Detection, Localization and Jamming of Communication Signals and Devices

Degree programme: Master of Science in Engineering | Specialisation: Information and Communication Technologies
Thesis advisor: Dr. Rolf Vetter
Expert: Dr. Friedrich Heitger
External project partner: COMLAB AG, Ittigen

Safeguarding sensible areas from unauthorized use of cellular phones or drone intrusions requires a reliable detection, localization and jamming of modern communication signals. Within the scope of this thesis concepts were developed, implemented and validated to provide a modular system preventing such threats.

Background

Numerous application fields require a robust detection and localization of modern communication signals. An example is given by drones which may constitute – when used with malicious intent – a threat to the security of sensible buildings and installations like nuclear power plants, airports and government buildings.

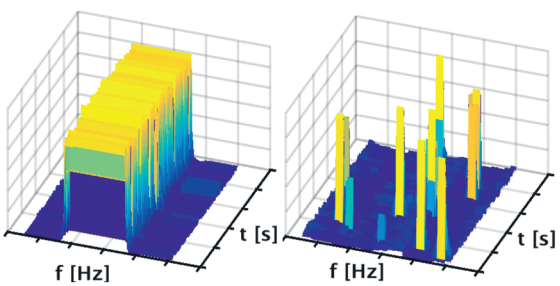
Methods

The methods and algorithms have been developed in a generic framework to cover applications for the prevention of cellphone use in prisons (2G, 3G and 4G) and drone intrusions of restricted areas. For the sake of clarity, only the drone intrusion application is presented herein. It is assumed that in such a scenario the drone is flown by remote control. As a result, the method consists of detecting and jamming communications from drone to the remote control. Jamming refers to a technique, where communications are disturbed such as to prevent information exchange between the drone and the remote control. This forces most modern drones to enter a safe mode, which consists of landing or returning to the takeoff place. In order to guarantee a reliable detection and localization of the drone, morphological filtering in the frequency domain has been applied to separate up and downlink remote control signals. Once the downlink communication signals from the drone to the remote control are isolated, a tracking can be performed. Modern beamforming techniques exploiting signals from multiples antennas (so-called antenna arrays) simultaneously, have been applied to provide the angle of drone arrival. Eventually, a disturbance signal is emitted in the direction of the drone using an antenna array and beamforming with the parameters estimated in the sensing mode. The emitting power is therefore only sent in the direction where it is needed to achieve an efficient disruption of the remote control signals. This strategy together with a highly reactive FPGA implemented jamming mode, which allows even the disruption of burst-like signals in under a millisecond, leads to an innovative and highly efficient system for drone shielding.

Jonas Schild

Results

Drone detection performance has been evaluated on synthetic signals and confirmed in field tests with a detection distance up to 2km. The spatial selectivity of the implemented beamforming technique has been assessed and the reactive jamming method was successfully verified on the three most popular drones.



Isolated drone communication signals, video stream downlink (l) and remote control (r)

Dual channel reactive jamming unit