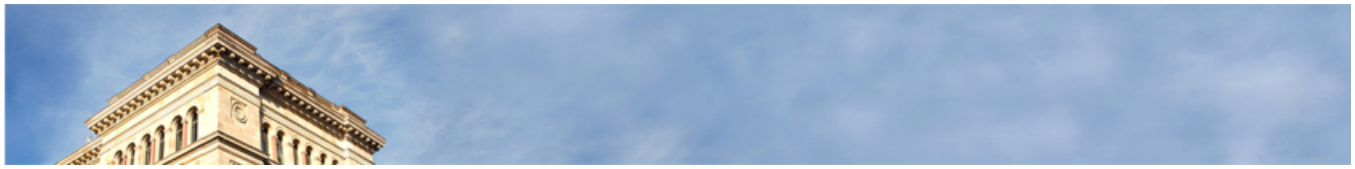
Technische Universität Berlin

On Phase Offsets of 802.11ac Commodity WiFi

Anatolij Zubow, Piotr Gawłowicz, Falko Dressler

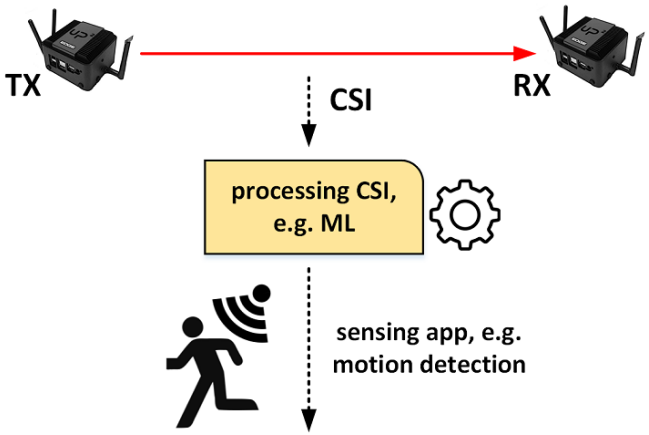
Talk@IEEE/IFIP WONS 2021

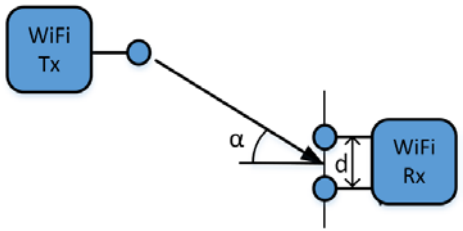


Technische Universität Berlin

Motivation

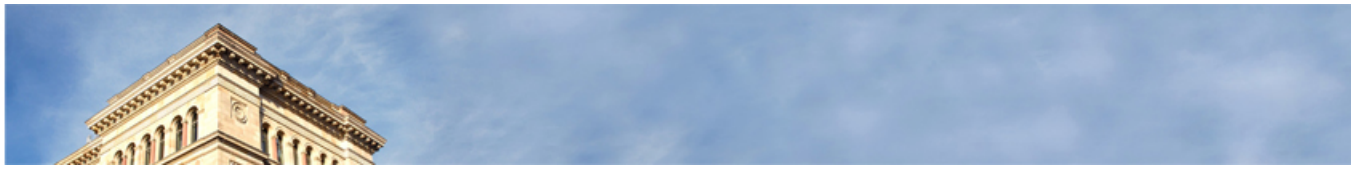
- Boom of **wireless sensing applications**
  - User localization and tracking, line-of-sight path identification, passive human sensing, motion recognition and wellness monitoring
- Indoor localization system (ILS) should be accurate, deployable and universal (using existing WiFi infrastructure)
- Angle of arrival (AoA) estimation schemes utilize **channel state information** (CSI) captured by MIMO commodity WiFi devices





