

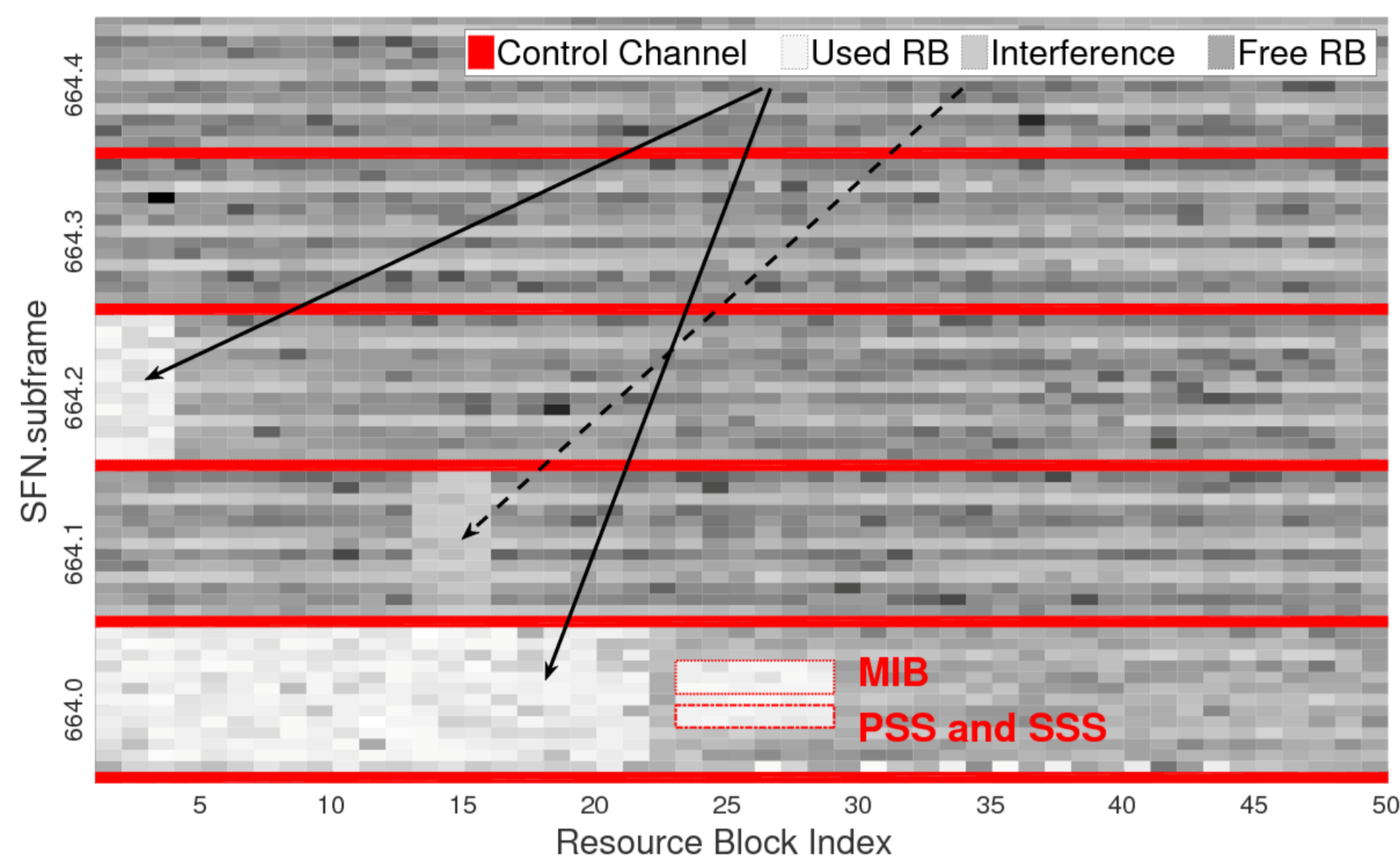
LTELeaks:

Privacy Concerns in Mobile Networks

Nicola Bui, Guevara Noubir

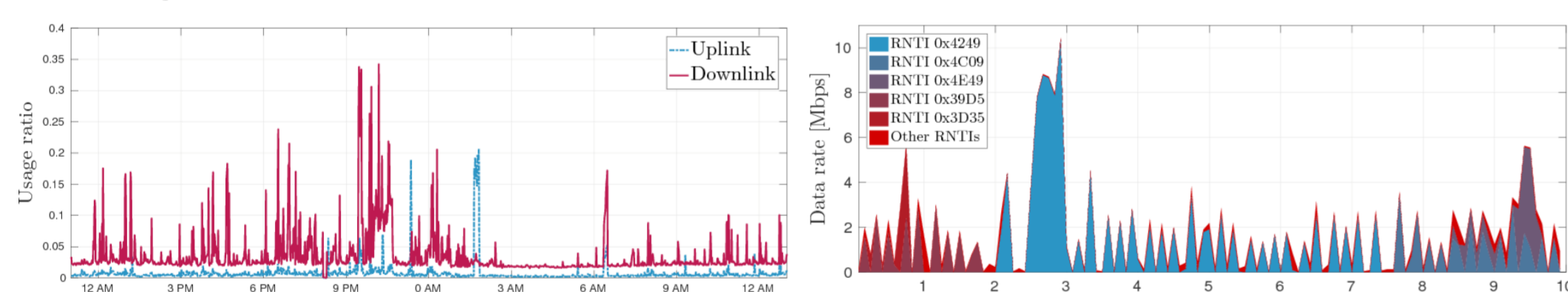
LTE Characteristics:

- Unencrypted control channel
- Detailed scheduling information can be obtained by passive listening
- Users' temporary ID
- TX and RX instant for each user
- Paging provides S-TMSI

