改进的 H(e)NB 位置锁定方案①

何 莉[1]，李泰成[1]，吴 槟[2,3]

[1](中国科学院研究生院 信息安全国家重点实验室，北京 100049)
[2](中国科学院软件研究所 信息安全国家重点实验室，北京 100190)
[3](信息安全共性技术国家工程研究中心，北京 100190)

摘 要：主要研究了 3GPP TR 33.820 等技术报告中的 H(e)NB 位置锁定机制。当前 3GPP 仅仅只是针对几种特定情形下的 H(e)NB 位置锁定提出了解决方案。鉴于此，在本文中我们提出了一个通用的改进的位置锁定方案。该方案可以用于一般情形下的 H(e)NB 位置锁定，解决了 H(e)NB 在实际使用中因不能可靠锁定位置所带来的多种安全威胁，并增加了 H(e)NB 位置锁定的可靠性以及锁定成功的概率。

关键词：LTE；SAE；网络安全；H(e)NB；位置锁定

Improved Location Locking Scheme for H(e)NB

HE Li[1], LI Tai-Cheng[1], WU Bin[2,3]

[1](State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing 100049, China)
[2](State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)
[3](National Engineering and Research Centre of Information Security, Beijing 100190, China)

Abstract: We study the location locking mechanism for H(e)NB in 3GPP TR 33.820. By now 3GPP has only proposed a few solutions for H(e)NB's location locking in certain specific situations. In this paper, we propose an improved scheme for H(e)NB, which can be used for locking H(e)NB's location in general situations. The scheme can deal with the security threats brought by unreliable location locking for H(e)NB in practical use. It also increases the reliability of H(e)NB's location locking and increases the probability of locking successfully.

Key words: LTE; SAE; network security; H(e)NB; location locking

1 简介

为了占有宽带无线接入市场，3GPP 在 2004 年底决定在长期演进计划(Long Term Evolution，简记 LTE)中采用过去为超 3G 或 4G 技术使用的 3G 频段。同时，3GPP 展开了系统架构演进(System Architecture Evolution，简记 SAE)[1]方面的研究。

H(e)NB 包括家庭基站和家庭演进基站，其中家庭基站(Home NodeB，简记 HNB)是通用陆地无线接入网(Universal Terrestrial Radio Access Network，简记 UTRAN)的基站，家庭演进基站(Home evolved NodeB，简记 HeNB)是演进的 UTRAN (Evolved UTRAN，简记 E-UTRAN)的基站[2]。在 LTE/SAE 网络的建设中，为了解决在 3G 系统中室内信号覆盖的难题，3GPP 对 H(e)NB 进行了研究。在 3GPP TR 23.830[2]和 TR 33.820[3]等技术报告中，H(e)NB 是针对家庭和中小企业推出的可以解决室内覆盖问题的接入设备，它能以更低的成本提供更高数据率的新服务，有着体积小、重量轻、可移动等特点，运营商已经表明了他们对这一领域的兴趣。

H(e)NB 的系统架构[4]如图 1 所示：

① 基金项目:中国科学院知识创新工程重要方向项目(YYYJ-1013)
收稿时间:2010-11-14;收到修改稿时间:2010-11-24

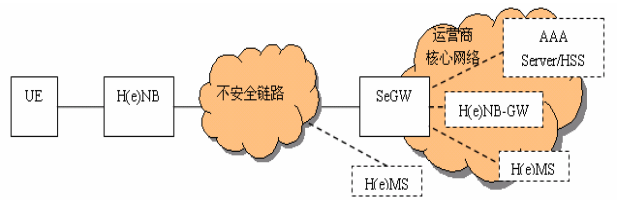

图 1　H(e)NB 的系统架构

图 1 中，H(e)NB 通过安全网关(Security Gateway，简记 SeGW)接入运营商的核心网。由于 H(e)NB 和 SeGW 之间的回程链路可能是不安全的，它们之间需要建立安全隧道来保护回程链路中传送的信息。SeGW 作为运营商核心网的边界实体，将完成其与 H(e)NB 之间的双向认证。家庭基站管理系统(Home (e)NodeB Management System，简记 H(e)MS)，H(e)NB 网关(H(e)NB-Gateway，简记 H(e)NB-GW)将执行 H(e)NB 的位置验证。H(e)MS 和 H(e)NB 之间需要安全的通信。

