OsmoBTS - Bug #1898

Wrong handover detection with l1sap on wrong ss=0/ts=0

12/27/2016 12:24 PM - zecke

Status:	Feedback	**Start date:**	12/27/2016
Priority:	Low	**Due date:**	
Assignee:		**% Done:**	50%
Category:			
Target version:			
Spec Reference:			

Description

So handover being detected on TS=0, SS=0... which is unlikely to be the right channel.. Need input validation and checking if the channel is allocated? But verify it.. not sure why it detects it like that.. Happens frequently at the 33C3

```
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<0006> l1_if.c:700 SACCH for pchan 9?
<000a> handover.c:111 (bts=0,trx=0,ts=0,ss=0) RACH on dedicated channel received with TA=0
<0007> l1sap.c:1205 modifying channel chan_nr=0x20 trx=0
<000a> oml.c:1852 (bts=0,trx=0,ts=0,ss=0) modifying channel for handover
<0006> oml.c:1077 (bts=0,trx=0,ts=0,ss=0) MPH-ACTIVATE.req (hL2=0x000000bb, SDCCH TxDL)
<0007> l1_if.c:166 Tx L1 prim MPH-ACTIVATE.req
<0000> rsl.c:578 Sending HANDOver DETect

Program received signal SIGSEGV, Segmentation fault.
rslms_rx_rll_udata_req (msg=msg@entry=0xc0748, dl=dl@entry=0xb6fc14b0) at lapdm.c:855
855    lapdm.c: No such file or directory.
(gdb) bt
#0  rslms_rx_rll_udata_req (msg=msg@entry=0xc0748, dl=dl@entry=0xb6fc14b0) at lapdm.c:855
#1  0x4fcacb00 in rslms_rx_rll (lc=0xb6fc133c, msg=0xc0748) at lapdm.c:1154
#2  lapdm_rslms_recvmsg (msg=msg@entry=0xc0748, lc=lc@entry=0xb6fc1294) at lapdm.c:1223
#3  0x000279d4 in ho_tx_phys_info (lchan=lchan@entry=0xb6fc11ec) at handover.c:61
#4  0x00027cbc in handover_rach (lchan=0xb6fc11ec, ra=<optimized out>, acc_delay=acc_delay@entry=0
 '\000') at handover.c:131
#5  0x0002a680 in l1sap_handover_rach (l1sap=<optimized out>, rach_ind=<optimized out>, rach_ind=<
optimized out>,
    rach_ind=<optimized out>, trx=0xb6fbd038) at l1sap.c:659
#6  l1sap_ph_rach_ind (rach_ind=0xbf4fc, l1sap=0xbf4ec, trx=0xb6fbd038) at l1sap.c:974
#7  l1sap_up (trx=trx@entry=0xb6fbd038, l1sap=l1sap@entry=0xbf4ec) at l1sap.c:1022
#8  0x0000d690 in handle_ph_ra_ind (l1p_msg=0xbf428, ra_ind=<optimized out>, fl1=0xbf428) at l1_if
.c:1064
#9  l1if_handle_ind (fl1=<optimized out>, msg=msg@entry=0xbf428) at l1_if.c:1090
#10 0x0000dfc8 in l1if_handle_l1prim (wq=<optimized out>, fl1h=<optimized out>, msg=msg@entry=0xbf
428) at l1_if.c:1144
#11 0x00017e48 in read_dispatch_one (queue=<optimized out>, msg=0xbf428, fl1h=<optimized out>) at
l1_transp_hw.c:190
#12 l1if_fd_cb (ofd=0xb86d0, what=<optimized out>) at l1_transp_hw.c:224
#13 0x4fcd6330 in osmo_fd_disp_fds (_eset=0xbefffb48, _wset=0xbefffac8, _rset=0xbefffa48) at selec
t.c:149
#14 osmo_select_main (polling=polling@entry=0) at select.c:189
```

```
#15 0x0002bf84 in bts_main (argc=<optimized out>, argv=<optimized out>) at main.c:349
#16 0x4fa61684 in __libc_start_main (main=0xbefffd84, argc=1337463808, argv=0x4fa61684 <__libc_sta
rt_main+276>,
    init=<optimized out>, fini=0x2ec70 <__libc_csu_fini>, rtld_fini=0x4fa27dc4 <_dl_fini>, stack_e
nd=0xbefffd84) at libc-start.c:269
#17 0x0000b8a4 in _start () at ../ports/sysdeps/arm/start.S:124
(gdb) frame 5
#5  0x0002a680 in l1sap_handover_rach (l1sap=<optimized out>, rach_ind=<optimized out>, rach_ind=<
optimized out>,
    rach_ind=<optimized out>, trx=0xb6fbd038) at l1sap.c:659
659    l1sap.c: No such file or directory.
#17 0x0000b8a4 in _start () at ../ports/sysdeps/arm/start.S:124
(gdb) frame 5
#5  0x0002a680 in l1sap_handover_rach (l1sap=<optimized out>, rach_ind=<optimized out>, rach_ind=<
