WSNLab – A Security Testbed and Security Architecture for WSNs

Fraunhofer FKIE

Nils Aschenbruck[1] [2], Jan Bauer[1], Jakob Bieling[1], Alexander Bothe[1], Matthias Schwamborn[1]

[1] *Insitute of Computer Science 4, University of Bonn*

[2] *Fraunhofer FKIE*

universitätbonn ICS

Motivation & Objectives

Wireless Sensor Networks (WSNs) are deployed in a steadily growing plethora of application areas. Especially their deployment in the industrial, military, and medical domain renders security in these networks an issue of high relevance.

The main objective of WSNLab is to build a WSN testbed for the evaluation of security measures. A second goal is to develop, implement, and evaluate a security architecture for WSNs. The testbed consists of multiple operating systems and sensor platforms to ensure broad system support.

WSN Testbed

OSs and Platforms

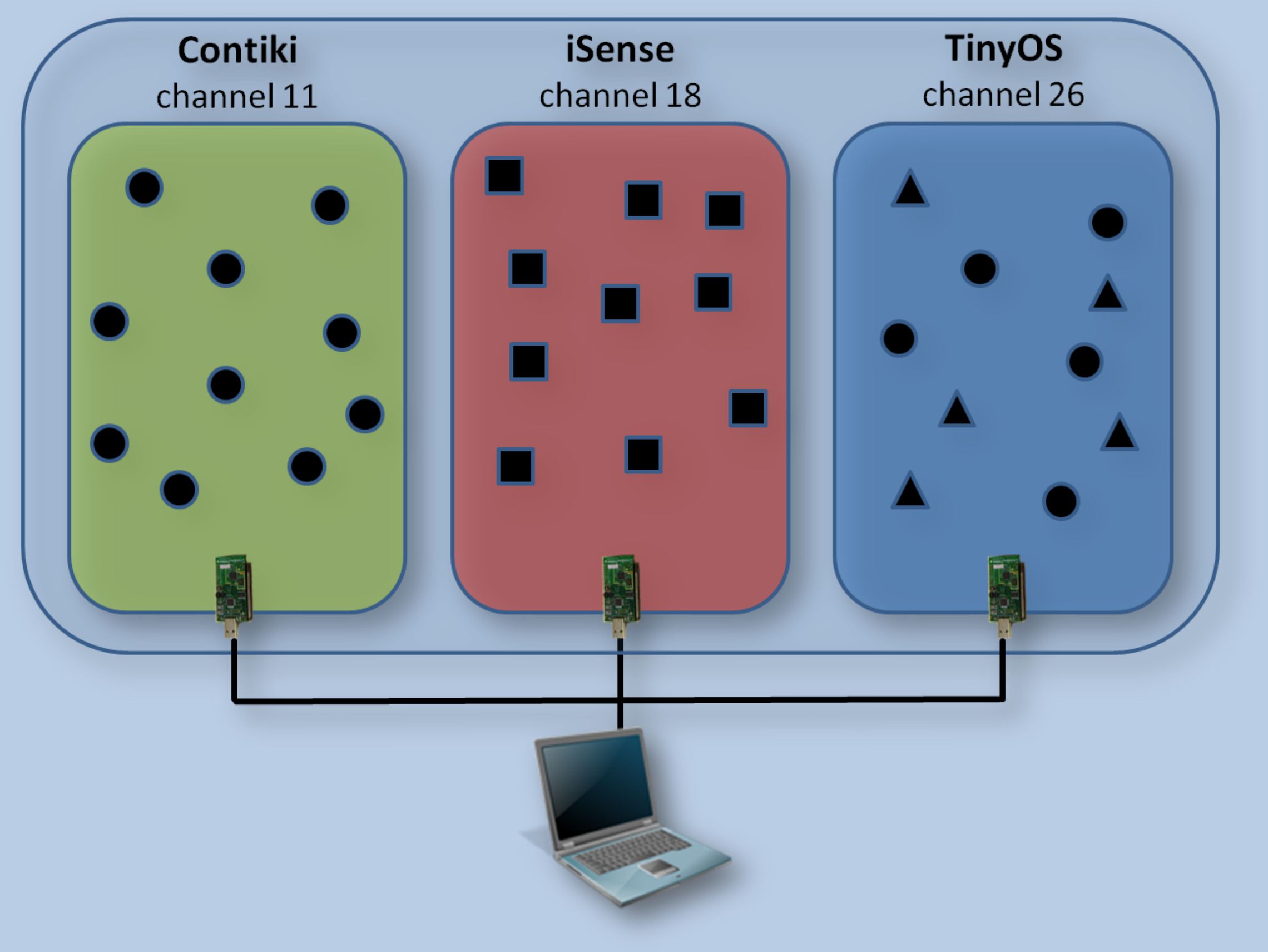
- Contiki: TelosB
- iSense: iSense-CM10C
- TinyOS: TelosB, MicaZ

