doi:10.3969/j.issn.1000-436x.2013.z1.023

LTE-A 中继场景下切换的安全处理研究

吴昊，王涛，吴韶波
（北京交通大学 轨道交通控制与安全国家重点实验室，北京 100044)

摘 要：中继作为 LTE-A 的关键技术之一，既能优化网络覆盖，还可以提高系统容量。然而中继的引入也为系统带来了诸多安全挑战。分析了中继部署场景下用户终端切换时的安全问题，给出不同切换场景模式的安全解决方案，以保证切换后通信的正常进行，并且通过建立 Petri 网络模型对所设计流程进行了分析。最后，对移动中继切换时的安全处理进行了讨论。
关键词：LTE-A；中继；安全；切换处理
中图分类号：TN929.5 **文献标识码**：B **文章编号**：1000-436X(2013)Z1-0176-06

Research on relay related handover security in LTE-A

WU Hao, WANG Tao, WU Shao-bo
(State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044,China)

Abstract: As one of the key technologies in LTE-A, relay can both optimize coverage of the network and increase the system capacity. However, the introducing of relay also brings many security challenges to the system. The security issues in relay related handover processes were mainly analyzed, and then the corresponding solutions were proposed for security handling. With those solutions, mobile users in the network can communicate effectively after the handover process. The designed process was also analyzed by using Petri network model. Finally, the handover security of mobile relay was discussed.
Key words: LTE-A; relay; security; handover

1 引言

LTE-A(LTE advanced)系统对容量具有较高需求，在 LTE-A 系统中引入了中继（relay）节点设备[1,2]，这可以给系统带来诸多好处，如提高系统频谱效率、增大系统容量、满足用户的高速数据传输要求等[3,4]。然而，由于中继节点设备本身所具有的一些特殊性，在具体实现时，中继的引入将给网络带来一系列新的有待解决的安全问题[5~7]。例如，由于中继节点分布于实际网络中，势必会导致由于用户终端 UE 移动而发生的切换事件的多样性增加，将会出现一些新的与中继有关的切换场景。原有的切换安全处理不再适用于这些新场景。因此，需要专门设计与中继相关的切换安全处理流程，保证切换前后用户终端通信的正常进行[8~10]。

本文将针对中继部署情况下用户终端切换时的安全问题进行分析，给出相应的安全解决方案，保证在切换过程中源节点和目标节点具有同步的安全信息，进而保证切换后通信的正常进行。论文最后还对移动中继切换时的安全处理进行了展望。

2 LTE-A 中继部署的安全架构

2.1 LTE-A 中继部署场景结构

在实际网络部署中，可以通过多种手段来提高网络的覆盖和吞吐量，部署中继就是其中之一。通过中继节点的部署，不但可以提高小区边缘的吞吐量，增加高数据率的覆盖，还可以用于支持群移动的通信场景或满足临时性的网络部署需求。

收稿日期：2013-07-05
基金项目：国家自然科学基金资助项目（U1261109）；教育部科学技术研究重大基金资助项目（313006）
Foundation Items: The National Natural Science Foundation of China(U1261109); Key Grant Project of Chinese Ministry of Education(313006)

在 LTE-A 的 E-UTRAN（演进的通用无线接入网）通过引入 RN（relay node）来支持中继通信，通常 RN 以无线方式与 eNB（演进的 NodeB 节点）相连，为 RN 提供服务的 eNB 节点称为 DeNB（donor eNB）。RN 和 DeNB 之间的空口，称为 Un 口，Un 口是基于对普通 UE（用户终端）和 eNB 之间的 Uu 接口修改得到的。LTE-A 网络中中继部署的场景如图 1 所示。

