LTE接入过程中的安全机制

许杨春　　诺基亚西门子通信

【摘　要】在简要介绍了LTE的安全机制后，文章分析了LTE的认证流程，然后通过举例探讨了非接入层（NAS）与接入层（AS）的加密和完整性保护流程。

【关键词】LTE　接入过程　安全机制　加密　完整性保护

在LTE接入过程中，有多种安全机制用于保证用户数据和信令的安全，已经有很多文献就此做出探讨，但是各知识点阐述得比较孤立。本文以一个完整的流程为实例来说明相关要点。

1　概述

LTE的安全机制主要在以3GPP TS 33.401为主的规范中加以规定，接入过程涉及终端和网络的双向认证、接入层（AS）的加密和完整性保护以及非接入层（NAS）的加密和完整性保护。

LTE使用的加密和完整性算法框架称之为MILENAGE，除了一系列算法外，还有以下参数：

◆ K，每个用户独有的密钥，它是*f*1、*f*1*、*f*2、*f*3、*f*4、*f*5和*f*5*算法的输入；

◆ OP，它是*f*1、*f*1*、*f*2、*f*3、*f*4、*f*5和*f*5*算法的一部分，其值由运营商设置。为了防止OP泄露，可以用K对它加密得到每个用户唯一的OPc。

K、OP（或OPc）分别存在USIM和网络侧HSS。

LTE的认证是UE和MME的双向认证，该过程称之为EPS AKA（Authentication and Key Agreement），认证过程中明确了K_{ASME}值，该EPS安全上下文存续期间使用的所有的密钥都可以由它推导得到。一个EPS安全上下文包括接入层和非接入层两部分，它用eKSI值来标识。如果当前有缓存的安全上下文，终端在Attach Request、TAU等消息里用eKSI来标识。

2　认证流程

图1中消息6和7为一次成功的认证。认证需要的参数由网络侧HSS生成，MME通过IMSI（用户识别码）检索相关参数，终端侧USIM负责校验。

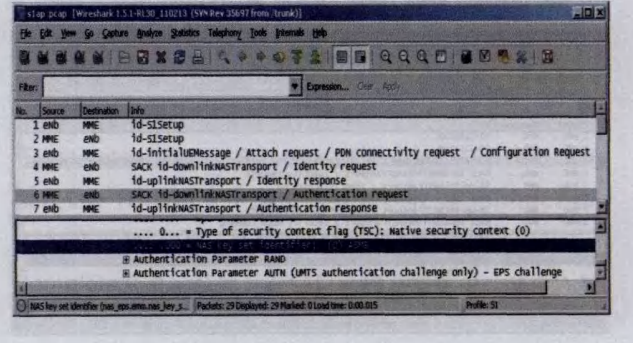

图1　认证流程

收稿日期：2011-05-12

如果网络无法由Attach Request（消息3）直接或间接得到从而获得终端的IMSI，MME会发送Identity Request（消息4）/Identity Response（消息5）向终端查询。MME获得IMSI后，向HSS检索与该终端对应的参数，其中随机数RAND、令牌AUTN会通过送Authentication Request（消息6）发给终端，XRES和KASME会保存备用。信令中的NAS Key Set Identifier即eKSI，如认证成功，终端和MME都使用其值来标识上下文。

终端收到Authentication Request消息后，用AUTN对网络进行认证。如果认证成功，终端计算RES值，在Authentication Response（消息7）中返回，MME收到RES后与存贮的XRES比较；终端和网络分别根据K值推出一对密钥CK/IK（加密/完整性密钥），这一对密钥再推出KASME值。KASME值可以看作根密钥，其他密钥都由它导出。如果认证失败，终端返回Authentication Reject。

3 NAS的加密和完整性保护流程

在NAS层，终端和MME协商使用一定的算法对信令进行加密和完整性保护，这是通过Security Mode Command/Security Mode Complete NAS信令实现的，这一过程对基站是透明的。3GPP TS 33.401中定义了EEA0/EEA1/EEA2三种加密算法、EIA0/EIA1/EIA2三种完整性算法，其中EIA0一般不使用。终端则通过Attach Request（消息3）中的UE Network Capability字段上报其支持算法，MME负责从中选择。本例中终端支持除EIA0之外的所有算法。

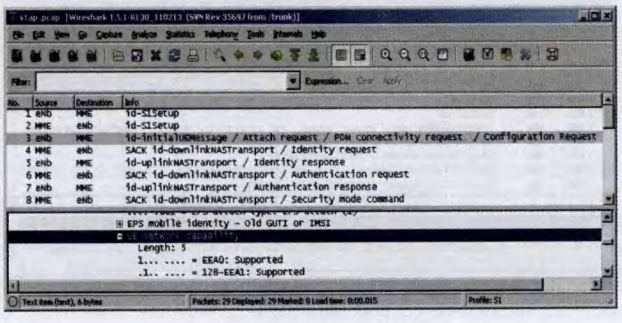

图2 Attach Request消息

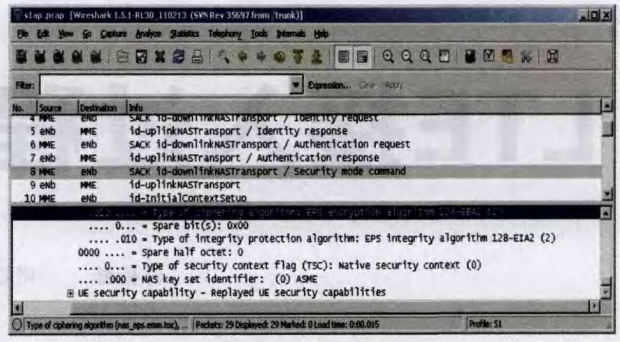

图3 Security Mode Command消息

认证过程结束后，MME选择一种它与终端都支持的算法，通过Security Mode Command（消息8）告知终端，本例中MME选择了EEA2/EIA2。终端收到该消息后，就开始上行数据的安全性保护，所以图3中消息9信令部分已经加密，无法解得具体内容。在Wireshark中设置K_{ASME}值后，消息9 NAS PDU部分解析得到Security Mode Complete信令（图4），Wireshark标记PDU是用AES也即是用MME选择的EEA2解密的。

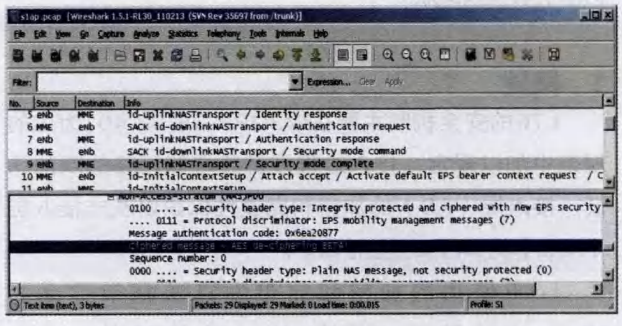

图4 已经被加密的Security Mode Complete信令

MME收到Security Mode Complete信令后，下行NAS信令例如消息10也开始加密。解密后的消息10显示：MME通过Initial UE Context Setup Request告知基站终端的能力（它不是封装在透传的NAS信令中，所以基站可以得知这些消息）。在该消息中，MME还指定了接入层使用的密钥（Security Key），如果值为0，并且UE也支持，完整性算法就使用EIA0。

责任编辑：左永君 zuoyongjun@mbcom.cn

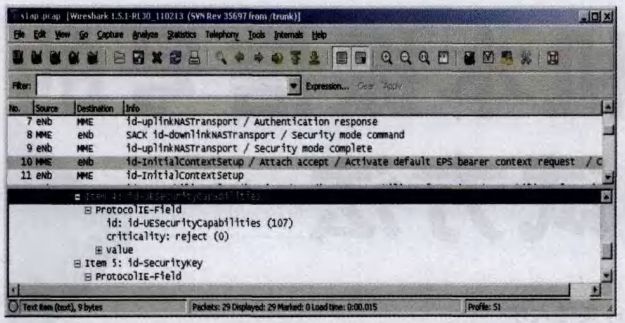

图5　Attach Accept消息

消息10过后就开始接入层（AS）的加密和完整性保护过程。

4　AS的加密和完整性保护流程

接入层终结于终端和基站，它们协商使用一定的算法对RRC信令和用户数据加密，完整性保护仅用于RRC信令。接入层可选的算法同样来自终端通过Attach Request上报的消息，但基站独立选择所使用的算法；接入层使用的密钥不同于NAS层，但同样由KASME推导得到。