AoA estimation

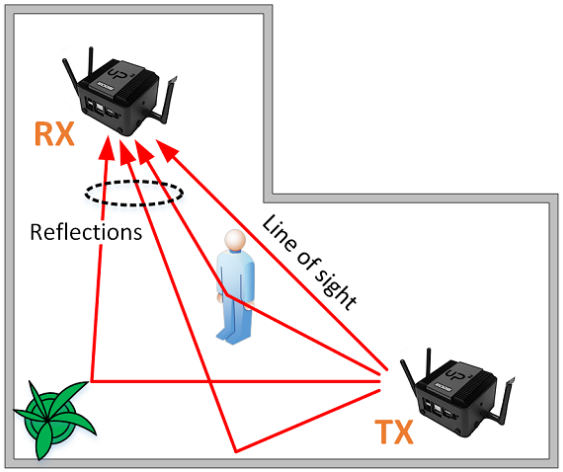
TKN



Technische Universität Berlin

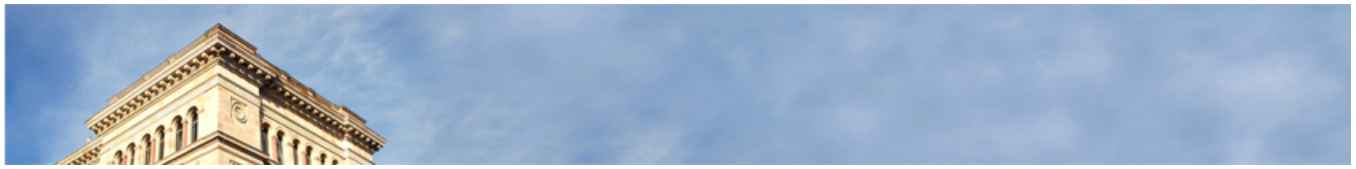
Channel State Information

- Channel State Information (CSI)
  - RF signal generated by TX propagates through multiple paths (direct propagation, reflection & scattering), and superimposes at RX, carrying information of **characteristics of environment**
- But CSI from COTS WiFi chip captures not only frequency response of wireless channel, but contains several kinds of **phase distortion** introduced by imperfect inertial circuits:
  - Carrier frequency offset, packet detection delay & sampling frequency offset => no problem for AoA (same among different RF chains)
  - But phase locked loop (PLL) initial phase is different among RF chains



Characteristics of RF propagation captured by CSI

TKN



Problem Statement & Contributions

- **Problem:**
  - Phase offset between RF chains (aka different antennas) in COTS WiFi chips
  - Measured CSI is distorted by phase offsets between RF chains

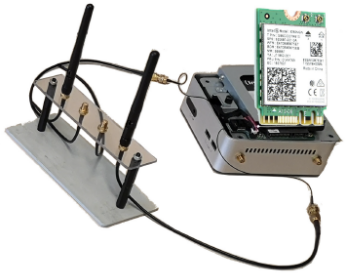
COTS 802.11ac chip (Intel 9260)

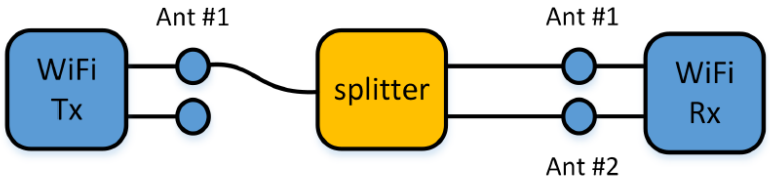
- **Contributions:**
  1. Analysis of difference of initial phase offsets on different RF chains of 802.11ac chips (Intel 9260) on a per-OFDM subcarrier level
  2. Algorithm for on the fly correction of RX antenna phase offset without calibration
  3. Proof-of-concept: AoA w/ MUSIC algorithm in 2.4 GHz band

Platform & Experiment Setup

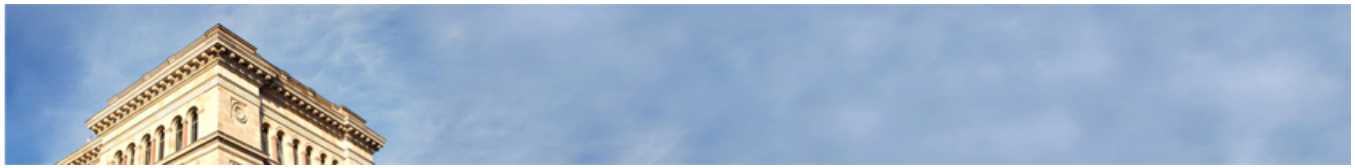
- Intel 9260 is 802.11ac wave 2 compliant radio w/ 2x2 MIMO
- We added CSI capturing functionality to the chip
- CSI capturing process:
  - TX & RX used in monitor/injection mode
  - For each received packet => CSI estimated by WiFi driver & passed to user space using Netlink API
  - Netlink messages received and processed using Python/Matlab for post-processing

- Two setups:
  - Over-the-cable
  - Over-the-air





Over-the-cable setup.



