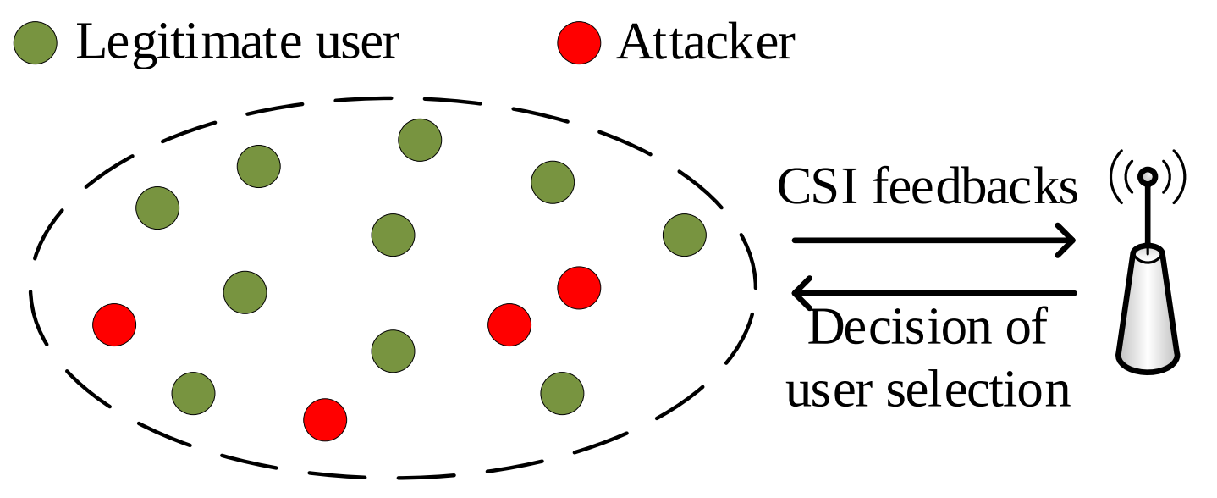


Figure: System Model.

1. spectrum tomography step

The purpose of this step is to obtain the user selection algorithm. In this step, attackers act as legitimate users which not only return their true CSI to AP, but also record CSI from other users and the decision vector from the AP.

Variable	Description
$\mathbf{H}$	The channel state matrix contains all CSI from all users $\mathbf{H}=\{\mathbf{h}_{ij}\}_{M\times n}$
$\mathbf{D}$	Decision vector, whose entry $d_{ij}=1$ if the jth user is selected at round i, and 0 otherwise. (e.g. (1, 1, 1, 0) for previous example)
f	A function indicating the user selection algorithm in AP.
g	A user selection algorithm inferred by attackers

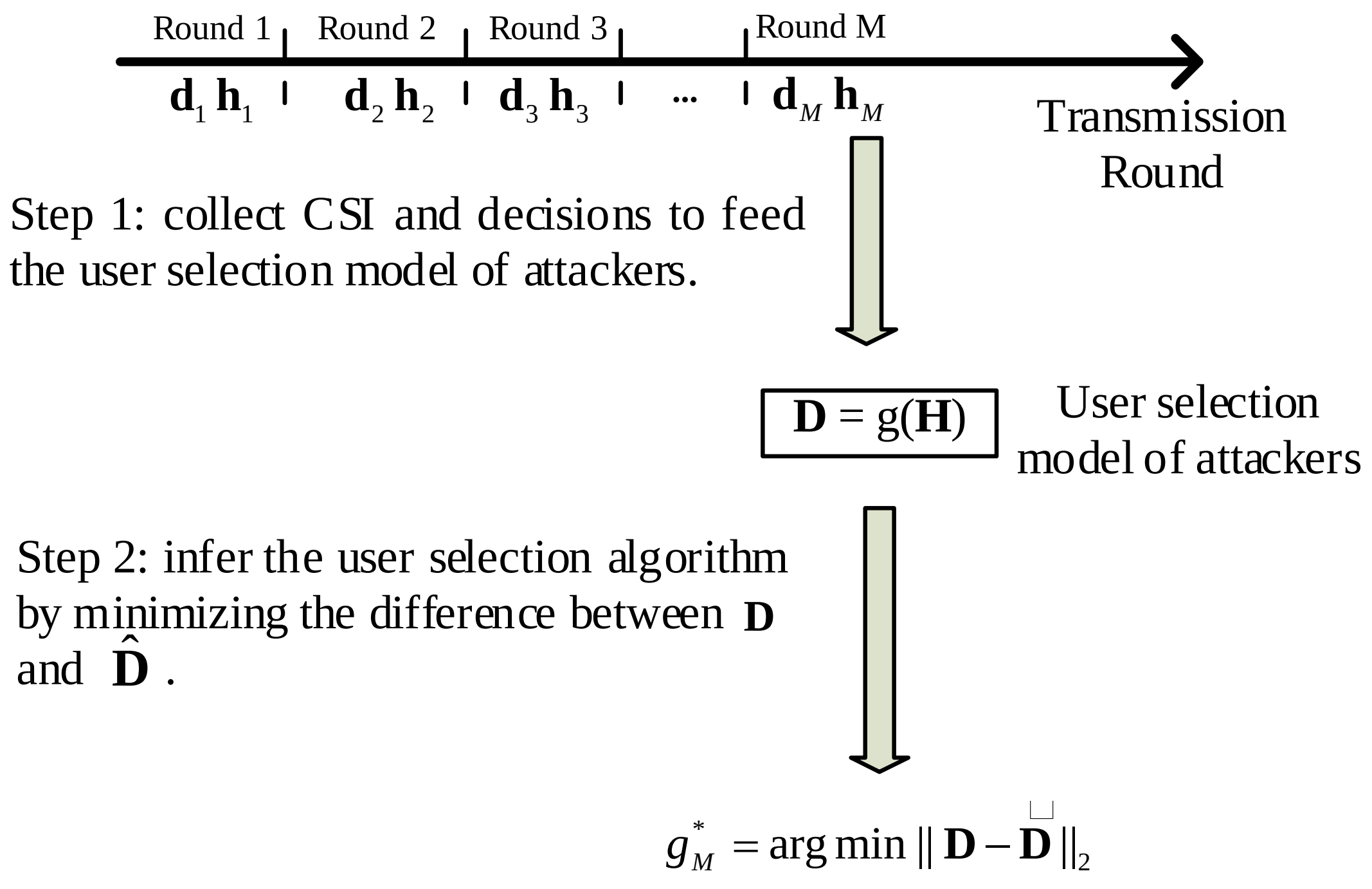
Then the user selection used by the AP can be expressed as

