New issue

Jump to bottom

srsenb can not decode S1AP PAGING #606

Closed **t1412** opened this issue on Dec 10, 2020 · 13 comments

Assignees

Labels bug

t1412 commented on Dec 10, 2020 • edited

Issue Description

[Describe the issue in detail]
We connect srsenb with REAL MME.
MME send S1AP PAGING with IMSI. After received this message, srsenb can not decode it.
enb.log
09:56:56.115863 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/asn1_utils.cc][1023] Decoding failure.
09:56:56.115865 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/s1ap_asn1.cc][32924] Decoding failure.
09:56:56.115882 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/s1ap_asn1.cc][37408] Decoding failure.
09:56:56.115884 [ASN1] [E] This method only supports unpacking up to 32 bits
09:56:56.115885 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/s1ap_asn1.cc][336] Decoding failure.
09:56:56.115887 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/s1ap_asn1.cc][50173] Decoding failure.
09:56:56.115889 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/s1ap_asn1.cc][50346] Decoding failure.
09:56:56.115891 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/s1ap_asn1.cc][56679] Decoding failure.
09:56:56.115893 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/s1ap_asn1.cc][57796] Decoding failure.
09:56:56.115894 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/s1ap_asn1.cc][58730] Decoding failure.
09:56:56.115924 [S1AP] [E] Failed to unpack received PDU

Does srsLTE support this coding Scheme?

Thank you.

andrepuschmann commented on Dec 10, 2020

Hey, thanks for reporting this Please send a S1AP PCAP with the message.

andrepuschmann assigned **frankist** on Dec 10, 2020

andrepuschmann added the bug label on Dec 10, 2020

t1412 commented on Dec 10, 2020 • edited

I attached pcap.
enb_s1ap.zip

Please help to resolve this issue.
Thanks.

andrepuschmann commented on Dec 10, 2020

Thanks, we'll be looking into it.

frankist commented on Dec 11, 2020

I confirm the issue with handling constrained-size octet strings. I provide a fix in the branch `pr_asn1_fix` . Let me know if it solves the problem for you.

t1412 commented on Dec 14, 2020

Thanks, I'll verify it soon

t1412 commented on Dec 15, 2020 • edited

Hi **@frankist** ,

I verified that fixed code is done for decoding, but i got issue when encoding paging message which is sent to UE.

10:51:27.805458 [RRC] [I] Assembled paging for ue_id=723, tti=199
10:51:27.805465 [ASN1] [E] The condition lb <= n <= ub (0 <= 84 <= 9) was not met
10:51:27.805468 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/include/srslte/asn1/asn1_utils.h][981] Encoding failure.
10:51:27.805470 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/rrc_asn1.cc][78920] Encoding failure.
10:51:27.805525 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/rrc_asn1.cc][79003] Encoding failure.
10:51:27.805529 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/include/srslte/asn1/asn1_utils.h][991] Encoding failure.
10:51:27.805531 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/rrc_asn1.cc][79076] Encoding failure.
10:51:27.805533 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/rrc_asn1.cc][79242] Encoding failure.
10:51:27.805534 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/rrc_asn1.cc][79205] Encoding failure.
10:51:27.805536 [ASN1] [E] [/home/tml/workspace/srsLTE/lib/src/asn1/rrc_asn1.cc][79254] Encoding failure.
10:51:27.805538 [RRC] [E] Failed to pack PCCH

Please help to resolve.
Content of S1AP PAGING is same as attached pcap.

t1412 commented on Dec 15, 2020

For more information:

In add_paging_id function:
Test with IMSI = 452040038647507
Current code:

```
if (ue_paging_id.type().value == asn1::s1ap::ue_paging_id_c::types_opts::imsi) {
paging_elem.ue_id.set_imsi();
paging_elem.ue_id.imsi().resize(ue_paging_id.imsi().size());
memcpy(paging_elem.ue_id.imsi().data(), ue_paging_id.imsi().data(), ue_paging_id.imsi().size());
rrc_log->console("Warning IMSI paging not tested\n");
```

With IMSI octet receive from MME:
ue_paging_id.imsi().data() = 54 02 04 30 68 74 05 f7
ue_paging_id.imsi().size() = 8
=> Encoding fail

When I change code (test purpose) to:

```
if (ue_paging_id.type().value == asn1::s1ap::ue_paging_id_c::types_opts::imsi) {
paging_elem.ue_id.set_imsi();
uint8_t test_data[15] = {4,5,2,0,4,0,0,3,8,6,4,7,5,0,7};
paging_elem.ue_id.imsi().resize(15);
memcpy(paging_elem.ue_id.imsi().data(), test_data, 15);
rrc_log->console("Warning IMSI paging not tested\n");
```

