OsmoSGSN - Bug #2955

No GMM ATTACH REJECT on GSUP UpdateLocation Error

02/17/2018 08:30 AM - laforge

Status:	New	**Start date:**	02/17/2018
Priority:	High	**Due date:**	
Assignee:	lynxis	**% Done:**	0%
Category:	GSUP interface		
Target version:			
Spec Reference:			

Description

When the HLR responds with a UpdateLocation Error during AttachRequest processing, OsmoSGSN doesn't send the expected GMM ATTACH REJECT to the MS:

```
Sat Feb 17 09:28:05 2018 DLLC <0012> gprs_llc.c:526 LLC RX: unknown TLLI 0xd5390b4c, creating LLME
 on the fly
Sat Feb 17 09:28:05 2018 DLLC <0012> gprs_llc_parse.c:81 LLC SAPI=1 C   U GEA0 IOV-UI=0x000000 FCS
=0x24bf94 CMD=UI DATA
Sat Feb 17 09:28:05 2018 DMM <0002> gprs_gmm.c:1271 MM(---/ffffffff) -> GMM ATTACH REQUEST MI(2624
20000000006) type="GPRS attach"
Sat Feb 17 09:28:05 2018 DMM <0002> gprs_sgsn.c:237 MM(/00000000) Allocated with GEA0 cipher.
Sat Feb 17 09:28:05 2018 DLGLOBAL <001d> rate_ctr.c:218 counter group 'sgsn:mmctx' already exists
 for index 0, instead using index 2. This is a software bug that needs fixing.
Sat Feb 17 09:28:05 2018 DMM <0002> gprs_gmm.c:556 MM(262420000000006/d724f6f6) <- GPRS IDENTITY R
EQUEST: mi_type=IMEI
Sat Feb 17 09:28:05 2018 DLLC <0012> gprs_llc_parse.c:81 LLC SAPI=1 C   U GEA0 IOV-UI=0x000000 FCS
=0x612fca CMD=UI DATA
Sat Feb 17 09:28:05 2018 DMM <0002> gprs_gmm.c:1194 MM(262420000000006/d724f6f6) -> GMM IDENTITY R
ESPONSE: MI(IMEI)=499990000000006
Sat Feb 17 09:28:05 2018 DMM <0002> sgsn_auth.c:160 MM(262420000000006/d724f6f6) Requesting author
ization
Sat Feb 17 09:28:05 2018 DMM <0002> sgsn_auth.c:185 MM(262420000000006/d724f6f6) Requesting authen
tication tuples
Sat Feb 17 09:28:05 2018 DMM <0002> gprs_subscriber.c:894 MM(262420000000006/d724f6f6) Requesting
 subscriber authentication info
Sat Feb 17 09:28:05 2018 DMM <0002> gprs_sgsn.c:726 MM(262420000000006/d724f6f6) Subscriber data u
pdate
Sat Feb 17 09:28:05 2018 DMM <0002> sgsn_auth.c:219 MM(262420000000006/d724f6f6) Updating authoriz
ation (unknown -> authenticate)
Sat Feb 17 09:28:05 2018 DMM <0002> sgsn_auth.c:248 MM(262420000000006/d724f6f6) Got authorization
 update: state unknown -> authenticate
Sat Feb 17 09:28:05 2018 DMM <0002> gprs_gmm.c:591 MM(262420000000006/d724f6f6) <- GPRS AUTH AND C
IPHERING REQ (rand = ba fd 0b 20 23 9b 1b c5 be 69 09 8c 8e d2 c6 e8 )
Sat Feb 17 09:28:05 2018 DLLC <0012> gprs_llc_parse.c:81 LLC SAPI=1 C   U GEA0 IOV-UI=0x000000 FCS
=0xeb6e08 CMD=UI DATA
Sat Feb 17 09:28:05 2018 DMM <0002> gprs_gmm.c:731 MM(262420000000006/d724f6f6) -> GPRS AUTH AND C
IPH RESPONSE
Sat Feb 17 09:28:05 2018 DMM <0002> gprs_gmm.c:778 MM(262420000000006/d724f6f6) checking auth: rec
eived GSM SRES = 4f 30 2f 17
Sat Feb 17 09:28:05 2018 DMM <0002> sgsn_auth.c:160 MM(262420000000006/d724f6f6) Requesting author
ization
Sat Feb 17 09:28:05 2018 DMM <0002> sgsn_auth.c:196 MM(262420000000006/d724f6f6) Missing informati
on, requesting subscriber data
Sat Feb 17 09:28:05 2018 DMM <0002> gprs_subscriber.c:869 MM(262420000000006/d724f6f6) Requesting
 subscriber data update
Sat Feb 17 09:28:05 2018 DGPRS <000f> gprs_subscriber.c:539 SUBSCR(262420000000006) GPRS update lo
cation failed, GMM cause = 'Network failure' (17)
Sat Feb 17 09:28:05 2018 DMM <0002> gprs_sgsn.c:726 MM(262420000000006/d724f6f6) Subscriber data u
pdate
Sat Feb 17 09:28:05 2018 DMM <0002> sgsn_auth.c:219 MM(262420000000006/d724f6f6) Updating authoriz
ation (authenticate -> authenticate)
Sat Feb 17 09:28:35 2018 DLINP <001f> input/ipa.c:67 connection closed with server
```

```
Sat Feb 17 09:28:45 2018 DLGSUP <0027> gsup_client.c:76 GSUP connecting to 127.0.0.1:4222
```

