

OsmoBTS - Bug #4009

Channel Activation starts SACCH too early in Synchronous Handover

05/19/2019 08:50 PM - laforge

Status: New	Start date: 05/19/2019
Priority: Normal	Due date:
Assignee:	% Done: 0%
Category:	
Target version:	
Spec Reference: 3GPP TS 48.058 Section 4.1.4	
Description	
<p>In case of a synchronous hand-over related channel activation, 3GPP TS 48.058 Section 4.1.4 is very specific:</p> <p>BTS starts transmission immediately on the main channel in the indicated mode and with encryption if so indicated. If the MS Power and Timing Advance element are present, BTS shall start transmission also on SACCH with the timing advance and MS power control parameters indicated. If only the MS power element is present the BTS may start transmission also on the SACCH.</p> <p>When receiving a correct access burst with the correct handover reference, BTS starts the normal reception process on the main channel in the indicated mode, with deciphering applied if so indicated, and starts receiving (and sending if not started earlier) on SACCH. The handover detection procedure towards BSC is also started. Alternatively, the reception of a correctly decoded frame from the MS on the main channel, in the indicated mode and deciphering applied if so indicated, allows the start of sending on SACCH (if not already started) and starts the handover detection procedure towards the BSC.</p> <p>However, as uncovered by an upcoming BTS_Tests.TC_sacch_chan_act_ho_sync test case, we appear to be activating the SACCH unconditionally from the first moment.</p> <p>The problem here is quite obvious: Until we have received the access burst from the MS, we don't yet know the timing offset, and hence the timing advance that we should advertise in the downlink SACCH. If we start SACCH transmission too early, it means that a wrong TA is advertised, which may be picked up by the MS, which will then apply a wrong TA value -> boom.</p>	
Related issues:	
Related to OsmoBTS - Feature #3750: Extension of BTS_Tests.ttcn test coverage	Resolved 01/08/2019
Related to OsmoBSC - Feature #4010: Test RSL CHAN ACT related details for dif...	New 05/19/2019

History

#1 - 05/19/2019 08:50 PM - laforge

- Related to Feature #3750: Extension of BTS_Tests.ttcn test coverage added

#2 - 05/19/2019 08:58 PM - laforge

- Related to Feature #4010: Test RSL CHAN ACT related details for different scenarios added

#3 - 05/22/2019 07:18 AM - laforge

There's good news and bad news.

The actual behavior of the BTS is very dependent on the specific PHY used. I've analyzed osmo-bts-trx and osmo-bts-sysmo as two representatives, where lc15 and oc2g are mostly like -sysmo.

osmo-bts-sysmo

osmo-bts-sysmo gets it half-way right. It

- checks if the activation is HO related, and only activates uplink RACH detection until a RACH is received
- then activates all other logical channels / SAPIs after the RACH was received

What it gets wrong:

- it doesn't activate DL main channel (FACCH/SDCCH) while waiting for the RACH
- it unconditionally delays activation of DL+UL SACCH, even if the MS Power IE and/or TA IE were present in RSL CHAN ACT

osmo-bts-trx

osmo-bts-trx gets it wrong in all cases:

- it always activates both main channel and SACCH in UL and DL from the very beginning, even before any RACH is received in UL

In fact, osmo-bts-trx and its scheduler don't even know the concept of L1 SAPI and hence don't have the infrastructure to enable/disable individual logical channels within one dedicated channel.

Summary

What does this all mean in practice for osmo-bts-trx? There is a significant risk of poor hand-over performance, as

- some phones could receive a massively wrong timing advance before we even know the TA
- some phones could simply refuse to send the RACH if there is no downlink FACCH/SDCCH visible

#4 - 06/19/2019 08:34 AM - laforge

- Priority changed from Urgent to High

#5 - 07/18/2019 05:10 AM - laforge

- Assignee deleted (laforge)

#6 - 07/18/2019 05:15 AM - laforge

- Priority changed from High to Normal