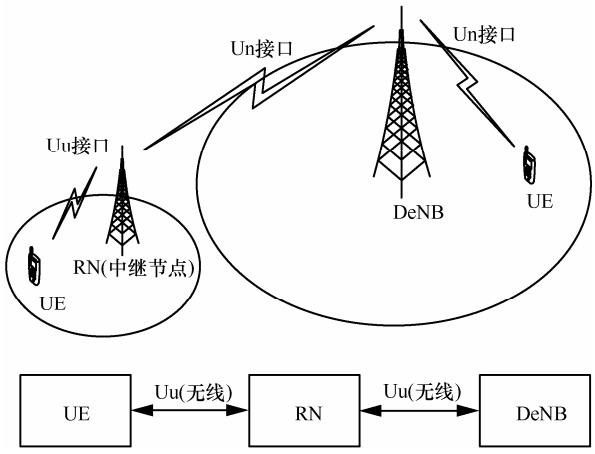

图 1　LTE-A 中中继部署场景

由图 1 可见，在 E-UTRAN 中引入 RN 后，传统 UE 与 eNB（此处为 DeNB）之间的空中接口被分为了两段，即 UE 和 RN 之间的无线接口 Uu 接口，也称作接入链路（access link）以及 RN 和 DeNB 之间的无线接口 Un 接口，也称作回程链路（backhaul link）。

RN 在网络中具有双重角色，相对于普通的 UE 用户，RN 扮演的是 eNB 角色，能够为连接到 RN 的 UE 提供网络接入服务。相对于网络侧的 DeNB，RN 在一定程度上扮演了 UE 的角色，接受 DeNB 提供的网络接入服务。

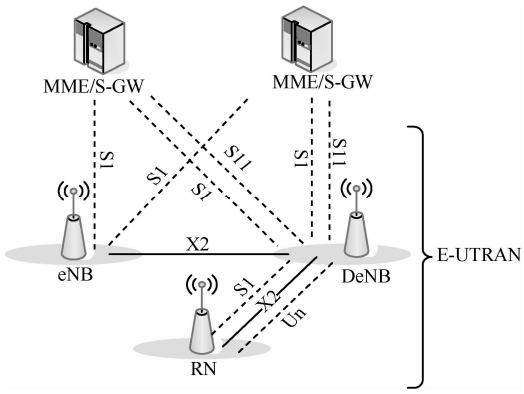

图 2　LTE-A 中中继部署网络结构

LTE-A 网络中引入中继节点之后的网络结构[1,2]，如图 2 所示。图中 MME 为移动管理实体(mobility management entity)，S-GW 为服务网关(serving gateway)。由图 2 可见，RN 与 DeNB 之间除了 Un 接口的无线连接外，还存在 S1/X2 接口，DeNB 与其他的 eNB 之间还有 X2 接口，DeNB 和 MME/S-GW 之间除了传统的 S1 接口外，还存在着 S11 连接。其中 RN 作为 S1/X2 接口、Un 接口的终结点，DeNB 在 RN 和其他网络实体（MME、S-GW、其他 eNB）之间充当 S1/X2 代理功能。S1/X2 代理功能包括传递 UE 的 S1/X2 信令消息以及 RN 和其他网络实体之间 S1/X2 相关的 GTP 数据分组。

2.2　中继部署场景下的密钥管理

在中继部署的场景中，中继一方面通过与 UE 用户之间的 Uu 口为 UE 用户提供网络接入服务，另一方面，又通过与 DeNB 之间的 Un 接口连接到网络侧。由之前介绍的中继部署架构可知，DeNB 具有多重功能角色，其中也包括多个功能模块。

对于中继扮演 UE 角色的情形，中继中将包含一些作为 UE 应该具有的密钥，其中包括 AKA（认证与密钥协商协议）过程中产生的 CK（加密密钥）、IK（完整性密钥）以及由 CK、IK 推演得到的父密钥 Kasme，和更下一层的子密钥 K_NAS、K_eNB[11~14]。在网络侧，AKA 过程中产生的 CK、IK 将存储在中继的 HSS（归属用户服务器）中，并在 HSS 中推演产生 Kasme，然后传送给 MME-RN，在 MME-RN 中完成利用 Kasme 推演 K_NAS 和 K_eNB 的过程，K_NAS 将在 MME-RN 中用于下一层 NAS 层（非接入层）的保护密钥的推演[15]，K_eNB 将被传送到 eNB 中，并用于进一步的 AS 层（接入层）密钥的推演。因此，对于扮演 UE 角色的中继架构中的密钥存储情况如图 3 所示。