I've created SGSN_Tests.TC_attach_gsup_lu_reject for this.

History

#1 - 05/17/2018 01:57 PM - laforge

- Assignee changed from sysmocom to lynxis

#2 - 04/09/2019 11:24 AM - laforge

- Priority changed from Normal to High

#3 - 04/15/2019 07:34 AM - laforge

#4 - 09/10/2019 07:35 PM - pespin

WIP patch here: https://git.osmocom.org/osmo-sgsn/log/?h=pespin/lu-err-attach-req

So with that patch the GMM Attach accept/reject is delayed until LU is answered. But code in gprs_subscriber.c and sgsn_auth.c doesn't seem to be triggering gsm0408_gprs_access_denied() function which should send:
osmo_fsm_inst_dispatch(ctx->gmm_att_req.fsm, E_REJECT, (void *) (long) gmm_cause);

So at this point neither Accept nor reject is sent.

```
20190910183949075 DGPRS <000e> gprs_subscriber.c:727 SUBSCR(262420000000006) Received GSUP message OSMO_GSUP_M
SGT_SEND_AUTH_INFO_RESULT
20190910183949075 DGPRS <000e> gprs_subscriber.c:247 SUBSCR(262420000000006) Got SendAuthenticationInfoResult,
 num_auth_vectors = 1
20190910183949075 DGPRS <000e> gprs_subscriber.c:259 SUBSCR(262420000000006) Adding auth tuple, cksn = 0
20190910183949075 DGPRS <000e> gprs_subscriber.c:841 SUBSCR(262420000000006) Updating subscriber authenticatio
n info
20190910183949075 DMM <0002> gprs_sgsn.c:800 MM(262420000000006/e703b7d5) Subscriber data update
20190910183949075 DMM <0002> sgsn_auth.c:224 MM(262420000000006/e703b7d5) Updating authorization (unknown -> a
uthenticate)
20190910183949075 DMM <0002> sgsn_auth.c:253 MM(262420000000006/e703b7d5) Got authorization update: state unkn
own -> authenticate
20190910183949075 DMM <0002> gprs_gmm.c:951 GMM_ATTACH_REQ_FSM(gb_gmm_req)[0x55d457e8d250]{AskVLR}: Received E
vent E_VLR_ANSWERED
20190910183949075 DMM <0002> gprs_gmm_attach.c:269 GMM_ATTACH_REQ_FSM(gb_gmm_req)[0x55d457e8d250]{AskVLR}: sta
te_chg to Authenticate
20190910183949075 DMM <0002> gprs_gmm.c:446 MM(262420000000006/e703b7d5) <- GPRS AUTH AND CIPHERING REQ (rand
= 3f 28 6b c5 cf 86 e5 99 9e 11 e3 52
39 dc 78 5b , mmctx_is_r99=0, vec->auth_types=0x1)
20190910183949075 DREF <000d> gprs_subscriber.c:777 subscr 262420000000006 usage decreases to: 1
20190910183949080 DBSSGP <0010> gprs_bssgp.c:396 BSSGP TLLI=0xc45f5aa5 Rx UPLINK-UNITDATA
20190910183949080 DLLC <0011> gprs_llc_parse.c:81 LLC SAPI=1 C   U GEA0 IOV-UI=0x000000 FCS=0xe62da8 CMD=UI DA
TA
20190910183949081 DMM <0002> gprs_gb.c:53 MM_STATE_Gb(0)[0x55d457e916d0]{Idle}: Received Event E_MM_PDU_RECEPT
ION
20190910183949081 DMM <0002> gprs_gmm.c:586 MM(262420000000006/e703b7d5) -> GPRS AUTH AND CIPH RESPONSE
20190910183949081 DMM <0002> gprs_gmm.c:114 MM(262420000000006/e703b7d5) Stopping MM timer 3360 but 0 is runni
ng
20190910183949081 DMM <0002> gprs_gmm.c:633 MM(262420000000006/e703b7d5) checking auth: received GSM SRES = 77
