OsmoSGSN - Bug #3936

Iu: first GMM Service Request does not find a MM ctx

04/16/2019 06:21 PM - lynxis

Status:	New	**Start date:**	04/16/2019
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Iu interface		
Target version:			
Spec Reference:	TS 24.008		

Description

As in OS#3920 on the first GMM Service Request after an successful PDP Context Request. The sgsn can not find the MM ctx. But it should find it!

```
Apr 16 20:24:38 Core osmo-sgsn[8553]: <0002> gprs_gmm.c:1831 MM(---/ffffffff) -> GMM SERVICE REQUE
ST MI(3913630026) type="data"
Apr 16 20:24:39 Core osmo-sgsn[8553]: <0018> gprs_gmm.c:205 Cannot find mm ctx for IU event 1
```

Related issues:

Related to OsmoSGSN - Support #3920: PCAPs files of 3G PS for Osmocom network...	**In Progress**	**04/12/2019**

History

#1 - 04/16/2019 06:22 PM - lynxis

- Related to Support #3920: PCAPs files of 3G PS for Osmocom network and Commercial one added

#2 - 04/28/2019 02:37 PM - efistokl

lynxis wrote:

> As in OS#3920 on the first GMM Service Request after an successful PDP Context Request. The sgsn can not find the MM ctx. But it should find it!

It could be a bug of libosmo-sccp/osmo-stp or osmo-iuh/osmo-hnbgw. The Initial-UE Service Request has one (new) ranap_ue_conn_ctx (conn_id), but the SecurityModeComplete that comes later has a different one (which was used for communication before). Then after 30 seconds my phone sends another Service Request (Direct Transfer), using old ranap_ue_conn_ctx, and all goes well here. I will try to debug osmo-stp/osmo-hnbgw conn_id use/allocation somehow...

#3 - 05/07/2019 01:37 PM - efistokl

efistokl wrote:

> It could be a bug of libosmo-sccp/osmo-stp or osmo-iuh/osmo-hnbgw. The Initial-UE Service Request has one (new) ranap_ue_conn_ctx (conn_id), but the SecurityModeComplete that comes later has a different one (which was used for communication before). Then after 30 seconds my phone sends another Service Request (Direct Transfer), using old ranap_ue_conn_ctx, and all goes well here. I will try to debug osmo-stp/osmo-hnbgw conn_id use/allocation somehow...

Uploaded a patch that fixed the problem for me: https://gerrit.osmocom.org/#/c/osmo-iuh/+/13896/