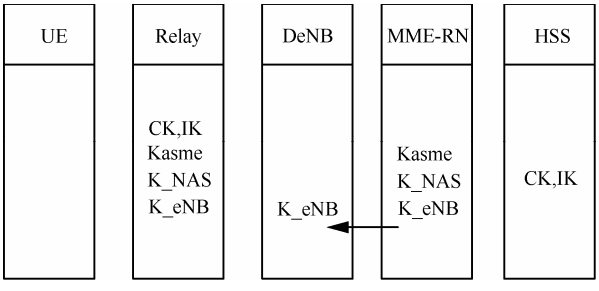

图 3　中继（relay）扮演 UE 角色时的密钥分布

当中继扮演 eNB 角色时，中继节点对于其管理下的 UE 而言仅充当一个 eNB 的功能，为 UE 提供接入服务。中继需要和相关的 OAM（操作管理维护）进行通信获取类似于 eNB 的相关配置信息。同时中继也必须提供 DeNB 连接到网络侧。中继将代表其管理下的 UE，通过 DeNB 中的相关功能模块和 S1-MME(UE)接口连接到对应 UE 的 MME-UE，同时也将通过 DeNB 中中继-GW 功能模块的 S1-U（UE）接口连接到 User-UE 的 S-GW/P-GW。其中在 MME-UE 中包含 UE 在网络侧的签约信息和相应的安全信息。

中继扮演 eNB 角色时，中继将为其管理下的 UE 提供服务，在这种情况下，中继中将包含其管理下 UE 的相关的密钥。具体的密钥存储情况为，在 UE 中，将包括 AKA 过程得到的 CK、IK 以及进一步得到的父密钥 Kasme，和更下一层的子密钥 K_NAS，K_eNB。在网络侧，对应 UE 的 HSS 中将存储 AKA 过程中产生的 CK、IK，在 HSS 中还将完成 IK、CK 到 Kasme 的推演，接着将 Kasme 通过相关消息传送给 MME-UE，并在 MME-UE 中使用 Kasme 推演 K_NAS、K_eNB。K_NAS 将在 MME-UE 中用于推演下一层的 NAS 层密钥，并用作 UE 的 NAS 层传输的保护，K_eNB 将被传送给中继，在中继中推演下一层的 AS 层密钥和用户面密钥，增强 UE 之间的数据保护。因此，对于 eNB 角色的中继架构中的密钥存储情况如图 4 所示。

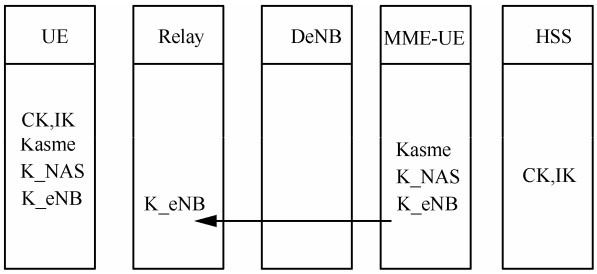

图 4 中继（Relay）扮演 eNB 角色时的密钥分布

3 中继场景下切换的安全处理

3.1 LTE-A 中继部署中 UE 的切换场景

在中继部署的情况下，处于 RN 下的 UE 将可能存在以下几种具体的切换场景。

场景 1 处于 RN 下的 UE 从 RN 切换到此 RN 所连接的 DeNB 下。此时，切换过程通过 DeNB 与 RN 之间的 X2 接口进行。

场景 2 在同一个 DeNB 下的 2 个 RN 之间进行切换。此时，DeNB 所连接的 MME 始终没有变化，切换将通过 RN 与 DeNB 之间的 X2 接口进行。

场景 3 处于 RN 下的 UE 从 RN 切换到另一个 DeNB 下。这种切换可能通过 2 种方式进行。如果源 RN 所连接的 DeNB 与目标 DeNB 连接的是相同的 MME，那么切换将通过 2 个 DeNB 之间的 X2 接口进行。如果源 RN 所连接的 DeNB 与目标 DeNB 分别连接的是不同的 MME，那么切换将通过 DeNB 与 MME 之间的 S1 接口进行，切换的过程将包括 MME 的重定向。