Technische Universität Berlin

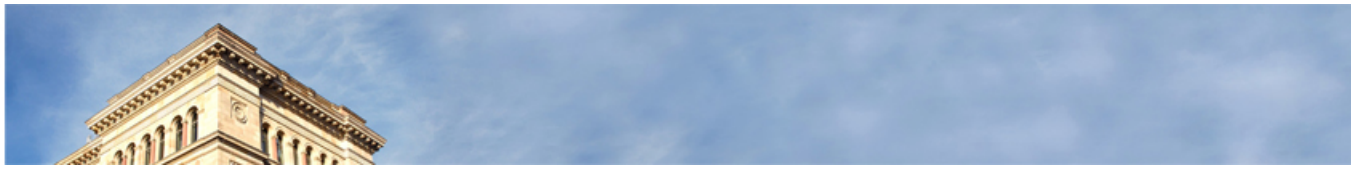
RX PHASE OFFSET CHARACTERISTICS

- **Objective**: understand the phase offset between receive chains (antennas) of IEEE 802.11ac

- Methodology:
  - Over-the-cable transmission (to avoid influence caused by environment & its changes)
  - Swapping external cables at splitter and average measurement results to eliminate constant phase offsets introduced by cables and splitters
  - 10k packets w/ HT20 & MCS0 transmitted on each channel

- Spectrum measured (580 MHz in total):
  - 2.4 GHz band: channels 1-13,
  - 5 GHz band: channels 36-64 and 100-165

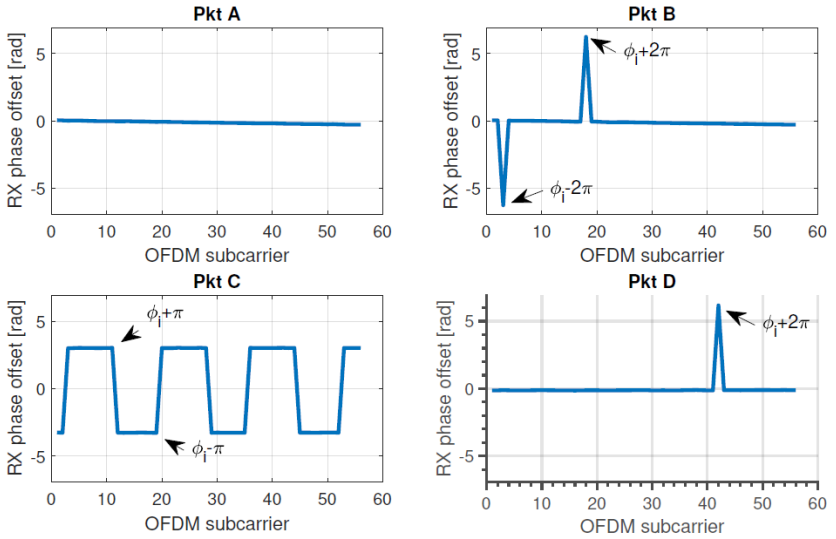
TKN



Technische Universität Berlin

RX PHASE OFFSET CHARACTERISTICS (II)

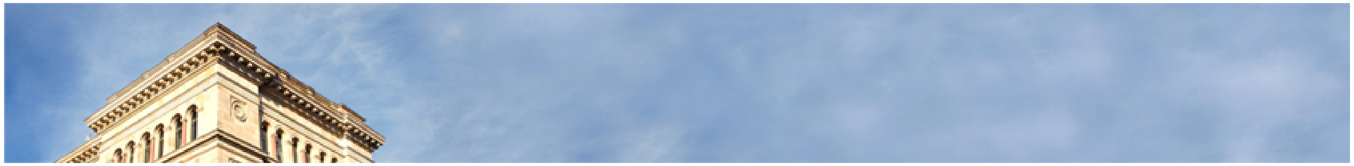
- **Results**:
  - Measured RX phase offset is random but semi-deterministic
  - The value of the true phase offset may rotate by multiple of π
  - Rotation strictly depends on whether the true φ is positive or negative:



RX phase offset measured from four different packets.

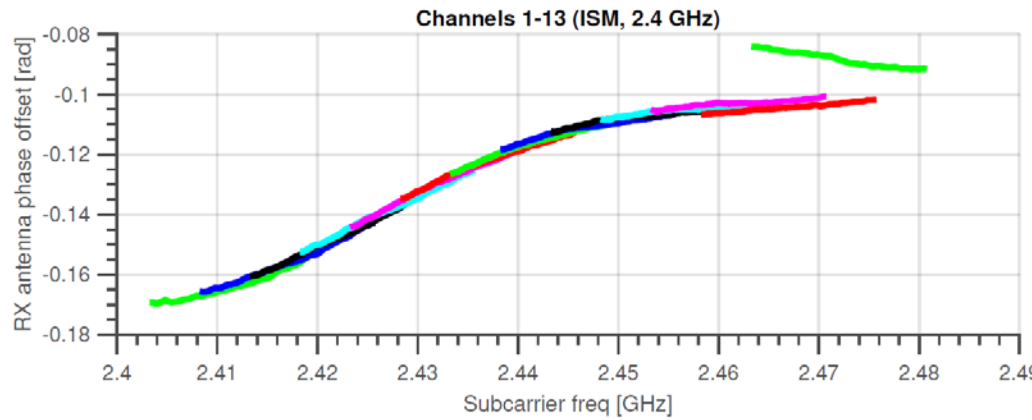
$$\hat{\phi} = \begin{cases} \phi + n\pi, n \in \{-2, -1, 0, 1\}, & \text{if } \phi \geqslant 0 \\ \phi + n\pi, n \in \{-1, -1, 0, 1, 2\}, & \text{otherwise.} \end{cases}$$

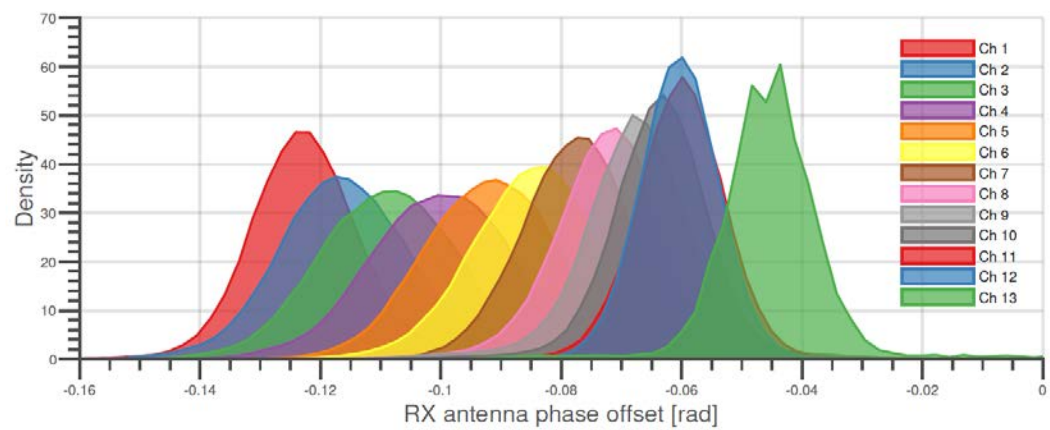
TKN



RX PHASE OFFSET CHARACTERISTICS (III)

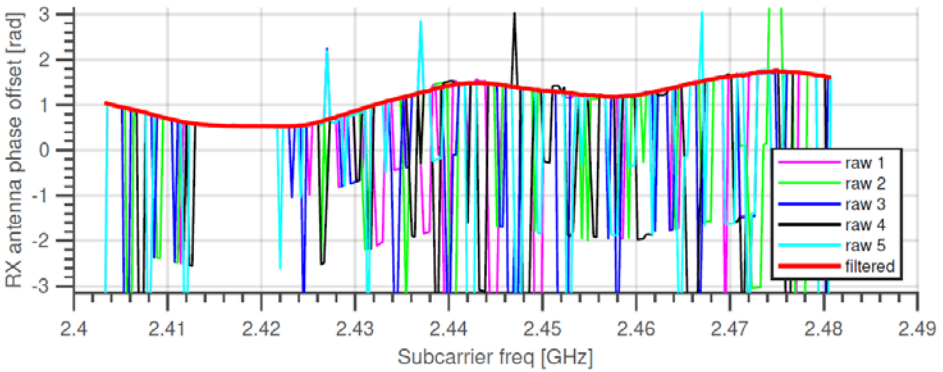
- After removing the random phase rotation & elimination of phase offsets introduced by cables & splitters
- RX phase offset is close to zero & slightly frequency-dependent
- Very narrow distribution, i.e. Standard deviation of just 0.05°
- Similar results for 5 GHz – see paper





