



Hochschule München
Fakultät für Mathematik und Informatik

Projektdokumentation Mobile Netze

GSM-Handover mit OpenBSC und OpenBTS

Autoren: Max Eschenbacher
Stefan Giggenbach
Thomas Waldecker

Abgabe: 11.03.2012

betreut von: Prof. Dr. Zugenmaier

Inhaltsverzeichnis

1 Einleitung

Von: Stefan Giggenbach

Im Rahmen des Moduls Mobile Netze im Masterstudiengang Informatik wird mit der Durchführung einer Projektarbeit, dass in der Vorlesung vermittelte Wissen vertieft und um die praktische Anwendung ergänzt. In der vorliegenden Projektarbeit wurde die Handover-Funktionalität in einem GSM-Netzwerk untersucht. In diesem Kapitel wird nach einer theoretischen Einführung in die GSM-Handover-Thematik das Projektziel und die entsprechende Vorgehensweise beschrieben.

1.1 GSM-Handover

Der Handover stellt in einem GSM-Netzwerk eine wichtige Aufgabe des Mobility Management dar. Ändert ein Teilnehmer bei aktiver Verbindung seinen Standort, ist es möglich das er den von einer Funkzelle abgedeckten Bereich verlässt. In einem solchen Fall wird die Verbindung durch den Wechsel zu einer benachbarten Funkzelle (Handover) aufrecht erhalten. Grundsätzlich unterscheidet man in einem GSM-Netzwerk folgende Handoverszenarien:

- Intra BSC Handover
- Inter BSC Handover
- Inter MSC Handover
- Subsequent MSC Handover

Die genauen Abläufe der einzelnen Szenarien werden in [?] ausführlich beschrieben. Aus Sicht der Mobile Station unterscheiden sich die genannten Handoverszenarien nicht. Im folgenden wird nur der Ablauf des Intra BSC Handover beschrieben, der für das Verständnis der Arbeit entscheidend ist.

Während einer aktiven Verbindung wird der BSC in regelmäßigen Zeitabständen über die Signalqualität im Up- und Downstream informiert. Zu diesem Zweck sendet die Mobile Station über den SACCH sogenannte Measurement Reports, die anschließend im BSC zur Bestimmung der Downstream-Signalqualität ausgewertet werden. In den Measurement Reports sind neben Messergebnissen zur aktuell verwendeten BTS auch Messergebnisse zu benachbarten BTS, die auf Anweisung des BSC während den Sendepausen von der Mobile Station ermittelt werden. Die Signalqualität des Upstreams wird durch Messergebnisse aus der entsprechenden BTS ebenfalls im BSC berechnet. Der BSC kann aufgrund der eingehenden Measurement Reports zu dem Ergebnis kommen, dass ein Handover

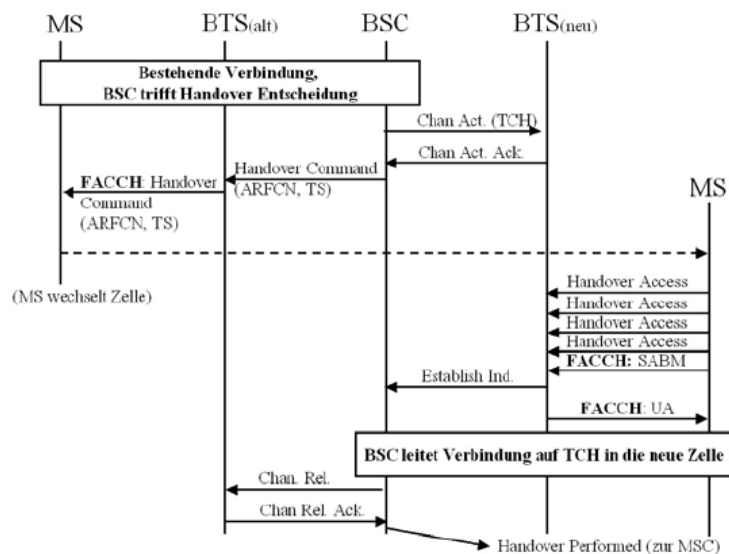


Abbildung 1: Ablaufdiagramm eines Intra BSC Handover [?]

zwischen zwei benachbarten BTS notwendig ist, um einen Abbruch der Verbindung zu verhindern.

