OsmoPCU - Bug #5205
Crash: SEGV on current master 945be910

08/06/2021 04:35 PM - iedemam

Status: New
Priority: High
Assignee: neels
Category: Spec Reference:
Target version:
Spec Reference:

Description
Let me know if I can provide any additional information. Thanks!

Log Tail

08/08/2021
```plaintext
08/08/2021

0002> pdch_ul_controller.c:315 PDCH(bts=0, trx=1, ts=6) Expiring FN=2006368 but previous FN=2006359 is still reserved!
0002> pdch_ul_controller.c:315 PDCH(bts=0, trx=1, ts=6) Expiring FN=2006368 but previous FN=2006363 is still reserved!
0002> pdch_ul_controller.c:315 PDCH(bts=0, trx=1, ts=4) Expiring FN=2006372 but previous FN=2006368 is still reserved!
0002> pdch_ul_controller.c:315 PDCH(bts=0, trx=1, ts=7) Expiring FN=2006376 but previous FN=2006372 is still reserved!
0002> pdch_ul_controller.c:329 PDCH(bts=0, trx=1, ts=7) Timeout for registered POLL (FN=2006372): TBF(TFI=0 TLLI=0x7d36bb1f DIR=UL STATE=ASSIGN)
0008> tbf.cpp:629 TBF(TFI=0 TLLI=0x7d36bb1f DIR=UL STATE=ASSIGN) poll timeout for FN=2006372, TS=7 (curr FN 2006376)
0008> tbf.cpp:407 TBF(TFI=0 TLLI=0x7d36bb1f DIR=UL STATE=ASSIGN) N3105 exceeded MAX (8)
0008> ./tbf.h:376 TBF(DL-TFI_9)[7bff80]{ASSIGN}: transition to state ASSIGN not permitted!
0002> pdch_ul_controller.c:315 PDCH(bts=0, trx=1, ts=7) Expiring FN=2006394 but previous FN=2006376 is still reserved!
0002> pdch_ul_controller.c:329 PDCH(bts=0, trx=1, ts=7) Timeout for registered POLL (FN=2006394): TBF(TFI=8 TLLI=0x7f818670 DIR=UL STATE=FLOW EGPRS)
0008> tbf.cpp:629 TBF(TFI=8 TLLI=0x7f818670 DIR=UL STATE=FLOW EGPRS) poll timeout for FN=2006376, TS=4 (curr FN 2006394)
0008> tbf.cpp:673 TBF(TFI=8 TLLI=0x7f818670 DIR=UL STATE=FLOW EGPRS) Timeout for polling PACKET CONTROL ACK: |Assignment was on PACCH|No uplink data received yet!
0002> pdch_ul_controller.c:315 PDCH(bts=0, trx=1, ts=4) Expiring FN=2006394 but previous FN=2006381 is still reserved!
0002> pdch_ul_controller.c:315 PDCH(bts=0, trx=1, ts=4) Expiring FN=2006394 but previous FN=2006385 is still reserved!
0002> pdch_ul_controller.c:315 PDCH(bts=0, trx=1, ts=4) Expiring FN=2006394 but previous FN=2006389 is still reserved!
0002> pdch_ul_controller.c:159 PDCH(bts=0, trx=1, ts=7) FN=2006415 Failed allocating POLL, all RRBP values are already reserved!
0002> pdch_ul_controller.c:329 PDCH(bts=0, trx=1, ts=7) Timeout for registered POLL (FN=2006394): TBF(TFI=22 TLLI=0x78d1db92 DIR=DL STATE=FLOW EGPRS)
0008> tbf.cpp:629 TBF(TFI=22 TLLI=0x78d1db92 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=2006394, TS=7 (curr FN 2006398)
0008> tbf.cpp:699 TBF(TFI=22 TLLI=0x78d1db92 DIR=DL STATE=FLOW EGPRS) Timeout for polling PACKET DOWNLINK ACK: |Assignment was on PACCH|Downlink ACK was received|
0008> tbf.cpp:407 TBF(TFI=22 TLLI=0x78d1db92 DIR=DL STATE=FLOW EGPRS) N3105 exceeded MAX (8)
0002> pdch_ul_controller.c:159 PDCH(bts=0, trx=1, ts=7) FN=2006420 Failed allocating POLL, all RRBP values are already reserved!
0002> gprs_rlcmac_ts_alloc.cpp:610 No TFI available (suggested TRX: -1).
0008> tbf.cpp:746 TBF(TFI=0 TLLI=0xb2be855e DIR=DL STATE=NULL EGPRS) Timeslot Allocation failed: trx = -1, single_slot = 1
0008> tbf_dl.cpp:263 MS(TLLI=0xb2be855e, IMSI=000, TA=0, 12/12,) No PDCH resource
0002> pdch_ul_controller.c:159 PDCH(bts=0, trx=1, ts=7) FN=2006424 Failed allocating POLL, all RRBP values are already reserved!
0008> tbf.cpp:458 TBF(TFI=5 TLLI=0xf4297700 DIR=DL STATE=WAIT_RELEASE EGPRS) T3193 timeout expired, freeing TBF
0008> tbf.cpp:458 TBF(TFI=5 TLLI=0xf4297700 DIR=DL STATE=WAIT_RELEASE EGPRS) T3193 timeout expired, freeing TBF
0002> pdch_ul_controller.c:159 PDCH(bts=0, trx=1, ts=7) FN=2006428 Failed allocating POLL, all RRBP values are already reserved!
0002> pdch_ul_controller.c:315 PDCH(bts=0, trx=1, ts=7) Expiring FN=2006428 but previous FN=2006411 is still reserved!
0002> pdch_ul_controller.c:315 PDCH(bts=0, trx=1, ts=7) Expiring FN=2006428 but previous FN=2006407 is still reserved!
0008> tbf.cpp:407 TBF(TFI=10 TLLI=0x78edc326 DIR=UL STATE=FLOW EGPRS) N3101 exceeded MAX (10)
0008> tbf.cpp:458 TBF(TFI=11 TLLI=0xb87baa9l DIR=DL STATE=WAIT_RELEASE) T3193 timeout expired, freeing TBF
0008> tbf.cpp:458 TBF(TFI=11 TLLI=0xb87baa9l DIR=DL STATE=WAIT_RELEASE) T3193 timeout expired, freeing TBF
0002> pdch_ul_controller.c:315 PDCH(bts=0, trx=1, ts=6) Expiring FN=2006428 but previous FN=2006372 is still reserved!
0002> gprs_rlcmac_ts_alloc.cpp:776 No USF available
0008> tbf.cpp:746 TBF(TFI=0 TLLI=0x7f4888cd DIR=UL STATE=NULL EGPRS) Timeslot Allocation failed: trx = 1, single_slot = 0
```
<0008> tbf_ul.cpp:151 MS (TLLI=0x7f4888cd, IMSI=, TA=0, 12/12,) No PDCH resource
<0002> pdch_ul_controller.c:315 PDCH (bts=0, trx=1, ts=7) Expiring FN=2006428 but previous FN=2006420 is still reserved!
<0008> tbf_ul.cpp:329 PDCH (bts=0, trx=1, ts=7) Expiret FN=2006428 but previous FN=2006420 is still reserved!
<0002> pdch_ul_controller.c:315 PDCH (bts=0, trx=1, ts=7) Expiring FN=2006428 but previous FN=2006424 is still reserved!
<0008> tbf.cpp:629 TBF (TFI=22 TLLI=0x78d1db92) releasing due to PACCH assignment timeout.
<0002> pdch_ul_controller.c:329 PDCH (bts=0, trx=1, ts=7) Timeout for registered POLL (FN=2006420): TBF (TFI=22 TLLI=0x78d1db92 DIR=DL STATE=RELEASING EGPRS)
<0008> tbf.cpp:793 TBF (TFI=0 TLLI=0x7f4888cd DIR=UL STATE=ASSIGN) releasing due to PACCH assignment timeout.
<0002> pdch_ul_controller.c:329 PDCH (bts=0, trx=1, ts=7) Timeout for registered SBA (FN=2006333, TA=0)
<0008> gprs_rlcmac_ts_alloc.cpp:776 No USF available
<0008> tbf.cpp:746 TBF (TFI=0 TLLI=0xa89db400 DIR=UL STATE=NULL) Timeslot Allocation failed: trx = 1, single_slot = 0
<0008> tbf.cpp:793 TBF (TFI=0 TLLI=0xa89db400 DIR=UL STATE=ASSIGN) releasing due to PACCH assignment timeout.
<0002> gprs_rlcmac_ts_alloc.cpp:776 No USF available
<0008> tbf.cpp:746 TBF (TFI=0 TLLI=0xa3ddab60 DIR=UL STATE=NULL EGPRS) Timeslot Allocation failed: trx = 1, single_slot = 0
<0008> tbf.cpp:793 TBF (TFI=0 TLLI=0xa3ddab60 DIR=UL STATE=ASSIGN) releasing due to PACCH assignment timeout.
<0002> gprs_rlcmac_ts_alloc.cpp:776 No USF available
<0008> tbf.cpp:746 TBF (TFI=0 TLLI=0xbd18e600 DIR=UL STATE=NULL EGPRS) Timeslot Allocation failed:trx = 1, single_slot = 0
<0008> tbf.cpp:793 TBF (TFI=0 TLLI=0xbd18e600 DIR=UL STATE=ASSIGN) releasing due to PACCH assignment timeout.
<0002> gprs_rlcmac_ts_alloc.cpp:776 No USF available
<0008> tbf.cpp:746 TBF (TFI=0 TLLI=0x7f818670 DIR=UL STATE=NULL EGPRS) Timeslot Allocation failed:trx = 1, single_slot = 0
<0008> tbf.cpp:793 TBF (TFI=0 TLLI=0x7f818670 DIR=UL STATE=ASSIGN) releasing due to PACCH assignment timeout.
<0002> gprs_rlcmac_ts_alloc.cpp:776 No USF available

