OsmoSGSN - Bug #2951

OsmoSGSN Accepts two MO L3 Messages with N(U) set to zero

02/16/2018 04:17 PM - laforge

Status:	Feedback	**Start date:**	02/16/2018
Priority:	Normal	**Due date:**	
Assignee:	osmith	**% Done:**	50%
Category:			
Target version:			
Spec Reference:			

Description

when

- the MS sends its first GMM message "ATTACH REQUEST" in LLC with N(U) set to 0 (expected)
- the SGSN then inquires abou the IMEI using GMM "IDENTITY REQUEST"
- the MS subsequently sends its GMM "IDENTITY RESPONSE" in LLC with N(U) set to 0 again (broken behavior!)

Then OsmoSGSN still accepts that IDENTITY RESPONSE. This is odd. Later on, OsmoSGSN detects duplicate N(U) sequence numbers. But at the initial stage (or maybe when it's 0?) it doesn't detect the duplicate sequence number [which should be dropped].

History

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

- Assignee changed from sysmocom to lynxis

#2 - 11/22/2018 11:04 AM - laforge

- Assignee changed from lynxis to osmith

#3 - 06/17/2019 01:02 PM - osmith

- Status changed from New to In Progress

#4 - 06/19/2019 09:29 AM - osmith

- File TC_attach_pdp_resp_nu_0.pcapng added

- % Done changed from 0 to 50

I've created a TTCN3 test case to reproduce and analyze this issue. The first two times, OsmoSGSN drops the message due to invalid N(U), hits a timeout and sends the identity request again:

```
20190619112529961 DLLC <0011> ../../../../src/osmo-sgsn/src/gprs/gprs_llc.c:858 TLLI=f0f864f2 dropping UI, N(U
=0) not in window V(URV(UR:1).
20190619112535947 DMM <0002> ../../../src/libosmocore/src/fsm.c:284 GMM_ATTACH_REQ_FSM(gb_gmm_req)[0x562334545
b70]{CheckIdentity}: Timeout of T3370
20190619112535947 DMM <0002> ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:565 MM(262420000000002/f0f864f2) <-
 GPRS IDENTITY REQUEST: mi_type=IMEI
```

The third time, it performs recovery handling:

```
/* HACK: non-standard recovery handling.  If remote LLE
 * is re-transmitting the same sequence number for
 * three times, don't discard the frame but pass it on
 * and 'learn' the new sequence number */
```

So this seems to be a feature, not a bug?

WIP test case: https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/14516

laforge: how to proceed here, should we instantly reject N(U) = 0 during identity response messages, because it never makes sense?

Do we have more information about how this issue was discovered?

#5 - 09/11/2019 12:24 PM - osmith

- Status changed from In Progress to Feedback

Files

TC_attach_pdp_resp_nu_0.pcapng	1.27 KB	06/19/2019	osmith