Demo: Channel Estimation and Custom Beamforming on the 60 GHz TP-Link Talon AD7200 Router

Joan Palacios*
IMDEA Networks Institute
Madrid, Spain
joan.palacios@imdea.org

Daniel Steinmetzer*
Secure Mobile Networking Lab
TU Darmstadt, Germany
dsteinmetzer@seemoo.de

Adrian Loch
IMDEA Networks Institute
Madrid, Spain
adrian.loch@imdea.org

Matthias Hollick
Secure Mobile Networking Lab
TU Darmstadt, Germany
mhollick@seemoo.de

Joerg Widmer
IMDEA Networks Institute
Madrid, Spain
joerg.widmer@imdea.org

ABSTRACT

Current IEEE 802.11ad millimeter-wave consumer devices use phased antenna arrays with a fixed set of pre-defined beam patterns. Such an approach has the advantage of being very low complexity and easy to implement. However, custom beam patterns adapted to the current channel can provide much better performance than generic pre-defined patterns. In this demo, we show how to measure channel state information and modify beam patterns on the TP-Link Talon AD7200 router operating in the 60 GHz band. This allows to generate custom beam patterns with arbitrary shape, as well as beam patterns that maximize the signal strength of a link given the current channel. Our demo allows users to select custom beam patterns and visualizes the beam pattern in use. It is also possible to compare the custom patterns to the pre-defined beam patterns of the router and measure the performance in terms of throughput and signal strength.

1 ADAPTIVE CODEBOOK OPTIMIZATION

The high bandwidth available in millimeter-wave bands allows for very high rate wireless communications, such as for example IEEE 802.11ad. However, building hardware components for such frequencies is technically challenging and beamforming is required to overcome the high path loss of this technology. To this end, current Commercial Off-The-Shelf (COTS) devices use phased antenna arrays with a fixed set of pre-defined beam patterns. The IEEE 802.11ad standard includes a beam-training step to determine a suitable directional beampattern for the communication.

Beam training, also called Sector Level Sweep (SLS), works as follows. The Access Point (AP) transmits beacon messages using each of its available beam patterns sequentially, while the station (STA) listens with a quasi-omnidirectional beam pattern. The STA then repeats the same process and includes in each of its messages the identifier of the beam pattern that it received best from the AP. Finally, the AP replies with the identifier of the best beam pattern of the STA in a dedicated control message. This mechanism is simple and robust, but it clearly does not exploit the full potential of the devices' antenna arrays since it ignores the specific current channel. In contrast, adapting to the channel requires Channel State Information (CSI) at the transmitter, which is challenging to obtain in current systems since sequential transmissions are not phase coherent and – with only a single RF chain – they do not allow for parallel measurements.

In this paper, we demonstrate an Adaptive Codebook Optimization (ACO) mechanism presented in our prior work [1] that enables CSI extraction on consumer-grade COTS IEEE 802.11ad devices using only non-coherent signal-to-noise ratio (SNR) measurements. Our ACO mechanism allows to extract both amplitude and phase information by using custom designed beam patterns such that their measured SNR relates to the relative phase shift among antenna elements and their amplitude. Using the computed CSI, ACO derives beam patterns that maximize the SNR, exploit reflections, and prevent destructive interference.

We implement ACO on commodity COTS hardware. To this end, we gain full access to the beamforming control of the TP-Link Talon AD7200 60 GHz router that features an IEEE 802.11ad Wi-Fi chipset. We disassemble the phased antenna array of the device to understand its structure and

*These authors contributed equally to this work.

