

基站下发Msg6消息(鉴权请求)，终端PDSCH解析错误

2025-05-28 10:20 - 白瑞朋

状态:	进行中	开始日期:	2025-05-28
优先级:	普通	计划完成日期:	
指派给:	白瑞朋	% 完成:	0%
类别:		预期时间:	0.00 小时
目标版本:		耗时:	0.00 小时
描述			
【问题描述】 终端进入ACTIVE态后，基站下发鉴权请求消息，UE PDCCH DCI CRC解析OK,PDSCH解析CRC错误。			

历史记录

#1 - 2025-05-28 10:23 - 白瑞朋

- 状态从新建变更为进行中

【问题现象】

- 1.PDSCH获取到的de-ofdm频域数据地址buffer ping-pong取反，导致异常；
- 2.PDSCH获取到错误的频域数据地址后，任务处理超时；

#2 - 2025-05-30 15:30 - 白瑞朋

【问题进展】

- 1.从de-ofdm进行时间统计，未发现任务超时问题；且de-ofdm和PDCCH发给PDSCH的两个slot号可以对上；
- 2.de-ofdm加trace log,监控ping-pong写频域地址buffer，没有发现写错位问题；偶地址：0xa0e0800，奇地址：0x9d94580；

【下一步】

- 1.检查deOfdm-PDCCH-PDSCH接口传递的sfn和slot，看是否有超时或者跳变；
- 2.deOfdm-PDCCH-PDSCH接口的sfn/slot，与PDSCH本地获取的sfn/slot进行对比；

#3 - 2025-05-30 15:52 - 白瑞朋

- 文件PDSCH log.jpg 已添加

#4 - 2025-06-03 19:13 - 赵强

- 文件20250603-190959.jpg 已添加

【问题进展】

- 1.环境存在msg6 CRC ERR的现象。查看log，存在跨帧现象（1024帧后出现帧翻转），怀疑与时序有关，导致数据解不对；

```

[INFO]
pdu_num[1]
sfn[973] slot[0]
pusch_ue_num[1]
rx_ante_num[2]
ofdm_symb_start[0]
numCb[1]
rvIndex[0]
harqProcessID[2]
TBSsize[92]
RNTI[17017]
nIdPusch[41]
qamModOrder[2]
mcsIndex[7]
mcsTable[0]
nrOfLayers[1]
BWFSstart[0]
BWFSsize[273]
initialULBwpSize[273]
rbStart[0]
rbSize[6]
puschDmrsScramblingId[41]
puschDmrsIdentity[41]
dmrsPorts[1]
dmrsConfigType[0]
nSCID[0]
maxLen[3]
StartSymbolIndex[1]
NrOfSymbols[13]
[INFO]pusch_Symbol_Process, start_sym 1, loop_cnt 0, end_symbol
[INFO]pdsch_proc done,slot:1,2 [183]ns
[INFO]crc:0 slot:2 sfn:973
[INFO]send dl tb : 92 to Mac, state:21

[ERR]Data from deofdm: sfn 974 974, slot 0 0, ptr 0xa0e0800
[INFO]pdu_num[1] sfn[974] slot[0] pusch_ue_num[1] rx_ante_num[2]
[INFO]rvIndex[0] harqProcessID[3] TBSsize[46] RNTI[17017] nIdPusch
[INFO]Pusch_Symbol_Process, start_sym 1, loop_cnt 0, end_symbol

30 [INFO]rvIndex[0] harqProcessID[2] TBSsize[88] RNTI[17017] nIdPusch[41] qamMod
31 [INFO]Pusch_Symbol_Process, start_sym 1, loop_cnt 0, end_symbol 6, rx_freqda
32 [INFO]pdsch_proc done,slot:18,19 [123]ns
33
34
35
36 [ERR]Data from deofdm: sfn 3 3, slot 0 0, ptr 0xa0e0800
37 [INFO]
38 pdu_num[1]
39 sfn[3] slot[0]
40 pusch_ue_num[1]
41 rx_ante_num[2]
42 ofdm_symb_start[0]
43 numCb[1]
44 rvIndex[0]
45 harqProcessID[3]
46 TBSsize[46]
47 RNTI[17017]
48 nIdPusch[41]
49 qamModOrder[2]
50 mcsIndex[7]
51 mcsTable[0]
52 nrOfLayers[1]
53 BWFSstart[0]
54 BWFSsize[273]
55 initialULBwpSize[273]
56 rbStart[0]
57 rbSize[3]
58 puschDmrsScramblingId[41]
59 puschDmrsIdentity[41]
60 dmrsPorts[1]
61 dmrsConfigType[0]
62 nSCID[0]
63 maxLen[3]
64 StartSymbolIndex[1]
65 NrOfSymbols[13]
66 [INFO]Pusch_Symbol_Process, start_sym 1, loop_cnt 0, end_symbol 14, rx_freqd
67

