# Spectrum Tomography Attacks: Inferring Spectrum Allocation Mechanisms in Multicarrier Systems

Shangqing Zhao, Zhe Qu, Zhuo Lu
University of South Florida, Tampa, FL 33620
Emails: {shangqing@mail., zhequ@mail., zhuolu@}usf.edu

Tao Wang
New Mexico State University, Las Cruces, NM 88003
Email: taow@nmsu.edu

***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.**

## I. Introduction

Orthogonal Frequency Division Multiple Access (OFDMA) has been selected as a promising multiple-access technique for next-generation wireless network standards (e.g., in 802.11ax [1]) to support high throughput and robustness in multipath fading environments [2], [3]. Different from the traditional OFDM, which allocates the whole channel to a single user [4], OFDMA assigns specific sets of subcarriers to a group of users for concurrent transmissions. Thus, in the dense wireless traffic environment, OFDMA can improve the average throughput significantly. However, restricted by the bandwidth, an access point (AP) can only simultaneously serve a limited number of users (e.g., up to 9 users for a 20MHz system [1]). Therefore, user selection is an essential process before taking advantage of the benefits of OFDMA.

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. According to 802.11 standards [1], [5], the user selection algorithm is not specified, and the PHY source code regarding this algorithm is also proprietary in most wireless vendors, rendering an obstacle to direct access to the algorithm. However, CSI is transmitted in plaintext [5], thus the broadcast nature of the wireless channel provides a possibility to obtain the algorithm indirectly. Specifically, we can first collect the CSI feedback from each user, as well as the final decision from the AP, and then build a statistic model to infer the algorithm. The basic idea behind this method is to infer the internal spectrum allocation mechanism from external measurements, which is very similar to the concept of tomography [6]; therefore, we call it spectrum tomography.

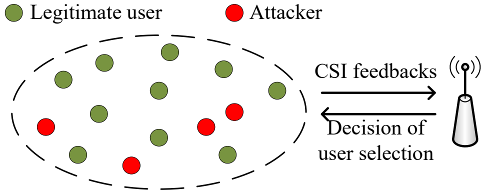

Fig. 1. System model consisting of 1 AP and multiple nodes, where green nodes indicate legitimate users and red nodes denote malicious users.

By nature, spectrum tomography exposes the vulnerability of revealing the user selection algorithm. Therefore, from attackers' perspective, equipping with spectrum tomography, powerful and effective attacks can be launched targeting the network, such as poisoning attacks [7], in which attackers can generate malicious CSI based on the inferred user selection algorithm to mislead the AP to select inappropriate users.

In this poster, by leveraging such vulnerability, we present a new attack strategy, called spectrum tomography attack, to damage OFDMA networks. Specifically, spectrum tomography attack consists of two steps: (i) the spectrum tomography step, in which attackers build a statistic model to infer the user selection algorithm by eavesdropping CSI from each user, and the final decision from the AP; (ii) the damage step, in which attackers mislead the AP by injecting malicious CSI, yielding a different decision of the user selection.

## II. Spectrum Tomography and Attack Strategies

In this section, we first present the spectrum tomography attack, and then we design this attack through three strategies with different objectives.

### A. System Model

Consider an up-link OFDMA system with one AP and $N$ users, where $N_u$ are legitimate users, and $N_m$ are attackers, satisfying $N_u + N_m = N$. In this system, AP serves as a central controller to decide which users can be selected. Assume there are $M$ transmission rounds. To support multi-user operations, at round $i$, the AP first initiates a channel sounding procedure. Then each user measures its CSI $\mathbf{h}_{ij}$ for $j = 1, \cdots, N$ and feedbacks it to the AP. The AP uses this information to decide which users are selected. Denote by $\mathbf{D} = \{d_{ij}\}_{M\times N}$ the decision matrix, whose entry $d_{ij} = 1$ if the $j$th user is selected at round $i$, and 0 otherwise. Let

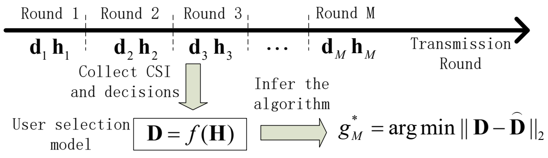
Round 1
Round 2
Round 3
Round M
$\mathbf{d}_1\, \mathbf{h}_1$
$\mathbf{d}_2\, \mathbf{h}_2$
$\mathbf{d}_3\, \mathbf{h}_3$
…
$\mathbf{d}_M\, \mathbf{h}_M$
Transmission Round
Collect CSI and decisions
Infer the algorithm
User selection model
$\mathbf{D} = f(\mathbf{H})$
$g^*_M = \arg\min \| \mathbf{D} - \widehat{\mathbf{D}} \|_2$

Fig. 2. Framework of the spectrum tomography step.

