具有一跳前向安全性的 X2 切换密钥更新协议①

李泰成[1]，何 莉[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：长期演进系统 LTE 是下一代移动通信系统的主要标准之一，其安全性对于系统的成功部署至关重要。研究 LTE 中本地信号切换也即 X2 切换时的密钥管理，并关注当前方案仅具备两跳前向安全性这一缺陷。我们提出一个改进的密钥更新方案，以达到更强的一跳前向安全性。新方案弥补了上述安全缺陷，且在不增加通信开销的情况下，最大限度地保留了现有的密钥材料及参数形式，因而当前标准可顺利升级到改进方案。

关键词：长期演进系统；网络安全；X2 切换；密钥更新；一跳前向安全性

Key Refresh During Cell Handover in LTE Featuring One-Hop Forward Security

LI Tai-Cheng[1], HE Li[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: Long Term Evolution (LTE) is the next-generation mobile communication system beyond 3G, whose security is predominant for the successful deployment of such networks. In this paper, we address the cryptographic key management during local cell handovers known as X2 handovers in LTE, which currently only achieves two-hop forward security. An enhanced key refresh scheme is proposed, which features the desired one-hop forward security. Our proposal not only makes up for the deficiency in the standardized LTE technical specification, but also retains all existent key materials and parameters without incurring extra communication costs. Therefore, it is technically feasible for the standardized key refresh to be smoothly upgraded to the enhanced proposal.

Key words: LTE; network security; X2 handover; key refresh; one-hop forward security

1 简介

为保持在下一代移动通信领域的优势，3GPP (The Third Generation Partnership Project) 组织提出了新的移动网络技术标准——长期演进系统(Long Term Evolution，LTE) [1]。

同 3G 相比，LTE 继承了所有传统的语音、数据和多媒体服务，还提供了更高的用户数据面带宽和更长的用户设备 (User Equipment，UE) 激活状态持续时间等[2,3]。同时，诸如手机电子商务和手机银行等应用也对手机通信的安全提出了更高的要求，如：更清晰的密钥分离要求[3]。LTE 的安全已经成了 LTE 网络成功部署实施的首要前提之一。

但是，LTE 中仍存在一些安全漏洞，例如：LTE 技术规范中标准的 X2 切换密钥更新协议只提供了两跳前向安全性，而这一缺陷在很多情况下将会给 UE 带来安全威胁。于是，我们提出了一个改进的 X2 切换密钥更新协议。

本文的其他章节安排如下：第 2 部分对本文涉及的 LTE 网络的相关内容进行了必要的介绍；第 3 部分分析了 LTE 技术规范中发生 X2 切换时的标准密钥处理过程及其缺陷——仅提供了两跳前向安全性；在第 4 部分中，我们提出了发生 X2 切换时具有一跳前向安

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:2010-11-25

全性的密钥更新协议；第 5 部分对本文进行了总结。本文中所涉及的缩略语见表 1。

表 1　缩略语

缩略语	全称	参考翻译
C-RNTI	Cell Radio Network Temporary Identifier	小区无线网络临时标识
EARFCN-DL	E-UTRA Absolute Radio Frequency Channel Number-Down Link	演进的统一陆地无线接入绝对频率信道值——下行链路
eNB	Evolved NodeB	基站
E-UTRAN	Evolved Universal Terrestrial Radio Access Network	演进的统一陆地无线接入网
KDF	Key Derivation Function	密钥推导函数
MME	Mobility Management Entity	移动性管理实体
NCC	Next Hop Chaining Count	下一跳链路计数器
NH	the Next Hop key	下一跳密钥
PCI	Physical Cell ID	物理小区标识
S-GW	SAE Gateway	核心网服务网关
UE	User Equipment	用户设备

2　背景知识介绍

2.1　整体网络架构

3GPP 将 LTE 标准应用于移动网络接入网的部分定义为 E-UTRAN[5]。如图 1 所示，系统架构中的 eNB 彼此通过 X2 接口进行互联，eNB 与 MME 或者 S-GW 之间通过 S1 接口进行互联[6]。同 3G 技术的 UTRAN 一样，UE 通过无线链路接口 Uu 与 eNB 进行互联。本文主要关注 X2 接口。

2.2 X2 切换涉及的密钥

LTE 为不同的密钥设计了详细的层次架构及推导流程，下面我们简要介绍 X2 切换中涉及的密钥。首先，UE 与 MME 在鉴权之后会共享一个高级别密钥——KASME，用来推导 KeNB 和 NH。完整性保护和加密保护密钥均从 KeNB 推导而出，NH 被用于推导下一轮的新密钥 KeNB*和 NH*。

2.3　研究目标及假设

本文主要关注 X2 切换，发生这种切换的一个典型场景如下：UE 从源 eNB 转移到目标 eNB 的服务范围，两个 eNB 隶属于同一个 MME，整个切换发生在 MME 内部，仅涉及 eNB 的改变。这种情景将触发切换过程，并引发 KeNB 和 NH 的更新。在密钥更新的过程中，一些密钥材料不可避免的将暴露在通信过程中。在这种情况下，KeNB 是否能够得到安全保护、能得到多大程度的保护是我们所关心的。我们的目标就是通过修改现有的密钥更新协议来增强对 KeNB 的保护。

我们假设 3GPP 选择的密钥推导算法是安全高效的，并且高级别的密钥，如 KASME，也得到了有效的保护。MME 隶属于核心网，主要由可信的移动运营商来负责，我们假设 MME 是安全的。衡量 LTE 安全架构的一个关键指标是前向安全性，其定义[4]如下：

在 KeNB 推导的过程中，前向安全性指的是与 UE 共享了同一个 KeNB 的 eNB 无法预测切换后该 UE 与另一个 eNB 共享的新密钥 KeNB*。N 跳前向安全性指的是 eNB 无法预测在 N (N= 1 或 2)轮切换之后，同一个 UE 与另一个 eNB 共享的 KeNB*。

从上面的定义可以看出，两跳前向安全性要比一跳前向安全性的安全级别低。

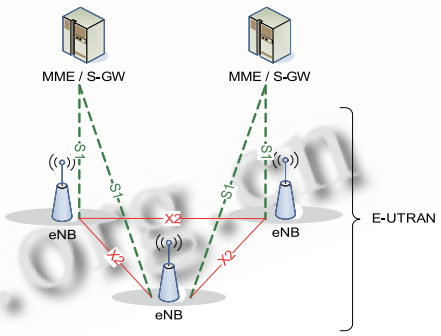

图 1　LTE (E-UTRAN) 整体架构[5]

3　现有协议及其分析

标准密钥分发机制中，切换发生时，要通过 X2 接口或者 S1 接口，X2 切换一般为不同 eNB 之间的切换，S1 切换一般为不同 MME 之间的切换，如 TS 33.401[4]中 7.2.8.4.2 节所述，现有密钥更新方案只有在两次 X2 切换之后，才能确保源 eNB 无法预测最新的密钥 KeNB，即在执行 X2 切换时，现有的密钥更新协议只具有两跳前向安全性，不具有一跳前向安全性。在本章节中，我们将对这一方面的漏洞进行具体的分析。方案中涉及到了一个变量 NCC，其作用可以理解为 NH 的计数器。

3.1 现有 X2 切换密钥更新协议

如图 2 所示，标准方案中的 X2 切换密钥更新协议如下：

0. UE 与源 eNB 共享上一轮切换后的 KeNB 、{NH，NCC}；

①UE 发送 Measurement Reports；

②源 eNB 做出切换决定；

③源 eNB 向目标 eNB 发送切换请求；

④目标 eNB 发送 Handover Request Ack，包含目标 PCI；

⑤源 eNB 通过 NH，目标 PCI 和 EARFCN-DL 来推导 KeNB*；

⑥源 eNB 将{KeNB*，NCC}发送给目标 eNB；

⑦目标 eNB 将收到的 KeNB*作为 KeNB；

⑧目标 eNB 发送 Handover Command 给源 eNB，包含 NCC；

⑨源 eNB 将 Handover Command 转发给 UE，并且包含目标 PCI 和 EARFCN-DL；

⑩a. UE 将原 NH 赋给 NH*，原 NCC 赋给 Temp-NCC，若 Temp-NCC 小于收到的 NCC，则通过 NH* = KDF (KASME, NH*) 重复推导 NH*、Temp-NCC 加 1，直到 Temp-NCC 与收到的 NCC 相等为止；

⑩b. UE 将最新的 NH*赋给 NH、将 Temp-NCC 赋给 NCC；

⑩c. UE 根据最新的 NH、目标 PCI、EARFCN-DL 生成 KeNB*；

⑩d. UE 将新生成的 KeNB*作为 KeNB，并根据 KeNB 继续推导 RRC、UP 层的其他密钥；

⑩e. UE 将 NCC 加 1；

⑩f. UE 根据 NH 和 KASME 计算新的 NH*；

⑩g UE 存储新的 {NH，NCC} 留作下一轮切换使用；

⑪ UE 发送 Handover Confirm 给目标 eNB，其中包含 NCC；

⑫目标 eNB 向 MME 发送 Path Switch 消息，其中包含 NCC；

⑬MME 执行与 10a 和 10b 相同的动作，根据 NCC 同步 NH；

⑭MME 发送 Path Switch Ack 给目标 eNB，包含{NH，NCC}；

⑮目标 eNB 发送 Release Resource Message 给源 eNB。

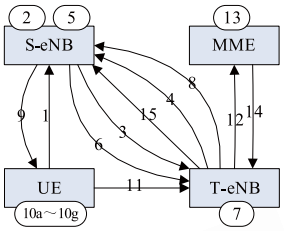

图 2 标准方案中的 X2 切换密钥更新协议

3.2 现有方案的安全分析

下面针对 2 种模型来对标准方案的安全性进行分析。

(1) 敌手仅拥有获取空口通信的能力

此种情况下，敌手能够得到的密钥参数包括：目标 PCI、EARFCN-DL、NCC，以及目标 eNB 选定的接入层保护算法标识。新密钥 KeNB* = KDF (NH，目标 PCI，EARFCN-DL)，它的推导绑定了参数 NH，敌手无法获得 NH，因此也就不能得到新的 eNB 密钥。

(2) 敌手拥有获取空口信号的能力，并控制了源 Enb

此种情况下，敌手可以获得模型 1 中的所有密钥参数。由于敌手又控制了源 eNB，还可以获得 NH 和 KeNB*，进而计算出本轮切换产生的新密钥 KeNB* = KDF (NH，目标 PCI，EARFCN-DL)，并进一步得到 RRC 和 UP 层的密钥。可见，完全控制源 eNB 的敌手可以得到本轮切换后新密钥。因此，上述方案不具备一跳前向安全性。

但是 NH 的推导有接入层最高级密钥 KASME 的参与，KASME 不离开 UE 和 MME，敌手无法得到 KASME，也就无法推导出下一轮切换之后新的 NH，因此控制了源 eNB 的敌手无法得到用户再次切换后的 eNB 新密钥，也就是说上述方案具有两跳前向安全性。

综上，标准的 X2 切换密钥更新协议不具有一跳前向安全性，但考虑到下一代移动通信网络的安全需求，X2 切换密钥更新协议应该具备一跳前向安全性。

4 改进方案

经过对标准 X2 切换密钥更新协议缺陷的分析，我们发现，源 eNB 知道所有目标 eNB 推导新密钥时所使用的密钥材料，因此如果敌手控制了源 eNB，就可

以推导出切换后的密钥，我们提出的改进方案的目标就是使源 eNB 不再知道目标 eNB 推导新密钥时的部分密钥材料，同时也能最大限度的继承原有方案的密钥和命令消息

4.1 改进的 X2 切换密钥更新协议

协议具体流程如图 3 所示。

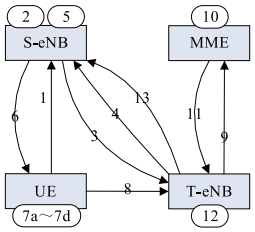

图 3　改进的 X2 切换密钥更新协议

0. UE 和源 eNB 共享上一轮切换后产生的 KeNB、{NH，NCC}；

①UE 发送 Measurement Reports；

②源 eNB 做出切换决定；

③源 eNB 向目标 eNB 发送切换请求；

④目标 eNB 发送 Handover Request Ack，包含目标 PCI；

⑤源 eNB 将自身的 NCC 加 1；

⑥源 eNB 向 UE 发送 Handover Command，其中包含 NCC、目标 PCI 和 EARFCN-DL；

⑦a UE 将原有的 NH 赋给 NH*，原有的 NCC 赋给 Temp-NCC，若 Temp-NCC 小于收到的 NCC，则通过 NH* = KDF (KASME, NH*) 重复推导 NH*、Temp-NCC 加 1，直到 Temp-NCC 与收到的 NCC 相等为止；

⑦b UE 将最新的 NH*赋给 NH、将 Temp-NCC 赋给 NCC；

⑦c UE 根据最新的 NH、目标 PCI、EARFCN-DL 生成 KeNB*；

⑦d UE 将 KeNB*赋给 KeNB，并继续推导 RRC、UP 层密钥；

⑧UE 发送 Handover Confirm 给目标 eNB，其中包含 NCC、EARFCN-DL；

⑨目标 eNB 向 MME 发送 Path Switch，包含接收到的 NCC；

⑩MME 执行与 7a、7b 相同的操作，根据 NCC 来同步 NH；

⑪MME 向目标 eNB 发送 Path Switch Ack，包含{NH，NCC}；

⑫目标 eNB 根据收到的 NH，目标 PCI 和 EARFCN-DL 推导 KeNB*，进而推导出 RRC、UP 层的其他密钥；

⑬目标 eNB 释放资源。

4.2 改进方案的密钥正确性验证

UE 在第 7a 步中用第 6 步接收到的 NCC 作为输入参数，用来生成最新的 NH*，并在第 7c 步中用 NH* 作为参数，生成最新的 KeNB*，再用刚生成的 KeNB* 作为最终的 KeNB，进而被用于生成 UP 层和 RRC 层的密钥。

网络侧的 MME 收到目标 eNB 在第 9 步中发送的 NCC，其值与第 6 步中的 NCC 相同，MME 在第 10 步中将其作为参数，生成与第 7a 步中相同的 NH*，并赋值给 NH，接着在第 11 步中将 NCC 和 NH 一起发送给目标 eNB，目标 eNB 来完成第 12 步生成 KeNB*的操作，进而推导出 RRC、UP 层的其他密钥，最终 UE 和目标 eNB 共享了相同的密钥。

4.3 对改进方案的安全性分析

改进方案具有一跳前向安全性。采用第 3 部分中的 2 种敌手模型对该方案进行分析：

(1) 敌手仅拥有获取空口通信的能力

此种情况下，敌手能够得到的密钥参数包括：目标 PCI、EARFCN-DL、NCC，以及目标 eNB 选定的接入层保护算法标识。新密钥 KeNB* = KDF (NH，目标 PCI，EARFCN-DL)，它的推导绑定了参数 NH，敌手无法得到 NH，因此也就不能得到新的 eNB 密钥。

(2) 敌手拥有获取空口信号的能力，并控制了源 Enb

此种情况下，敌手可以获得模型 1 中的所有密钥参数。由于敌手又控制了源 eNB，还可以获得原来的 NH。然而，要推导出切换之后目标 eNB 的密钥 KeNB* = KDF (NH，目标 PCI，EARFCN-DL)，敌手首先要得最新的 NH，但是最新的 NH 的推导有接入层最高级密钥 KASME 的参与，KASME 不离开 UE 和 MME，敌手无法得到 KASME，也就无法推导出最新的 NH，因此控制了源 eNB 的敌手无法也得到用户切换后的 eNB 新密钥，也就是说上述方案具有一跳前向安全性。

4.4 改进方案与标准方案的性能对比分析

首先，硬件方面，改进方案对原方案的硬件设备改动很小，只需要调整实现 KDF 函数的电路，若 KDF 函数采用软件实现，则不需要对硬件做改动，为升级带来了便利。可见，硬件方面，改进方案的性能与原方案保持一致。

其次，在消息、信令的网络传输方面，改进方案通过 X2 接口传递的网络消息数量比标准方案少 2 次，通过 Uu 和 S1 接口传递的网络消息数量与标准方案一致。由于在终端和实体上的处理时间相对于网络传输时延可以忽略不计，可见，改进方案在网络传输方面比标准方案开销略小。

最后，在设计思想方面，改进方案最大限度的继承了标准方案的思想，没有调整标准方案中的密钥参数个数以及种类，也不需要修改相应的 S1 切换密钥更新协议，只需调整网络传输的参数和部分密钥推导函数等软、硬件，使得标准方案可以顺利过渡到本方案，在性能上比标准方案略好。

5 结语

本文主要针对 LTE 标准技术规范中的 X2 切换密钥更新协议进行了介绍，并分析了其缺陷——仅能提供两跳前向安全性。同时，我们提出了一个改进方案，不仅最大限度的继承了原有方案的思想，还弥补了原方案的缺陷，提供了一跳前向安全性，并使得原方案可以顺利过渡到本方案。

参考文献

1 Astély D, Dahlman E, Furuskär A, et al. LTE: the evolution of mobile broadband. IEEE Communications Magazine, 2009, 47: 44-51.

2 Forsberg D, Huang L, Tsuyoshi K, Alanara S. Enhancing security and privacy in 3GPP E-UTRAN radio interface, in proc. 18th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC07). 2007. 1-5.

3 Forsberg D. LTE key management analysis with session keys context. Computer Communications, 2010,33:1907-1915.

4 3GPP, 3GPP System Architecture Evolution (SAE), Security architecture, 3GPP TS 33.401 v9.4.0, 2010.

5 3GPP, Evolved Universal Terrestrial Radio Access (E-UTR A) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN), Overall description, 3GPP TS 36.300 v10.0.0, 2010.

6 3GPP, Evolved Universal Terrestrial Radio Access Network (E-UTRAN), architecture description, 3GPP TS 36.401 v9.2.0, 2010.

(上接第 51 页)

4 雷秀娟,史忠科,孙瑰琪.基于遗传算子的粒子群优化算法的比较分析.计算机工程与应用,2008,44(14):65-67.

5 高鹰,谢胜利.免疫粒子群优化算法.计算机工程与应用,2004,6:4-6.

6 高鹰,谢胜利.基于模拟退火的粒子群优化算法.计算机工程与应用,2004,1:47-49.

7 Thangaraj R, Pant M, Nagar AK. Maximization of Expected Target Damage Value Using Quantum Particle Swarm Optimization. Developments in eSystems Engineering (DESE), 2009 Second International Conference on. 2009. 329-334.

8 Shi YH, Eberhart RC. A modified particle swarm optimizer. Proc. of the IEEE Congress on Evolutionary Computation. Piscataway, USA: IEEE Service Center, 1998. 69-73.

9 Sun J, Feng B, Xu WB. Particle swarm optimization with particles having quantum behavior. Proc. of 2004 Congress on Evolution Computation. Piscataway. NJ: IEEE Press, 2004. 325-331.

10 刘昊,李大卫,王莉.遗传并行粒子群优化算法及其性能分析.辽宁科技大学学报,2008,31(5):495-499.

11 林星,冯斌,孙俊.基于边界变异的量子粒子群优化算法.计算机工程,2008,34(12):187-188.

12 李剑,王乘.一种改进的自适应微粒群优化算法.华中科技大学学报(自然科学学报),2008,38(3):118-121.