```

【下一步】

1.终端与基站侧sfn/slot拉齐进行测试

#5 - 2025-06-03 20:18 - 白瑞朋

【问题进展】

修改基站参数'PDSCH_DMRS附加位置配置'1改为2后，有以下几个现象：

- 1) 有10%概率msg6 CRC可以解对，并上报鉴权TB给协议栈；协议栈收到消息后鉴权失败；
- 2) 核心网增加了UE的op code，待复现后和协议栈继续分析；
- 3) 基站在S-slot调度msg6，CRC必错；
- 4) 基站调度msg6的rbSize<4，CRC必错；

下一步

继续尝试复现分析；

#6 - 2025-06-04 15:38 - 白瑞朋

【问题进展】

协议栈鉴权失败后，会回复鉴权失败给基站，重新做一次鉴权，

下一步需要PHY确认：

- 1) 是否回复msg6的ACK给基站，基站是否收到；
- 2) 是否收到PUSCH的调度信息(解PDCCH的dci0_1)，并解对CRC；(第一个0表示上下行，0：ul；1：dl；第二个1表示coreset，0：公共；1：专有)

#7 - 2025-06-04 15:41 - 白瑞朋

- 文件 鉴权流程.jpg 已添加

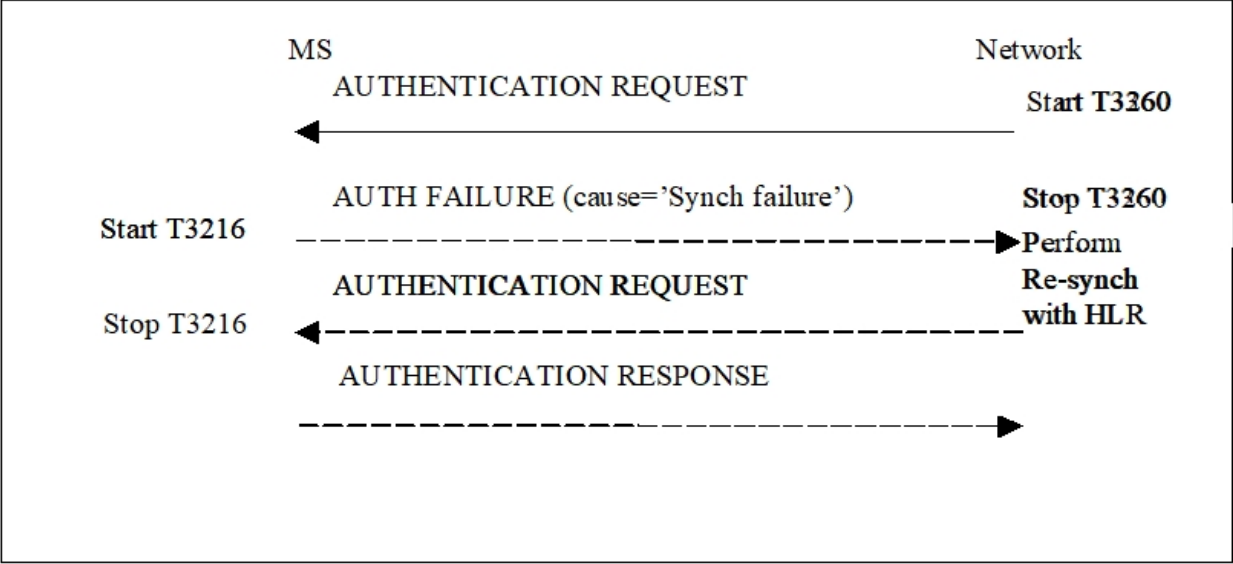


Figure 4.2a/3GPP TS 24.008: Authentication Failure Procedure (reject cause "Synch failure")

#8 - 2025-06-04 18:30 - 白瑞朋

【问题进展】

log中的异常信息有

- 1) [INFO]L1C fill pucch cfg to phy: Format199603 not supported. -> PUCCH参数错误，目前只支持UCI format 0;
- 2) [INFO]Res is not having sufficient PRB to accomodate UciBits. -> PUCCH参数错误，进入了format234的错误分支；

下一步：
分析msg6 ACK没有上报的原因，以及L1C参数配置问题。

文件

PDSCH log.jpg	293 KB	2025-05-30	白瑞朋
20250603-190959.jpg	270 KB	2025-06-03	赵强
鉴权流程.jpg	106 KB	2025-06-04	白瑞朋