OsmoSGSN - Bug #3727

SGSN segfaults on network type change

12/12/2018 11:29 PM - manatails

![Table](https://i.imgur.com/6V.png)

**Description**
When the phone changes its network type between GSM and UMTS osmo-sgsn crashes with the following log:

<0012> gprs_llc_parse.c:81 LLC SAPI=1 C U GEA0 IOV-UI=0x000000 FCS=0x760d06 CMD=UI DATA
<0002> gprs_gmm.c:1609 -> GMM RA UPDATE REQUEST type="RA updating"
<0002> gprs_gmm.c:1685 MM Looked up by matching TLLI and P_TMSI. BSSGP TLLI: b99cab1e, P-TMSI: f99cab1e (00000000), TLLI: 00000000 (00000000), RA: 450-09-1-1

Program received signal SIGSEGV, Segmentation fault.
0x0000000000409667 in gsm48_gmm_authorize (ctx=0x758600) at gprs_gmm.c:1051
1051            if (ctx->ran_type == MM_CTX_T_UTRAN_Iu && !ctx->iu.ue_ctx->integrity_active) {
(gdb)

**Related issues:**
- Related to OsmoSGSN - Bug #3995: OsmoSGSN doesn't close SCCP connection after... Closed 05/10/2019
- Related to OsmoSGSN - Bug #1977: 3G IuPS is unreliable Closed 03/09/2017

**Associated revisions**
Revision 33f97551 - 02/04/2020 08:27 AM - daniel

gprs_gmm: Check for RAT change and ensure this only happens for RAU/ATT

Change-Id: I38cb31907eddeade5350cdb648df179408d908d2
Related: OS#3727

**History**
#1 - 12/13/2018 12:07 AM - manatails

cxt->iu.ue_ctx is null at the time of crash

#2 - 04/09/2019 11:17 AM - laforge
- Assignee set to lynxis

#3 - 04/11/2019 04:13 AM - lynxis

Can you create a backtrace when this problem happens (gdb cli: bt). It would be also nice if you can provide a pcap trace. I would guess this problem happens when a MS/UE moves from 3G to 2G. Not sure if the SGSN also crashes the other way around :).

I should write a TTCN-3 test first to cover this.

#4 - 04/15/2019 07:26 AM - laforge

#5 - 05/03/2019 09:25 AM - manatails

lynxis wrote:

Can you create a backtrace when this problem happens (gdb cli: bt). It would be also nice if you can provide a pcap trace. I would guess this problem happens when a MS/UE moves from 3G to 2G. Not sure if the SGSN also crashes the other way around :).
2G->3G backtrace

08/07/2021

2/5
I've tested the ttcn3 branch laforge/iu, rebased it and pushed to gerrit as lynxis/sgsn_iu
Next step is writing a testcase:

- do a gmm attach via geran
- do a LU via lups

GMM Attach via Iu succeed (with a connection close patch).

I could reproduce the crash geran -> utran

IMHO, gsm48_rx_gmm_ra_upd_req() needs to be refactored. It does not check whether the received msgb actually contains any data (like we do in OsmoMSC), so sending an incorrect / incomplete message would crash OsmoSGSN.

is there any status update on this one? How did you handle this at CCCamp2019? I think this is a rather important bug to resolve, if possible without rewriting all of the SGSN :)

I think I saw some related patches in osmo-sgsn.git branch "cccamp2019" and they will be submitted soon, probably after refactoring patches are merged.

I've started refactoring those patches to be mergable.
https://gerrit.osmocom.org/q/topic:%22upstream_camp%22+(status:open%20OR%20status:merged)

- Related to Bug #3995: OsmoSGSN doesn't close SCCP connection after successful LU over IuPS added

is there any status update on this one? How did you handle this at CCCamp2019? I think this is a rather important bug to resolve, if possible without rewriting all of the SGSN :)

I think I saw some related patches in osmo-sgsn.git branch "cccamp2019" and they will be submitted soon, probably after refactoring patches are merged.

I've started refactoring those patches to be mergable.
https://gerrit.osmocom.org/q/topic:%22upstream_camp%22+(status:open%20OR%20status:merged)
Hi lynxis, can you write a short summary on the status of what you did here?

From what I understand, all patches you shared link with are merged except this one which is not ready yet: 
https://gerrit.osmocom.org/c/osmo-sgsn/+/15487

You added SGSN_Tests_Iu to osmo-ttcn3-hacks.git, and it currently is running only one test (TC_iu_attach) in jenkins dockerized setup, which is passing fine.

I see then that there’s also more tests not enabled by default in SGSN_Tests_Iu.ttcn's control(), which probably are the tests you were using to test the patch that was yet not merged and which is expected to support ran swapping:
TC_iu_attach_geran_rau
TC_geran_attach_iu_rau

Can you share your thoughts if I'm missing something?

#21 - 01/21/2020 05:32 PM - daniel

I looked at the patches mentioned and I think the one that would fix this issue is: 
https://gerrit.osmocom.org/c/osmo-sgsn/+/15487 which is still WIP

#22 - 01/21/2020 06:19 PM - lynxis

pespin The only parts missing, is resolv your comments and take a look if the outcommend test cases now succeed.

#23 - 01/21/2020 06:46 PM - daniel

- Status changed from Stalled to In Progress
- Assignee changed from sysmocom to daniel

Okay, I cherry-picked it to master and am testing with the disabled tests now. Will look at the review comments as well.

#24 - 01/21/2020 07:08 PM - daniel

Some improvements - the SGSN doesn't crash anymore and one of the tests passes:

```
<testcase classname='SGSN_Tests_Iu' name='TC_iu_attach_geran_rau' time='2.081220'/>
<testcase classname='SGSN_Tests_Iu' name='TC_geran_attach_iu_rau' time='2.093987'>
<error type='DTE'></error>
</testcase>
```

#25 - 01/22/2020 05:34 PM - daniel

- % Done changed from 50 to 60

Both tests pass sometimes. The failure seems to be an issue with shutting down the test. Sometimes the RAU Accept is being sent on a closed port/connection after the test has passed. It seems when getting a SecurityModeCmd the function f_routing_area_update doesn't wait for the RAU accept, but returns after receiving the Command.
See change https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/16983 for a fix

#26 - 01/30/2020 05:04 PM - daniel
- % Done changed from 60 to 80

A bit back and forth about the proper way to address this issue, but there is progress.

See https://gerrit.osmocom.org/q/topic:%22OS%25233727%22+(status:open%20OR%20status:merged) for a list of changes related to this issue

#27 - 02/07/2020 09:30 AM - daniel
- Status changed from In Progress to Resolved
- % Done changed from 80 to 100

The important patches, notably https://gerrit.osmocom.org/c/osmo-sgsn/+/15487 got merged.

The one remaining change https://gerrit.osmocom.org/c/osmo-sgsn/+/17080 is not really relevant to this segfault, so closing this issue.