

LTE-Netzwerkanalyse

Eder Martin, Kowasch Andreas, Nagy Christian, Wolf Michael SS16, Mobile Netze, Prof. Dr. Wischhof

30.9.2016





Ablauf Vortrag

Aufgabenstellung

Installation

Theorie

Analyse

CellTracker

Fazit

Ablauf Vortrag

Aufgabenstellung

Installation srsUE/LTE/GUI openLTE

Theorie

Analyse openLTE srsUE/LTE

Demo

CellTracker

Demo



Aufgabenstellung

Ablauf Vortrag



Aufgabenstellung

Installation

Theorie

Analyse

CellTracker

- Projekt
 - Analyse kommerzieller LTE-Mobilfunknetzwerk
 - MIB, SIB, Paging dekodieren/interpretieren
 - Mobilfunkmasten lokalisieren
- Software Inbetriebnahme/Dokumentation
 - srsUE/LTE/GUI
 - openLTE
- Hardware
 - Ettus Research USRP B210/N210
 - Antenne Vert900/Vert2450



Installation srsUE/LTE/GUI

Ablauf Vortrag

Aufgabenstellung Distribution: (großes Repository)



Installation

Theorie

Analyse

CellTracker

Fazit

Auflösen der Software-Abhängigkeiten

- Kompilieren von srsLTE und srsUE
- Vorbereitung der USRP-Plattform
 - Download UHD-Images
 - USRP N210 Netzwerkkonfiguration

Wireshark Dissector



Installation openLTE

Ablauf Vortrag

Aufgabenstellung

Installation

Theorie

Analyse

CellTracker

- Hardwareanforderungen
 - USB 3.0 Interface
 - Intel Core i5 / i7 mit SSE4.1, SSE4.2 und AVX
- Betriebssystem



- Software-Abhängigkeiten
 - UHD Treiber
 - GNURadio
- Kompilieren von openLTE



Master Information Block

Ablauf Vortrag

Aufgabenstellung

Installation

Theorie

Analyse

CellTracker

Fazit

Lesbar nach Synchronisation

- Inhalt
 - Bandbreite des Downlinkkanals
 - PHICH Konfiguration
 - System Frame Nummer
- PHICH → PDCCH lesbar



MIB Übertragung

Ablauf Vortrag

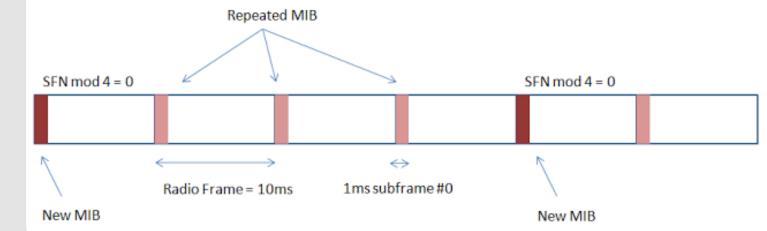
Aufgabenstellung

Installation

Theorie

Analyse

CellTracker





Ablauf Vortrag

Aufgabenstellung

Installation

Theorie

Analyse

CellTracker

Fazit

System Information Block

- 19 unterschiedliche SIBs
- Übertragen auf PDSCH
 - zum Lesen PDCCH nötig
- SIB 1 und 2 wichtig für Verbindungsaufbau



Ablauf Vortrag

Aufgabenstellung

Installation

Theorie

Analyse

CellTracker

Fazit

System Information Block

- SIB 1
 - Alle 80ms
 - Zellen Information f
 ür Evaluierung des Zugangs
 - Scheduling der anderen SIBs
- SIB 2
 - Radioressourcen-Konfigurationen
 - RACH-Konfiguration
 - Ohne die SIB → keine ATTACH Prozedur



Analyse openLTE

Ablauf Vortrag

Aufgabenstellung

Installation

Theorie

Analyse

CellTracker

Fazit

Funkzellen finden (LTE_fdd_dl_scan)

Paketdaten aufzeichnen (LTE_fdd_dl_scan)

Paketdaten analysieren (manuell)

• Gefunden: MIB, SIB1-2-5-6



Analyse srsLTE/srsUE

Demo

Ablauf Vortrag

Aufgabenstellung

Installation

Theorie

Analyse

CellTracker

Fazit

Funkzellen finden (cell_search)

Paketdaten aufzeichen (ue)

Paketdaten analysieren (wireshark)

MIB, SIB1-2, TIMSI

 Standort des Mobilfunkmasten auf openCellID.org finden



CellTracker

Demo

Ablauf Vortrag

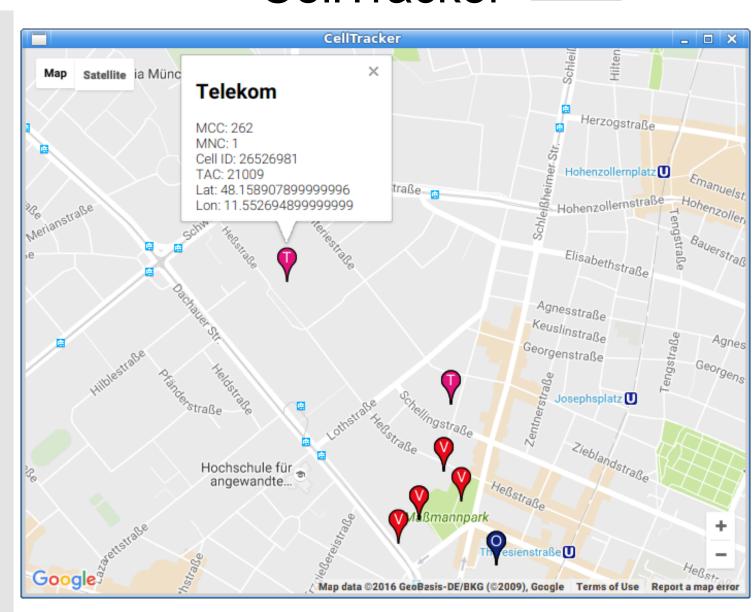
Aufgabenstellung

Installation

Theorie

Analyse

CellTracker





Fazit

Ablauf Vortrag

Aufgabenstellung

Installation

Theorie

Analyse

CellTracker

- Verbesserte Verständnis für das Gelernte
- Umgang mit mangelhaften Dokumentationen verbessert
- Kein leichter Weg zu den ersten Messergebnisse
- Ein erfolgreiches Projekt