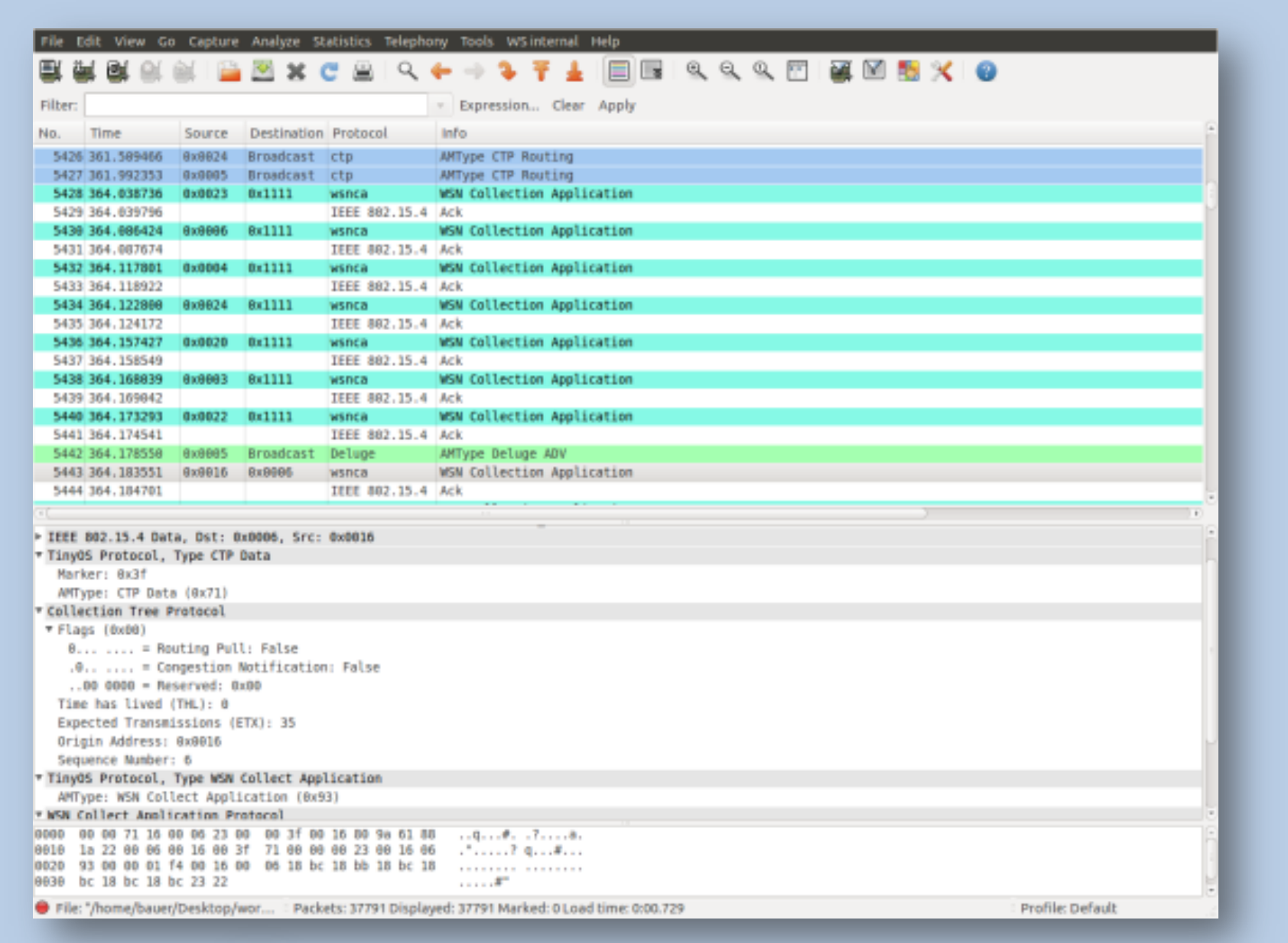
Software on Motes

- Collector application
- Routing: RPL or CTP
- Over-the-Air-Programming