RX PHASE OFFSET CORRECTION

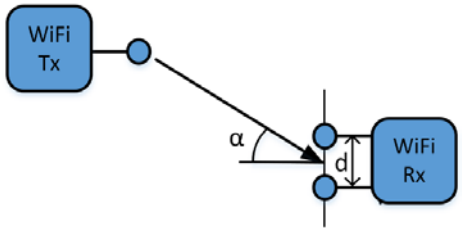
- **Key observations**:
  - φ* is semi-time invariant with 4 possible values and hence semi-deterministic
  - Some subcarrier can be randomly rotated at some point in time, but the measured phase offset is correct for the majority of time
- **Approach**:
  - Measure φ* from sufficient large number of packets => effect of random phase rotation can be averaged out
  - Measure a subcarrier multiple times on same and/or overlapping channels & combine results using detection and replacement of outliers

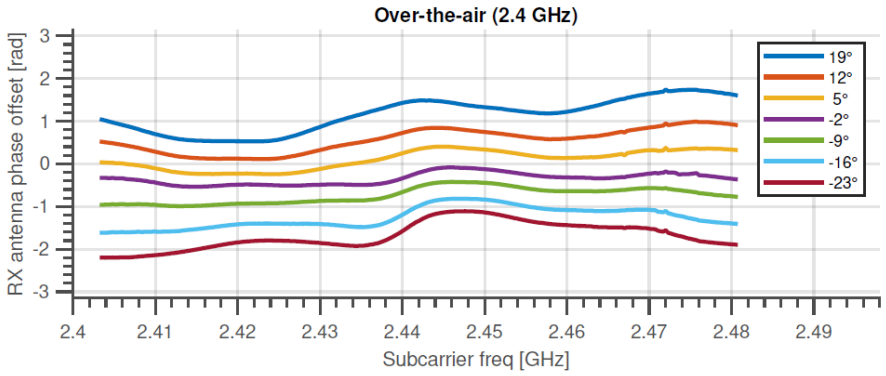


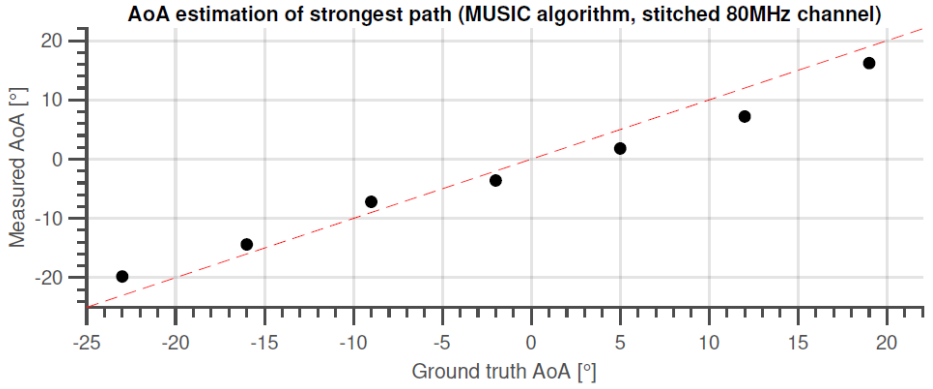
no calibration required & on-the-fly

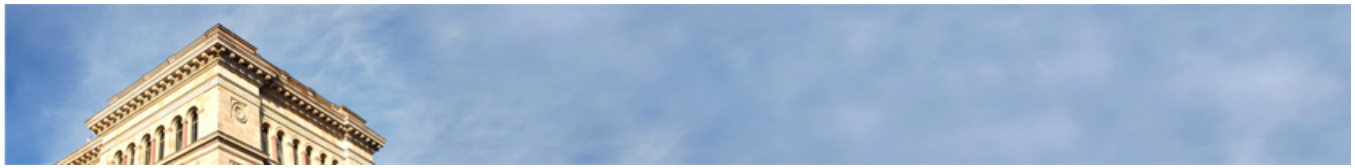
CASE STUDY - AOA

- **Setup:**
  - Over-the-air experiments to estimate the AoA of TX
  - 7 different TX locations analyzed
  - In each location: sending 20 packets on each of 13 channels in 2.4 GHz (12 channel switches)
  - Post-processing in Matlab to create a single 80 MHz channel by stitching together all channels, RX phase offset correction
- **Results:**









Technische Universität Berlin

Conclusions

- We analyzed phase offset φ* between RX antennas of modern 802.11ac NICs using Intel 9260 chips
- Results show that φ* is due to random phase rotations semi-time-invariant with up to 4 possible values
- φ* it is frequency dependent, i.e. depends on subcarrier and channel
- We proposed algorithm for cleansing CSI to derive the true φ
- As proof-of-concept angle of arrival was implemented & tested
- Future work: making the toolbox open source

TKN