Abbildung ?? zeigt den Ablauf eines Handover nach der Entscheidung eines BSC. Im ersten Schritt wird ein TCH in der neuen BTS aufgebaut. War dieser Vorgang erfolgreich, wird der Mobile Station über den FACCH der bestehenden Verbindung ein Handover Command übermittelt. Das Handover Command enthält als Parameter die Frequenz und den Timeslot des TCH der neuen BTS. Nach der Synchronisation der Mobile Station mit der neuen BTS, sendet es in vier aufeinanderfolgenden Bursts eine Handover Access Message und anschließend eine Set Asynchronous Balanced Mode Message. Die neue BTS quittiert den erfolgreichen Handover mit einem Established Indicator gegenüber dem BSC und einer UA Message gegenüber der Mobile Station. Nachdem der BSC die Verbindung auf den neuen TCH umschaltet, wird der TCH in der alten BTS abgebaut. Der Handover Vorgang ist damit abgeschlossen. Die wichtigsten Punkte für die Analyse bzw. Implementierung einer Handover-Funktionalität sind damit:

- Erfassung und Auswertung der Measurement Reports
- Logik für die Entscheidungsfindung eines Handover
- Inter BTS Kommunikation zum Aufbau eines neuen TCH
- Erzeugen und Senden eines Handover Command
- Umschalten der bestehenden Verbindung und Abbau des alten TCH

1.2 Projektziel und -durchführung

Ziel der Projektarbeit ist die Integration der in Abschnitt ?? eingeführten Handover-Funktionalität in die Open Source Software OpenBTS. Das OpenBTS Projekt ermöglicht, zusammen mit einer entsprechenden Radio-Hardware und zusätzlichen Software-Komponenten (GNURadio und Asterisk), den Betrieb eines kompletten GSM-Netzwerks. Mit der kommerziell vertriebenen Version der Software ist bereits ein Handover zwischen zwei BTS möglich. Die Voraussetzungen für eine erfolgreiche Integration eines Handover-Moduls sind somit gegeben. Die Architektur und Inbetriebnahme des verwendeten OpenBTS-Systems werden in Kapitel ?? ausführlich behandelt.

Vor der Integrations- und Implementierungsphase wird der Ablauf eines Handover genauer analysiert. Zu diesem Zweck wird ein OpenBSC-System aufgesetzt, mit dem das in Abschnitt ?? beschriebene Handoverszenario reproduziert werden kann. Der Aufbau, die Inbetriebnahme und die Konfiguration des OpenBSC-Systems für die Durchführung eines Intra BSC Handover werden in Kapitel ?? behandelt. Die anschließende Analyse der durchgeführten Handover erfolgt mit Hilfe der auf der Um- und Abischnittstelle erstellen Wireshark Traces und ist in Abschnitt ?? beschrieben.

Der Architekturentwurf für die Integration und die teilweise durchgeführte Implementierung des Handover-Moduls werden in Kapitel ?? behandelt. Der erreichte Projektstand und geschaffenen Ansatzpunkte für weitere Projektarbeiten an der Integration des Handover-Moduls schließen die Arbeit ab.

2 Handover mit OpenBSC

Von: Stefan Giggenbach

Bei OpenBSC handelt es sich wie bei OpenBTS um Open Source Software. Der Vorteil von OpenBSC liegt in der network in the box (nitb) genannten Version, die ohne zusätzliche Software-Komponenten den Betrieb eines GSM-Netzwerks ermöglicht. Es wird lediglich eine unterstützte BTS-Hardware benötigt. Im Projekt werden zwei nanoBTS der Firma ip.access verwendet. Abbildung zeigt die Architektur des eingesetzten Systems.