H(e)NB 将基站功能延伸到了室内环境中，解决了室内覆盖的难题，但同时也带来了一系列新的安全威胁[5]，其中一个重要的安全问题就是 H(e)NB 位置的锁定。由于 H(e)NB 可移动，当它由于各种原因移动到一个新位置之后，如果它的位置不能被锁定，那么来自于这个 H(e)NB 的紧急呼叫将不能可靠定位，因此不能路由到正确的紧急中心，并且给出合法的监听位置的报告也变得不可能。此外，对于运营商来说，在新位置处运营商的频率计划可能会受到影响；同时，客户甚至可能在他们被授权的家庭/办公室区域之外获得优先呼叫率，这会造成运营商的收益流失。为了应对上述威胁，必须设计和实现安全的位置锁定方案。然而当前的 3GPP 技术报告 TR 33.820 仅仅只是针对几种特定情形下的 H(e)NB 位置锁定提供了解决方案，而且 3GPP 的现有技术规范也还没有提出关于 H(e)NB 位置锁定的一个通用解决方案。鉴于此，在本文中我们提出了一个通用的改进的 H(e)NB 位置锁定方案。该方案可以用于一般情形下的 H(e)NB 位置锁定，解决了 H(e)NB 在实际使用中因不能可靠锁定位置所带来的多种安全威胁，并增加了 H(e)NB 位置锁定的可靠性以及锁定成功的概率。

本文后面的章节安排如下：在第二节我们首先介绍了 3GPP TR 33.820 中的 H(e)NB 位置锁定机制及现有的 H(e)NB 位置锁定解决方案，然后在第三节提出了一个改进的 H(e)NB 位置锁定解决方案，并分析了所提出的方案，最后在第四节给出了我们的工作的总结。

2　H(e)NB的位置锁定机制

2.1　位置锁定机制概述

3GPP TR 33.820[3]介绍了 H(e)NB 的位置锁定机制，主要包括以下三步：

①H(e)NB 位置的确认；

②位置信息的认证(验证)；

③H(e)NB 操作的授权。

对于位置确认来说，H(e)NB 有两种类型的位置确认方法，分别是：使用邻居小区或用户设备(User Equipment，简记 UE)的位置信息来获得 H(e)NB 的位置确认；使用 H(e)NB 自身本地可用的位置信息。

其他方法可以归为上述两种类型中的一种。

对于位置认证来说，一些可能的攻击可能导致报告一个错误的位置。位置认证想要禁止这些攻击或者使它们难以成功，除了使用一个单独的位置确认方法外，两个或多个方法的结合也可能被用于验证所报告的位置信息。

H(e)MS 和/或 H(e)NB-GW (在本文中当作是“验证节点(verifying node)”)会执行位置验证。运营商可能在验证节点中选择性的存储一种或多种类型的 H(e)NB 位置信息，用来进行位置验证。

对于 H(e)NB 操作的授权来说，在确认过的和认证过的位置处，H(e)NB 操作的授权是由运营商决定的。

2.2　现有的 H(e)NB 位置锁定解决方案

核心网络获得 H(e)NB 位置的信息，并将它与存储的对应的 H(e)NB 的位置信息进行比较。如果匹配，那么核心网络同意 H(e)NB 基于 H(e)NB 位置信息的服务接入。

H(e)NB 的位置信息可以从以下地方获得：宽带接入设备的 IP 地址；H(e)NB 周围宏小区(macro cell)的信息；嵌入到 H(e)NB 本身或位于 H(e)NB 的 UE 里面的 GPS 位置信息。

3GPP TR 33.820 中描述了下列几种特定情形下的解决方案：基于 IP 地址的解决方案、基于邻居宏小区的 H(e)NB 报告的解决方案、基于 IP 地址和邻居宏小区的 H(e)NB 报告的解决方案、基于 UE 信息的解决方