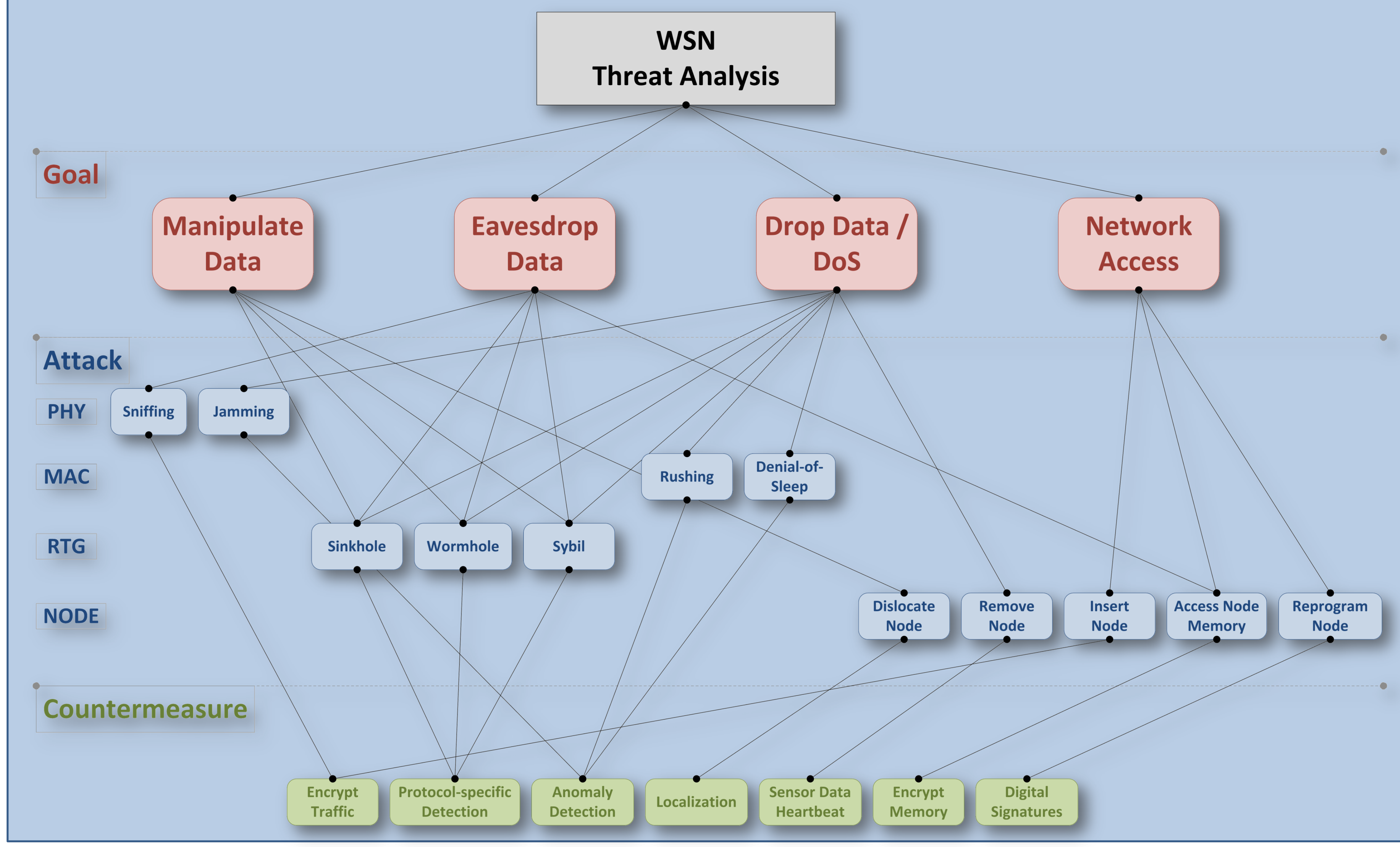
Tools

- Jackdaw IEEE 802.15.4 Sniffer
- Wireshark Packet Analyzer
- GNU Radio USRP-Board Jammer



