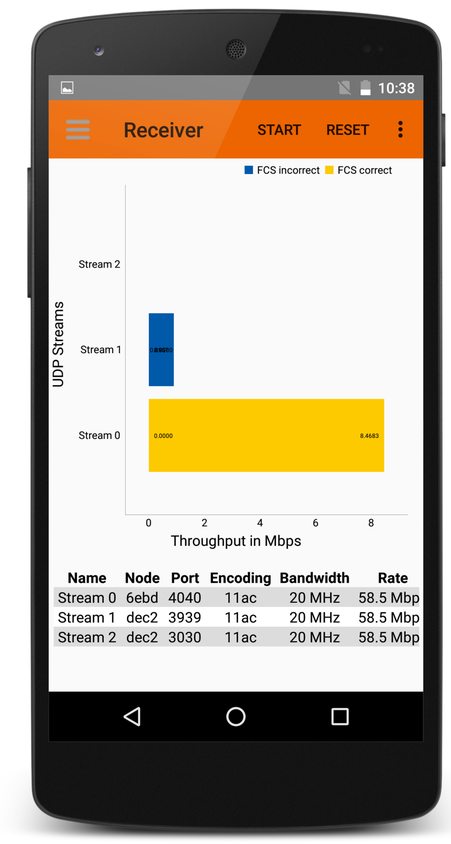
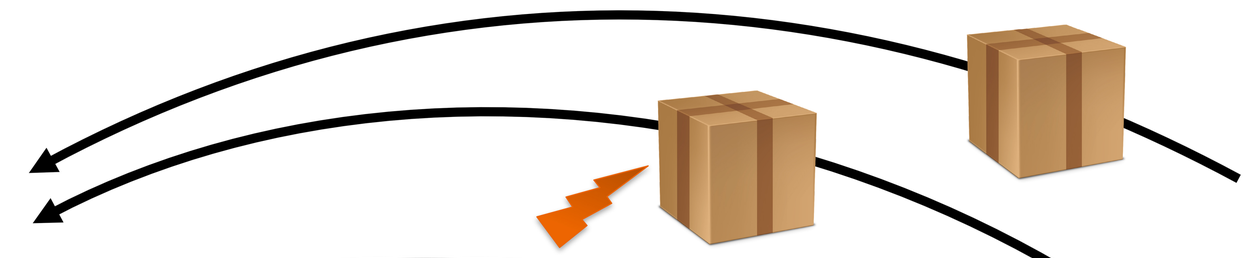
DEMO: Demonstrating Reactive Smartphone-Based Jamming