=> Endcoding Success

```
11:15:47.507577 [RRC ] [I] Assembled paging for ue_id=723, tti=199
11:15:47.507593 [RRC ] [I] Assembling PCCH payload with 1 UE identities, payload_len=10 bytes, nbits=80
11:15:47.507644 [RRC ] [D] PCCH-Message - Tx paging (10 B)
0000: 40 19 45 20 40 03 86 47 50 70
11:15:47.507667 [RRC ] [D] Content:
[
{
"PCCH-Message": {
"message": {
"c1": {
"paging": {
"pagingRecordList": [
{
"ue-Identity": {
"imsi": [
4,
5,
2,
0,
4,
0,
0,
3,
8,
6,
4,
7,
5,
0,
7
]
},
"cn-Domain": "ps"
}
]
}
}
}
}
}
]
```

mynameismikemike commented on May 9, 2021

@frankist I think I am seeing a similar issue with the S1SetupResponse even using the pr_asn1_fix branch :/

---cut--
00:50:14.509585 [S1AP] [I] Received S1AP PDU
0000: 20 11 00 24 00 00 03 00 3d 40 09 80 07 6d 6d 65
0010: 5f 73 76 63 00 69 00 0b 00 00 00 f1 10 00 00 0b
00:50:14.509619 [ASN1] [E] Extension of PrintableString not supported
00:50:14.509628 [PHY0] [D] [2792] Setting TTI=2794, tx_mutex=2, tx_time=4:0.298741 to worker 0
00:50:14.509632 [ASN1] [E] [/home/mike/srs_fix/srsRAN/lib/src/asn1/s1ap_asn1.cc][40908] Decoding failure.
00:50:14.509636 [ASN1] [E] This method only supports unpacking up to 32 bits
00:50:14.509642 [ASN1] [E] [/home/mike/srs_fix/srsRAN/lib/src/asn1/s1ap_asn1.cc][336] Decoding failure.
00:50:14.509661 [PHY0] [D] [2794] Worker 0 running
00:50:14.509669 [ASN1] [E] [/home/mike/srs_fix/srsRAN/lib/src/asn1/s1ap_asn1.cc][51713] Decoding failure.
00:50:14.509675 [ASN1] [E] [/home/mike/srs_fix/srsRAN/lib/src/asn1/s1ap_asn1.cc][51810] Decoding failure.
00:50:14.509678 [ASN1] [E] [/home/mike/srs_fix/srsRAN/lib/src/asn1/s1ap_asn1.cc][57374] Decoding failure.
00:50:14.509683 [ASN1] [E] This method only supports unpacking up to 32 bits
00:50:14.509688 [ASN1] [E] [/home/mike/srs_fix/srsRAN/lib/src/asn1/s1ap_asn1.cc][58539] Decoding failure.
00:50:14.509703 [ASN1] [E] [/home/mike/srs_fix/srsRAN/lib/src/asn1/s1ap_asn1.cc][58732] Decoding failure.
00:50:14.509706 [S1AP] [E] Failed to unpack received PDU
---cut---

Thoughts? (sorry, I'm new to github)

frankist commented on May 27, 2021 • edited

Hey, have you tried the newer release? There were some fixes in the ASN1 library.

mynameismikemike commented on May 27, 2021 • edited

Thank you for your response **@frankist**. I just attempted with Version 21.4.0:

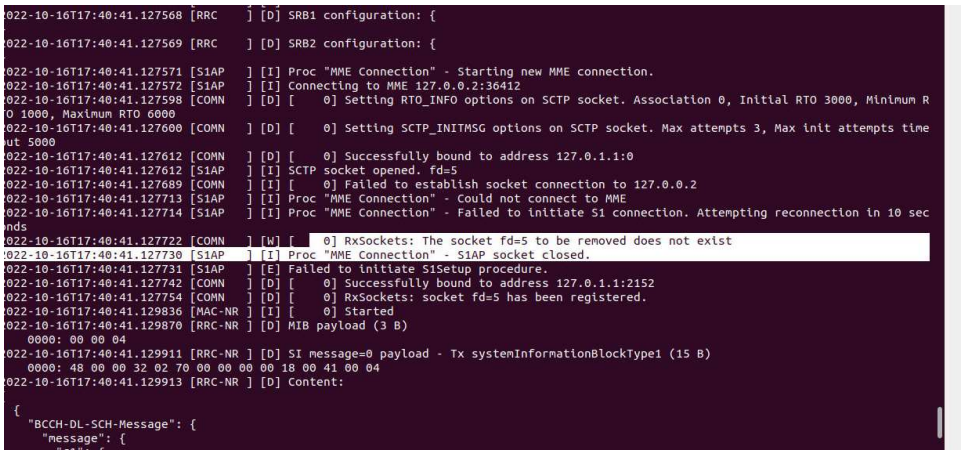
---cut---
20:33:39.269675 [ENB] [I] Using binary srsenb with arguments:
20:33:39.269870 [ENB] [I] Built in Release mode using commit `89f16ee` on branch master.
20:33:41.838901 [COMN] [D] [0] Setting RTO_INFO options on SCTP socket. Association 0, Initial RTO 3000, Minimum RTO 1000, Maximum RTO 6000
20:33:41.838915 [COMN] [D] [0] Setting SCTP_INITMSG options on SCTP socket. Max attempts 3, Max init attempts timeout 5000
20:33:41.899003 [COMN] [D] [0] RxSockets: socket fd=15 has been registered.
20:33:41.899135 [COMN] [D] [0] RxSockets: socket fd=16 has been registered.
20:33:41.902994 [ASN1] [E] [0] Extension of PrintableString not supported
20:33:41.903007 [ASN1] [E] [0] [/home/mike/srsRAN_latest/srsRAN/lib/src/asn1/s1ap.cc][47482] Decoding failure.
20:33:41.903009 [ASN1] [E] [0] This method only supports unpacking up to 32 bits
20:33:41.903010 [ASN1] [E] [0] [/home/mike/srsRAN_latest/srsRAN/lib/src/asn1/s1ap.cc][200] Decoding failure.
20:33:41.903010 [ASN1] [E] [0] [/home/mike/srsRAN_latest/srsRAN/lib/src/asn1/s1ap.cc][59396] Decoding failure.
20:33:41.903011 [ASN1] [E] [0] [/home/mike/srsRAN_latest/srsRAN/lib/src/asn1/s1ap.cc][59493] Decoding failure.
20:33:41.903012 [ASN1] [E] [0] [/home/mike/srsRAN_latest/srsRAN/lib/src/asn1/s1ap.cc][65396] Decoding failure.
20:33:41.903012 [ASN1] [E] [0] This method only supports unpacking up to 32 bits
20:33:41.903013 [ASN1] [E] [0] [/home/mike/srsRAN_latest/srsRAN/lib/src/asn1/s1ap.cc][66623] Decoding failure.
20:33:41.903014 [ASN1] [E] [0] [/home/mike/srsRAN_latest/srsRAN/lib/src/asn1/s1ap.cc][66831] Decoding failure.
20:33:41.903015 [S1AP] [E] Failed to unpack received PDU
0000: 20 11 00 24 00 00 03 00 3d 40 09 80 07 6d 6d 65
0010: 5f 73 76 63 00 69 00 0b 00 00 00 f1 10 00 00 0b
20:33:47.063625 [S1AP] [E] Proc "MME Connection" - S1Setup failed.
---cut---

Thoughts?

Thanks again!

sareek commented on Oct 16, 2022

Have anybody resolved this issue yet. Coz I am also facing something similar,



andrepuschmann commented on Oct 16, 2022

> Have anybody resolved this issue yet. Coz I am also facing something similar,

```
2022-10-16T17:40:41.127568 [RRC    ] [D] SRB1 configuration: {

2022-10-16T17:40:41.127569 [RRC    ] [D] SRB2 configuration: {

2022-10-16T17:40:41.127571 [S1AP   ] [I] Proc "MME Connection" - Starting new MME connection.
2022-10-16T17:40:41.127572 [S1AP   ] [I] Connecting to MME 127.0.0.2:36412
2022-10-16T17:40:41.127598 [COMN   ] [D] [    0] Setting RTO_INFO options on SCTP socket. Association 0, Initial RTO 3000, Minimum R
TO 1000, Maximum RTO 6000
2022-10-16T17:40:41.127600 [COMN   ] [D] [    0] Setting SCTP_INITMSG options on SCTP socket. Max attempts 3, Max init attempts time
out 5000
2022-10-16T17:40:41.127612 [COMN   ] [D] [    0] Successfully bound to address 127.0.1.1:0
2022-10-16T17:40:41.127612 [S1AP   ] [I] SCTP socket opened. fd=5
2022-10-16T17:40:41.127689 [COMN   ] [I] [    0] Failed to establish socket connection to 127.0.0.2
2022-10-16T17:40:41.127713 [S1AP   ] [I] Proc "MME Connection" - Could not connect to MME
2022-10-16T17:40:41.127714 [S1AP   ] [I] Proc "MME Connection" - Failed to initiate S1 connection. Attempting reconnection in 10 sec
onds
2022-10-16T17:40:41.127722 [COMN   ] [W] [    0] RxSockets: The socket fd=5 to be removed does not exist
2022-10-16T17:40:41.127730 [S1AP   ] [I] Proc "MME Connection" - S1AP socket closed.
2022-10-16T17:40:41.127731 [S1AP   ] [E] Failed to initiate S1Setup procedure.
2022-10-16T17:40:41.127742 [COMN   ] [D] [    0] Successfully bound to address 127.0.1.1:2152
2022-10-16T17:40:41.127754 [COMN   ] [D] [    0] RxSockets: socket fd=5 has been registered.
2022-10-16T17:40:41.129836 [MAC-NR ] [I] [    0] Started
2022-10-16T17:40:41.129870 [RRC-NR ] [D] MIB payload (3 B)
   0000: 00 00 04
2022-10-16T17:40:41.129911 [RRC-NR ] [D] SI message=0 payload - Tx systemInformationBlockType1 (15 B)
   0000: 48 00 00 32 02 70 00 00 00 00 18 00 41 00 04
2022-10-16T17:40:41.129913 [RRC-NR ] [D] Content:

 {
   "BCCH-DL-SCH-Message": {
     "message": {
```

