(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2011 年 11 月 10 日 (10.11.2011)

PCT

(10) 国际公布号
WO 2011/137805 A1

(51) 国际专利分类号:
*H04W 8/24* (2009.01) *H04W 88/16* (2009.01)
*H04W 12/04* (2009.01) *H04W 88/08* (2009.01)

(21) 国际申请号: PCT/CN2011/074418

(22) 国际申请日: 2011 年 5 月 20 日 (20.05.2011)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201010229797.4 2010 年 7 月 15 日 (15.07.2010) CN

(71) 申请人 (对除美国外的所有指定国): **华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **张冬梅 (ZHANG, Dongmei)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **焦斌 (JIAO, Bin)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **刘晓寒 (LIU, Xiaohan)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **陈璟 (CHEN, Jing)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **张爱琴 (ZHANG, Aiqin)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF,

[见续页]

(54) **Title**: METHOD, APPARATUS AND SYSTEM FOR SECURITY PROCESSING IN SWITCH PROCESS

(54) **发明名称** : 切换过程中的安全处理方法、装置和系统

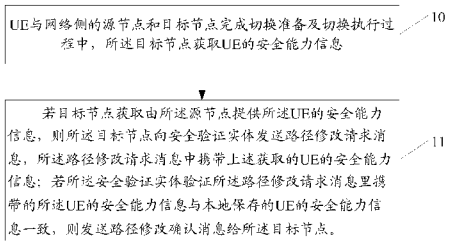


图 1 / Fig. 1

10 IN THE PROCESS THAT THE UE PERFORMS SWITCH PREPARATION AND SWITCH EXECUTION WITH THE SOURCE NODE AND THE TARGET NODE ON THE NETWORK SIDE, THE TARGET NODE ACQUIRES THE UE SECURITY CAPABILITY INFORMATION

11 IF THE TARGET NODE ACQUIRES THE UE SECURITY CAPABILITY INFORMATION PROVIDED BY THE SOURCE NODE, THE TARGET NODE SENDS A PATH MODIFICATION REQUEST MESSAGE TO THE SECURITY AUTHENTICATION ENTITY, THE PATH MODIFICATION REQUEST MESSAGE CARRIES THE ACQUIRED UE SECURITY CAPABILITY INFORMATION; IF THE SECURITY AUTHENTICATION ENTITY VALIDATES THAT THE UE SECURITY CAPABILITY INFORMATION CARRIED BY THE PATH MODIFICATION REQUEST MESSAGE IS CONSISTENT WITH THE LOCAL STORED UE SECURITY CAPABILITY INFORMATION, THE SECURITY AUTHENTICATION ENTITY SENDS A PATH MODIFICATION CONFIRMING MESSAGE TO THE TARGET NODE

(57) **Abstract**: A method, an apparatus and a system for security processing in a switch process in the communication technology field, wherein the method includes that: in the process that a User Terminal(UE) performs switch preparation and switch execution with a source node and a target node on the network side, the target node acquires UE security capability information provided by the source node or a security authentication entity; the security authentication entity includes a gateway in a scene that the UE switches between base stations or a donor base station in a scene that the UE switches between relay nodes; if the UE security capability information is provided by the source node, the method further includes that: if the security authentication entity validates that the UE security capability information carried by a path modification request message is consistent with the local stored UE security capability information, the security authentication entity sends a path modification confirming message to the target node. The embodiments of the present invention ensure that the target node can select an appropriate security arithmetic, accordingly the security of the optimization switch process is further improved.

[见续页]

WO 2011/137805 A1

CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

**本国际公布**:

— 包括国际检索报告(条约第 21 条(3))。

— 在修改权利要求的期限届满之前进行，在收到该修改后将重新公布(细则 48.2(h))。

— 根据申请人的请求，在条约第 21 条(2)(a)所规定的期限届满之前进行。

**(57) 摘要**:

一种通信技术领域切换过程中的安全处理方法、装置及系统，包括：用户设备UE与网络侧的源节点和目标节点完成切换准备及切换执行过程中，所述目标节点获取由所述源节点或安全验证实体提供的UE的安全能力信息；所述安全验证实体包括：基站下的UE切换场景中的网关或中继节点relay下的UE切换场景中的锚点基站；若由所述源节点提供所述UE的安全能力信息，则所述方法还包括：若所述安全验证实体验证所述路径修改请求消息里携带的所述UE的安全能力信息与本地保存的UE的安全能力信息一致，则发送路径修改确认消息给所述目标节点。本发明实施例保证了目标节点能够选择合适的安全算法，从而进一步提高了优化切换过程的安全性。

# 切换过程中的安全处理方法、装置和系统

本申请要求于2010年7月15日提交中国专利局、申请号为201010229797.4、发明名称为“切换过程中的安全处理方法、装置和系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

## 技术领域

本发明涉及网络通讯技术领域，具体涉及切换过程中的安全处理技术。

## 发明背景

长期演进（Long Term Evolution，LTE）系统中，终端设备可以通过接入设备接入到核心网中的移动性管理实体（Mobility Management Entity，MME）。接入设备如家庭演进基站（Home Evolved NodeB，HeNB）、锚点演进基站（Donor evolved NodeB，DeNB）或者中继（Relay）等。其中HeNB可能需要通过家庭演进基站网关（Home Evolved NodeB Gate Way，HeNB GW）路由到合适的MME。

在实际的应用中，用户设备（User Equipment，UE）可以在HeNB GW之间或者Relay之间进行切换。在切换过程中，切换信令通常终结在MME上，即MME需要参与到切换过程中，由MME进行切换过程中的安全处理，以保证切换前向安全和后向安全。

在一些应用场景（如企业网以及Relay系统等）中，为了减少MME的信令处理压力，提出了优化切换，即切换信令终结在HeNB GW或者DeNB上，而不是终结在MME上。

在实现本发明的过程中，发明人发现：优化切换可以避免或者减少MME与接入设备之间的信息交互，现有的优化切换过程中没有考虑安全处理的解决方案。

## 发明内容

本发明实施方式提供的切换过程中的安全处理方法、装置及系统，为优化切换提供了安全处理的解决方案。

本发明实施方式提供的切换过程中的安全处理方法，包括:

本发明实施方式提供一种切换过程中的安全处理方法，包括:

用户设备UE与网络侧的源节点和目标节点完成切换准备及切换执行过程中，所述目标节点获取由所述源节点或安全验证实体提供的UE的安全能力信息；所述安全验证实体包括：基站下的UE切换场景中的网关或中继节点relay下的UE切换场景中的锚点基站;

若目标节点获取由所述源节点提供所述UE的安全能力信息，则所述方法还包括:

所述目标节点向安全验证实体发送路径修改请求消息，所述路径修改请求消息中携带上述获取的UE的安全能力信息；若所述安全验证实体验证所述路径修改请求消息里携带的所述UE的安全能力信息与本地保存的UE的安全能力信息一致，则发送路径修改确认消息给所述目标节点。

本发明实施方式提供一种安全验证实体，所述安全验证实体为：基站下的用户设备UE切换场景中的网关或中继节点relay下的UE切换场景中的锚点基站；所述安全验证实体包括:

接收单元，用于接收目标节点发送的路径修改请求消息，所述路径修改请求消息中携带源节点提供给目标节点的UE的安全能力信息;

验证单元，用于验证所述路径修改请求消息里携带的所述UE的安全能力信息与本地保存的UE的安全能力信息是否一致;

发送单元，用于在验证所述路径修改请求消息里携带的所述UE的安全能力信息与本地保存的UE的安全能力信息一致情况下发送路径修改确认消息给所述目标节点。

本发明实施方式提供一种切换过程中安全处理系统，包括：源节点、目标节点及如上所述的安全验证实体;

所述目标节点在切换准备及切换执行过程中获得由所述源节点提供的UE的安全能力信息;

所述安全验证实体通过将所述源节点提供的所述UE的安全能力信息与本地保存的UE的安全能力信息比较，以验证所述源节点提供的所述UE的安全能力信息是否安全。

本发明实施方式提供一种安全验证实体，所述安全验证实体为：基站下的用户设备UE切换场景中的网关或中继节点relay下的UE切换场景中的锚点基站；所述安全验证实体包括:

接收单元，用于接收源节点发送的切换请求消息；

转发单元，用于转发所述切换请求消息给目标节点，在转发的所述切换请求消息中携带所述安全验证实体本地保存的UE的安全能力信息。

本发明实施方式提供一种切换过程中的安全处理系统，包括：源节点、目标节点及如上所述的安全验证实体；

所述安全验证实体在切换准备过程中提供UE的安全能力信息给所述目标节点。

由上述本发明实施例提供的技术方案可以看出，本发明实施例在优化切换过程中，目标节点获得由安全验证实体提供的可靠的UE的安全能力信息，或者获得由源节点提供的UE的安全能力信息，再经安全验证实体对该源节点提供的UE的安全能力信息的验证，保证了源节点发送的UE的安全能力信息的可信性，因此保证了目标节点能够选择合适的安全算法，从而进一步提高了优化切换过程的安全性。

## 附图简要说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图1是本发明实施例一切换过程中的安全处理方法示意图；

图2是本发明实例一切换过程中的安全处理方法流程图；

图3是本发明实例二切换过程中的安全处理方法流程图；

图4是本发明实例五切换过程中的安全处理方法流程图；

图5是本发明实例六切换过程中的安全处理方法流程图；

图6是本发明实例七切换过程中的安全处理方法流程图；

图7是本发明实施例二安全验证实体一种结构示意图；

图8是本发明实施例二安全验证实体另一种结构示意图；

图9是本发明实施例二安全验证实体又一种结构示意图；

图10是本发明实施例四安全验证实体一种结构示意图；

图11是本发明实施例四安全验证实体另一种结构示意图；

图12是本发明实施例四安全验证实体又一种结构示意图；

图13是本发明实施例四安全验证实体再一种结构示意图。

## 实施本发明的方式

下面通过实施例对本发明的具体实现过程进行例举说明。显然，下面所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

本发明实施例提供一种切换过程中的安全处理方法，如图1中所示，包括如下步骤:

步骤10：UE与网络侧的源节点和目标节点完成切换准备及切换执行过程中，所述目标节点获取UE的安全能力信息;

本发明实施例所述的安全验证实体包括：基站下的UE切换场景中的网关，例如，HeNB GW，或中继节点relay下的UE切换场景中的锚点基站，例如HeNB; 本实施例所述源节点及目标节点包括：基站下的UE切换场景中的基站，如，HeNB；或，relay下的UE切换场景中的relay;

也就是，本发明实施例所述方法既适用于relay下的UE切换又适用于基站下的UE切换。

另外，所述源节点和目标节点完成切换准备及切换执行过程中，源节点可以经过所述安全验证实体发送所述切换请求消息给所述目标节点；所述目标节点经过所述安全验证实体发送所述切换响应消息给所述源节点。也可以所述源节点与所述目标节点间直接通信，传递切换请求消息和切换响应消息。

所述目标节点获取的UE的安全能力信息由所述源节点或安全验证实体提供；若由所述源节点提供所述UE的安全能力信息给所述目标节点，则执行步骤11;

步骤11：所述目标节点向安全验证实体发送路径修改请求消息，所述路径修改请求消息中携带上述获取的UE的安全能力信息；若所述安全验证实体验证所述路径修改请求消息里携带的所述UE的安全能力信息与本地保存的UE的安全能力信息一致，则发送路径修改确认消息给所述目标节点。

可选地，所述安全验证实体发送的路径修改确认消息中携带下次切换备用的新鲜的安全参数，所述目标节点保存所述新鲜的安全参数。

若所述路径修改请求消息里携带的所述UE的安全能力信息与安全验证实体本地保存的UE的安全能力信息不一致，则启动报警过程。

若由安全验证实体提供所述UE的安全能力信息给所述目标节点，则可结束操作。

其中，所述安全验证实体提供所述UE的安全能力信息的方法包括：所述安全验证实体转发所述源节点发送给所述目标节点的切换请求消息，在转发的所述切换请求消息中携带所述安全验证实体本地保存的所述UE的安全能力信息。所述安全验证实体本地保存的所述UE的安全能力信息通过如下方法获得:

1）所述安全验证实体从核心网节点发送给所述安全验证实体的切换消息中获得所述UE的安全能力信息，例如，UE初始从非所述安全验证实体下的节点接入，然后切换到所述安全验证实体下的节点中，则在MME发送给所述安全验证实体下的节点的切换消息中携带UE的安全能力信息，所述安全验证实体从所述切换消息中获得所述UE的安全能力信息，具体一个实例如，UE初始从eNB接入，然后切换到HeNB中。则在UE从eNB切换到HeNB的过程中，MME会在发送给HeNB的切换消息中携带UE安全能力信息，HeNB GW可以获取该切换消息中获得UE安全能力信息;

或

2）所述安全验证实体从核心网节点发送的初始上下文建立请求消息中获得所述UE的安全能力信息，例如，UE直接接入所述安全验证实体下的节点，所述安全验证实体从MME发送的初始上下文建立请求消息中获得所述UE的安全能力信息。

在所述安全验证实体转发的所述切换请求消息中还包括：所述源节点使用的安全算法，及源节点计算的新接入层根密钥及对应的NCC。

在转发的所述切换请求消息中还可以包括：所述安全验证实体根据新鲜的安全参数计算的新的接入层根密钥及对应的NCC’；或者，在转发的所述切换请求消息中包括所述安全验证实体提供的新鲜的安全参数;

若转发的所述切换请求消息中包括所述安全验证实体根据新鲜的安全参数计算的新的接入层根密钥及对应的NCC’，则所述目标节点关联保存所述安全验证实体根据新鲜的安全参数计算的新的接入层根密钥及对应的NCC’；所述新鲜的安全参数包括新鲜的下跳链计数（NCC，next-hop chain counter）及下一跳（NH，nexthop）值。所述安全验证实体根据新鲜的安全

参数计算新的接入层根密钥的方法包括：所述安全验证实体根据目标节点所在小区的物理小区标识（PCI，physical cell identity）和下行演进型通用陆地无线接入绝对信道数（DL-EARFCN，down-link E-UTRA absolute radio frequency channel number）以及所述新鲜｛NCC，NH｝对中的NH计算新的接入层根密钥；所述目标节点的PCI和DL-EARFCN从所述源节点发送的切换请求消息中获得，或者，从所述源节点发送的切换请求消息中获得目标节点所在小区PCI，根据从切换请求消息中获得的所述PCI在本地获取DL-EARFCN。

若转发的所述切换请求消息中包括所述安全验证实体提供的新鲜的安全参数，则所述目标节点根据所述切换请求消息中携带的新鲜的安全参数计算新的接入层根密钥。

不论是安全验证实体在发送的路径修改确认消息中携带下次切换备用的新鲜的安全参数，还是安全验证实体根据新鲜的安全参数计算的新的接入层根密钥及对应的NCC'，还是在转发的所述切换请求消息中包括所述安全验证实体提供的新鲜的安全参数，对于所述安全验证实体来说，都需要获得所述新鲜的安全参数，本发明实施例所述安全验证实体获得所述新鲜的安全参数的方法包括：

一）所述安全验证实体向核心网节点发送UE安全上下文请求消息，所述消息中包含UE标识；

接收所述核心网节点发送的UE安全上下文响应消息，所述UE安全上下文响应消息中包含新鲜NCC及NH以及计算新鲜NH需要的输入参数KASME，或包含UE当前使用的NCC，NH以及计算新鲜NH需要使用的输入参数KASME，根据所述UE当前使用的NCC计算得到新鲜的NCC，根据UE当前使用的NH以及所述KASME计算得到新鲜的NH。

二）所述安全验证实体中保存有非新鲜的NCC及NH，所述安全验证实体向核心网节点发送UE安全上下文请求消息，所述消息中包含UE标识，接收所述核心网节点发送的UE安全上下文响应消息，所述UE安全上下文响应消息中包含计算新鲜NH需要使用的输入参数KASME，保存所述KASME，根据所述非新鲜的NCC计算得到新鲜的NCC，根据所述非新鲜的NH以及KASME计算得到新鲜的NH；所述保存的非新鲜的NCC及NH为所述安全验证实体从上次有核心网节点参与的切换过程中，核心网节点发送的路径修改确认消息或切换请求消息中获得；

或

所述安全验证实体中保存有非新鲜的NCC、NH及计算新鲜NH需要使用的输入参数KASME；则所述安全验证实体根据所述非新鲜的NCC计算新鲜的NCC，以及根据所述非新鲜的NH以及KASME计算得到新鲜的NH；所述保存的非新鲜的NCC及NH为所述安全验证实体在上次所述UE的切换过程中计算获得。

三）所述新鲜的安全参数从安全验证实体保存的｛NCC，NH｝列表中按照NCC值从小到大的顺序取用NCC值及对应的NH值，在所述｛NCC，NH｝列表中所有NCC，NH均被使用完后，或者所述安全验证实体内没有新鲜的NCC，NH时，所述安全验证实体获得所述｛NCC，NH｝列表，所述安全验证实体获取所述｛NCC，NH｝列表的方法包括：

安全验证实体向核心网节点发送UE安全上下文请求消息，所述消息中包含UE标识；

接收所述核心网节点发送的UE安全上下文响应消息，所述UE安全上下文响应消息中包含｛NCC，NH｝列表，所述｛NCC，NH｝列表中包含核心网节点当前的NCC及NH，以及核心网节点计算的下1跳、…下n跳的NCC及对应的NH，n为大于1的自然数；

所述安全验证实体保存所述｛NCC，NH｝列表。

若所述安全验证实体保存的所述｛NCC，NH｝列表中存在未使用的新鲜的安全参数情况下，所述UE执行有核心网节点参与的正常切换，则所述核心网节点使用本地保存的最新的安全参数进行安全处理，以及通过切换命令实现与UE的所述最新的安全参数的同步。

四）所述安全验证实体在上次优化切换的安全处理过程中，从核心网节点发送给目标节点的路径修改确认消息中截取所述新鲜的安全参数。也就是对于当前执行的优化切换的安全处理过程，在切换完成后，所述安全验证实体转发目标节点的路径修改请求消息给核心网节点，并从核心网节点发送给目标节点的路径修改确认消息中截取新鲜的安全参数保存在本地，不下发给所述目标节点，可以在下一次的优化切换的安全处理过程中使用。

本发明实施例在优化切换过程中，目标节点获得由安全验证实体提供的可靠的UE的安全能力信息，或者获得由源节点提供的UE的安全能力信息，再经安全验证实体对该源节点提供的UE的安全能力信息的验证及触发

告警，保证了源节点发送的UE的安全能力信息的可信性，因此保证了目标节点能够选择合适的安全算法，从而进一步提高了优化切换过程的安全性。

为便于理解上述实施例所述方法，下面以具体应用场景对上面实施例进行详细介绍:

实例一 场景为：基于X2接口的HeNB下的UE切换过程中的安全处理方法，该方法的流程如附图2所示，包括如下步骤:

步骤1、UE向源HeNB发送测量报告消息。

步骤2、源HeNB查看本地是否有UE的新鲜安全参数，如新鲜的NCC和NH，如果有UE的新鲜安全参数，则源HeNB根据新鲜安全参数中的NH计算新的接入层根密钥KeNB*；否则，源HeNB根据原接入层根密钥KeNB计算KeNB*。

所述新鲜的安全参数即未使用的安全参数，包括未使用的NCC，NH。

步骤2中源HeNB计算新的KeNB*的过程可以被描述为:

KeNB* = KDF（KeNB/NH，PCI，DL-AERFCN）；其中的KDF（*）表示密钥推衍函数，KeNB/NH、PCI和DL-AERFCN为密钥推衍函数的输入参数，PCI代表目标小区标识，DL-AERFCN代表目标小区的下行E-UTRA绝对(无线频率)信道数(down-link E-UTRA absolute radio frequency channel number）。

步骤2的一个具体例子为：如果存在连续的多次优化切换，则第一次优化切换可能会由于源HeNB本地存储有UE的新鲜安全参数，而使用KDF（NH，PCI，DL-AERFCN）计算获得KeNB*，而在后续的优化切换过程中，由于源HeNB本地没有存储UE的新鲜安全参数，因此，使用KDF（KeNB，PCI，DL-AERFCN）计算获得KeNB*。

步骤3、源HeNB向HeNB GW发送切换请求消息，该切换请求消息中包含有KeNB*、NCC、源HeNB使用的安全算法（包括完整性保护算法及加密算法）以及UE的安全能力信息。

其中，该切换请求消息中的NCC为：与KeNB*对应的NH配对的NCC，即如果利用新鲜的NH计算KeNB*，则切换请求消息中的NCC为与新鲜的NH配对的NCC；如果利用KeNB计算KeNB*，则切换请求消息中的NCC为与用于计算KeNB的NH配对的NCC。后面实施例所述的对应的NCC均为本段所述对应关系。

步骤4、HeNB GW根据目标小区信息判断出需要进行优化切换处理，则

HeNB GW将接收到的切换请求消息转发给目标HeNB。

即HeNB GW判断出所述切换是切换信令终结于所述HeNB GW，且源HeNB及目标HeNB均归属于所述HeNB GW的切换。

转发的所述切换请求消息中包含有KeNB*、NCC、源HeNB使用的安全算法（包括完整性保护算法及加密算法）以及UE的安全能力信息。

步骤5、目标HeNB接收到切换请求消息后，通过HeNB GW向源HeNB发送对应的切换响应消息，该切换响应消息中包含有NCC、目标HeNB选择的安全算法（包括完整性保护算法及加密算法）。其中该切换响应消息中包含的NCC与切换请求消息中包含的NCC相同。

步骤6、源HeNB接收到切换响应消息后，向UE发送切换命令消息，该切换命令消息中包含有NCC、目标HeNB选择的完整性保护算法以及目标HeNB选择的加密算法等。

其中，该切换命令消息中包含的NCC与切换响应消息中包含的NCC相同。

步骤7、目标HeNB将接收到的切换请求消息中包含的KeNB*作为KeNB，与NCC关联存储，该NCC为所述切换请求消息中包含的NCC。

需要说明的是，步骤7的执行时间很灵活，可以在步骤4之后，到本次安全处理结束之间的任一时间执行，本实施例不限制步骤7的具体执行时间。

步骤8、UE接收到切换命令消息后，向目标HeNB发送进行了完整性保护和加密保护的切换完成消息。

其中，UE在接收到所述切换命令消息后，将切换命令消息中包含的NCC与本地的NCC进行比较，如果两个NCC不相同，则UE根据切换命令消息中包含的NCC更新本地的NH，并利用更新后的NH计算获得KeNB*；如果两个NCC相同，则UE利用本地KeNB计算获得KeNB*。之后，UE利用KeNB*推演接入层密钥（包括接入层加密密钥和接入层完整性保护密钥），并利用KeNB*推衍出的接入层加密密钥和目标HeNB选择的加密算法对切换完成消息进行加密处理，以及利用KeNB*推衍出接入层完整性保护密钥，和目标HeNB选择的完整性保护算法对切换完成消息进行完整性保护处理；

步骤9、目标HeNB在接收到切换完成消息后，向HeNB GW发送路径修改请求消息。路径修改请求消息中包含有UE的安全能力信息。该UE的安全能力信息可以是目标HeNB在上述步骤5中从接收到的切换请求消息中获取

的。

在目标HeNB接收到切换完成消息后，完成了切换准备及切换执行过程。

步骤10、HeNB GW根据接收到的路径修改请求消息判断出需要进行优化切换处理，则HeNB GW将路径修改请求消息中包含的UE的安全能力信息与本地存储的UE的安全能力信息进行比较，如果一致，则HeNB GW不更新本地存储的NCC和NH，HeNB GW向目标HeNB发送路径修改确认消息，该消息中不包含NCC，NH。否则，HeNB GW触发报警，以表示UE的安全能力信息被更改。

本实例一是以HeNB和HeNB GW为例进行说明的，本实例所描述的安全处理方法也可以适用于Relay和DeNB的应用场景中，在此不再重复说明。

从上述实例一的描述可知，目标HeNB只知道从源HeNB发送来的KeNB*，而密钥推衍函数的不可逆推特性保证了目标HeNB无法根据KeNB*反推出源HeNB的密钥KeNB，从而实现了后向安全（即目标HeNB不能根据收到的密钥推演出切换的源侧使用的密钥）；通过由HeNB GW执行UE的安全能力信息验证以及触发报警等操作，可以在避免MME参与优化切换过程的同时，在一定程度上保证了小区的安全；从而实例一为优化切换提供了一种安全处理的解决方案。

实例二

场景为：基于X2接口的HeNB下的UE切换过程中的安全处理方法，在本实例中源HeNB和目标HeNB之间不存在直接的X2接口，需要通过HeNB GW中转源HeNB和目标HeNB之间的X2消息。该方法的流程如附图3所示，包括如下步骤:

其中，步骤1到步骤3与实例一中相同，本实例在此不再赘述。

步骤4、HeNB GW根据目标小区信息判断出需要进行优化切换处理，如果HeNB GW本地有UE的新鲜安全参数，则可以直接到步骤7；如果HeNB GW本地没有该UE的新鲜安全参数，则HeNB GW向MME发送UE Security Key Request（UE安全上下文请求）消息，所述消息中包含UE标识，以请求获取该UE的安全参数和密钥KASME。

在步骤4中，HeNB GW判断本地没有UE的新鲜安全参数的方法有多种，一个具体的例子：如果HeNB GW确定出本地没有存储UE的安全参数，则HeNB GW确定出本地没有该UE的新鲜安全参数；如果HeNB GW判断出本

地存储有UE安全参数，且UE安全参数中的NCC小于源HeNB发送来的切换请求消息中携带的NCC，则HeNB GW确定出本地没有UE的新鲜安全参数。本实施例不限制HeNB GW判断本地没有UE的新鲜安全参数的具体实现方式。

步骤5、MME向HeNB GW返回UE Security Key Response（UE安全上下文响应）消息，该UE安全上下文响应消息中可以包含有UE的安全参数。UE安全上下文响应消息中的UE的安全参数可以包含UE的新鲜安全参数（如新鲜的NCC和新鲜的NH）；也可以为UE当前使用的安全参数，即UE在源HeNB下的安全参数，还应该包含计算新鲜NH需要用的输入参数接入安全管理实体密钥（Key of Access Security Management Entity， KASME）。

步骤6、在MME向HeNB GW返回的UE安全上下文响应消息中包含的UE的安全参数是UE当前使用的安全参数的情况下，HeNB GW根据UE安全上下文响应消息中的NCC进行NCC + 1的计算，并根据UE安全上下文响应消息中的NH和密钥KASME进行计算，以获得一个新的NH，该新的NH记为NH'。这里的NCC + 1和NH'用于UE的下一次优化切换。

在MME向HeNB GW返回的UE安全上下文响应消息中包含的UE的安全参数是UE的新鲜安全参数的情况下，直接到步骤7。UE安全上下文响应消息中包含的新鲜安全参数用于UE的下一次优化切换。

需要说明的是，步骤4、步骤5和步骤6的执行时间非常灵活，可以设置于步骤3之后步骤13之前的任何位置，本实施例不限制步骤4、步骤5和步骤6所在的具体位置。

步骤7、HeNB GW向目标HeNB转发切换请求消息，转发的所述切换请求消息中包含有KeNB*、NCC、源HeNB使用的安全算法（包括完整性保护算法及加密算法）以及UE的安全能力信息。此处的UE的安全能力信息为步骤3中源HeNB在发送的切换请求消息中携带的UE的安全能力信息。

步骤8－步骤12与实例一中步骤5－步骤9相同，此处不再赘述。

步骤13、HeNB GW判断出本次切换为优化切换处理，则HeNB GW将路径修改请求消息中包含的UE的安全能力信息与本地存储的UE的安全能力信息进行比较，如果UE的安全能力信息一致，则HeNB GW向目标HeNB发送包含有UE的新鲜安全参数（如NCC+1和NH'）的路径修改确认消息，否则，HeNB GW触发报警，以表示UE的安全能力信息被更改。

步骤14、目标HeNB存储路径修改确认消息中包含的NCC+1和NH'。

本实例二是以HeNB和HeNB GW为例进行说明的，本实例所描述的安全处理方法也可以适用于Relay和DeNB的应用场景中，在此不再重复说明。

在优化切换后，该UE进行第一次正常的有MME参与的切换或者和MME通信时，需要由HeNB GW将本地保存的最新的安全参数通过UE安全上下文通知消息UE Security Context inform发送给MME，完成安全参数同步，其中，一个UE安全上下文通知消息定义的例子如下：MME UE S1AP ID，eNB UE S1AP ID，NCC，NH，还可能包括UE安全能力，NAS加密算法和完整性保护算法，以及上行/下行NAS COUNT值等；MME收到消息后回复UE安全上下文通知确认，该UE安全上下文通知确认消息定义的一个例子如下：

UE安全上下文通知确认：

MME UE S1AP ID，eNB UE S1AP ID。

从上述实例二的描述可知，目标HeNB只知道从源HeNB发送来的KeNB*，而密钥推衍函数的不可逆推特性保证了目标HeNB无法根据KeNB*反推出源HeNB的密钥KeNB，从而实现了后向安全（即目标HeNB不能根据收到的密钥推演出切换的源侧使用的密钥）；并且目标HeNB在下一次切换时作为下一次切换的源HeNB，其使用获得的新鲜的安全参数推演新的接入层根密钥，而本次切换的源HeNB无法得知该新的接入层根密钥，因此实现了前向安全。本实例通过由HeNB GW向MME请求UE安全上下文，并由HeNB GW执行NCC，NH的更新及下发操作，可以在减少MME参与优化切换过程中的安全处理操作的同时，保证了切换时的安全；通过由HeNB GW执行UE的安全能力信息验证以及触发报警等操作，保证了源小区发送的UE安全能力的可信性；从而实例二为优化切换提供了一种安全处理的解决方案。

实例三

场景同实例二，其与实例二操作不同点在于步骤4－步骤6被如下步骤代替，本实例仅介绍不同的步骤，其他步骤不再赘述。

步骤4、HeNB GW根据接收到的切换请求消息判断出需要进行优化切换处理，如果HeNB GW本地有UE的新鲜安全参数，则可以直接到步骤7；

如果HeNB GW本地保存有非新鲜的NCC及NH，则HeNB GW向MME发送UE Security Key Request（UE安全上下文请求）消息，所述消息中包含UE标识，以请求获取该UE的安全参数和密钥KASME。

HeNB GW本地保存的非新鲜的NCC及NH为所述安全验证实体从上次有MME参与的切换过程中，MME发送的路径修改确认消息或切换请求消息中获得;

其中，HeNB GW判断本地没有UE的新鲜安全参数的方法有多种，一个具体的例子：如果HeNB GW确定出本地没有存储UE的安全参数，则HeNB GW确定出本地没有该UE的新鲜安全参数；如果HeNB GW判断出本地存储有UE安全参数，且UE安全参数中的NCC小于源HeNB发送来的切换请求消息中携带的NCC，则HeNB GW确定出本地没有UE的新鲜安全参数。本实施例不限制HeNB GW判断本地没有UE的新鲜安全参数的具体实现方式。

步骤5、MME向HeNB GW返回UE Security Key Response（UE安全上下文响应）消息，该UE安全上下文响应消息中可以包含有计算新鲜NH需要使用的输入参数KASME。

步骤6、HeNB GW保存所述KASME，HeNB GW根据本地保存的非新鲜的NCC进行NCC + 1的计算得到新鲜NCC+1，并根据NCC + 1、非新鲜NH和KASME进行计算，以获得一个新的NH，该新的NH记为NH'。这里的NCC + 1和NH'用于UE的下一次优化切换。

在该UE的下一次优化切换过程中，该HeNB GW中已经保存有该UE的NCC、NH及KASME，此种情况下的NCC及NH为HeNB GW在本次切换过程中计算获得，则HeNB GW根据所述非新鲜的NCC进行NCC + 1的计算得到新鲜NCC+1，并根据NCC + 1、非新鲜NH和KASME进行计算，以获得一个新的NH。换一种方式讲，如果本次步骤4中，HeNB GW判断保存有非新鲜的NCC、NH及KASME，则所述非新鲜的NCC、NH为HeNB GW在所述UE的上一次切换过程中计算得到，所述KASME也可以为所述HeNB GW在本次切换之前的切换过程中通过向MME发送安全上下文请求获得。

本实例三是以HeNB和HeNB GW为例进行说明的，本实例所描述的安全处理方法也可以适用于Relay和DeNB的应用场景中，在此不再重复说明。

从上述实例三的描述可知，目标HeNB只知道从源HeNB发送来的KeNB*，而密钥推衍函数的不可逆推特性保证了目标HeNB无法根据KeNB*反推出源HeNB的密钥KeNB，从而实现了后向安全（即目标HeNB不能根据收到的密钥推演出切换的源侧使用的密钥）；并且目标HeNB在下一次切换时作为下一次切换的源HeNB，其使用获得的新鲜的安全参数推演新的接入层根密钥，而本次切换的源HeNB无法得知该新的接入层根密钥，因此实现

了前向安全。本实施例通过由HeNB GW向MME请求UE安全上下文，并由HeNB GW执行NCC，NH的更新及下发操作，可以在减少MME参与优化切换过程中的安全处理操作的同时，保证了切换时的安全；通过由HeNB GW执行UE的安全能力信息验证以及触发报警等操作，进一步保证了源小区发送的UE安全能力的可信性；从而实例三为优化切换提供了一种安全处理的解决方案。

实例四

场景同实例二，其与实例二操作不同点在于步骤4－步骤6被如下步骤代替，本实例仅介绍不同的步骤，其他步骤不再赘述。

步骤4、HeNB GW根据接收到的切换请求消息判断出需要进行优化切换处理，如果HeNB GW本地有UE的新鲜安全参数，则可以直接到步骤7;

如果HeNB GW本地没有新鲜的NCC及NH，则HeNB GW向MME发送UE Security Key Request（UE安全上下文请求）消息，所述消息中包含UE标识。

其中，HeNB GW判断本地没有UE的新鲜安全参数的方法有多种，一个具体的例子：如果HeNB GW确定出本地没有存储UE的安全参数，则HeNB GW确定出本地没有该UE的新鲜安全参数；如果HeNB GW判断出本地存储有UE安全参数，且UE安全参数中的NCC小于源HeNB发送来的切换请求消息中携带的NCC，则HeNB GW确定出本地没有UE的新鲜安全参数。本实施例不限制HeNB GW判断本地没有UE的新鲜安全参数的具体实现方式。

步骤5、MME向HeNB GW返回UE Security Key Response（UE安全上下文响应）消息，所述UE安全上下文响应消息中包含｛NCC，NH｝列表，所述｛NCC，NH｝列表中包含MME当前的NCC及NH，以及MME计算的NCC+1，NH1，NCC+2，NH2…直到下n跳NCC+n及其对应的NHn，n为大于1的自然数;

步骤6、所述HeNB GW保存所述｛NCC，NH｝列表，每次切换过程中按照NCC值从小到大的顺序取用NCC值及对应的NH值；并在所述｛NCC，NH｝列表中所有NCC，NH均被使用完时，再次向MME发送所述UE安全上下文请求消息，并接收MME发送的UE安全上下文响应消息。如果优化切换次数较少，HeNB GW本地的新鲜{NCC,NH}值没有用完，则MME本地的NCC肯定大于HeNB GW处的NCC，下一次有MME参与的正常切换时，MME可以直接用本地的最新NCC，NH进行安全处理，通过在切换命令里下发最

新的NCC，UE和MME里即可完成NH值的同步。

本实例四是以HeNB和HeNB GW为例进行说明的，本实例所描述的安全处理方法也可以适用于Relay和DeNB的应用场景中，在此不再重复说明。

从上述实例四的描述可知，目标HeNB只知道从源HeNB发送来的KeNB*，而密钥推衍函数的不可逆推特性保证了目标HeNB无法根据KeNB*反推出源HeNB的密钥KeNB，从而实现了后向安全（即目标HeNB不能根据收到的密钥推演出切换的源侧使用的密钥）；并且目标HeNB在下一次切换时作为下一次切换的源HeNB，其使用获得的新鲜的安全参数推演新的接入层根密钥，而本次切换的源HeNB无法得知该新的接入层根密钥，因此实现了前向安全。本实例通过由HeNB GW向MME请求UE安全上下文，MME下发｛NCC，NH｝列表，而不需下发KASME，可以减少MME参与优化切换过程中的安全处理操作，同时，由HeNB GW向MME请求UE安全上下文，并由HeNB GW执行NCC，NH的更新及下发操作，可以在减少MME参与优化切换过程中的安全处理操作的同时，保证了切换时的安全；通过由HeNB GW执行UE的安全能力信息验证以及触发报警等操作，进一步保证了源小区发送的UE安全能力的可信性；从而实例四为优化切换提供了一种安全处理的解决方案。

上述实例一至实例四同样适用于源HeNB和目标HeNB之间存在X2接口，即X2接口终结在HeNB上的场景，则此种情况下，对于实例二至实例四中的步骤4－步骤6应该在HeNB GW接收到目标HeNB发送的路径修改请求消息之后执行，源HeNB和目标HeNB之间直接通信而不需要HeNB GW转发，具体执行过程本实施例不再赘述。

实例五

场景为：基于S1接口的HeNB下的UE切换过程中的安全处理方法，该方法的流程如附图4所示，包括如下步骤：

步骤1：UE向源HeNB发送测量报告消息；

步骤2：源HeNB查看本地是否有新鲜的{NCC，NH}值，如果有，根据NH值计算KeNB*，否则，根据KeNB计算KeNB*；

步骤2中源HeNB计算新的KeNB*的过程可以被描述为：

KeNB* = KDF（KeNB/NH，PCI，DL-AERFCN）；其中的KDF（*）表示密钥推衍函数，KeNB/NH、PCI和DL-AERFCN为密钥推衍函数的输入参数，PCI代表目标HeNB所在小区标识，DL-AERFCN代表下行E-UTRA绝

对（无线频率）信道数（down-link E-UTRA absolute radio frequency channel number）。

步骤3：源HeNB向HeNB GW发送切换请求消息，消息中包含KeNB*和NCC，以及源HeNB使用的安全算法；

源HeNB使用的安全算法包括源HeNB使用的完整性保护算法和源HeNB使用的加密算法等。

其中，该切换请求消息中的NCC为：与KeNB*对应的NH配对的NCC，即如果利用新鲜的NH计算KeNB*，则切换请求消息中的NCC为与新鲜的NH配对的NCC；如果利用KeNB计算KeNB*，则切换请求消息中的NCC为与用于计算KeNB的NH配对的NCC。

步骤4：HeNB GW根据目标小区信息判断出需要进行优化切换处理，如果HeNB GW本地有UE的新鲜安全参数，则执行步骤7；如果HeNB GW本地没有该UE的新鲜安全参数，则HeNB GW向MME发送UE Security Context Request（UE安全上下文请求）消息，携带UE的标识，以请求获取该UE的安全上下文。HeNB GW向MME发送的UE安全上下文请求消息还可以使HeNB GW和MME之间进行UE安全上下文的同步。

在步骤4中，HeNB GW判断本地没有UE的新鲜安全参数的方法有多种，一个具体的例子：如果HeNB GW确定出本地没有存储UE的安全参数，则HeNB GW确定出本地没有该UE的信息安全参数；另一个具体的例子：如果HeNB GW判断出本地存储有UE安全参数，且UE安全参数中的NCC小于源HeNB发送来的切换请求消息中携带的NCC值，则HeNB GW可以确定出本地有没有UE的新鲜安全参数。本实施例不限制HeNB GW判断本地没有UE的新鲜安全参数的具体实现方式。

在步骤4中，HeNB GW发送的UE安全上下文请求消息的一个具体定义为：

UE Security Context Request:

MME UE S1AP ID，eNB UE S1AP ID;

上述定义例举了UE安全上下文请求消息中包含的信元，如MME在S1接口上对UE的标识MME UE S1AP ID，eNB在S1接口上对UE的标识eNB UE S1AP ID。UE安全上下文请求消息还可以包含有其它信元，本实施例不限制UE安全上下文请求消息包含的具体信元。

步骤5： MME向HeNB GW回复UE安全上下文响应消息，实现HeNB

GW和MME同步，该UE安全上下文响应消息中可以包含有UE的安全参数。UE安全上下文响应消息中的UE的安全参数可以包含UE的新鲜安全参数（如新鲜的NCC和新鲜的NH）；也可以为UE非新鲜的安全参数（即在上次切换过程中已下发给当次切换目标eNB的NCC和NH），还应该包含计算新鲜NH需要用的输入参数KASME，消息信元定义如下：

UE安全上下文响应：

MME UE S1AP ID，eNB UE S1AP ID, KASME,NCC,NH，….;

上述定义例举了UE安全上下文响应消息中包含的信元，如MME以及eNB在S1接口上对UE的标识MME UE S1AP ID，eNB UE S1AP ID，认证后生成的KASME，以及NCC，NH。UE安全上下文请求消息还可以包含有其它信元，如UE安全能力信息、NAS加密算法、完整性保护算法、上行非接入层消息计数值NAS COUNT和下行NAS COUNT值等。本实施例不限制UE安全上下文响应消息包含的具体信元。

如果上面的安全上下文请求消息通过现有的切换请求（handover required）消息完成，则该处的安全上下文可以携带在现有的切换请求（handover request）消息里，HeNB GW收到该消息后，从中取出UE安全上下文信息，然后把不包含UE安全上下文的切换请求消息转发给目标eNB。这种方法需要在切换请求（handover request）消息里增加UE安全上下文各个信元。

步骤6：HeNB GW根据接收到的UE安全上下文响应消息与MME进行UE安全上下文同步，并执行更新存储的NCC和NH的操作，该操作可以具体为：

对于消息中携带的是非新鲜的安全参数情况，HeNB GW利用UE安全上下文响应消息中包含的NCC进行NCC + 1计算，并利用NCC + 1更新本地存储的NCC，HeNB GW利用NCC + 1、UE安全上下文响应消息中包含的NH和KASME计算NH'，并利用NH'更新本地存储的NH；对于消息中携带的是新鲜的NCC和NH的情况，则HeNB GW将UE安全上下文响应消息中包含的NCC和NH作为本地存储的NCC和NH。

步骤7：HeNB GW向目标HeNB转发切换请求消息，切换请求消息中包含有HeNB GW本地保存的UE的安全能力信息、UE的新鲜安全参数（如NCC + 1和NH'）以及HeNB GW接收到的切换请求消息中包括的KeNB*和NCC，源HeNB使用的安全算法等。

步骤8：目标HeNB根据接收到的切换请求消息中包含的新鲜安全参数计算KeNB**，如利用NH'，目标小区PCI，DL-AERFCN作为输入参数计算获得KeNB**。

步骤9：目标HeNB通过HeNB GW向源HeNB发送切换响应消息，切换响应消息中包含有UE的新鲜安全参数（如NCC + 1）、目标HeNB选择的加密算法和目标HeNB选择的完整性保护算法等。

步骤10：源HeNB接收到切换响应消息后，向UE发送切换命令消息，该切换命令消息中包含有UE的新鲜安全参数（如NCC + 1）、目标HeNB选择的加密算法和目标HeNB选择的完整性保护算法等。

步骤11：UE接收到切换命令消息后，将切换命令消息中包含的NCC + 1与本地的NCC进行比较，由于比较结果一定不相同，因此，UE根据切换命令消息中包含的NCC + 1更新本地NH，并利用更新后的NH计算获得KeNB*；之后，UE利用本身计算的KeNB*和目标HeNB选择的加密算法和完整性保护算法推演接入层加密密钥和完整性保护密钥，利用推演出的加密密钥对切换完成消息进行加密处理，利用推演出的完整性保护密钥对切换完成消息进行完整性保护处理，然后，UE向目标HeNB发送进行了完整性保护和加密保护的切换完成消息。

步骤12：目标HeNB接收到切换完成消息后，向HeNB GW发送切换通知消息。

本实例五是以HeNB和HeNB GW为例进行说明的，该安全处理方法也可以适用于Relay和DeNB的应用场景中，在此不再重复说明。

从上述实例五的描述可知，目标HeNB通过利用UE的新鲜的NH来计算KeNB*，UE利用KeNB*推演出接入层密钥，使攻击者不能够根据目标HeNB里的密钥KeNB*推算出源HeNB里的密钥KeNB，进而也就不能获得UE在源HeNB下使用的接入层密钥，从而实现了后向安全；由于目标HeNB在计算KeNB*过程中利用了UE的新鲜的NH，而NH是HeNB GW直接下发给目标eNB的，所以源侧是无法得到目标eNB计算出的KeNB*的，因此，本实施例可以实现前向安全（即攻击者不能根据源HeNB使用的密钥推演出切换的目标HeNB使用的密钥）；本实施例通过由HeNB GW向MME请求UE安全上下文，并由HeNB GW执行NCC、NH的更新及下发操作，可以在减少MME参与优化切换过程的同时，保证了切换时的安全；从而实例五为优化切换提供了一种安全处理的解决方案。

可以理解的是，本实例五中的HeNB GW向MME发送安全上下文请求消息，并获取新鲜安全参数的方法也可以同上面实例三及实例四中的步骤4－步骤6所述，此处不再赘述。

实例六

场景为：HeNB GW上保存新鲜的{NCC、NH}对，当执行优化切换时，HeNB GW利用其保存的{NH，NCC}对实现切换的前向安全。其中HeNB GW获得新鲜的{NCC、NH}对的方法参照实施例三中所述，HeNB GW利用其保存的新鲜的{NCC、NH}对实现切换的前向安全的方法参照图5，具体包括如下步骤：

步骤1：UE发送测量报告给源HeNB;

步骤2：源HeNB在本地计算KeNB*；如果有UE的新鲜安全参数，则源HeNB根据新鲜安全参数中的NH计算新的接入层根密钥KeNB*；否则，源HeNB根据原接入层根密钥KeNB计算KeNB*;

源HeNB计算新的KeNB*的过程可以被描述为：

KeNB* = KDF（KeNB/NH，PCI，DL-AERFCN）；其中的KDF（*）表示密钥推衍函数，KeNB、PCI和DL-AERFCN为密钥推衍函数的输入参数，PCI代表目标HeNB所在小区标识，DL-AERFCN代表下行E-UTRA绝对（无线频率）信道数（down-link E-UTRA absolute radio frequency channel number），KeNB为原接入层根密钥。

步骤3：源HeNB向HeNB GW发送切换请求消息，消息中包含KeNB*及对应的NCC，源侧使用的安全算法（包括完整性保护算法及加密算法）。

可选地，为使得HeNB GW可利用其上保存的新鲜的{NCC、NH}对计算KeNB*，源HeNB发送的切换请求消息中可进一步包含目标小区的PCI和DL-AERFCN;

步骤4：HeNB GW根据目标小区信息判断出需要进行优化切换，则HeNB GW可进一步判断是否需要利用其保存的新鲜的{NCC、NH}对为目标HeNB计算新的接入层根密钥，若HeNB GW决定计算，则HeNB GW根据本地保存的新鲜的{NCC、NH}对中的NH，以及目标小区的PCI和DL-EARFCN，在本地计算KeNB**;

所述PCI和DL-EARFCN可直接携带于源HeNB发送的切换请求消息中，或者切换请求消息里携带目标小区PCI，HeNB GW根据该PCI在本地获取DL-EARFCN。对于HeNB GW决定不计算的场景，在下面的实例七中描述。

HeNB GW可根据从源HeNB接收到的切换请求消息中携带的NCC和其本地保存的NCC的大小关系来判断本地保存的{NCC、NH}对是否为新鲜的，若本地保存的{NCC、NH}对中的NCC小于切换请求消息中携带的NCC，则该{NCC、NH}对不是新鲜的，若本地保存的{NCC、NH}不是新鲜的，则HeNB GW可删除此{NCC、NH}对。

步骤5：HeNB GW转发切换请求消息给目标HeNB，消息中携带HeNB GW计算的KeNB**，对应的NCC'以及HeNB GW本地保存的UE的安全能力信息；还可以携带源HeNB计算的KeNB*及对应的NCC，以及源HeNB使用的安全算法；

步骤6：目标HeNB将收到的KeNB**作为本地KeNB，和NCC'关联保存；

步骤7：目标HeNB通过HeNB GW向源HeNB发送切换响应消息，消息里包含NCC'及目标HeNB选择的安全算法；

步骤8：源HeNB向UE发送切换命令消息，消息里包含NCC'和目标HeNB选择的安全算法；

步骤9：UE向目标HeNB发送切换完成消息；至此切换准备和切换执行过程完成。本步骤中UE的具体操作过程可以参照上面实例五中的描述，此处不再赘述。

上述步骤1－9完成了切换准备及切换执行过程，目标HeNB在接收到所述切换完成消息后，目标HeNB可以向HeNB GW发送路径修改请求消息；HeNB GW转发该消息给MME；HeNB GW从MME发送的路径修改确认消息中截取新鲜的NCC，NH值，保存在本地作为下次优化切换的新鲜NCC，NH值；HeNB GW转发没有新鲜NCC，NH的路径修改确认消息给目标HeNB。

本实例所描述的安全处理方法也可以适用于Relay和DeNB的应用场景中，在此不再重复说明。

从上述实例六的描述可知，目标HeNB通过利用UE的新鲜的NH来计算KeNB*，UE利用KeNB*推演出接入层密钥，使攻击者不能够根据目标HeNB里的密钥KeNB*推算出源HeNB里的密钥KeNB，进而也就不能获得UE在源HeNB下使用的接入层密钥，从而实现了后向安全；由于目标HeNB获得的KeNB*为HeNB GW根据新鲜的NH计算的，所以源侧是无法得到目标HeNB里的KeNB*的，因此，本实施例可以实现前向安全（即攻击者不能根据源HeNB使用的密钥推演出切换的目标HeNB使用的密钥）；本实施例保证了切换时的安全性，为优化切换提供了一种安全处理的解决方案。

实例七

场景为：HeNB GW上保存新鲜的{NCC、NH}对，当执行优化切换时，HeNB GW将其保存的{NH，NCC}对发送给目标HeNB，目标HeNB根据此NH计算密钥，实现切换的前向安全。其中HeNB GW获得新鲜的{NCC、NH}对的方法参照实施例三中所述，参照图6，包括如下步骤：

步骤1：UE发送测量报告给源HeNB;

步骤2：源HeNB在本地计算KeNB*；计算方法同实例六，此处不再赘述。

步骤3：源HeNB向HeNB GW发送切换请求消息，消息中包含KeNB*及对应的NCC，源侧使用的安全算法。

步骤4：HeNB GW根据目标小区信息判断出需要进行优化切换，则HeNB GW可进一步判断是否需要为目标HeNB计算密钥，若HeNB GW决定不计算，则HeNB GW转发切换请求消息给目标HeNB，消息中携带HeNB GW本地保存的新鲜的{NCC、NH}对以及HeNB GW本地保存的UE的安全能力信息；还可以携带源HeNB计算的KeNB*及对应的NCC以及源HeNB使用的安全算法;

HeNB GW可根据从源HeNB接收到的切换请求消息中携带的NCC和其本地保存的NCC的大小关系来判断本地保存的{NCC、NH}对是否为新鲜的，若本地保存的{NCC、NH}对中的NCC小于切换请求消息中携带的NCC，则该{NCC、NH}对不是新鲜的，若本地保存的{NCC、NH}不是新鲜的，则HeNB GW可删除此{NCC、NH}对）。

步骤5：目标HeNB根据新鲜{NCC、NH}对中的NH计算KeNB**，将KeNB**作为本地KeNB，和对应的NCC'关联保存;

步骤6：目标HeNB通过HeNB GW向源HeNB发送切换响应消息，消息里包含NCC'及目标HeNB使用的安全算法;

步骤7：源HeNB向UE发送切换命令消息，消息里包含NCC';

步骤8：UE向目标HeNB发送切换完成消息；本步骤中UE的具体操作过程可以参照上面实例五中的描述，此处不再赘述。

步骤9：目标HeNB发送切换通知给HeNB GW，至此切换准备和切换执行过程完成。本步骤9是针对S1切换的步骤，若为X2切换，则不需执行此步骤9。

上述步骤1－9完成了切换准备及切换执行过程，目标HeNB在接收到所

述切换完成消息后，目标HeNB可以向HeNB GW发送路径修改请求消息；HeNB GW转发该消息给MME；HeNB GW从MME发送的路径修改确认消息中截取新鲜的NCC，NH值，保存在本地作为下次优化切换的新鲜NCC，NH值；HeNB GW转发没有新鲜NCC，NH的路径修改确认消息给目标HeNB。

本实例所描述的安全处理方法也可以适用于Relay和DeNB的应用场景中，在此不再重复说明。

从上述实例六的描述可知，目标HeNB通过利用UE的新鲜的NH来计算KeNB*，UE利用KeNB*推演出接入层密钥，使攻击者不能够根据目标HeNB里的密钥KeNB*推算出源HeNB里的密钥KeNB，进而也就不能获得UE在源HeNB下使用的接入层密钥，从而实现了后向安全；由于目标HeNB在计算KeNB*过程中利用了UE的新鲜的NH，而NH是HeNB GW直接下发给目标eNB的，所以源侧是无法得到目标eNB计算出的KeNB*的，因此，本实施例可以实现前向安全（即攻击者不能根据源HeNB使用的密钥推演出切换的目标HeNB使用的密钥）；本实施例保证了切换时的安全性，为优化切换提供了一种安全处理的解决方案。

本发明实施例二提供一种安全验证实体，本实施例所述安全验证实体可以为：基站下的用户设备UE切换场景中的网关或relay下的UE切换场景中的锚点基站；如图7中所示，所述安全验证实体包括：

接收单元70，用于接收目标节点发送的路径修改请求消息，所述路径修改请求消息中携带源节点提供给目标节点的UE的安全能力信息；

验证单元71，用于验证所述路径修改请求消息里携带的所述UE的安全能力信息与本地保存的UE的安全能力信息是否一致；

发送单元72，用于在验证所述路径修改请求消息里携带的所述UE的安全能力信息与本地保存的UE的安全能力信息一致情况下发送路径修改确认消息给所述目标节点。

如图8中所示，所述安全验证实体还可以包括：

安全参数获取单元73，用于获取下次切换备用的新鲜的安全参数；

所述发送单元72在发送的所述路径修改确认消息中携带所述下次切换备用的新鲜的安全参数。

如图9中所示，所述安全验证实体还包括：

安全能力信息获取单元74，用于从核心网实体发送的切换消息中或者初始上下文建立请求消息中获得UE的安全能力信息；

安全能力信息保存单元75，用于保存所述UE的安全能力信息；

所述验证单元71从所述安全能力信息保存单元中获得所述本地保存的UE的安全能力信息。

所述安全验证实体还可以包括：

报警单元76，用于在所述验证单元验证所述路径修改请求消息里携带的所述UE的安全能力信息与安全验证实体本地保存的UE的安全能力信息不一致情况下启动报警过程。

本发明实施例所述安全验证实体可以对该源节点提供的UE的安全能力信息进行验证及触发告警，保证了源节点发送的UE的安全能力信息的可信性，因此保证了目标节点能够选择合适的安全算法，从而进一步提高了优化切换过程的安全性。且通过该安全验证实体执行UE的安全能力信息验证以及触发报警等操作，可以在避免核心网节点参与优化切换过程的同时，在一定程度上保证了小区的安全。

本发明实施例三提供一种切换过程中安全处理系统，该系统包括：源节点、目标节点及如上面实施例二所述的安全验证实体；

所述目标节点在切换准备及切换执行过程中获得由所述源节点提供的UE的安全能力信息；

所述安全验证实体通过将所述源节点提供的所述UE的安全能力信息与本地保存的UE的安全能力信息比较，以验证所述源节点提供的所述UE的安全能力信息是否安全。所述安全验证实体的具体结构及功能参照上面实施例中所述，此处不再赘述。

本发明实施例所述系统由安全验证实体对该源节点提供给目标节点的UE的安全能力信息进行验证及触发告警，保证了源节点发送的UE的安全能力信息的可信性，因此保证了目标节点能够选择合适的安全算法，从而进一步提高了优化切换过程的安全性。且通过该安全验证实体执行UE的安全能力信息验证以及触发报警等操作，可以在避免核心网节点参与优化切换过程的同时，在一定程度上保证了小区的安全。

