Spectrum Tomography Attacks: Inferring Spectrum Allocation Mechanisms in Multicarrier Systems

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

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.

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).

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

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.

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 matrix as much as possible. The real CSI is also available to attackers, so they can derive both D and H. This strategy can be expressed as

\[ \hat{H} = \arg \max |||| \text{CSI matrix} \]

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.

Mathematically, we split the channel state matrix into two parts, \( H_i \) and \( \hat{H}_i \), where \( H_i \) and \( \hat{H}_i \) indicate channel state matrix of legitimate users and attackers respectively.

Then attackers can generate a malicious \( \hat{H}_i \), yielding a fake decision vector

\[ \hat{H} = g(H_i, \hat{H}_i) \]

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 \( D \) as much as possible. The real CSI is also available to attackers, so they can derive both \( D \) and \( H \). This strategy can be expressed as

\[ H_i \approx \arg \max |||| \text{CSI matrix} \]

2) Target User Attack

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

\[ H_i \approx \arg \max |||| \text{CSI matrix} \]

such that \( d_j = 0 \) for \( j \in \Lambda \)

3) Minimum Throughput Attack

Give the decision \( \hat{B} \), the network throughput can be further derived. Therefore, attackers can also launch an attack to directly affect the network throughput. Denoted by \( T_{\text{th}} \), the throughput with the decision result \( \hat{B} \). This strategy can be expressed as

\[ H_i \approx \arg \min T_{\text{th}} \]

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 find the system model. In the future, we plan to leverage the machine learning model to obtain the user selection algorithm.

Conclusion and Acknowledge

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

4. IEEE 802.11 Wireless LANs, IEEE 802.11-15/0132r1, 2016.