This is just an unfinished S1 Setup procedure. Check your IPs are right. It has nothing to do with the S1AP paging issue.

@mynameismikemike
Just reviewing the thread an it seems there are no new PCAP captures after the various ASN1 fixes have been merged.

> 20:33:41.903015 [S1AP] [E] Failed to unpack received PDU
> 0000: 20 11 00 24 00 00 03 00 3d 40 09 80 07 6d 6d 65
> 0010: 5f 73 76 63 00 69 00 0b 00 00 00 f1 10 00 00 0b

The issue here is that the logged message is not complete. Its cut after 32 Bytes.

Since the issue is already quite old I am going to close it assuming that it's not present in the newest ASN1 unpacking code. If it does still exist, please feel free to reopen again and provide full logs or PCAPs.

Thanks

 **andrepuschmann** closed this as completed on Oct 16, 2022

---

sareek commented on Oct 17, 2022

> unfinished S1 Setup procedure. Check your IPs are right

@andrepuschmann i believe i have set ip addresses correctly. Also, epc log says sending S1 setup response but enb is not able to connect.

```
HSS Initialized.
MME S11 Initialized
MME GTP-C Initialized
MME Initialized. MCC: 0xf001, MNC: 0xff01
SPGW GTP-U Initialized.
SPGW S11 Initialized.
SP-GW Initialized.
Received S1 Setup Request.
S1 Setup Request - eNB Name: enb1, eNB id: 0x19b
S1 Setup Request - MCC:001, MNC:01
S1 Setup Request - TAC 7, B-PLMN 0xf110
S1 Setup Request - Paging DRX v128
Sending S1 Setup Response
```

Where do i need to make change exactly?
epc config

```
 9 # mcc:                  Mobile Country Code
10 # mnc:                  Mobile Network Code
11 # mme_addr:             IP address of MME for S1 connnection
12 # gtp_bind_addr:        Local IP address to bind for GTP connection
13 # gtp_advertise_addr:   IP address of eNB to advertise for DL GTP-U Traffic
14 # s1c_bind_addr:        Local IP address to bind for S1AP connection
15 # s1c_bind_port:        Source port for S1AP connection (0 means any)
16 # n_prb:                Number of Physical Resource Blocks (6,15,25,50,75,100)
17 # tm:                   Transmission mode 1-4 (TM1 default)
18 # nof_ports:            Number of Tx ports (1 port default, set to 2 for TM2/3/4)
19 #
20 ######################################################################
21 [enb]
22 enb_id = 0x19B
23 mcc = 001
24 mnc = 01
25 mme_addr = 127.0.1.100
26 gtp_bind_addr = 127.0.1.1
27 s1c_bind_addr = 127.0.1.1
28 s1c_bind_port = 0
29 n_prb = 50
30 #tm = 4
31 #nof_ports = 2
32
33 ######################################################################
34 # eNB configuration files
35 #
36 # sib_config:  SIB1, SIB2 and SIB3 configuration file
```

enb config

```
23 #####################################################################
24 [mme]
25 mme_code = 0x1a
26 mme_group = 0x0001
27 tac = 0x0007
28 mcc = 001
29 mnc = 01
30 mme_bind_addr = 127.0.1.100
31 apn = srsapn
32 dns_addr = 8.8.8.8
33 encryption_algo = EEA0
34 integrity_algo = EIA1
35 paging_timer = 2
36 request_imeisv = false
37
38 #####################################################################
39 # HSS configuration
40 #
41 # db_file:         Location of .csv file that stores UEs information.
42 #
43 #####################################################################
44 [hss]
45 db_file = user_db.csv
46
47 #####################################################################
48 # SP-GW configuration
49 #
50 # gtpu_bind_addr:   GTP-U bind address.
51 # sgi_if_addr:      SGi TUN interface IP address.
```

Thanks

SitrakaResearchAndPOC mentioned this issue 4 minutes ago

CMAS unsuccessful SitrakaResearchAndPOC/srsLTE_CMAS_ETWS_Hacking#1 Open

Assignees


frankist

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants