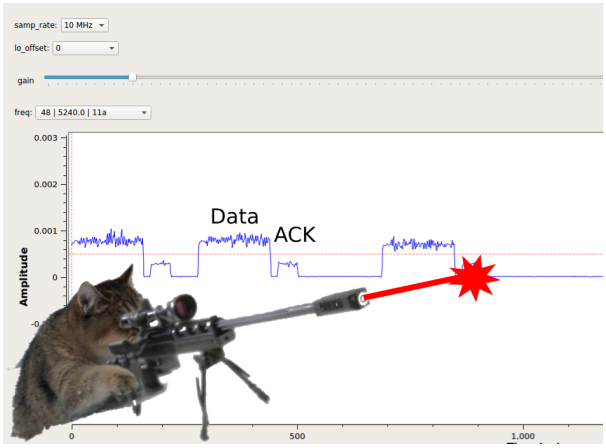
Bachelor Thesis

MAC Layer Experimentation with Modified WiFi Firmware

Description:



Even with today's capable network simulators, experiments with real hardware are still essential. When studying Wireless LANs, they allow us to validate simulation results and test actual hardware implementations. Setting up experiments is, however, far from trivial – especially when the MAC layer is involved. Given the short timings (in the micro second scale), it is challenging to force specific interference scenarios in a reliable and reproducible manner. Recent work suggests that the firmware of certain WiFi adapters can be modified for that purpose. More precisely, the authors showed that it is generally possible to jam specific frames. The exact strengths and limitations of this approach are, however, yet unexplored and should be investigated in the context of this thesis.

Tasks:

We will have an in-depth look into the firmware of WiFi adapters supported by the Linux *ath9k-htc* driver. In particular, we are interested in the possibility to jam specific frames. Using Software Defined Radio, we will monitor the wireless channel to investigate (1) the reliability that a jam signal is sent, (2) the effectiveness of the jam signal, and (3) the minimum delay between detection of the frame and transmission of the jam signal. Once these parameters are determined, we will have a solid understanding of the capabilities of the jammer and are able to estimate its impact on network throughput. In a final experiment, we will validate these findings by measuring the throughput of a saturated UDP connection, comparing it with our estimated value.

Requirements:

Programming in C, Linux, Wireless Networking, Software Defined Radio (SDR)

Advisors:

Bastian Bloessl <bloessl@ccs-labs.org>
Florian Klingler <Klingler@ccs-labs.org>
Christoph Sommer <sommer@ccs-labs.org>