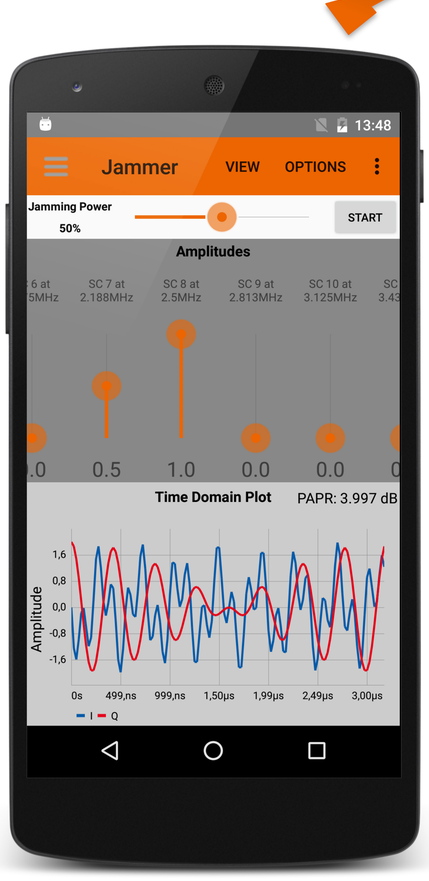
nexmon JAMMER DEMO

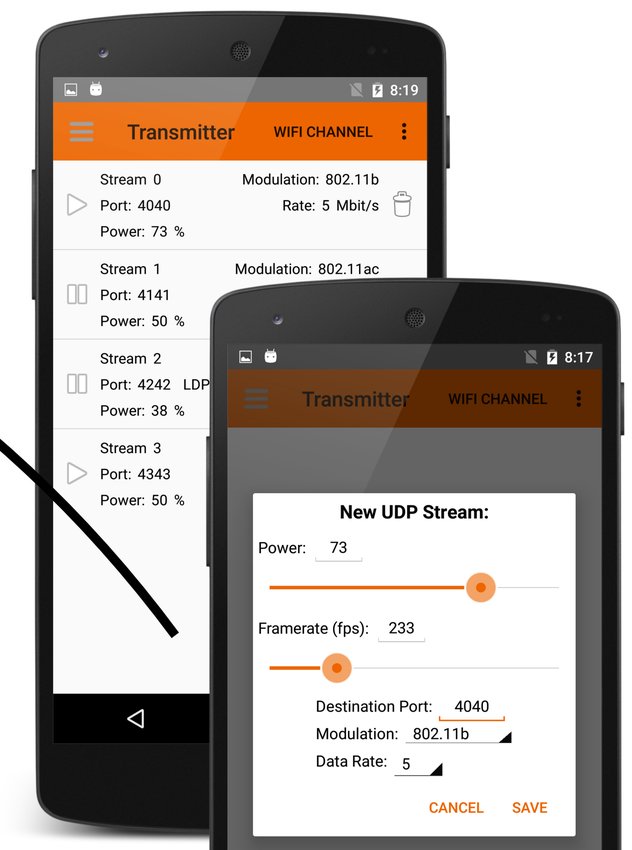
Matthias Schulz, Efstathios Deligeorgopoulos, Matthias Hollick and Francesco Gringoli

Reactive Jamming Setup









Receiver:

- Illustrates the throughput of received UDP streams in bar graphs
- Runs in monitor mode with activated reception of frames with wrong frame check sequence (FCS) to identify jammed frames

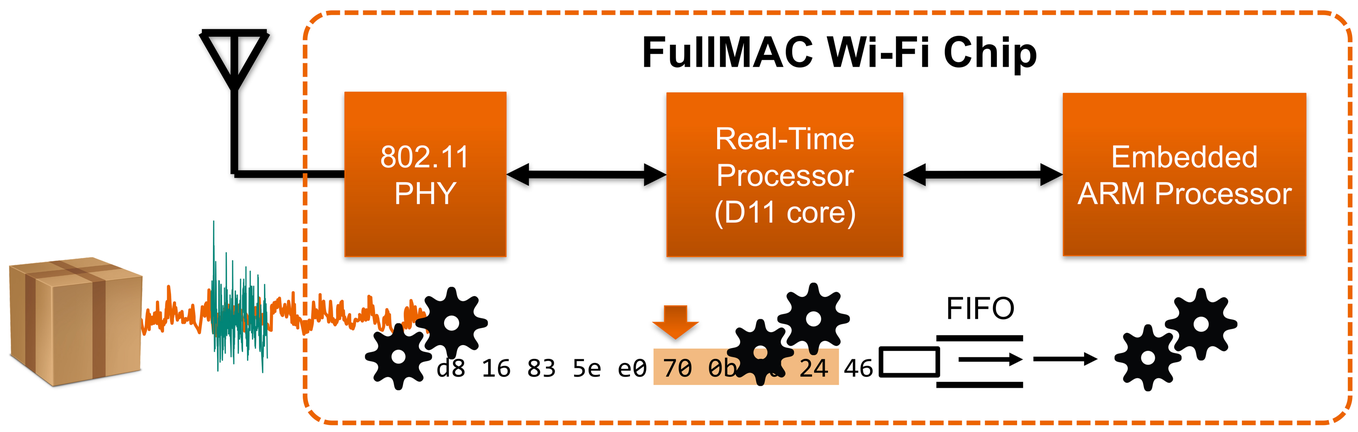
Jammer:

- Listens for incoming frames and starts the transmission of a configurable jamming signal triggered by a matching UDP port
- Only frames with the MAC addresses “NEXMON” and “JAMMER” are considered as targets to avoid abuse

Transmitters:

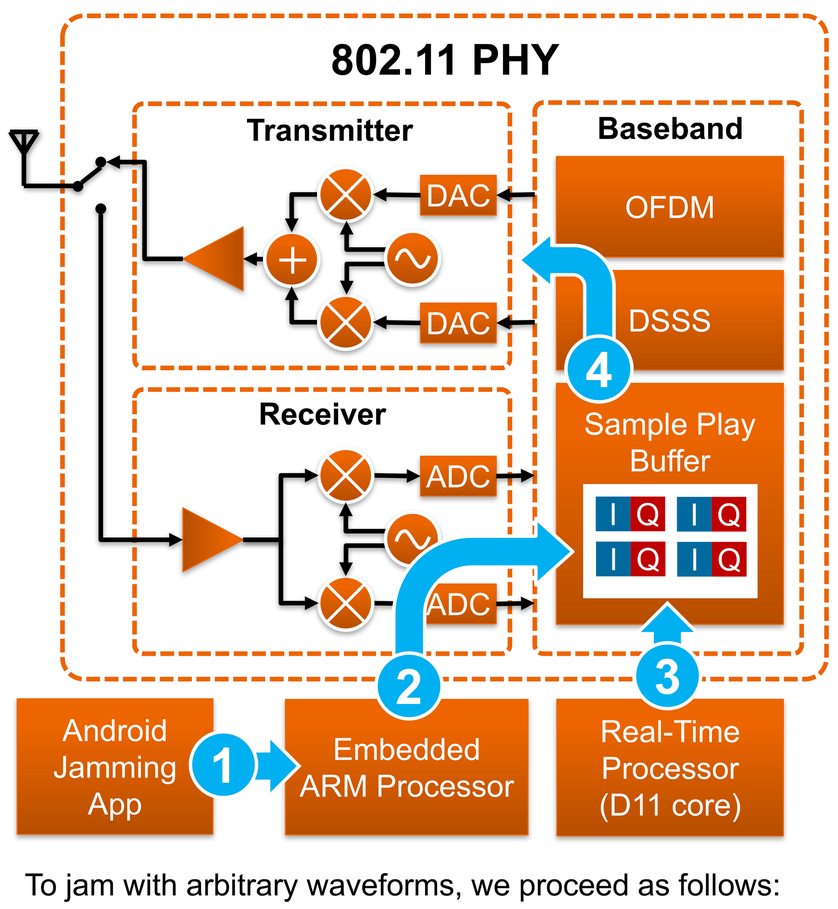
- Generate UDP streams at fixed frame rates
- Allow to configure ports, and modulation settings

Implementation of our Jammer



The 802.11 physical layer (PHY) receives and demodulates **Wi-Fi signals** into a byte stream that the Real-Time Processor analyses on-the-fly before storing the frame in a FIFO for further processing. For jamming, we need to inspect the frame content during reception and, hence, implement our reactive jammer in the firmware of the Real-Time Processor. It checks for MAC addresses and UDP ports and conditionally triggers the transmission of a **jamming signal**.

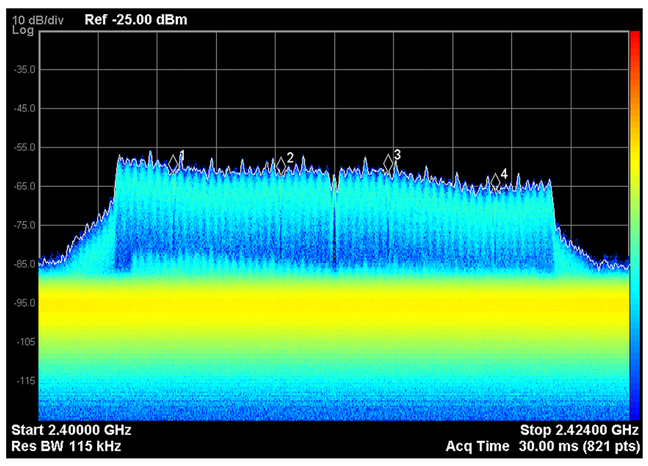
Arbitrary Waveform Transmission



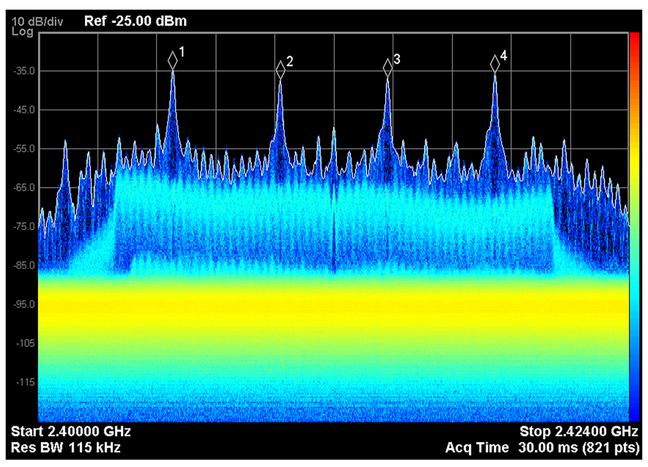
To jam with arbitrary waveforms, we proceed as follows:

1. We define amplitude and phase values for each subcarrier and load them into the Wi-Fi chip.
2. We calculate the inverse discrete Fourier transform on the subcarrier values and generate IQ samples that we store in the Sample Play Buffer.
3. To jam, we trigger the playback of the Sample Play Buffer from the Real-Time Processor.
4. During playback, samples are passed on to the digital to analog converters (DACs). The resulting signals are upconverted, amplified and transmitted.

Spectral Analysis of the Jamming Signal



no jammer



reactive pilot-tone jammer

SEEMOO SECURE MOBILE NETWORKING

UNIVERSITAS STUDIORUM BRIXIAE

TECHNISCHE UNIVERSITÄT DARMSTADT