案、基于 UE 信息和邻居宏小区的 H(e)NB 报告的解决方案、以及基于 H(e)NB 中辅助 GPS (Assisted-GPS，简记(A-)GPS)的解决方案等。这些方案按如下步骤进行：在 H(e)NB 向验证节点发起注册请求时，验证节点存储所报告的位置信息；当 H(e)NB 请求接入时，验证节点再将此时收到的位置信息与存储的信息进行对比，从而确定是否同意 H(e)NB 接入。在此对各个方案不作详细介绍。

2.3 关于 H(e)NB 位置的重锁定

①H(e)NB 位置相同

H(e)NB 的位置没有改变，当它正在从某个不可用(例如关机、发生故障等)状态中恢复到可用状态的时候，H(e)NB 会根据位置锁定机制的三个步骤来执行自己位置的重锁定。

②H(e)NB 位置不同

只要 H(e)NB 位置改变(例如 H(e)NB 由拥有者从一个房间移动到另一个房间)，它位置的移动应该由运营商管理。

当 H(e)NB 被置于一个新位置时，如果新位置的可用性被运营商验证了，H(e)NB 按照位置锁定机制的三个步骤来重锁定自己的新位置。

3 改进的H(e)NB位置锁定方案

在上一节我们已经提到，3GPP 现有的技术报告仅仅只是针对几种特定情形下的 H(e)NB 位置锁定提供了解决方案。然而，在实际应用中，H(e)NB 可能会在不同的时间和不同的地点获取多种不同类型的位置信息。因此迫切需要一种能够通过多种不同类型位置信息的认证的 H(e)NB 位置锁定方案，以解决和 H(e)NB 位置相关的威胁，并增加 H(e)NB 位置锁定的可靠性以及锁定成功的概率。在这一节我们针对一般情形提出了改进的 H(e)NB 位置锁定方案。

3.1 方案描述

对验证节点的假设：

①验证节点中的位置记录对于运营商来说是可信的。

②验证节点中关于 H(e)NB 的一条位置记录可以存储多种不同类型的位置信息：IP 地址对应的接入线路位置标识、小区 ID (cell ID)、GPS 有效位置区域的范围等。

③验证节点中的记录可能存在空项，比如可能记录有 H(e)NB 的小区 ID 和 IP 地址对应的接入线路位置标识，而没有 GPS 的相关信息。

④在 H(e)NB 没有向验证节点注册之前，验证节点可能存储有某些 H(e)NB 的特定的位置信息，这些情形下，H(e)NB 可以不用进行注册，并且这些位置信息也不允许更改。

用于查询连接会话位置和存储功能(Connectivity Session Location and Repository Function，简记 CLF)的实体位于验证节点中，可以是 H(e)NB 的归属寄存器。

H(e)NB 在第一次通电或者进行位置重锁定时，需要向验证节点进行注册。注册时，H(e)NB 向验证节点发送自己的位置信息，验证节点将这些信息作为 H(e)NB 的属性进行注册。在 H(e)NB 请求接入时，再次将位置信息发送给验证节点；验证节点将收到的位置信息同存储的信息进行比较，从而确定是否允许 H(e)NB 接入网络。