optimized out>,
    rach_ind=<optimized out>, trx=0xb6fbd038) at l1sap.c:659
659    l1sap.c: No such file or directory.
(gdb) p lc
No symbol "lc" in current context.
(gdb) p lc^CQuit
(gdb) p *lchan
value has been optimized out
(gdb) p *rach_ind
value has been optimized out
(gdb) p rach_ind->chan_nr
value has been optimized out
(gdb) frame 6
#6  l1sap_ph_rach_ind (rach_ind=0xbf4fc, l1sap=0xbf4ec, trx=0xb6fbd038) at l1sap.c:974
974    in l1sap.c
(gdb) p *rach_ind
$1 = {chan_nr = 64 '@', ra = 0, acc_delay = 0 '\000', fn = 2107, is_11bit = 0 '\000', burst_type =
 GSM_L1_BURST_TYPE_ACCESS_0}
(gdb) frame 3
#3  0x000279d4 in ho_tx_phys_info (lchan=lchan@entry=0xb6fc11ec) at handover.c:61
61    handover.c: No such file or directory.
(gdb) p *lchan
$2 = {ts = 0xb6fc08f8, nr = 0 '\000', type = GSM_LCHAN_SDCCH, rsl_cmode = 0, tch_mode = GSM48_CMOD
E_SIGN, csd_mode = LCHAN_CSD_M_NT,
  state = LCHAN_S_NONE, broken_reason = 0x0, bs_power = 0 '\000', ms_power = 0 '\000', encr = {alg
_id = 0 '\000',
    key_len = 0 '\000', key = '\000' <repeats 15 times>}, mr_ms_lv = "\000\000\000\000\000\000",
  mr_bts_lv = "\000\000\000\000\000\000", sapis = "\000\000\000\000\000\000\000", sacch_deact = 0,
 abis_ip = {bound_ip = 0,
    connect_ip = 0, bound_port = 0, connect_port = 0, conn_id = 0, rtp_payload = 0 '\000', rtp_pay
load2 = 0 '\000',
    speech_mode = 0 '\000', rtp_socket = 0x0}, rqd_ta = 0 '\000', name = 0x6b778 "(bts=0,trx=0,ts=
0,ss=0)", sapi_cmds = {
    next = 0xc0150, prev = 0xc0240}, sapis_dl = '\000' <repeats 22 times>, sapis_ul = '\000' <repe
ats 22 times>, lapdm_ch = {list = {
      next = 0x0, prev = 0x0}, name = 0x0, lapdm_acch = {datalink = {{dl = {send_dlsap = 0x0, send
_ph_data_req = 0x0,
            update_pending_frames = 0x0, cr = {loc2rem = {cmd = 0 '\000', resp = 0 '\000'}, rem2lo
c = {cmd = 0 '\000',
                resp = 0 '\000'}}, mode = LAPD_MODE_USER, use_sabme = 0, reestablish = 0, n200 = 0
, n200_est_rel = 0, lctx = {
              dl = 0x0, n201 = 0, cr = 0 '\000', sapi = 0 '\000', tei = 0 '\000', lpd = 0 '\000',
format = 0 '\000', p_f = 0 '\000',
              n_send = 0 '\000', n_recv = 0 '\000', s_u = 0 '\000', length = 0, more = 0 '\000'},
maxf = 0, k = 0 '\000',
            v_range = 0 '\000', v_send = 0 '\000', v_ack = 0 '\000', v_recv = 0 '\000', state = 0,
 seq_err_cond = 0,
            own_busy = 0 '\000', peer_busy = 0 '\000', t200_sec = 0, t200_usec = 0, t203_sec = 0,
t203_usec = 0, t200 = {node = {
                rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x
0}, timeout = {tv_sec = 0,
                tv_usec = 0}, active = 0, cb = 0x0, data = 0x0}, t203 = {node = {rb_parent_color =
 0, rb_right = 0x0,
```

```
                rb_left = 0x0}, list = {next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec =
0}, active = 0, cb = 0x0,
              data = 0x0}, retrans_ctr = 0 '\000', tx_queue = {next = 0x0, prev = 0x0}, send_queue
 = {next = 0x0, prev = 0x0},
            send_buffer = 0x0, send_out = 0, tx_hist = 0x0, range_hist = 0 '\000', rcv_buffer = 0x
0, cont_res = 0x0}, mctx = {
            dl = 0x0, lapdm_fmt = 0, chan_nr = 0 '\000', link_id = 0 '\000', ta_ind = 0 '\000', tx
_power_ind = 0 '\000'},
          entity = 0x0}, {dl = {send_dlsap = 0x0, send_ph_data_req = 0x0, update_pending_frames =
0x0, cr = {loc2rem = {
                cmd = 0 '\000', resp = 0 '\000'}, rem2loc = {cmd = 0 '\000', resp = 0 '\000'}}, mo
de = LAPD_MODE_USER,
