OsmoMSC - Bug #4324

SMS-over-GSUP: inconsistent SM-RP DA/OA coding

12/13/2019 07:08 AM - fixeria

Status:	Resolved	**Start date:**	12/13/2019
Priority:	Low	**Due date:**	
Assignee:	fixeria	**% Done:**	100%
Category:	SMS		
Target version:			
Resolution:		**Spec Reference:**	

Description

The existing TTCN-3 test cases for SMS over GSUP currently do not check the contents of SM-RP DA (Destination Address) and OA (Originating Address) IEs. I did a quick investigation, and as it turns out: in different code parts of OsmoMSC encoding of these IEs is different.

By definition, both DA and OA IEs may contain either of the following identities: IMSI, SMSC Address, MSISDN (that's what we support so fat, there is also LMSI and roaming number). However, unlike IMSI, MSISDN (SMSC Address is also MSISDN) is not just a set of digits. There is also a small (1 octet) header in front containing NPI (Numbering Plan Identification, 4 bit), ToN (Type of Number, 3 bit) and an Extension bit. Thanks to this header, we can have alphanumeric extensions in SMS. The problem is that in some cases OsmoMSC omits that header (I am not even sure if it gets NPI/ToN from the HLR), and sometimes includes the length of the encoded BCD number instead.

Here is what I implemented in TTCN-3:

https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/16565 library/GSUP_Types.ttcn: fix MSISDN / SMSC coding in SM-RP-OA/DA [WIP]
https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/16566 MSC_Tests.ttcn: fix: verify the contents of SM-RP DA/OA for MO SMS

Before I start changing the code in OsmoMSC and fixing the test expectations, let's first discuss the following:

- Should we include the length octet together with MSISDN / SMSC Address? This is what we do for OSMO_GSUP_MSISDN and OSMO_GSUP_IMEI IEs (see records GSUP_MSISDN and GSUP_IMEI respectively), so we can use gsm48_decode_bcd_number2() without messing around with transitional buffer and memcpy(). On the other hand, since SM-RP DA/OA is a TLV, adding an additional L looks redundant to me. We could introduce generic decode_bcd_number() function that would not require the L part (preferred).

- What are the default NPI / ToN values for MSISDNs that we have in OsmoHLR? Can I just use NPI='0001'B (ISDN/Telephony Numbering), ToN='001'B (International Number)?

Related issues:

Related to OsmoMSC - Bug #2883: GSUP encoding of MSISDN is wrong	**New**	**01/26/2018**
Related to Cellular Network Infrastructure - Support #4333: GSUP binary compa...	**Feedback**	**12/16/2019**

History

#1 - 12/14/2019 05:07 AM - fixeria

- Related to Bug #2883: GSUP encoding of MSISDN is wrong added

#2 - 12/15/2019 01:53 PM - fixeria

- Checklist item [ ] OsmoMSC: fix MSISDN encoding for MO SMS added
Checklist item [ ] Check SM-RP-DA/OA in the existing TTCN-3 test cases added
Checklist item [ ] Update the Wireshark dissector to show ToN/NPI added
Checklist item [ ] Update GSUP documentation added

- Status changed from New to Feedback

- % Done changed from 0 to 60

https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/16597 MSC/BSC_ConnectionHandler: only keep SMSC address in SmsParametersRp
https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/16565 library/GSUP_Types.ttcn: fix MSISDN / SMSC coding in SM-RP-OA/DA
https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/16566 MSC_Tests.ttcn: fix: verify the contents of SM-RP-DA/OA for MO/MT SMS

This patch set reveals the problem of MSISDN coding during MO SMS forwarding.

#3 - 12/16/2019 01:57 PM - neels

This also relates to the OSMO_GSUP_MSISDN_IE. We should consider also making that able to transport the ToN/NPI.
But in this issue, you are talking only about the OA and DA, right?

I am wondering whether there is a backwards compatible way to change the coding.
Do ToN/NPI numbers start with some nibble or byte like 0xf that never appears in plain MSISDN?
I guess not...

I know, we can fairly easily adjust the SMS coding, because AFAIK no-one is using it yet (or is there someone)?
But I think it would be good to discuss binary compat in GSUP in general.

Added #4333 to discuss that.

#4 - 12/16/2019 01:57 PM - neels

- Related to Support #4333: GSUP binary compatibility: add GSUP protocol version IE? added

#5 - 12/18/2019 01:14 AM - fixeria

Hi Neels!

> But in this issue, you are talking only about the OA and DA, right?

Yep, and I also think the ToN/NPI header should be a part of 'generic' MSISDN IE. For SMS it's a bit more critical, because alphanumeric MSISDNs in general used quite often (e.g. 2FA services). I have never seen a call from alphanumeric MSISDNs though ;)

> Do ToN/NPI numbers start with some nibble or byte like 0xf that never appears in plain MSISDN?
> I guess not...

I also don't think so. See https://osmocom.org/issues/2883#note-3 for all possible values.

> I am wondering whether there is a backwards compatible way to change the coding.
> I know, we can fairly easily adjust the SMS coding, because AFAIK no-one is using it yet (or is there someone)?

Yep, given that it's already broken. The only potential user I am aware of is efistokl, maybe he has any objections/ideas?

P.S. I wish I had proper TTCN-3 coverage for SM-RP-DA/OA back then, when SMS-over-GSUP was to be merged.

#6 - 12/19/2019 08:02 AM - fixeria

- Checklist item [x] Update GSUP documentation set to Done

https://gerrit.osmocom.org/c/osmo-gsm-manuals/+/16654 chapters/gsup.adoc: further documentation for SM-RP-DA/OA IE coding

#7 - 12/19/2019 08:36 AM - fixeria

- Checklist item [x] OsmoMSC: fix MSISDN encoding for MO SMS set to Done

- % Done changed from 60 to 80

https://gerrit.osmocom.org/c/osmo-msc/+/16655 libmsc/gsm_04_11_gsup.c: fix SM-RP-OA encoding for MO SMS over GSUP

#8 - 01/05/2020 09:48 PM - fixeria

- Checklist item [x] Check SM-RP-DA/OA in the existing TTCN-3 test cases set to Done

- Status changed from Feedback to Stalled

- Priority changed from High to Low

- % Done changed from 80 to 90

Updating Wireshark is the last thing to do.

#9 - 01/06/2020 01:10 AM - fixeria

- Checklist item [x] Update the Wireshark dissector to show ToN/NPI set to Done

- Status changed from Stalled to Resolved

- % Done changed from 90 to 100

https://code.wireshark.org/review/35664 GSUP/SMS: also dissect ToN/NPI header in SM-RP-DA/OA