$$\mathbf{D}=f(\mathbf{H})$$

Both $\mathbf{H}$ and $\mathbf{D}$ are available by attackers. For attackers, let

$$\hat{\mathbf{D}}=g(\mathbf{H})$$

The objective of attackers is to infer g, which is as similar as f


Round 1
Round 2
Round 3
Round M
$\mathbf{d}_1\,\mathbf{h}_1$
$\mathbf{d}_2\,\mathbf{h}_2$
$\mathbf{d}_3\,\mathbf{h}_3$
…
$\mathbf{d}_M\,\mathbf{h}_M$
Transmission Round
$\mathbf{D}=\mathrm{g}(\mathbf{H})$
User selection model of attackers

Step 1: collect CSI and decisions to feed the user selection model of attackers.

Step 2: infer the user selection algorithm by minimizing the difference between $\mathbf{D}$ and $\hat{\mathbf{D}}$.

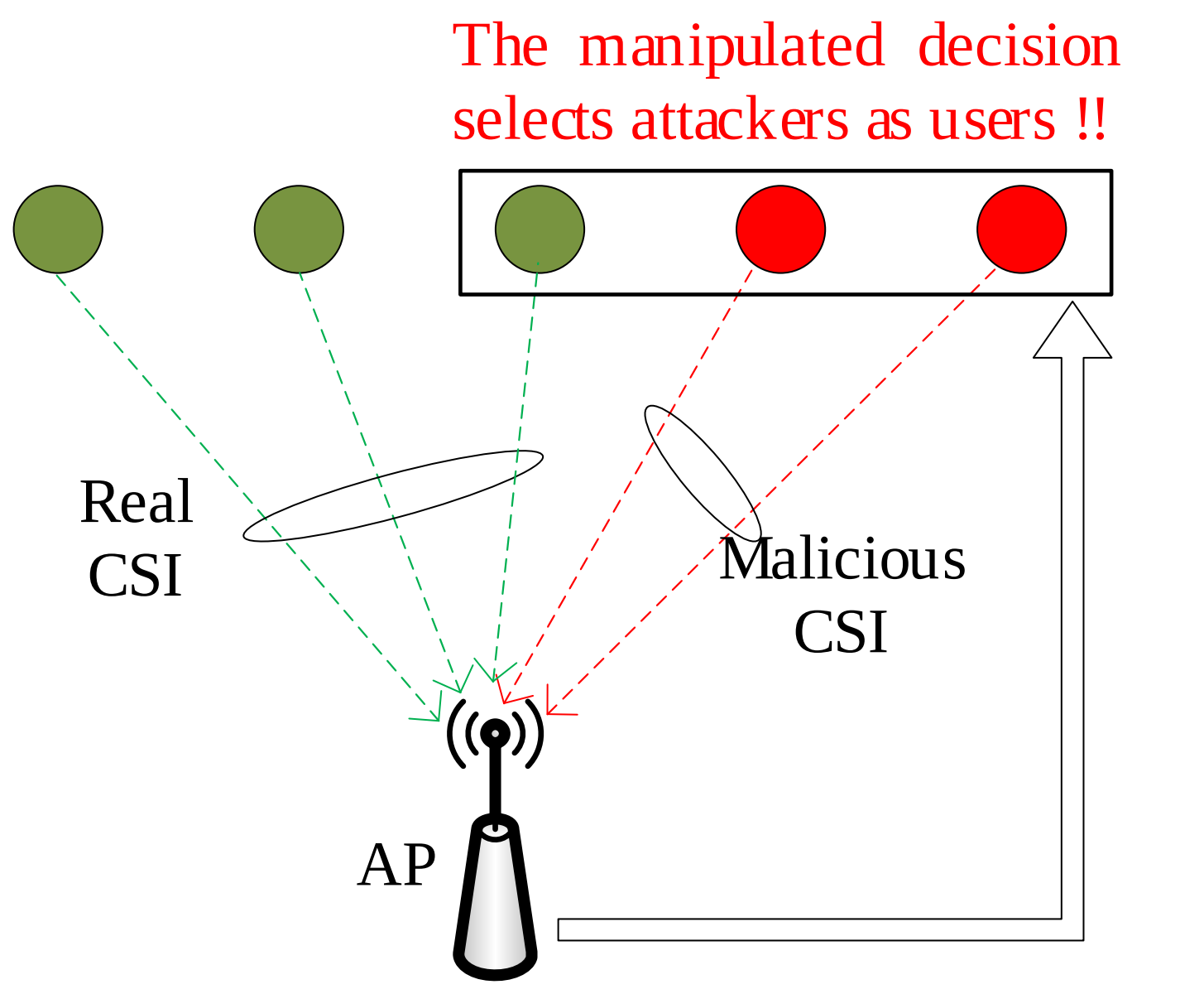
$$g_M^*=\arg\min\|\mathbf{D}-\hat{\mathbf{D}}\|_2$$