场景 4 一个 RN 下的 UE 从 RN 切换到连接了另一个 DeNB 的 RN 下。这种切换可能通过 2 种方法进行。当源侧 RN 所连接的 DeNB 与目标侧 RN 所连接的 DeNB 都与相同的 MME 来连接时，切换将通过这 2 个 DeNB 之间的 X2 接口进行。当源侧 RN 的 DeNB 与目标侧 RN 的 DeNB 分别连接了不同的 MME 时，切换的进行需要通过 DeNB 与 MME 之间的 S1 接口交换信息，执行的是 S1 切换。

场景 5 UE 从 eNB（或 DeNB）切换到 RN 下。这种场景下的切换通过 DeNB 与 RN 之间的 X2 接口进行。

3.2 切换过程及安全处理举例

由于篇幅受限，本文仅以场景三为例讨论处于 RN 下的 UE 从 RN 切换到另一个 DeNB 下的切换过程及安全处理。

当 RN 下的 UE 通过 X2 接口切换到另一个 DeNB 下时，目标侧使用的安全密钥可以在源中继节点中推演产生，也可以由源 DeNB 产生[16]。具体的切换流程由图 5 所示。

图 5 中 NCC(next hop chaining counter)为下一跳链路计数器，NH(next hop key)为下一跳密钥，主要用于切换或密钥更新过程中进行前向的安全保护。KeNB 主要用于进行 RRC 层密钥和用户面加密密钥的推演，同时 KeNB 也是切换过程中需要使用的密钥。K*eNB 主要是由用户设备(ME, mobile equipment)和 eNB 在垂直和水平密钥推演得到的安全密钥。当源侧的 RN 连接到的 DeNB 与目标侧 DeNB 所连接的是不同的 MME，那么将进行 S1 切换，其中包括 MME 的重定向过程。切换中目标侧