WiNTECH '18, November 2, 2018, New Delhi, India

ACM ISBN 978-1-4503-5930-6/18/11.
https://doi.org/10.1145/3267204.3268070

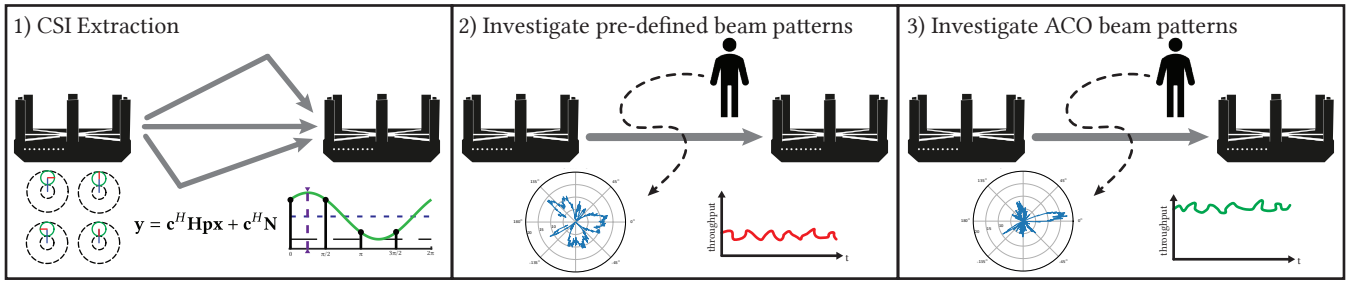

Figure 1: Illustration of the contribution of our demonstrator.

experimentally reconstruct the antenna weighting network. By means of reverse engineering and firmware modification, we obtain control over the antenna array to adjust antenna steering parameters and create custom beam patterns, without requiring any hardware modifications. We embed ACO in the regular operation of the router, that is, *we do not obtain our results in post-processing* but as part of the normal data transmissions in our testbed. This enables us to quantify the performance improvements of ACO in terms of SNR, data rate, and throughput using the Transmission Control Protocol (TCP).

2 DEMONSTRATOR

2.1 Experiment Platform

To obtain access to the antenna steering parameters, as well as the IEEE 802.11ad beam training operation, we utilize our framework described in [2, 3]. Steering a phased antenna array is achieved by driving an antenna weighting network with amplifiers and phase shifters for each of the antenna elements. A specific configuration of this weighting network is referred to as a so-called sector, of which multiple are stored in an antenna steering codebook. The standard IEEE 802.11ad beam training (the SLS) is implemented in the firmware of the chipset. It sweeps through a set of sectors from a pre-configured codebook. Through firmware patching, we extract the SNR and RSSI of received frames during this training process.

Since no documentation for the antenna module is available, we had to analyze the internal structure of the antenna elements experimentally. By modifying individual parameters, we reconstructed the structure of the antenna weighting network. In particular, we revealed which configuration bits belong to which component in the weighting network by changing single values and monitoring the signal strength at an unmodified device. Disassembling the antenna and shielding all except one antenna element, we reconstructed the the physical element positions. This know-how and the capability to control the weighting network allows us to optimize the beam patterns in the codebook.

2.2 Demo Description

Our demo presents the dynamic generation of specific beam patterns using commodity phased antenna arrays on the TP-Link Talon AD7200 tri-band router as described in [1]. In particular, we 1) demonstrate the CSI extraction using non-coherent SNR measurements with phase-shifted probing patterns, 2) visualize and benchmark the pre-defined beam pattern on the devices, and 3) allow the generate and compare the CSI-based directional beams. Figure 1 illustrates the setup of our demo. During our presentation, we allow users to interact with the channel, e.g., by (partially) blocking the link with their hand or body or moving devices. We allow users to customize the beam patterns, changing the beam direction and active antenna elements, and visualize the selected pattern in real-time. By showing the best default pattern and our optimized patterns based on the current CSI next to each other, users can compare the difference in shape and directionality. Moreover, we demonstrate the throughput and the SNR that are achieved with the default and the optimized beam patterns.

2.3 Demo Requirements

The demo requires at least one table, but ideal would be two tables with space in between, so that the 802.11ad link can be interrupted by users walking through it, as well as a monitor to better visualize the beampatterns.

REFERENCES

[1] Joan Palacios, Daniel Steinmetzer, Adrian Loch, Matthias Hollick, and Joerg Widmer. 2018. Adaptive Codebook Optimization for Beam Training on Off-The-Shelf IEEE 802.11ad Devices. In *24th ACM Annual International Conference on Mobile Computing and Networking (MobiCom '18)*. ACM, New Delhi, India.

[2] Daniel Steinmetzer, Daniel Wegemer, and Matthias Hollick. 2017. Talon Tools: The Framework for Practical IEEE 802.11ad Research. (2017). https://seemoo.de/talon-tools/

[3] Daniel Steinmetzer, Daniel Wegemer, Matthias Schulz, Joerg Widmer, and Matthias Hollick. 2017. Compressive Millimeter-Wave Sector Selection in Off-the-Shelf IEEE 802.11ad Devices. In *International Conference on emerging Networking EXperiments and Technologies (CoNEXT '17)*. ACM, Incheon, Republic of Korea, 414–425.