接入层的RRC信令可以在终端或基站获取。以下以一基站的记录为例说明涉及的RRC信令，为了节省篇幅，无关部分已省略。

在第3节，NAS层的安全流程结尾时，MME通过S1AP消息Initial Context Setup Request通知基站可以开始接入层的安全流程，消息中有两个元素：UE Security Capabilities、Security Key，它们说明了终端支持的算法和密钥。基站在配置的时候对于支持的加密算法和完整性算法定义了优先级，收到该消息后，基站选择双方支持并且优先级最高的算法，然后通过RRC信令Security Mode Command通知终端。

```
DL-DCCH-Message : {
 message c1: securityModeCommand : {
   rrc-TransactionIdentifier 2,
 criticalExtensions c1:securityModeCommand-r8:{
     securityConfigSMC {
      securityAlgorithmConfig {
          cipheringAlgorithm eea1,
          integrityProtAlgorithm eia2
        ...
}
```

本例中，由于基站选择的是EEA1加密算法和EIA2完整性算法，这说明加密算法和完整性算法的选择也是独立的。

当UE收到Security Mode Complete消息后，如果接受则通过RRC信令Security Mode Complete答复。发送完该消息后，空口数据已加密。但在传送NAS信令和数据前RRC还需做以下工作：

在此之前，所有的NAS信令都和RRC消息混在一起通过SRB（信令无线承载）1传输，还需要增加SRB2用于NAS信令传输（它还继续封装在RRC中透传）、DRB（数据无线承载）用于用户面数据传输。这是通过以下消息实现的：

```
DL-DCCH-Message : {
 message c1 : rrcConnectionReconfiguration : {
              ...
      srb-ToAddModList {
      {
       srb-Identity 2,
       ......
      },
      drb-ToAddModList {
      {
       eps-BearerIdentity 5,
       drb-Identity 4,
            ...
      }
```

第3节消息10中出现的NAS信令：Attach Accept和Activate DEF EPS Bearer Context REQ也可以封装在这一RRC信令中递交给终端。收到Connection Reconfiguration后，终端以Connection Reconfiguration Complete答复。至此，在空口，接入层信令、非接入层信令和用户面数据实现了分离。

接入层的安全流程可概括为：MME通过Initial

LTE基站发射机本振信号的主要指标与测试方法

石高巍　上海交通大学

【摘　要】文章根据LTE基站发射机实际研发测试指标，对其本振信号测试的主要指标进行了简单的阐述，并介绍了所需要的测试设备，最后给出了相应的实际测试结果。

【关键词】LTE　基站发射机　本振　测试指标

1　引言

LTE作为4G时代的移动无线技术的主流标准，旨在增加系统的频谱利用率、提高数据的传输率和降低系统的传输延迟。因此，LTE系统对信息速率和可靠性提出了更高的要求。

收稿日期：2011-05-12

发射机是无线通信基站发射信号的核心部件，其性能的好坏直接决定了无线通信系统的性能。通常，发射机通过本振与中频调制信号混频，使其频率变换到所需的发射频率。对于发射机来说，频率变换理论上不会使信号产生畸变；而实际上，混频器和本振都会使发射机输出信号产生畸变，从而降低发射机的性能。混频器对信号的恶化主要是混频杂波，所以本振信号的纯度是

Context Setup Request通知基站终端的安全能力。基站收到消息后，通过RRC信令Security Mode Command告知终端接入层选择的算法，终端以Security Mode Complete加以确认，然后激活无线数据承载。

5　总结

通过多种安全机制的引入，LTE中从终端到基站的空口数据得到加密和完整性算法的保护，可以防止被窃听和篡改。基站到核心网的信令也得到类似算法的保护，算法使用的密钥是在认证过程中确定的。

如果基站处于非安全区，它到核心网的数据通路也需要一定的机制加以保护，如IPsec等VPN技术，这些安全机制应该在基站开通时配置完成。

参考文献

[1]3GPP TS 33.401. 3GPP System Architecture Evolution(SAE):Security architecture[S].
[2]3GPP TS 35.206. Specification of the MILENAGE algorithm set[S]. ★

【作者简介】

许杨春：系统分析师，硕士毕业于北京邮电大学，现任职于诺基亚西门子通信，从事LTE相关工作。

责任编辑：左永君 zuoyongjun@mbcom.cn