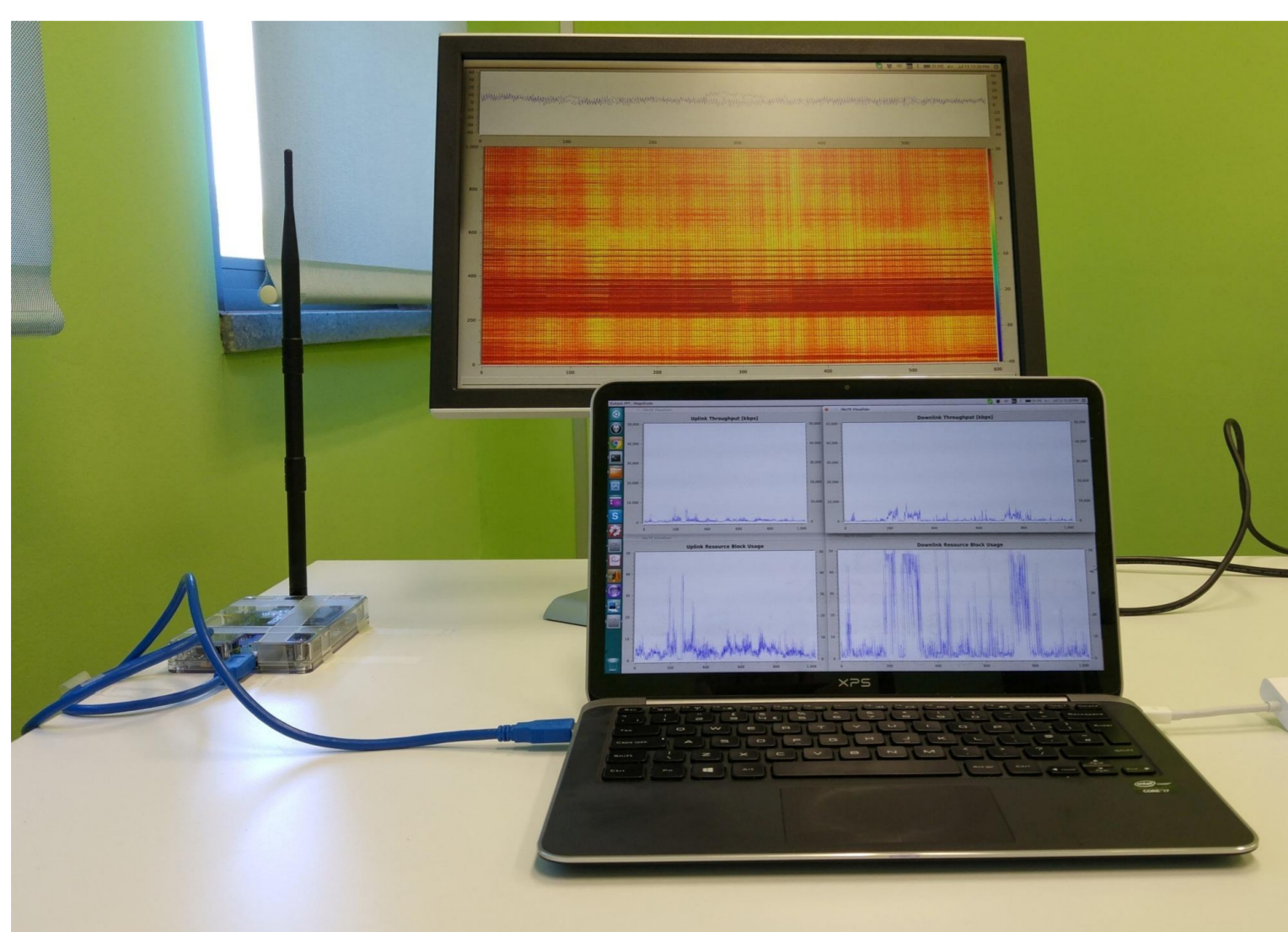


Passive listening:

- The cell traffic can be logged and classified by means of machine learning
- Single users patterns can be identified

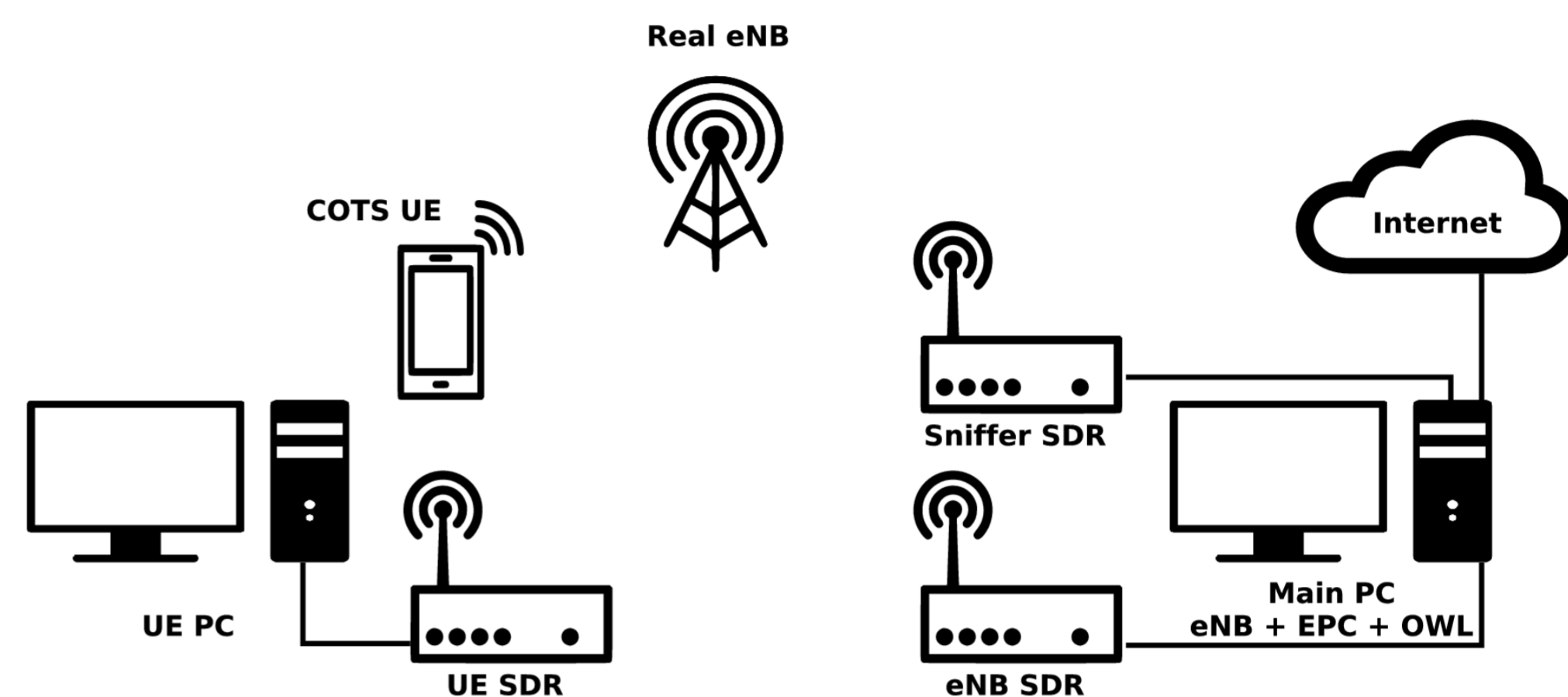


- Simple and portable setup: a laptop connected to a software defined radio
- Application specific training set can be used to recognized users' activity



