

A Practical IEEE 802.11ad Research Platform: The Hidden Potential of Off-the-Shelf Devices



TECHNISCHE
UNIVERSITÄT
DARMSTADT



Daniel Steinmetzer, Daniel Wegemer, and Matthias Hollick

TP-Link Talon AD7200

Commodity tri-band router

- Supports IEEE 802.11 abgn+ad
- QCA 9500 60 GHz WiFi module
- Phased antenna array with 32 elements



Our Research Framework

Open System Access



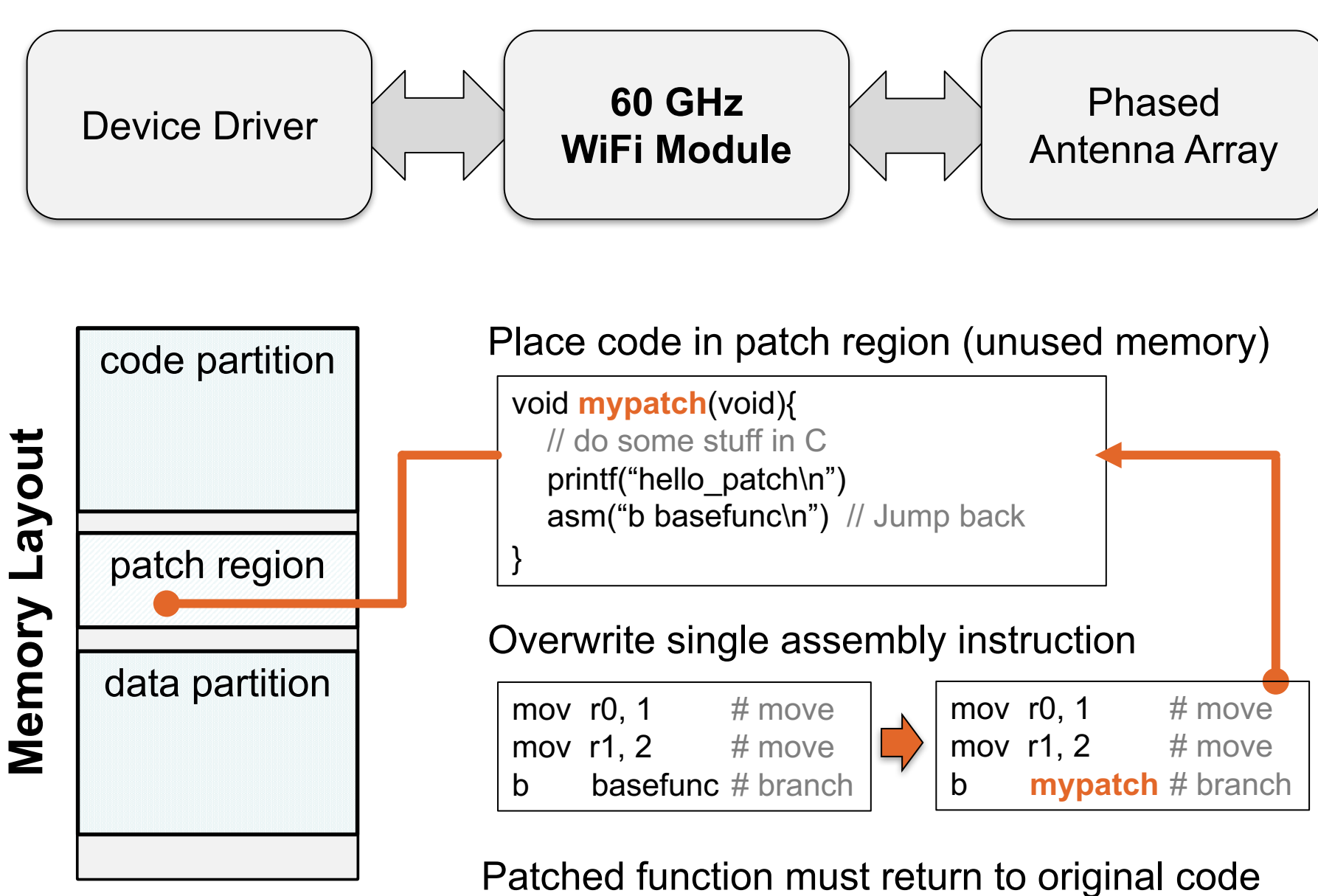
- Linux Embedded Development Environment (LEDE)
- Latest IEEE 802.11ad device drivers (wil6210)
- Highly customizable