$S$ denote the maximum number of spatial streams which is determined by the bandwidth, then we have that $\|\mathbf{d}_i\| \leq S$, where $\|\mathbf{d}_i\| = [d_{i1}, \cdots, d_{iN}]$ denotes the $i$th row in $\mathbf{D}$, and $\| \cdot \|$ is the Ł$_1$-norm operator. Let $\mathbf{H} = \{\mathbf{h}_{ij}\}_{M \times N}$ be the channel response matrix, then we can define the user selection algorithm as a function $f$ with input $\mathbf{H}$ and output $\mathbf{D}$, i.e., $\mathbf{D} = f(\mathbf{H})$.

### B. Spectrum Tomography Attack

The spectrum tomography attack consists of two steps: (i) the spectrum tomography step and (ii) the damage step. In the following, we elaborate each of them in detail.

*1) Spectrum Tomography Step:* 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. Therefore, both $\mathbf{D}$ and $\mathbf{H}$ are available for attackers. Denoted by $g$ the user selection model used by attackers, and let $\hat{\mathbf{D}} = g(\mathbf{H})$, then, at the $M$th transmission round, we formulate this step as inferring the user selection function $g^*_M$ which minimizes the difference between $\mathbf{D}$ and $\hat{\mathbf{D}}$, i.e.,

$$\text{Objective} : g^*_M = \arg\min_g \|\mathbf{D} - \hat{\mathbf{D}}\|_2 \tag{1}$$

where $\| \cdot \|_2$ denotes the Ł2-norm operator. Fig. 2 shows the framework of this step.

By nature, the inference accuracy increases as the transmission round goes on. We define the inference accuracy $\eta$ as the ratio between the number of users which is correctly inferred by attackers and the total number of selected users. Therefore, given a transmission round $M$, we have

$$\eta(M) = 1 - \|\mathbf{D} - g^*_M(\mathbf{H})\|_2 / \|\mathbf{D}\|_2. \tag{2}$$

In fact, (2) is used to determine how many rounds is needed to reach to a certain accuracy.

*2) Damage Step:* The inferred model $g^*_M$, obtained in the first step, should be as accurate as possible. Therefore, given predefined accuracy threshold $\eta_{th}$, attackers will first obtain the minimum number of transmission rounds required to achieve such accuracy, i.e., obtain $M^* = \arg\min M$, such that $\eta(M) > \eta_{th}$. Then, attackers can launch attack on the $(M^*+1)$th round by generating malicious CSI to mislead the AP to make different decisions. Fig. 3 shows the framework of this step.

Without loss of generality, we assume the first $N_u$ users are legitimate, and remaining are attackers. The CSI matrix can be then divided into two parts $\mathbf{H} = \{\mathbf{H}_u^T, \mathbf{H}_m^T\}^T$. Attackers can inflict damage by transmitting malicious CSI $\hat{\mathbf{H}}_m$ to replace the original $\mathbf{H}_m$ in order to induce a misled decision $\hat{\mathbf{D}}$ at the AP. Attackers can derive different $\hat{\mathbf{H}}_m$, yielding different $\hat{\mathbf{D}}$ to achieve different purposes. In the following, we present three attack strategies.

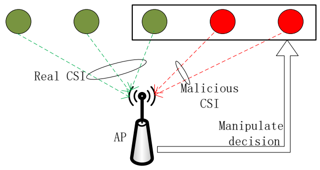

Fig. 3. Framework of the damage step.

- **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 $\hat{\mathbf{D}}$. This strategy can be expressed as $\hat{\mathbf{H}}_m = \arg\max \|\mathbf{D} - \hat{\mathbf{D}}\|_2$.
- **User Target Attack**: Under this scenario, attackers have a specific set of users to attack, denoted as $\mathcal{V}$. Then, the objective of this strategy is to attack users in $\mathcal{V}$. Specifically, it is to generate a $\hat{\mathbf{H}}_m$, such that $d_{M^*+1,j} = 0$ if $j \in \mathcal{V}$. This strategy is effective if users in $\mathcal{V}$ play important roles in the network.
- **Minimum Throughput Attack**: Give the decision $\mathbf{D}$, the network throughput can be further derived. Therefore, attackers can also launch an attack to directly affect the network throughput. Denoted by $T_{\mathbf{D}}$ the throughput with decision $\mathbf{D}$. This strategy can be expressed as $\hat{\mathbf{H}}_m = \arg\min T_{\hat{\mathbf{D}}}$.

## III. Conclusion

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.

## Acknowledgement

This work was supported in part by NSF CNS-1717969.

## References

[1] "IEEE P802. 11 Wireless LANs," *IEEE 802.11-15/0132rI6*, 2016.

[2] 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.

[3] 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.

[4] Y. Na and H. Minn, "Line search based iterative joint estimation of channels and frequency offsets for uplink OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 6, 2007.

[5] "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Std 802.11*, 2016.

[6] A. Krishnamurthy and A. Singh, "Robust multi-source network tomography using selective probes," in *Proc. of IEEE INFOCOM*, 2012.

[7] B. Biggio, B. Nelson, and P. Laskov, "Poisoning attacks against support vector machines," *arXiv preprint arXiv:1206.6389*, 2012.