Laboratory:

Software-based LTE cell



Software:

OpenAirInterface, srsLTE

Hardware:

Software Defined Radios (USRPs, BladeRFs, LimeSDRs), Fast servers

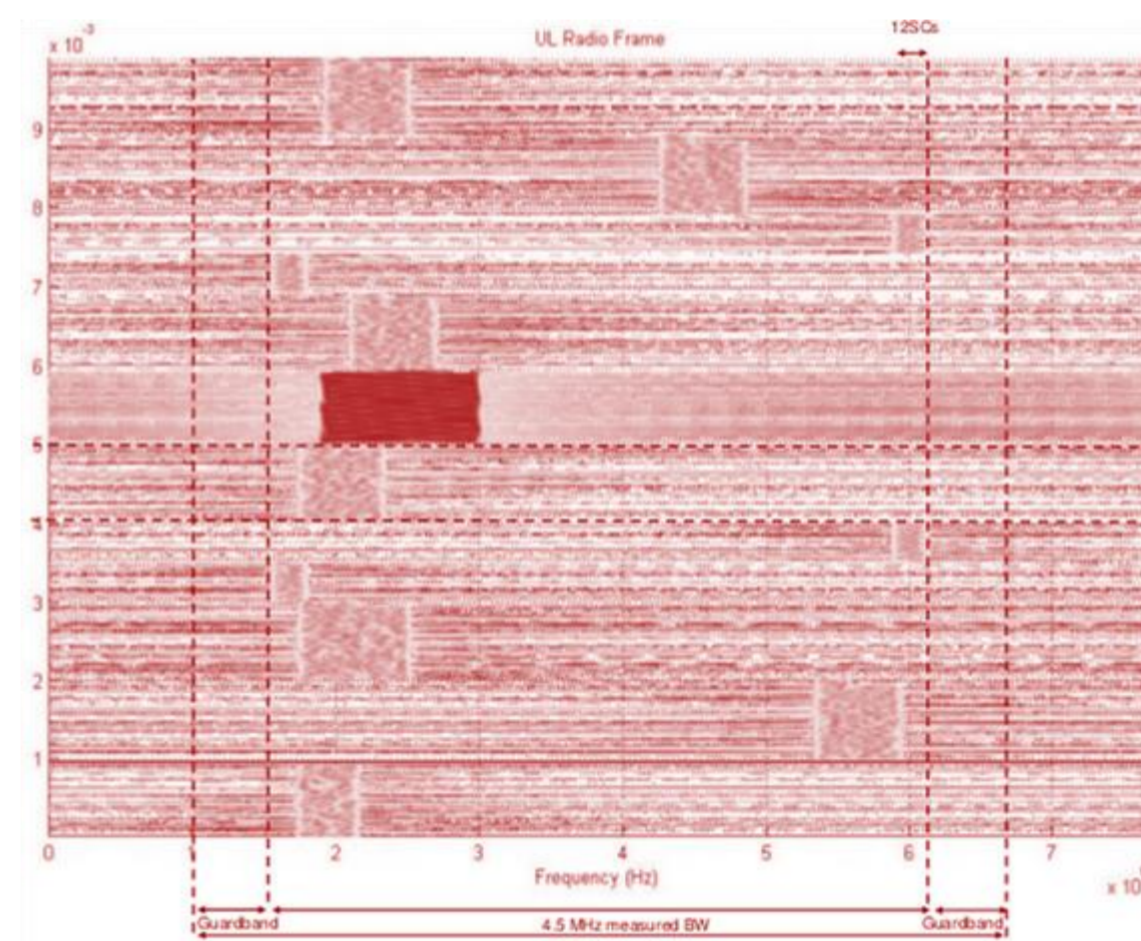
On-going activities:

RF fingerprinting:

Device identification based on RF specific characteristics.

SAR-based localization:

Uplink channel analysis to track angle of arrival of communications



Traffic signature:

Application, user profiles, etc.

Privacy threats:

Complete characterization of information leaks by passive listening

Countermeasures:

Physical layer, Protocol-based, Crypto-based solutions to enhanced the network security

Visit us at ISEC 655 for a live demo

