GSM Übung 01

9. Januar 2012

Die folgenden Übungsaufgaben sind in Gruppen zu bearbeiten. Dabei sollen sich alle Studenten gleichmäßig auf die 4 vohandenen Motorola C123 Handys verteilen.

1 OsmocomBB Compilieren

Compilieren Sie den gesamten OsmocomBB Code. Gehen Sie dabei wie in der Anleitung *osmocom-bb-compilieren.txt* vor.

1. Warum wird eine ARM Toolchain zum compilieren verwendet?
2. Was wären mögliche Folgen, wenn Punkt 2 der Anleitung übersprungen wird?
3. Wo ist Layer 1 implementiert? (Ordnername bzw. übergeordneter Ordner)
4. Wo sind Layer 2 und Layer 3 implementiert? (Ordnername bzw. übergeordneter Ordner)

2 OsmocomBB Layer 1 Starten

Starten Sie den OsmocomBB Layer 1 auf einem Motorola C123 Handy. Gehen Sie dabei wie in der Anleitung *bcch-abhören.txt* (bis einschließlich Punkt 7) beschrieben vor.

1. Welche Datei wird dafür auf das Handy übertragen?
2. Wird der Layer 1 persistent aufgespielt, oder ist nach einem Neustart des Handys die ursprüngliche Firmware wieder vorhanden?

3 BCCH Abhören

Starten Sie die Layer 2 & 3 Anwendung *bcch_scan*. Gehen Sie dabei wie in der Anleitung *bcch-abhören.txt* vor. Wenn Layer 1 aus der vorigen Aufgabe korrekt läuft, kann mit Punkt 8 der Anleitung begonnen werden. (Normalerweise muss nicht länger als 2 Minuten gescannt werden um die Fragen beantworten zu können.)

1. Warum wird *-i 127.0.0.1* als Parameter für *bcch_scan* verwendet?
2. Notieren Sie Cell-ID, LAC (*Location Area Code*) und Betreiber von 3 BTS in Ihrem Empfangsbereich.
3. Finden Sie 2 unterschiedliche Zellen die in der selben LA stehen.
4. Wie viele IMSI und wie viele TMSI haben Sie über *Paging Requests* mitgehört? (Wireshark Filter: *gsm_a.imsi* bzw. *gsm_a.tmsi*)