Attack Strategy

2. The damage step

In this step, attackers generate malicious CSI to mislead the AP to select inappropriate users.

Attackers obtain the inferred user selection algorithm through first M rounds, and launch the attack at the (M+1)$_{th}$ round.



Step 1: all users and attackers send real CSI and malicious CSI respectively to the AP.

Step 2: Based on collected CSI, AP feedbacks decisions to acknowledge which users are selected.

Mathematically, we split the channel state matrix into two parts,

$$\mathbf{H}=[\mathbf{H}_u,\mathbf{H}_m]$$

where $\mathbf{H}_u$ and $\mathbf{H}_m$ indicate channel state matrix of legitimate users and attackers respectively.

Then attackers can generate a malicious $\hat{\mathbf{H}}_m$, yielding a fake decision vector

$$\tilde{\mathbf{D}}=g([\mathbf{H}_u,\hat{\mathbf{H}}_m])$$

We propose three attack strategies to generate the malicious CSI to achieve different purposes.

1) Maximum Difference Attack

The most straightforward objective of attackers is to change the decision matrix $\mathbf{D}$ as much as possible. The real CSI is also available to attackers, so they can derive both $\mathbf{D}$ and $\tilde{\mathbf{D}}$. This strategy can be expressed as

$$\hat{\mathbf{H}}_m=\arg\max\|\tilde{\mathbf{D}}-\tilde{\mathbf{D}}\|_2 .$$

2) Target User Attack

Under this scenario, attackers have a specific set of users to attack, denoted as Λ. Then, the objective of this strategy is to attack users in Λ. Specifically, it generates a $\hat{\mathbf{H}}_m$, such that users in Λ cannot be selected.

$$\hat{\mathbf{H}}_m=\arg\max\|\tilde{\mathbf{D}}-\tilde{\mathbf{D}}\|_2 .$$

such that $d_{ij}=0$ for $j\in\Lambda$

3) Minimum Throughput Attack

Give the decision $\tilde{\mathbf{D}}$, the network throughput can be further derived. Therefore, attackers can also launch an attack to directly affect the network throughput. Denoted by $T_{\tilde{\mathbf{D}}}$ the throughput with the decision result $\tilde{\mathbf{D}}$.This strategy can be expressed as

$$\hat{\mathbf{H}}_m=\arg\min T_{\tilde{\mathbf{D}}}$$

Further Work

- In the future, we plan to expend the application scenario to other multiuser systems, such as MU-MIMO and so on.
- Instead of spectrum tomography, machine learning is another way to obtain the system model. In the future, we plan to leverage the machine learning model to obtain the user selection algorithm.

Conclusion and Acknowledgement

In this poster, we analyze the vulnerability of OFDMA systems under spectrum tomography, and present a powerful attack, called spectrum tomography attack, to damage the user selection mechanism in OFDMA systems. We introduce three attack strategies to implement the attack. Our attack strategy can be used in any wireless systems with resource allocation mechanisms that are similarly vulnerable to such inference-based tomography attacks. This work was supported in part by NSF CNS-1717969.

Reference

1. H.C. Nguyen, E.De Carvalho, and R. Prasad, “Multi-user interference cancellation schemes for carrier frequency offset compensation in uplink OFDMA”, *IEEE trans. Wireless Commun.*, vol. 13, 2014.
2. Y. Zeng and A. R. Leyman, “Pilot-based simplified ML and fast algorithm for frequency offset estimation in OFDMA uplink,” *IEEE Trans. Veh. Technol.*, vol. 57, 2008.
3. A. Krishnamurthy and A. singh, “Robust multi-source network tomography using selective probes,” in *Proc. Of IEEE INFOCOM*, 2012.
4. “IEEE P802.11 Wireless LANs”, *IEEE 802.11-15/0132r16*, 2016