H(e)NB 位置锁定解决方案见图 2。

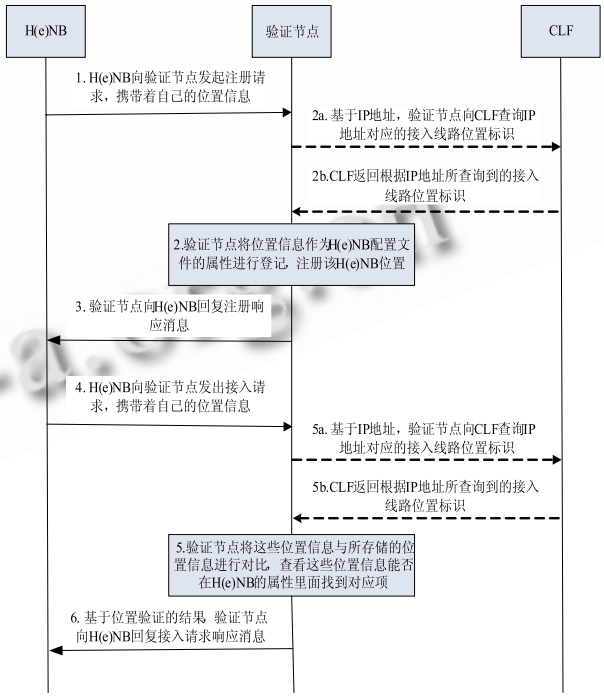

图 2 H(e)NB 位置锁定方案示意图

其具体操作如下：

H(e)NB 位置信息的注册：

如果 H(e)NB 在验证节点中已经同运营商有一个约定好的位置信息，那么这种情况下 H(e)NB 可以不

用注册，并且验证节点中存储的这个 H(e)NB 位置信息不可更改。其他情形下，可以进行 H(e)NB 位置信息的注册、更新(注意在更新的时候，新位置的可用性必须先经过运营商的验证)。注册步骤如下：

①H(e)NB 向验证节点发起注册请求，并携带着自己的位置信息。H(e)NB 上报何种位置信息，可以预先配置或者在验证节点要求时提供，这些由运营商的策略决定。这些位置信息可以包括 H(e)NB 的 IP 地址、小区 ID、H(e)NB 自己提供的或者由 UE 提供的 GPS 信息。

②验证节点将这些信息作为 H(e)NB 配置文件的属性进行登记，注册这个 H(e)NB 的位置。若出现增项，将增加的内容添加到属性中；若出现更新过且合法的项，则按新位置信息进行修改。当 H(e)NB 的位置信息包含 IP 地址时，验证节点需向 CLF 查询来获得与 IP 地址相关联的接入线路位置标识(即图 2 中的步骤 2a、2b)，并将接入线路位置标识同其他位置信息作为 H(e)NB 的属性一起存储，而不是存储 IP 地址。

③验证节点向 H(e)NB 回复注册响应消息。

H(e)NB 位置信息的认证：

④H(e)NB 向验证节点发起接入请求，携带着它的位置信息。

⑤验证节点将这些位置信息与所存储的位置信息对比，查看这些位置信息能否在 H(e)NB 的属性里面找到对应项。如果包含 IP 地址，验证节点还需查询 CLF 来获得接入线路位置标识(即图 2 中的步骤 5a、5b)，并判断此时获得的位置标识同存储的是否相同。如果位置信息同 H(e)NB 属性相匹配(匹配多少项由运营商策略来决定，但建议不能只匹配 IP 地址项)，即能找到对应项，就说明 H(e)NB 的位置没有改变，验证节点返回一个 H(e)NB 接入响应来允许 H(e)NB 接入。如果不能匹配，那么验证节点返回一个 H(e)NB 接入响应消息来拒绝 H(e)NB 接入，并在原因值里表明“无效位置”。

H(e)NB 操作的授权：

⑥取决于位置验证的结果，验证节点向 H(e)NB 回复接入请求响应消息。验证节点会采取以下一种或多种行动：发出警报、允许 H(e)NB 发送或阻止 H(e)NB 发送。

当 H(e)NB 需要进行位置的重锁定时，同样按照上面的操作流程来执行。

3.2 方案分析

安全性分析：现有 3GPP 方案中，H(e)NB 上报位置信息时需考虑上报何种类型位置的信息，如果上报的位置信息类型不匹配，则不能锁定成功，那么来自于这个 H(e)NB 的紧急呼叫将不能可靠定位，也不能路由到正确的紧急中心，并且新位置处运营商的频率计划可能会受到影响，运营商的收益也可能流失。本文提出的改进方案可以使 H(e)NB 上报当前所能获得的任何位置信息，不必考虑信息类型的问题，因此能及时进行位置锁定，从而可以解决 H(e)NB 在实际使用中因不能可靠锁定位置所带来的多种安全威胁。

可靠性分析：现有 3GPP 方案中，当 H(e)NB 上报位置信息时，需要根据 H(e)NB 当前情形上报特定类型的位置信息。改进方案中，H(e)NB 可以直接上报多种不同类型的位置信息，验证节点可以对多种位置信息同时进行处理，能够通过多种不同类型的 H(e)NB 位置信息的认证，从而增加了 H(e)NB 位置锁定的可靠性，也增加了锁定成功的概率。