使用的密钥可以由源侧的中继进行推演，也可以由源侧的 DeNB 进行推演，具体的切换过程中安全处理如图 6 所示。

以上针对目标侧与源侧连接是否是相同的 MME，分别给出了经过 X2 接口以及 S1 接口进行的切换过程的安全处理。通过以上的处理，可以使

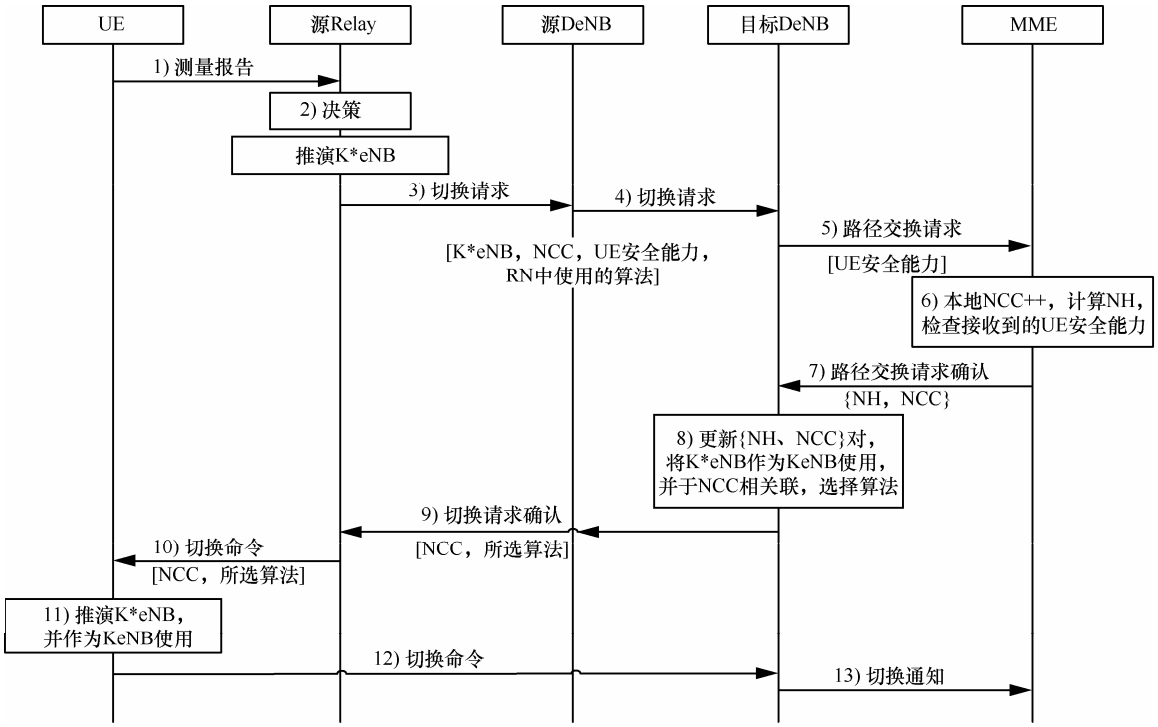

图 5　UE 通过 X2 接口从 RN 切换到另一个 DeNB

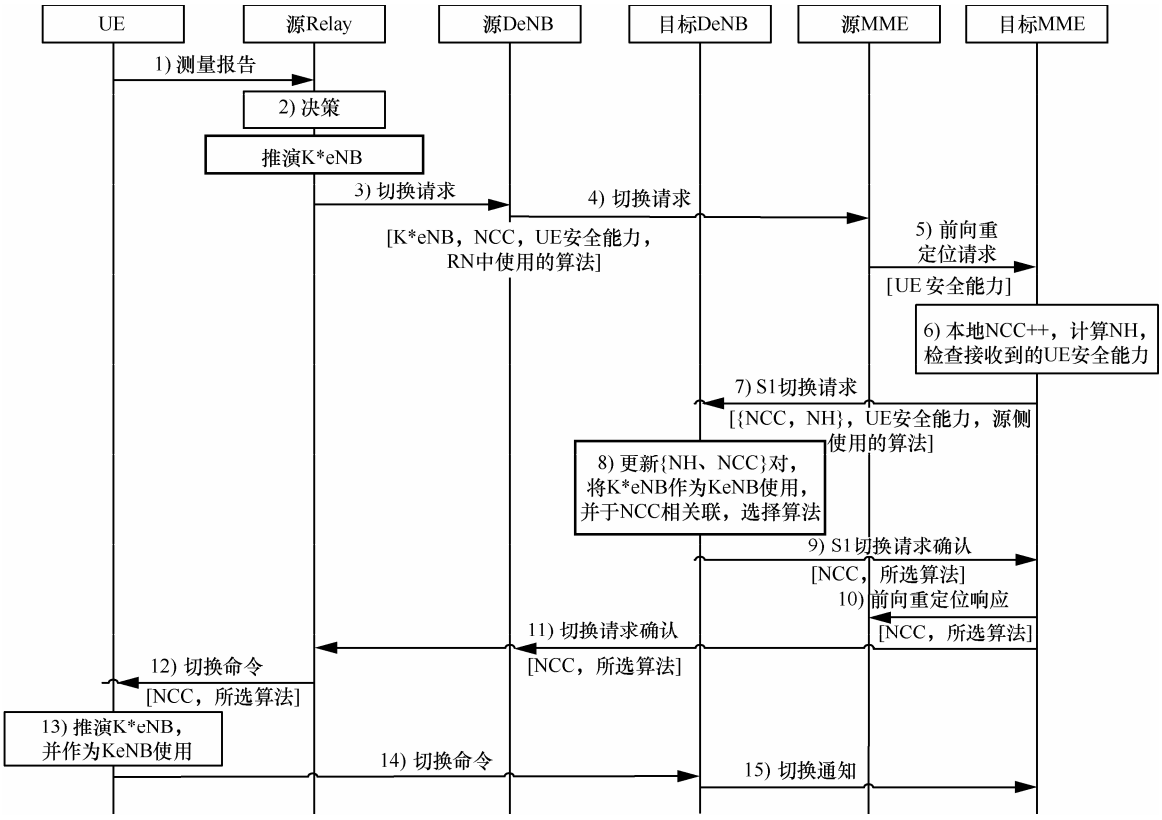

图 6　UE 经过 S1 接口从 RN 切换到另一个 DeNB

目标侧和源侧具有一致的安全信息，从而保证 UE 切换前后通信的正常进行。

4 切换安全处理过程分析

不同场景下的切换处理过程，具有以下的共同特点。

源侧负责为目标小区和重建小区进行安全密钥的推演，并将对应的安全密钥放在相应的切换消息发送到目标侧。其中，当源小区为 RN 下的小区时这些目标侧密钥的推演可以由源侧的 RN 进行，也可以由源侧 RN 所连接的 DeNB 进行。