nexmon
binary firmware patching

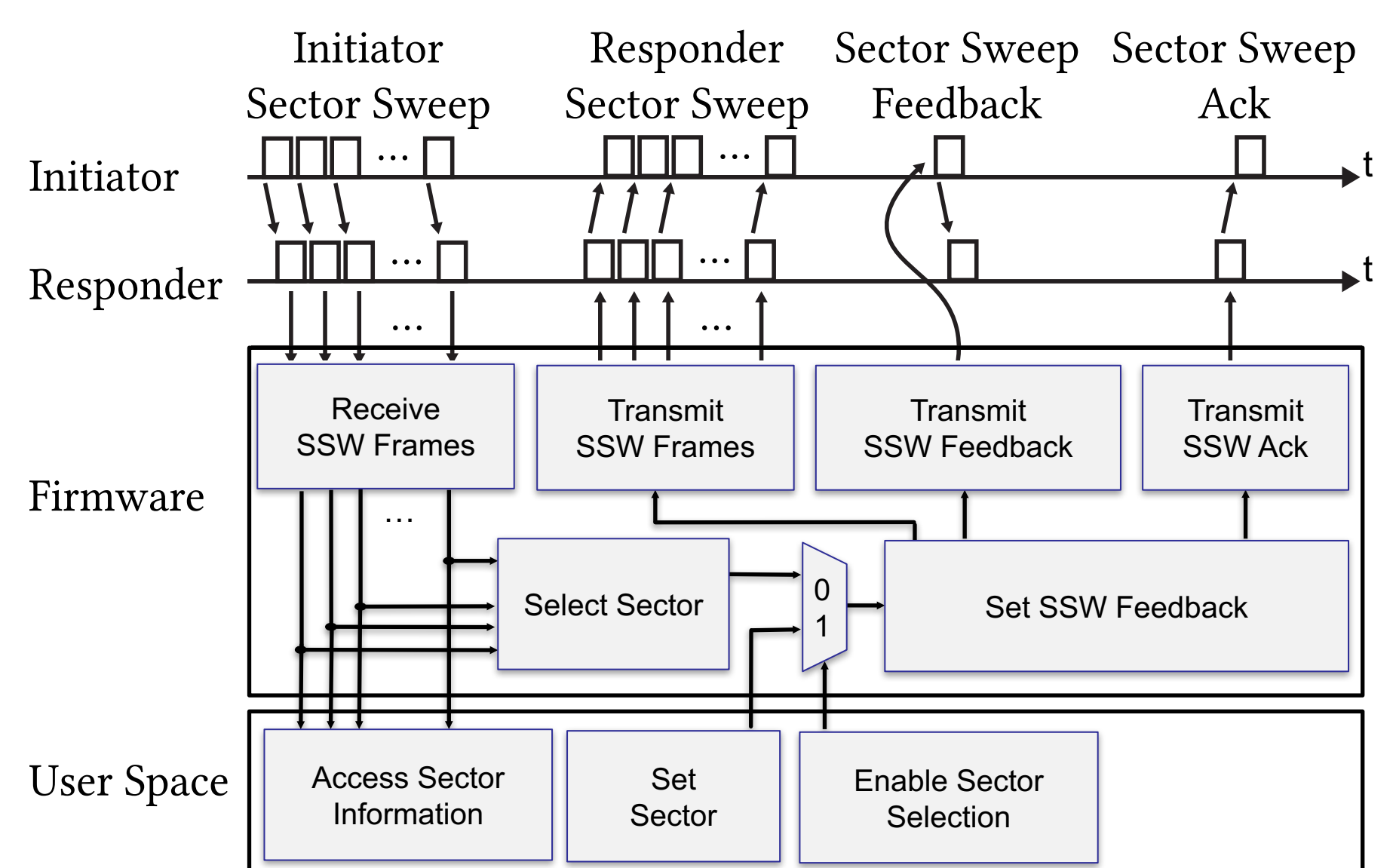
Firmware Patches

- Custom modifications to binary firmware images
- Developing patches in C by new attributes to the GCC compiler
- Adding new features to the 802.11ad chip's firmware

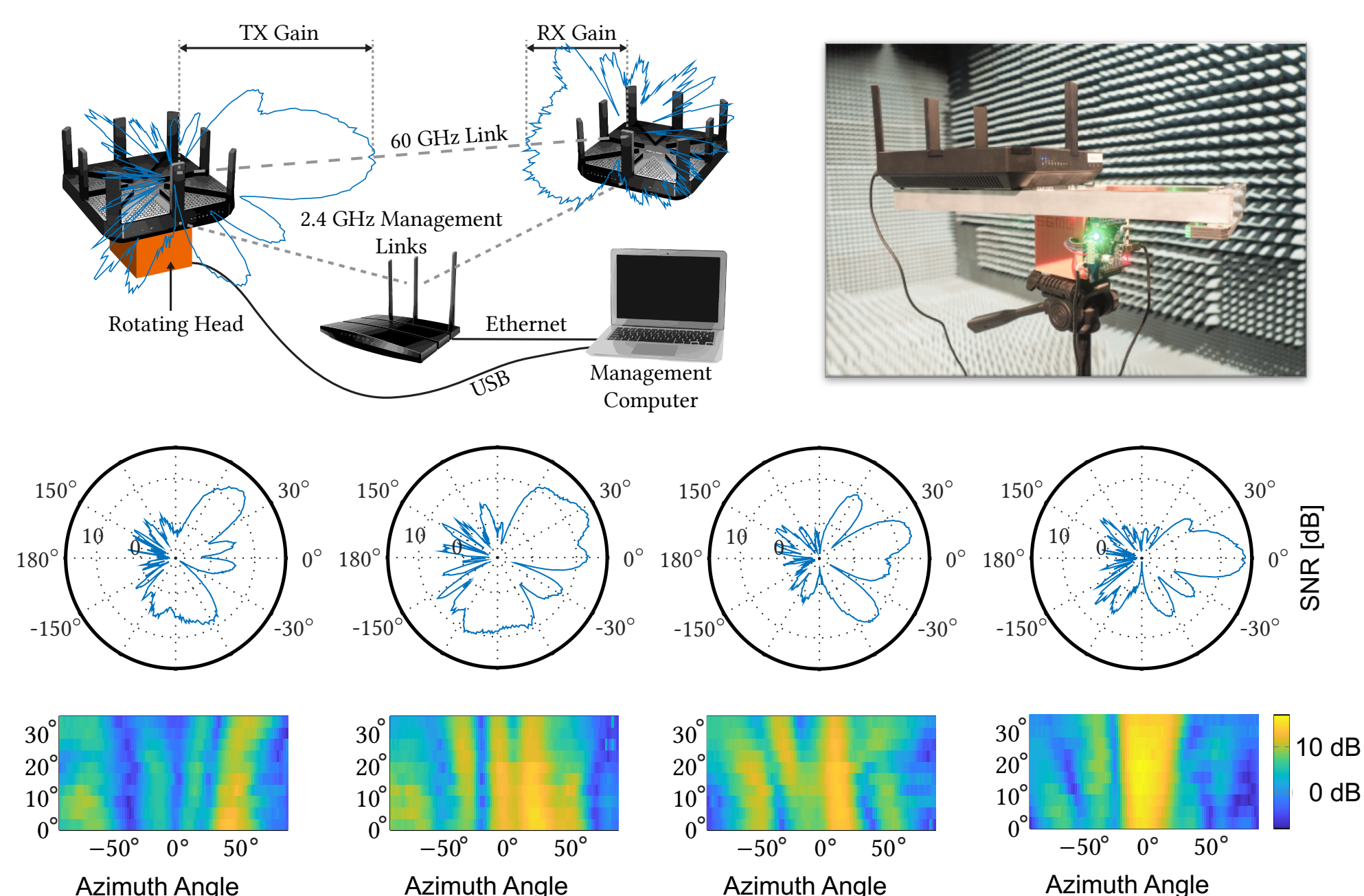
Binary Firmware Patching



Extended Sector Sweep



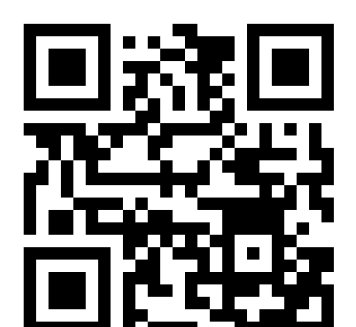
Pattern Measurements



References

Availability

Our framework, including a LEDE image, the nexmon sources, and pattern measurements, is available for download [1].



GitHub

Our Papers

- [1] D. Steinmetzer, D. Wegemer, and M. Hollick. Talon Tools: The Framework for Practical IEEE 802.11ad Research. Accessible at <https://seemoo.de/talon-tools/>. 2017.
- [2] D. Steinmetzer, D. Wegemer, M. Schulz, J. Widmer, M. Hollick. Compressive Millimeter-Wave Sector Selection in Off-the-Shelf IEEE 802.11ad Devices. 13th International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2017), December 2017, Seoul/Incheon, South Korea.
- [3] D. Steinmetzer, A. Loch, A. García-García, J. Widmer, M. Hollick. Mitigating Lateral Interference: Adaptive Beam Switching for Robust Millimeter-Wave Networks. 1st ACM Workshop on Millimeter Wave Networks and Sensing Systems (mmNets 2017), October 2017, Snowbird, Utah, USA.
- [4] G. Bielsa, J. Palacios, A. Loch, D. Steinmetzer, P. Casari, and J. Widmer. Indoor Localization Using Commercial Off-The-Shelf 60 GHz Access Points. IEEE International Conference on Computer Communications. April 2018, Honolulu, Hawaii, USA.