ICEPNG

LTE RRCConnectionRelease Redirect问题分析

3 YEARS AGO 5G 8 MINUTES READ (ABOUT 1238 WORDS)

这个问题是在16年被国内研究员发现提出，并实现了完整的攻击。因为这是一个很经典的问题，在学习LTE/5G安全过程中复现一下也是很有必要的。我大概是在今年初分析复现这个问题。

RRCConnectionRelease在5GNR中是RRCRelease.

RRCConnectionRelease正常的使用是：

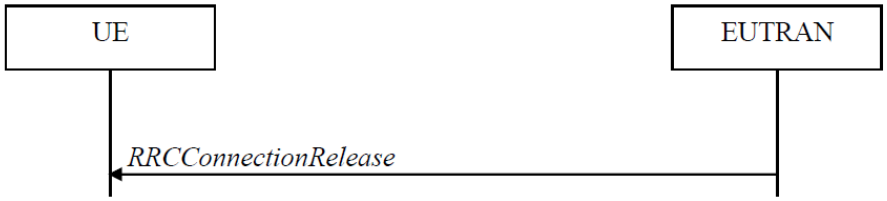

Figure 5.3.8.1-1: RRC connection release, successful

The purpose of this procedure is:

- to release the RRC connection, which includes the release of the established radio bearers as well as all radio resources; or
- to suspend the RRC connection for both suspended RRC connection or RRC_INACTIVE, which includes the suspension of the established radio bearers.
- to configure, reconfigure or release radio resources for transmission using PUR.
- to complete the UP-EDT procedure and UP transmission using PUR, which includes the release or suspension of the established radio bearers.

由基站发给UE，作用包括释放一个rrc connection...

基本原理

当在nas层reject当前连接后，ue接收后，会触发基站发送rrcconnectionrelease给UE，此

ICEPNG

协议上最开始的描述，UE接收后并不会对rrcconnectionrelease的完整性进行校验，而直接接收解析。

在rrcconnectionrelease中可以携带redirectedCarrierInfo结构，可以直接查看asn文件中对该结构的定义：

```
typedef struct LTE_RRCConnectionRelease_r8_IEs {
        LTE_ReleaseCause_t       releaseCause;
        struct LTE_RedirectedCarrierInfo        *redirectedCarrierInfo
        struct LTE_IdleModeMobilityControlInfo  *idleModeMobilityContr
        struct LTE_RRCConnectionRelease_v890_IEs        *nonCriticalEx

        /* Context for parsing across buffer boundaries */
        asn_struct_ctx_t _asn_ctx;
} LTE_RRCConnectionRelease_r8_IEs_t;
//////
typedef enum LTE_RedirectedCarrierInfo_PR {
        LTE_RedirectedCarrierInfo_PR_NOTHING,   /* No components prese
        LTE_RedirectedCarrierInfo_PR_eutra,
        LTE_RedirectedCarrierInfo_PR_geran,
        LTE_RedirectedCarrierInfo_PR_utra_FDD,
        LTE_RedirectedCarrierInfo_PR_utra_TDD,
        LTE_RedirectedCarrierInfo_PR_cdma2000_HRPD,
        LTE_RedirectedCarrierInfo_PR_cdma2000_1xRTT,
        /* Extensions may appear below */
        LTE_RedirectedCarrierInfo_PR_utra_TDD_r10,
        LTE_RedirectedCarrierInfo_PR_nr_r15
} LTE_RedirectedCarrierInfo_PR;
//////
typedef struct LTE_RedirectedCarrierInfo {
        LTE_RedirectedCarrierInfo_PR present;
        union LTE_RedirectedCarrierInfo_u {
                LTE_ARFCN_ValueEUTRA_t   eutra;
                LTE_CarrierFreqsGERAN_t  geran;
```

ICEPNG

```
31                  LTE_CarrierFreqCDMA2000_t       cdma2000_HRPD;
32                  LTE_CarrierFreqCDMA2000_t       cdma2000_1xRTT;
33                  /*
34                   * This type is extensible,
35                   * possible extensions are below.
36                   */
37                  LTE_CarrierFreqListUTRA_TDD_r10_t       utra_TDD_r10;
38                  LTE_CarrierInfoNR_r15_t  nr_r15;
39          } choice;
40
41          /* Context for parsing across buffer boundaries */
42          asn_struct_ctx_t _asn_ctx;
43  } LTE_RedirectedCarrierInfo_t;
```

可以发现redirectedCarrierInfo其实是给UE提供了一个/多个可选的频率/频道/arfcn。当UE收到后会根据该信息选择一个合适的cell。(The procedure can also be used to release and redirect a UE to another frequency)

环境

不影响现网，因此用oai和openair-cn搭建一个LTE网。用正常手机(UE)连接。（USRP B210+笔记本）

选用的是通过核心网/MME发送的attach reject来触发基站的RRCConnectionRelease.

初始状态的测试，attach reject选用cause 17，network failure，比较“弱”的一个cause。

oai代码不动，默认RRCConnectionRelease中是不携带redirectedCarrierInfo。修改openair-cn，当接收到第一次attach request时候，发送attach reject，cause 17；而第二次将正常处理attach request(即accept)。

搭建一个2G环境，保持运行状态。（一个Linux虚拟机+limesdr mini）

现象：UE在第一次attach reject之后，继续向LTE网络发起attach request，然后正常连接LTE网络。

ICEPNG

oai在asn1_msg.c中，do_RRCConnectionRelease函数中，是用来构造RRCConnectionRelease包，添加redirectedCarrierInfo结构。比如我的添加：

```
1   LTE_RedirectedCarrierInfo_t rInfo;
2
3     // geran
4     rInfo.present = LTE_RedirectedCarrierInfo_PR_geran;
5     LTE_CarrierFreqsGERAN_t cfgt;
6     cfgt.startingARFCN = 636;
7     cfgt.bandIndicator = 0;
8     cfgt.followingARFCNs.present = LTE_CarrierFreqsGERAN__followingARFCN
9     cfgt.followingARFCNs.choice.equallySpacedARFCNs.arfcn_Spacing = 1;
10    cfgt.followingARFCNs.choice.equallySpacedARFCNs.numberOfFollowingARF
11
12    rInfo.choice.geran = cfgt;
13
14  ......
15    rrcConnectionRelease->criticalExtensions.choice.c1.choice.rrcConnect
```

arfcn和频率对应可以参考，保持和你搭建的伪基站一致即可：

https://wenku.baidu.com/view/55e2d6677cd184254a35355b.html

现象是在一次attach reject之后直接连接到了搭建的2G伪基站上。

后续

很早就发现的问题，但3GPP协议文档却很晚才体现添加修复。测试用的一款19年底的手机也是受影响的。

当UE收到RCCConnectionRelease/RRCRelease时，处理流程上36331和38331都有相关修改。比如36331描述如下：

ICEPNG

```
3       2>  if upper layers indicate that redirect to GERAN without AS secu
4           3>      perform the actions upon leaving RRC_CONNECTED as speci
```

```
1   1> if the RRCConnectionRelease message includes redirectedCarrierInfo i
2   1> if the RRCConnectionRelease message includes idleModeMobilityControl
3       2> if AS security has not been activated; and
4       2> if upper layers indicate that redirect to GERAN without AS secur
5           3> ignore the content of the RRCConnectionRelease;
6           3> perform the actions upon leaving RRC_CONNECTED or RRC_INACTI
```

描述中在AS Security之后必须得有完整性保护；如果在AS Security之前的话，携带redirectedCarrierInfo字段是不会被处理的。其实也还有这么一个条件if upper layers indicate that redirect to GERAN 所以和基带的实现也有很大关系。

而在38331中，到了release 15.6.0（19年6月）才额外添加一句ignore：

```
1   1> if the AS security is not activated:
2       2> ignore any field included in RRCRelease message except waitTime;
3       2> perform the actions upon going to RRC_IDLE as specified in 5.3.1
```

相关文档参考

Forcing a Targeted LTE Cellphone into an Eavesdropping Network

seeker: 伪基站高级利用技术——彻底攻破短信验证码
[1] LTE RRC: TS 36331
[2] 5G RRC: TS 38331

#5G

ICEPNG