            use_sabme = 0, reestablish = 0, n200 = 0, n200_est_rel = 0, lctx = {dl = 0x0, n201 = 0
, cr = 0 '\000', sapi = 0 '\000',
              tei = 0 '\000', lpd = 0 '\000', format = 0 '\000', p_f = 0 '\000', n_send = 0 '\000'
, n_recv = 0 '\000',
              s_u = 0 '\000', length = 0, more = 0 '\000'}, maxf = 0, k = 0 '\000', v_range = 0 '\
000', v_send = 0 '\000',
            v_ack = 0 '\000', v_recv = 0 '\000', state = 0, seq_err_cond = 0, own_busy = 0 '\000',
 peer_busy = 0 '\000',
            t200_sec = 0, t200_usec = 0, t203_sec = 0, t203_usec = 0, t200 = {node = {rb_parent_co
lor = 0, rb_right = 0x0,
                rb_left = 0x0}, list = {next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec =
0}, active = 0, cb = 0x0,
              data = 0x0}, t203 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, li
st = {next = 0x0, prev = 0x0},
              timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0}, retrans_ctr
= 0 '\000', tx_queue = {
              next = 0x0, prev = 0x0}, send_queue = {next = 0x0, prev = 0x0}, send_buffer = 0x0, s
end_out = 0, tx_hist = 0x0,
            range_hist = 0 '\000', rcv_buffer = 0x0, cont_res = 0x0}, mctx = {dl = 0x0, lapdm_fmt
= 0, chan_nr = 0 '\000',
            link_id = 0 '\000', ta_ind = 0 '\000', tx_power_ind = 0 '\000'}, entity = 0x0}}, last_
tx_dequeue = 0, tx_pending = 0,
      mode = LAPDM_MODE_MS, flags = 0, l1_ctx = 0x0, l3_ctx = 0x0, l1_prim_cb = 0x0, l3_cb = 0x0,
lapdm_ch = 0x0, ta = 0 '\000',
      tx_power = 0 '\000'}, lapdm_dcch = {datalink = {{dl = {send_dlsap = 0x0, send_ph_data_req =
0x0, update_pending_frames = 0x0,
            cr = {loc2rem = {cmd = 0 '\000', resp = 0 '\000'}, rem2loc = {cmd = 0 '\000', resp = 0
 '\000'}}, mode = LAPD_MODE_USER,
            use_sabme = 0, reestablish = 0, n200 = 0, n200_est_rel = 0, lctx = {dl = 0x0, n201 = 0
, cr = 0 '\000', sapi = 0 '\000',
              tei = 0 '\000', lpd = 0 '\000', format = 0 '\000', p_f = 0 '\000', n_send = 0 '\000'
, n_recv = 0 '\000',
              s_u = 0 '\000', length = 0, more = 0 '\000'}, maxf = 0, k = 0 '\000', v_range = 0 '\
000', v_send = 0 '\000',
            v_ack = 0 '\000', v_recv = 0 '\000', state = 0, seq_err_cond = 0, own_busy = 0 '\000',
 peer_busy = 0 '\000',
            t200_sec = 0, t200_usec = 0, t203_sec = 0, t203_usec = 0, t200 = {node = {rb_parent_co
lor = 0, rb_right = 0x0,
                rb_left = 0x0}, list = {next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec =
0}, active = 0, cb = 0x0,
              data = 0x0}, t203 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, li
st = {next = 0x0, prev = 0x0},
              timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0}, retrans_ctr
= 0 '\000', tx_queue = {
              next = 0x0, prev = 0x0}, send_queue = {next = 0x0, prev = 0x0}, send_buffer = 0x0, s
end_out = 0, tx_hist = 0x0,
            range_hist = 0 '\000', rcv_buffer = 0x0, cont_res = 0x0}, mctx = {dl = 0x0, lapdm_fmt
= 0, chan_nr = 0 '\000',
            link_id = 0 '\000', ta_ind = 0 '\000', tx_power_ind = 0 '\000'}, entity = 0x0}, {dl =
{send_dlsap = 0x0,
            send_ph_data_req = 0x0, update_pending_frames = 0x0, cr = {loc2rem = {cmd = 0 '\000',
resp = 0 '\000'}, rem2loc = {
                cmd = 0 '\000', resp = 0 '\000'}}, mode = LAPD_MODE_USER, use_sabme = 0, reestabli
sh = 0, n200 = 0,
            n200_est_rel = 0, lctx = {dl = 0x0, n201 = 0, cr = 0 '\000', sapi = 0 '\000', tei = 0
```

```
'\000', lpd = 0 '\000',
              format = 0 '\000', p_f = 0 '\000', n_send = 0 '\000', n_recv = 0 '\000', s_u = 0 '\0
00', length = 0, more = 0 '\000'},
            maxf = 0, k = 0 '\000', v_range = 0 '\000', v_send = 0 '\000', v_ack = 0 '\000', v_rec
v = 0 '\000', state = 0,
            seq_err_cond = 0, own_busy = 0 '\000', peer_busy = 0 '\000', t200_sec = 0, t200_usec =
 0, t203_sec = 0, t203_usec = 0,
            t200 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {next = 0x
0, prev = 0x0}, timeout = {
                tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0}, t203 = {node = {rb_pa
rent_color = 0, rb_right = 0x0,
                rb_left = 0x0}, list = {next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec =
 0}, active = 0, cb = 0x0,
              data = 0x0}, retrans_ctr = 0 '\000', tx_queue = {next = 0x0, prev = 0x0}, send_queue
 = {next = 0x0, prev = 0x0},
            send_buffer = 0x0, send_out = 0, tx_hist = 0x0, range_hist = 0 '\000', rcv_buffer = 0x
0, cont_res = 0x0}, mctx = {
            dl = 0x0, lapdm_fmt = 0, chan_nr = 0 '\000', link_id = 0 '\000', ta_ind = 0 '\000', tx
_power_ind = 0 '\000'},
          entity = 0x0}}, last_tx_dequeue = 0, tx_pending = 0, mode = LAPDM_MODE_MS, flags = 0, l1
_ctx = 0x0, l3_ctx = 0x0,
      l1_prim_cb = 0x0, l3_cb = 0x0, lapdm_ch = 0x0, ta = 0 '\000', tx_power = 0 '\000'}}, dl_tch_
queue = {next = 0xb6fc16c0,
    prev = 0xb6fc16c0}, si = {valid = 0, last = 0, buf = {'\000' <repeats 22 times> <repeats 24 ti
mes>}}, meas = {flags = 0 '\000',
    res_nr = 0 '\000', bts_tx_pwr = 0 '\000', num_ul_meas = 0 '\000', uplink = {{ber10k = 0, ta_of
fs_qbits = 0, c_i = 0,
        is_sub = 0 '\000', inv_rssi = 0 '\000'} <repeats 104 times>}, l1_info = "\000", ul_res = {
full = {rx_lev = 0 '\000',
        rx_qual = 0 '\000'}, sub = {rx_lev = 0 '\000', rx_qual = 0 '\000'}}}, tch = {amr_mr = {gsm
48_ie = "\000", ms_mode = {{
          mode = 0 '\000', threshold = 0 '\000', hysteresis = 0 '\000'}, {mode = 0 '\000', thresho
ld = 0 '\000',
          hysteresis = 0 '\000'}, {mode = 0 '\000', threshold = 0 '\000', hysteresis = 0 '\000'},
{mode = 0 '\000',
          threshold = 0 '\000', hysteresis = 0 '\000'}}, bts_mode = {{mode = 0 '\000', threshold =
 0 '\000', hysteresis = 0 '\000'},
        {mode = 0 '\000', threshold = 0 '\000', hysteresis = 0 '\000'}, {mode = 0 '\000', threshol
d = 0 '\000',
          hysteresis = 0 '\000'}, {mode = 0 '\000', threshold = 0 '\000', hysteresis = 0 '\000'}},
 num_modes = 0 '\000'}, dtx = {
      dl_amr_fsm = 0x0, cache = '\000' <repeats 19 times>, facch = '\000' <repeats 22 times>, len
= 0 '\000', fn = 0,
      is_update = false, ul_sid = false, dl_active = false}, last_cmr = 0 '\000', last_fn = 0}, ci
ph_state = 0 '\000',
  ciph_ns = 0 '\000', loopback = 0 '\000', ho = {active = 2 '\002', ref = 0 '\000', t3105 = {node
= {rb_parent_color = 0,
        rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv
_usec = 0}, active = 0, cb = 0x0,
      data = 0x0}, phys_info_count = 1}, s = 0, rel_act_kind = 0, rtp_tx_marker = false, ms_power_
ctrl = {current = 0 '\000',
    fixed = 0 '\000'}}
(gdb) frame 4
#4  0x00027cbc in handover_rach (lchan=0xb6fc11ec, ra=<optimized out>, acc_delay=acc_delay@entry=0
 '\000') at handover.c:131
131    in handover.c
(gdb) p ra
$3 = <optimized out>
(gdb)
$4 = <optimized out>
(gdb) c
Continuing.

Program terminated with signal SIGSEGV, Segmentation fault.
The program no longer exists.
(gdb)
```

History

#1 - 12/28/2016 02:57 PM - zecke

- Description updated

#2 - 01/26/2017 06:07 PM - zecke

- Priority changed from Normal to Urgent

#3 - 02/28/2017 03:10 PM - laforge

- Assignee set to msuraev

#4 - 02/28/2017 03:46 PM - msuraev

Is there a way to reproduce this? Some particular phone or config? I can add input validation but would be nicer to digg out the root cause - why it gets detected there in a first place.

#5 - 03/02/2017 11:33 AM - msuraev

- Status changed from New to In Progress

- % Done changed from 0 to 20

Patches are sent for review in gerrit: 1959 should prevent segfault, 1960 checks for appropriate channel type.

#6 - 03/03/2017 12:58 PM - msuraev

https://projects.osmocom.org/projects/openbsc/wiki/Multi-BTS_with_handover - useful docs.

#7 - 03/03/2017 01:38 PM - zecke

> On 2 Mar 2017, at 19:33, msuraev [REDMINE] <redmine@lists.osmocom.org> wrote:
>
> Issue #1898 has been updated by msuraev.
>
> Status changed from New to In Progress
> % Done changed from 0 to 20
>
> Patches are sent for review in gerrit: 1959 should prevent segfault, 1960 checks for appropriate channel type.

the point is that no handover is in progress ;)

#8 - 03/03/2017 02:49 PM - msuraev

zecke wrote:

> the point is that no handover is in progress ;)

Do you have any ideas as to how to provoke this "no handover" situation?

#9 - 03/07/2017 05:15 PM - msuraev

- Status changed from In Progress to Stalled

Gerrit 1960 is under review.

#10 - 03/14/2017 03:00 PM - msuraev

- % Done changed from 20 to 50

Gerrit 1960 has been merged, so in theory it should be enough to workaround this error. However, we still don't know:
- how to reproduce this
- what's causing erroneous HO RACH detection

#11 - 10/16/2017 12:04 PM - msuraev

- Status changed from Stalled to Feedback

Shall we wait for next congress to see if the issue would re-appear?

#12 - 10/21/2017 06:27 PM - laforge

- Assignee deleted (msuraev)

#13 - 11/07/2017 09:54 PM - laforge

- Priority changed from Urgent to Low