Backtrace

Program received signal SIGSEGV, Segmentation fault.
gprs_rlcmac_pdch::rcv_control_egprs_dl_ack_nack (this=this@entry=0x7af720, ack_nack=ack_nack@entry=0x88641b0, fn=fn@entry=2006476, meas=meas@entry=0x7fffffffe2a0) at pdch.cpp:525
525  pdch.cpp: No such file or directory.
 0 gprs_rlcmac_pdch::rcv_control_egprs_dl_ack_nack (this=this@entry=0x7af720, ack_nack=ack_nack@entry=0x88641b0, fn=fn@entry=2006476, meas=meas@entry=0x7fffffffe2a0) at pdch.cpp:525
 1 0x000000000004297c2 in gprs_rlcmac_pdch::rcv_control_block (this=0x7af720, data=0x7fffffffe3f26 "A!\123\376\250\134\002", data_len=<optimized out>, fn=2006476, meas=0x7fffffffe2a0, cs=<optimized out>) at pdch.cpp:845
 2 0x00000000000429e4 in gprs_rlcmac_pdch::rcv_block_gprs (this=this@entry=0x7af720, data=data@entry=0x7fffffffe326 "A!\123\376\250\134\002", data_len=<optimized out>, fn=fn@entry=2006476, meas=meas@entry=0x7fffffffe2a0, cs=<optimized out>) at pdch.cpp:1001
 3 0x0000000000042a14 in gprs_rlcmac_pdch::rcv_block (this=this@entry=0x7af720, data=data@entry=0x7fffffffe326 "A!\123\376\250\134\002", len=<optimized out>, fn=fn@entry=2006476, meas=meas@entry=0x7fffffffe2a0) at pdch.cpp:897
 4 0x0000000000040fefd in pcu_rx_data_ind_ptch (bts=bts@entry=0x7ad200, pdch=pdch@entry=0x7af720, data=data@entry=0x7fffffffe326 "A!\123\376\250\134\002", len=<optimized out>, fn=fn@entry=2006476, meas=meas@entry=0x7fffffffe2a0) at pcu_l1_if.cpp:284
 5 0x00000000000410834 in pcu_rx_data_ind (data_ind=0x7fffffffe326, bts=0x7ad200) at pcu_l1_if.cpp:418
 6 pcu_rx (pcu_prim=pcu_prim@entry=0x7fffffffe320, pcu_prim_len=<optimized out>) at pcu_l1_if.cpp:992
 7 0x00000000000431399 in pcu_sock_read (bfd=<optimized out>) at osmobts_sock.c:156
 8 0x00000000000431585 in pcu_sock_cb (btd=0x6974e0 <pcu_sock_state>, flags=1) at osmobts_sock_c:211

08/08/2021
$1 = \{si_signo = 11, si_errno = 0, si_code = 1, _sifields = \{_pad = \{128672, 0, 160, 0, 70560, 0, 47148128, 0, -1447626532, 32767, 1214498954, 32735, 1, 0, 160, 0, 36003808, 0, 45862720, 0, 44, 0, 6622689, 0, 8149536, 0, 44527648, 0\}, _kill = \{si_pid = 128672, si_uid = 0\}, _timer = \{si_tid = 128672, si_overrun = 0, si_sigval = \{sival_int = 160, sival_ptr = 0xa0\}\}, _rt = \{si_pid = 128672, si_uid = 0, si_signal = \{sival_int = 160, sival_ptr = 0xa0\}\}, _sigchld = \{si_pid = 128672, si_uid = 0, si_status = 160, si_utime = 303052892405760, si_stime = 202499667827621888\}, _sigfault = \{si_addr = 0x1f6a0, _addr_lsb = 160, _addr_bnd = \{lower = 0x113a0, upper = 0x2cf6c60\}\}, _sigpoll = \{si_band = 128672, si_fd = 160\}\}\)

Possible Fix

diff --git a/src/pdch.cpp b/src/pdch.cpp
index 2ec40ce..b4fced7 100644
--- a/src/pdch.cpp
+++ b/src/pdch.cpp
@@ -452,6 +452,7 @@
 return;
 }
 tbf = as_dl_tbf(poll->tbf_poll.poll_tbf);
+if (!tbf) return;
 if (tbf->tfi() != tfi) {
   LOGPTBFDL(tbf, LOGL_NOTICE,
     "PACKET DOWNLINK ACK with wrong TFI=\d, ignoring!\n", tfi);
@@ -522,6 +523,7 @@
 return;
 }
 tbf = as_dl_tbf(poll->tbf_poll.poll_tbf);
+if (!tbf) return;
 if (tbf->tfi() != tfi) {
   LOGPDCH(this, DRLCMAC, LOGL_NOTICE, "EGPRS PACKET DOWNLINK ACK with "
     "wrong TFI=\d, ignoring!\n", tfi);