效率分析：当 H(e)NB 位置发生改变时，在现有的 3GPP 位置锁定方案中，同样需要考虑上报特定类型的位置信息。改进方案相对比较灵活，H(e)NB 可以上报不同类型的位置信息，从而 H(e)NB 可以很方便的进行位置信息的更新、注册，并按照位置锁定的步骤进行位置重锁定。因此改进方案增加了 H(e)NB 移动的灵活性，提高了位置锁定的效率。

适用性分析：改进方案对现有网络设备没有实质影响，只需要略微增加验证节点的存储量即可，可以适用于现有的 3GPP 网络。

4 结语

H(e)NB 是一种可以解决室内覆盖问题的接入设备，它具有灵活的移动性。如果它不能进行可靠的位置锁定，将会给它的应用带来一系列威胁。但是在现有的 3GPP 技术规范中，并没有对位置锁定给出一个通用的解决方案，只是在技术报告中描述了在几种特定情形下的解决方案。本文所提出的改进的 H(e)NB 位置锁定方案，能够通过多种不同类型位置信息的认证，解决了和 H(e)NB 位置锁定相关的威胁，增加了 H(e)NB 位置锁定的可靠性及锁定成功的概率。

(下转第 133 页)

修正结果如图 7 所示。该修正表格包含了修正前后的阻力系数值及其对应的风速和横摆角。

根据图 4 和图 5，我们可以直观看出气动六分力和相关系数随着横摆角的增加而增大；模型的修正后的阻力系数要比测量值小一些。

5.2 软件运行结果评价

软件运行实例表明：

(1) 系统界面简明，软件的使用十分便捷。

(2) 数据处理结果直观性强。实验研究人员可以直观判断结果的合理性；通过软件容易得到气动力系数随速度和横摆角的变化规律。

(3) 数据处理效率高。这主要体现在数据处理时间方面，以往处理一次试验的数据文件需要花费十几个小时，而采用该软件几分钟便可完成。

(4) 处理结果精度高。长时间的人工数据处理容易使人产生疲劳，这大大增加了人为误差甚至错误的出现，而采用该软件可以消除手工计算的误差和可能出现的误错。

6 结论

（1）VB 是数据库应用程序的重要开发工具之一，EXCEL 是数据处理和统计分析的重要工具之一，将二者结合起来能够使数据的处理变得轻松易行。

（2）基于 VB 开发的汽车风洞试验数据处理软件，可以直观地得出汽车试验模型各个空气动力学特性参数的大小，为进一步分析数据提供了方向。

（3）系统数据处理效率很高，实验研究人员不必花费大量时间和精力进行实验数据的处理,更着眼于采集更多的实验数据，增加重复次数，提高实验结果的置信度。

参考文献

1 高利,范炜,蔡红民,周瑞兴,上官云信.国产客车模型风洞试验研究.汽车技术,2002,(7):27-31.

2 谷正气.汽车空气动力学.北京:人民交通出版社,2005.56-58.

3 Mercker E. A blockage correction for automotive testing in a wind tunnel with close test section. Journal of Wind Engineering and Industrial Aerodynamics, 1986,(22):149-167.

4 林卓然.VB 语言程序设计.北京:电子工业出版社,2003.59-153.

5 蔡旭.VB 在 Excel 中的综合应用分析.现代商贸工业,2009,(14):242-243.

(上接第 66 页)

参考文献

1 工业和信息化部电信研究院等.系统结构演进(SAE)研究报告.http://www.ptsn.net.cn/article_new/show_article.phpcategories_id=f8b50d51-3d0b-8842-956c-452ddac16142&article_id=sr_cf3904a6-7aa9-1ee7-a033-4c280662b117,2010,9.

2 3GPP. 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; Architecture aspects of Home Node B and Home eNodeB (Release 9). 3GPP TR 23.830 v9.0.0, 2009,9.

3 3GPP. 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; Security of H(e)NB (Release 8). 3GPP TR 33.820 v8.3.0, 2009,12.

4 3GPP. 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; Security of Home Node B (HNB) / Home evolved Node B (HeNB) (Release 9). 3GPP TS 33.320 v9.1.0, 2010,3.

5 Han CK, Choi HK, Kim IH. Building Femtocell More Secure with Improved Proxy Signature. Global Telecommunications Conference (GLOBECOM), 2009.