OpenBSC übernimmt nicht nur die Funktion des BSC sondern auch die des MSC. Die Teilnehmer Datenbanken HLR und VLR werden mit einer SQLite3 Datenbank realisiert. Durch die Anbindung von zwei nanoBTS über die Abis-over-IP-Schnittstelle ist die Durchführung eines Intra BSC Handover mit geringen Installations- und Konfigurationsaufwand möglich.

2.1 Installation und Konfiguration

Die Installation von OpenBSC ist im Wiki des Projekts Schritt für Schritt dokumentiert. In diesem Abschnitt werden deshalb nur die wichtigsten Punkte der Installation und die Konfiguration für den Multi-BTS-Betrieb behandelt.

3 Erweiterung von OpenBTS

3.1 Measurement Report

Von: Max Eschenbacher

Measurement Reports enthalten Messwerte bzgl. der Empfangsleistung, Empfangsqualität und Informationen zu Nachbarzellen. Sie werden beim Einbuchen in das Netzwerk und während eines Gesprächs (ca. 2 mal in der Sekunde) von der MS an die BTS gesandt. Measurement Reports sind im RR-Sublayer (Radio Resource) angesiedelt und mit dem Nachrichtentyp *MEASUREMENT REPORT* gekennzeichnet. Die Messwerte sind für das Weiterreichen (Handover) der MS von großer Bedeutung.

OpenBTS verwaltet diese Messwerte intern in einer eigenen Klasse, bietet aber auch die Möglichkeit, diese in eine externe SQL-DB abzulegen. Mit der Option `Control.Reporting.PhysStatusTable` kann der Pfad der Datenbank angegeben werden:

```
OpenBTS> config Control.Reporting.PhysStatusTable \  
/etc/OpenBTS/phystatus.db
```

Leider werden keinerlei Informationen bzgl. der Nachbarzellen in die Datenbank eingetragen. Deshalb musste die entsprechende Tabelle der Datenbank um weitere Felder für die Nachbarzellen erweitert und die Methode `PhysicalStatus::setPhysical()` angepasst werden. Zusätzlich wurde ein neuer CLI-Befehl namens `showmr` implementiert, welcher den Inhalt der Measurement Report DB entsprechend formatiert und auflistet.

Beispielausgabe von showmr:

```

OpenBTS> showmr
#####
                        Measurement Report:
#####
CN_TN_TYPE_OFFSET      =      C0T0 SDCCH/4-0
ARFCN                  =      867
ACCESSED               =      1330702677
RSSI                   =      -63.750000
TIME_ERR               =      -0.222656
TIME_ADVC              =      1
TRANS_PWR              =      30 dBm
FER                    =      0.000000
RXLEV_FULL_SERVING_CELL =      -48 dBm
RXLEV_SUB_SERVING_CELL =      -48 dBm
RXQUAL_FULL_SERVING_CELL_BER =      0.181000 dBm
RXQUAL_SUB_SERVING_CELL_BER =      0.181000 dBm
NO_NCELL               =      1
RXLEV_CELL_1 = 0, BCCH_FREQ_CELL_1 = 0, BSIC_CELL_1 = 0
RXLEV_CELL_2 = 0, BCCH_FREQ_CELL_2 = 0, BSIC_CELL_2 = 0
RXLEV_CELL_3 = 0, BCCH_FREQ_CELL_3 = 0, BSIC_CELL_3 = 0
RXLEV_CELL_4 = 0, BCCH_FREQ_CELL_4 = 0, BSIC_CELL_4 = 0
RXLEV_CELL_5 = 0, BCCH_FREQ_CELL_5 = 0, BSIC_CELL_5 = 0
RXLEV_CELL_6 = -33, BCCH_FREQ_CELL_6 = 63, BSIC_CELL_6 = 1
#####
CN_TN_TYPE_OFFSET      =      C0T1 TCH/F
ARFCN                  =      867
ACCESSED               =      1330696371
RSSI                   =      -57.250000
TIME_ERR               =      0.263672
TIME_ADVC              =      1
TRANS_PWR              =      30 dBm
FER                    =      0.042869
RXLEV_FULL_SERVING_CELL =      -48 dBm
RXLEV_SUB_SERVING_CELL =      -48 dBm
RXQUAL_FULL_SERVING_CELL_BER =      0.000000 dBm
RXQUAL_SUB_SERVING_CELL_BER =      0.000000 dBm
NO_NCELL               =      7
RXLEV_CELL_1 = 0, BCCH_FREQ_CELL_1 = 0, BSIC_CELL_1 = 0
RXLEV_CELL_2 = 0, BCCH_FREQ_CELL_2 = 0, BSIC_CELL_2 = 0
RXLEV_CELL_3 = 0, BCCH_FREQ_CELL_3 = 0, BSIC_CELL_3 = 0
RXLEV_CELL_4 = 0, BCCH_FREQ_CELL_4 = 0, BSIC_CELL_4 = 0
RXLEV_CELL_5 = 0, BCCH_FREQ_CELL_5 = 0, BSIC_CELL_5 = 0
RXLEV_CELL_6 = 0, BCCH_FREQ_CELL_6 = 0, BSIC_CELL_6 = 0
#####