 4b 72 ce
20190910183949081 DMM <0002> gprs_gmm.c:647 GMM_ATTACH_REQ_FSM(gb_gmm_req)[0x55d457e8d250]{Authenticate}: Rece
ived Event E_AUTH_RESP_RECV_SUCCESS
20190910183949081 DMM <0002> gprs_gmm_attach.c:175 MM(262420000000006/e703b7d5) Missing information, requestin
g subscriber data
20190910183949081 DMM <0002> gprs_gmm_attach.c:176 GMM_ATTACH_REQ_FSM(gb_gmm_req)[0x55d457e8d250]{Authenticate
}: state_chg to WaitLocationUpdateResp
20190910183949081 DMM <0002> gprs_subscriber.c:882 MM(262420000000006/e703b7d5) Requesting subscriber data upd
ate
20190910183949081 DREF <000d> gprs_subscriber.c:855 subscr 262420000000006 usage increases to: 2
20190910183949081 DGPRS <000e> gprs_subscriber.c:821 SUBSCR(262420000000006) subscriber data is not available
20190910183949081 DGPRS <000e> gprs_subscriber.c:214 SUBSCR(262420000000006) Sending GSUP, will send: 04 01 08
 62 42 02 00 00 00 00 f6 28 01 01
20190910183949081 DREF <000d> gprs_subscriber.c:889 subscr 262420000000006 usage decreases to: 1
20190910183949081 DLINP <0022> input/ipa.c:139 172.18.8.103:4222 connected write
20190910183949081 DLINP <0022> input/ipa.c:89 172.18.8.103:4222 sending data
20190910183949081 DLINP <0022> input/ipa.c:139 172.18.8.103:4222 connected write
20190910183949081 DLINP <0022> input/ipa.c:89 172.18.8.103:4222 sending data
```

```
20190910183949081 DLINP <0022> input/ipa.c:135 172.18.8.103:4222 connected read
20190910183949081 DLINP <0022> input/ipa.c:56 172.18.8.103:4222 message received
20190910183949081 DREF <000d> gprs_subscriber.c:144 subscr 262420000000006 usage increases to: 2
20190910183949081 DGPRS <000e> gprs_subscriber.c:727 SUBSCR(262420000000006) Received GSUP message OSMO_GSUP_M
SGT_UPDATE_LOCATION_ERROR
20190910183949081 DGPRS <000e> gprs_subscriber.c:533 SUBSCR(262420000000006) Update location has failed with c
ause 17, handled as: No route to host
20190910183949081 DGPRS <000e> gprs_subscriber.c:552 SUBSCR(262420000000006) GPRS update location failed, GMM
cause = 'Network failure' (17)
20190910183949081 DGPRS <000e> gprs_subscriber.c:841 SUBSCR(262420000000006) Updating subscriber authenticatio
n info
20190910183949081 DMM <0002> gprs_sgsn.c:800 MM(262420000000006/e703b7d5) Subscriber data update
20190910183949081 DMM <0002> sgsn_auth.c:224 MM(262420000000006/e703b7d5) Updating authorization (authenticate
 -> authenticate)
```

#5 - 09/10/2019 07:39 PM - pespin

Set a WIP for now:
remote: https://gerrit.osmocom.org/c/osmo-sgsn/+/15476 sgsn_auth: Move UL check to a helper function [WIP]
remote: https://gerrit.osmocom.org/c/osmo-sgsn/+/15477 sgsn: Don't send Attach Accept if initial LU is rejected [WIP]

Files

20180216-sgsn-ul-reject.pcap	2.2 KB	02/17/2018	laforge