当切换的目标小区处于某一个 RN 下，并且重建小区有可能包括此 RN 所连接的 DeNB 下的小区时，DeNB 应该具备截取发往目标侧的消息中的关于重建小区安全信息的能力。

UE 的 EPS（演进分组系统）安全能力应该通过相应的切换消息由源侧发送到目标侧，目标侧网络实体将根据接收到的 UE 安全能力和本身存储的算法优先级列表，选择 UE 能够支持并且优先级较高的加密算法和完整性保护算法作为目标侧使用的算法。算法的选择由目标侧进行，并通过切换命令指示给 UE。

需要注意的是在切换请求消息中还需要包含 UE 在源小区中使用的安全算法的信息，这是为了在切换过程中能够对与源侧之间交互的切换消息进行加解密和完整性检查。

使用了 Petri 网络仿真工具对不同切换进行建模并分析时间开销等参数。以场景三为例，通过将模型中不同的接口传输时延和节点处理开销进行了量化，以一定的随机分布加入了网络链路的开销，同时设置一定数量的网络数据分组作为 2 种切换中点之间传输的信息[17]。对仿真得到的 2 种不同切换处理过程的开销进行统计，结果如图 7 所示。

图 7 所示为网络中中继下的 UE 用户从不同的接口切换到其他 DeNB 下的过程中占用的时延开销的分布。其中实心圆点所示为通过 DeNB 与 MME 之间的 S1 接口进行切换的情况，空心圆点为通过源 DeNB 和目标 DeNB 之间的 X2 接口进行切换的情况。

由图 7 可知，在以上 2 种切换过程中，由于中间将经过较多步的处理和传输，具体的处理时延受链路特性和网络节点处理随机性的影响较明显，因此对应的时延处理的分布较广，并且在中间段的出现的频次相对集中。另一方面，相应的 X2 切换占用的平均延时较 S1 切换的时延大一些。如图 7 中，相比起 S1 切换的时延分布情况，X2 切换的时延分布更加集中一些，并且更多地处于开销较大的区域。

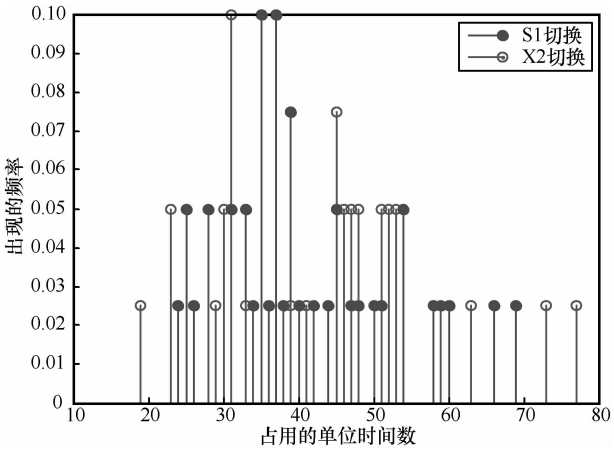

图 7 RN 切换到其他 DeNB 情况的开销分布

通过以上场景对应的切换过程中指出的安全处理方法，可以在保证切换顺利进行的同时，使在切换完成之后，UE 和切换的目标侧网络实体中具有相同的安全上下文信息并保证双方将使用一致的安全算法。从而保证切换完成之后，UE 能够进行正常的通信，并采用有效的算法和安全信息保证通信的安全进行。

5 结束语

由于中继的引入，网络中将出现较多的切换场景。要保证切换前后用户通信的通畅，就必须要使在切换的目标侧能够推演出用户所使用的安全密钥和算法。在本文中，讨论了不同的切换场景下相应的切换流程和安全处理，保证了用户切换的目标侧能够获得与用户终端一致的安全上下文，从而保证用户通信的正常进行。

目前标准中讨论的部署在 LTE-A 网络中的中继节点主要是固定部署的，RN 不支持在 DeNB 之间进行移动的特性。而随着目前以高速铁路为代表的高速交通网的大力建设，为了满足人们网络接入和通信服务需求，移动中继将成为未来发展的趋势。

在移动中继的部署场景下，由于在 DeNB 之间进行移动的节点是移动 中继本身，相对于 UE 用户而言为其提供服务的中继并没有发生变化。因此在

这个过程中为了保证移动 中继节点进行切换以后通信的正常进行，在切换过程中需要进行从源侧节点到目标侧节点的相关的密钥的传递过程。因此可以考虑尽量维持 Uu 接口上 UE 与中继之间使用的密钥不变。这在未来的研究工作中将展开深入的分析与讨论。

参考文献：

[1] KANCHEI L, WU C C, SHEU S T. IMT-advanced relay standards[J]. IEEE Communications Magazine, 2010, 48(8): 40-48.

[2] 王竞, 刘光毅. LTE-Advanced 系统中中继技术研究和标准化[J]. 电信科学, 2010, 26(12): 138-143.
WANG J, LIU G Y. Research and standardization of relay in LTE-advanced[J]. Telecommunications Science, 2010, 26(12): 138-143.

[3] SALEM M, ABDULKAREEM A, YANIKOMEROGLU H. Opportunities and challenges in OFDMA-based cellular relay networks: a radio resource management perspective[J]. IEEE Transactions on Vehicular Technology, 2010, 59(5): 2496-2510.

[4] 宋斌, 何锟. 中继技术在 LTE-Advanced 系统中的应用[J]. 广东通信技术, 2009, 29(12): 40-43.
SONG B, HE K. The Application of Relay in LTE-Advanced Systems[J]. Guangdong Communication Technology. 2009, 29(12): 40-43.

[5] 3GPP TR 33.816. Feasibility Study on LTE Relay Node Security[S]. 2011.

[6] 3GPP TR 33.801. Access Security Review[S]. 2005.

[7] HERCEG D. LTE transport security[A]. The 34th International and Communication Technology, Electronics and Microelectronics[C]. MIPRO, Opatija, 2011. 1464-1467.

[8] HAN C K, CHOI H K, JUNG W Z. Evaluation of authentication signaling loads in 3GPP LTE/SAE networks[A]. IEEE 34th Conference on Local Computer Networks (LCN 2009)[C]. Zurich, Switzerland, 2009.37-44.

[9] HUANG X L. Ulupinar fatih, agashe parag, LTE relay architecture and it's upper layer solutions[A]. IEEE Global Telecommunications Conference (GLOBECOM 2010)[C]. Miami, 2010. 1-6.

[10] SHI Z Y, JI Z L, GAO Z B. Layered security approach in LTE solution and simulation[A]. Proceedings of the 3rd International Conference on Anti-Counterfeiting, Security and Identification in Communication[C]. Hong Kong, 2009.171-173.

[11] 3GPP TR 33.859. UTRAN Key Management Enhancement[S]. 2012.

[12] FORSBERG D. LTE key management analysis with session keys context[J]. Computer Communications, 2010, 33(16): 1907-1915.

[13] LIU H, SONG J L. Research and implementation of encryption and integrity protection in LTE access stratum[A]. Asia-Pacific Youth Conference on Communication Technology (APYCCT 2010)[C]. Kunming, China, 2010.37-41.

[14] MUN H, HAN K, KIM K. 3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA[A]. 2009 Wireless Telecommunications Symposium[C]. Prague, 2009. 309-316.

[15] LIU H, BAI S. Research and implementation of LTE NAS security[A]. International Conference on Educational and Information Technology Proceedings (ICEIT 2010)[C]. Chongqing, China, 2010.453-456.

[16] RAJAVELSASMY R, CHOI S. Security aspects of inter-access system mobility between 3GPP and non-3GPP networks[A]. 2008 3rd International Conference on Communication System Software and Middleware and Workshops[C]. Bangalore, 2009.209-213.

[17] ZHANG Y C, LIU W, LOU W J, *et al*. Location-based compromise-tolerant security mechanisms for wireless sensor networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 247-260.

作者简介：

吴昊（1973-），女，河南许昌人，博士，北京交通大学教授，主要研究方向为移动通信、网络安全和车载网。

王涛（1986-），男，云南大理人，北京交通大学硕士生，主要研究方向为移动通信和网络安全。

吴韶波（1970-），女，黑龙江哈尔滨人，北京交通大学博士生，主要研究方向为异构无线网络安全。