```

Erläuterungen zur Beispielausgabe

Der erste Measurement Report wurde um 1330702677 (Unix-Time, entspricht 02.03.2012 - 16:37:57 Realzeit) im SDCCCH (*Standalone Dedicated Control Channel*) mit der Nummer 0 (von 4 Möglichen) auf der ARFCN 867 gesendet. Die empfangene Signalstärke (RSSI = Received Signal Strength Indication) betrug -63.75 dBm. Der zugeordnete Timing Advance Parameter der MS betrug 1 Symbolperiode und wies einen Fehler (TIME_ERR), d.h. Zeitversatz von -0.222656 Symbolperioden auf. Die Sendeleistung der MS betrug 30 dBm und hatte bis dato eine Uplink-FER (= Frame Erasure Rate; gibt das Verhältnis zwischen gelöschten Frames und der Gesamtanzahl der Frames an) von 0. Der Empfangspegel der verwendeten Zelle (RXLEV_FULL_SERVING_CELL) betrug -48 dBm und die Empfangsqualität RXQUAL_FULL_SERVING_CELL_BER = 0.181000 dBm. Die Angaben SUB und FULL bei der Empfangsleistung und -qualität beziehen sich auf die Verwendung von DTX (Discontinuous Transmission). FULL bezieht dabei alle Frames mit ein, also auch die zu dessen Zeit keine Sprache gesendet wurde. SUB hingegen nur die effektiven „Sprachframes“. Da jeweils beide Werte im obigen Beispiel gleich sind, kann man davon ausgehen das kein DTX verwendet wurde. Die restlichen Angaben beziehen sich auf die Nachbarzellen. NO_NCELL gibt die Anzahl der sichtbaren Nachbarzellen an. Dabei gibt es zwei Sonderfälle: NO_NCELL=0 - es existieren keine Messwerte, NO_NCELL=7 - es existieren keine Nachbarzellen. Im obigen Beispiel sieht die MS 1 Nachbarzelle (Nr. 6) mit einer Empfangsleistung von -33 dBm.

3.2 Handover Modul

Von: Stefan Giggenbach

3.3 Inter OpenBTS Handover

Von: Thomas Waldecker

A Anhang

A.1 Literaturverzeichnis

- [1] Martin Sauter: *Grundkurs Mobile Kommunikationssysteme*, Vieweg+Teubner Verlag, Wiesbaden 2011
- [2] OpenBTS System Diagramm: https://wush.net/trac/rangepublic/attachment/wiki/BuildInstallRun/openbts_system_diagram.png, Abgerufen am 03.03.2012
- [3] Range Networks Inc.: *OpenBTS P2.8 Users Manual Doc. Rev. 1*, Range Networks Inc. 2011