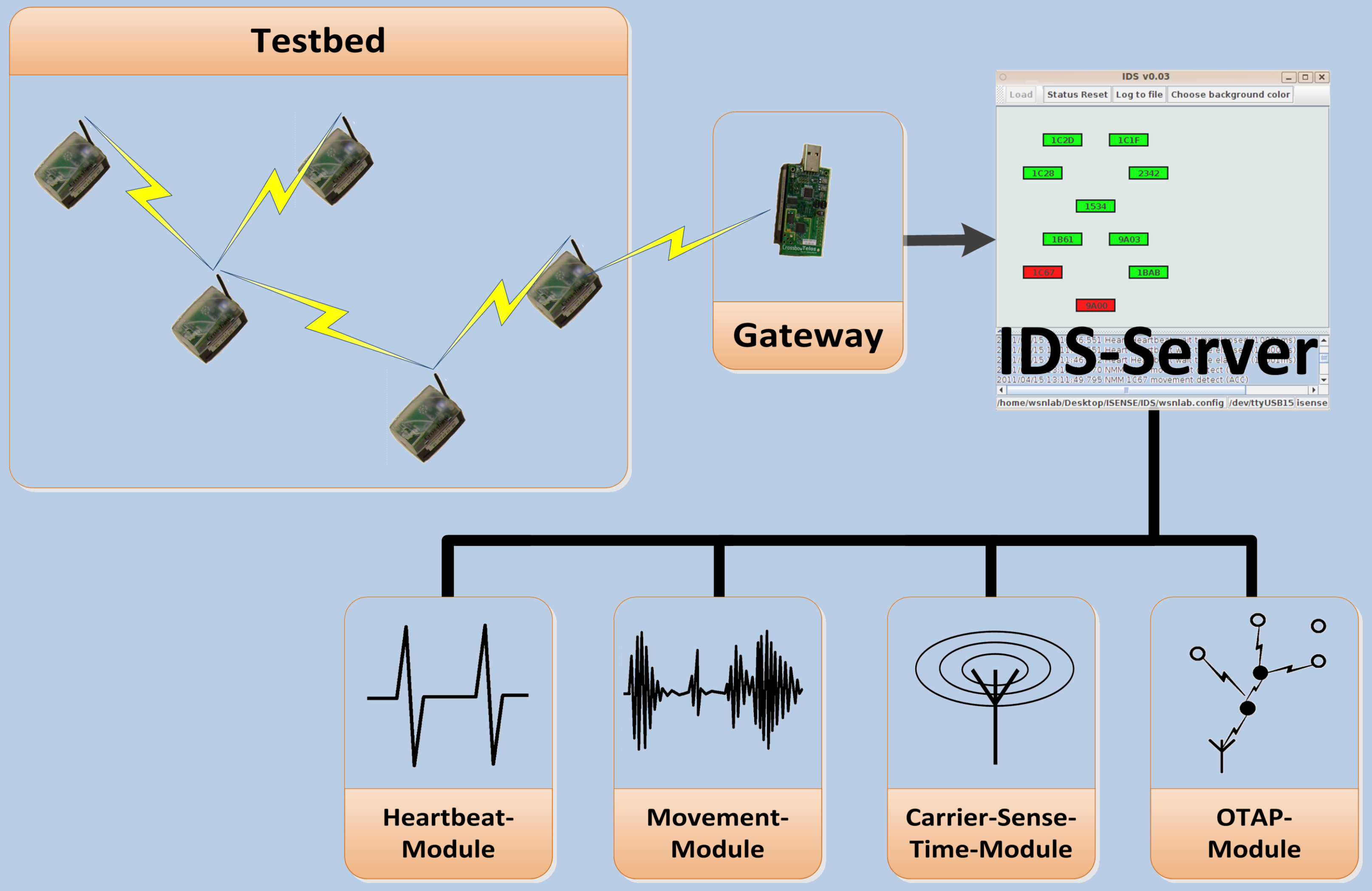


Security Architecture and IDS



An attacker can achieve his objective(s) through different kinds of attacks. These can be categorized based on the targeted layer. From the specific properties of WSNs result special attacks as well as new challenges for countermeasure development.

Sensor node resource scarcity in terms of computing power, memory, energy, and bandwidth requires countermeasures to be light-weight and effective at the same time.



http://tacnet.net.cs.uni-bonn.de / http://www.fkie.fraunhofer.de