本发明实施例四提供一种安全验证实体，本实施例所述安全验证实体可以为：基站下的用户设备UE切换场景中的网关或中继节点relay下的UE切换场景中的锚点基站；如图10中所示，所述安全验证实体包括：

接收单元100，用于接收源节点发送的切换请求消息；

转发单元101，用于转发所述切换请求消息给目标节点，在转发的所述

切换请求消息中携带所述安全验证实体本地保存的UE的安全能力信息。

如图11中所示，所述安全验证实体还包括:

安全能力信息获取单元102，用于从核心网实体发送的切换消息中或者初始上下文建立请求消息中获得UE的安全能力信息;

安全能力信息保存单元103，用于保存所述UE的安全能力信息;

所述转发单元101从所述安全能力信息保存单元103中获得所述本地保存的UE的安全能力信息。

如图12中所示，所述安全验证实体还可以包括:

安全参数获取单元104，用于获取新鲜的安全参数；所述新鲜的安全参数包括：新鲜的下跳链计数NCC及下一跳NH值;

所述转发单元101在转发的所述切换请求消息中携带所述新鲜的安全参数。

如图13中所示，所述安全验证实体还可以包括:

安全参数获取单元105，用于获取新鲜的安全参数;

计算单元106，用于根据所述新鲜的安全参数计算接入层根密钥;

所述转发单元101在转发的所述切换请求消息中携带所述计算单元计算的接入层根密钥以及对应的NCC。

本发明实施例所述安全验证实体可以提供UE的安全能力信息给目标节点，保证了目标节点获得可靠的UE的安全能力信息，因此保证了目标节点能够选择合适的安全算法，从而进一步提高了优化切换过程的安全性。且通过该安全验证实体获得并提供新鲜的安全参数给目标节点，可以在避免核心网节点参与优化切换过程的同时，在一定程度上保证了小区的安全。

本发明实施例五提供一种切换过程中的安全处理系统，包括：源节点、目标节点及如上面实施例四所述的安全验证实体;

所述安全验证实体在切换准备过程中提供UE的安全能力信息给所述目标节点。所述安全验证实体的具体结构及功能参照上面实施例四中所述，此处不再赘述。

本发明实施例所述系统由安全验证实体提供UE的安全能力信息给目标节点，保证了目标节点获得可靠的UE的安全能力信息，因此保证了目标节点能够选择合适的安全算法，从而进一步提高了优化切换过程的安全性。且通过该安全验证实体获得并提供新鲜的安全参数给目标节点，可以在避免核心网节点参与优化切换过程的同时，在一定程度上保证了小区的安全。

综上所述，本发明实施例在优化切换过程中，目标节点获得由安全验证实体提供的可靠的UE的安全能力信息，或者获得由源节点提供的UE的安全能力信息，再经安全验证实体对该源节点提供的UE的安全能力信息的验证及触发告警，保证了源节点发送的UE的安全能力信息的可信性，因此保证了目标节点能够选择合适的安全算法，从而进一步提高了优化切换过程的安全性。

另外，本发明实施例由所述的安全验证实体完成UE的安全能力信息的验证或新鲜的安全参数的更新操作，可以减少核心网节点参与优化切换过程。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的硬件平台的方式来实现，当然也可以全部通过硬件来实施，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案对背景技术做出贡献的全部或者部分可以以软件产品的形式体现出来，所述的软件产品在可以用于执行上述的方法流程。该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例或者实施例的某些部分所述的方法。

虽然通过实施例描绘了本发明，本领域普通技术人员知道，本发明有许多变形和变化而不脱离本发明的精神，本发明的申请文件的权利要求包括这些变形和变化。

# 权利要求

1、一种切换过程中的安全处理方法，其特征在于，包括:

用户设备UE与网络侧的源节点和目标节点完成切换准备及切换执行过程中，所述目标节点获取由所述源节点或安全验证实体提供的UE的安全能力信息；所述安全验证实体包括：基站下的UE切换场景中的网关或中继节点relay下的UE切换场景中的锚点基站;

若目标节点获取由所述源节点提供所述UE的安全能力信息，则所述方法还包括:

所述目标节点向安全验证实体发送路径修改请求消息，所述路径修改请求消息中携带上述获取的UE的安全能力信息；若所述安全验证实体验证所述路径修改请求消息里携带的所述UE的安全能力信息与本地保存的UE的安全能力信息一致，则发送路径修改确认消息给所述目标节点。

2、如权利要求1所述的方法，其特征在于，所述源节点及目标节点包括：基站下的UE切换场景中的基站或relay下的UE切换场景中的relay。

3、如权利要求1所述的方法，其特征在于，还包括:

若所述路径修改请求消息里携带的所述UE的安全能力信息与安全验证实体本地保存的UE的安全能力信息不一致，则启动报警过程。

4、如权利要求1所述的方法，其特征在于，所述安全验证实体提供所述UE的安全能力信息的方法包括:

所述安全验证实体转发所述源节点发送给所述目标节点的切换请求消息，在转发的所述切换请求消息中携带所述安全验证实体本地保存的所述UE的安全能力信息。

5、如权利要求4所述的方法，其特征在于，在转发的所述切换请求消息中还包括：所述安全验证实体根据新鲜的安全参数计算的新的接入层根密钥及对应的下跳链计数NCC’，则所述方法还包括:

所述目标节点关联保存所述安全验证实体根据新鲜的安全参数计算的

新的接入层根密钥及对应的NCC';

所述新鲜的安全参数包括新鲜的NCC及下一跳NH值。

6、如权利要求5所述的方法，其特征在于，所述安全验证实体根据新鲜的安全参数计算新的接入层根密钥的方法包括:

所述安全验证实体根据目标小区的物理小区标识PCI和目标小区的下行演进型通用陆地无线接入绝对信道数DL-EARFCN以及所述新鲜{NCC，NH}对中的NH计算新的接入层根密钥; 所述目标节点的PCI和DL-EARFCN从所述源节点发送的切换请求消息中获得，或者，从所述源节点发送的切换请求消息中获得目标节点所在小区PCI，根据从切换请求消息中获得的所述PCI在本地获取DL-EARFCN。

7、如权利要求4所述的方法，其特征在于，在转发的所述切换请求消息中还包括: 所述安全验证实体提供的新鲜的安全参数，则所述方法还包括:

所述目标节点根据所述切换请求消息中携带的新鲜的安全参数计算新的接入层根密钥。

8、如权利要求4、5或7所述的方法，其特征在于，在转发的所述切换请求消息中还包括: 所述源节点使用的安全算法，及源节点计算的新接入层根密钥及对应的NCC。

9、如权利要求1所述的方法，其特征在于，所述安全验证实体发送的路径修改确认消息中携带下次切换备用的新鲜的安全参数，所述目标节点保存所述新鲜的安全参数。

10、如权利要求5、7或9所述的方法，其特征在于，所述安全验证实体获得所述新鲜的安全参数的方法包括:

所述安全验证实体向核心网节点发送UE安全上下文请求消息，所述消息中包含UE标识;

接收所述核心网节点发送的UE安全上下文响应消息，所述UE安全上下

文响应消息中包含新鲜NCC及NH以及计算新鲜NH需要的输入参数接入安全管理实体密钥KASME，或包含UE当前使用的NCC，NH以及计算新鲜NH需要使用的输入参数KASME，根据所述UE当前使用的NCC计算得到新鲜的NCC，根据UE当前使用的NH以及所述KASME计算得到新鲜的NH。

11、如权利要求5、7或9所述的方法，其特征在于，所述安全验证实体获得所述新鲜的安全参数的方法包括:

所述安全验证实体中保存有非新鲜的NCC及NH，所述安全验证实体向核心网节点发送UE安全上下文请求消息，所述消息中包含UE标识，接收所述核心网节点发送的UE安全上下文响应消息，所述UE安全上下文响应消息中包含计算新鲜NH需要使用的输入参数KASME，保存所述KASME，根据所述非新鲜的NCC计算得到新鲜的NCC，根据所述非新鲜的NH以及KASME计算得到新鲜的NH; 所述保存的非新鲜的NCC及NH为所述安全验证实体从上次有核心网节点参与的切换过程中，核心网节点发送的路径修改确认消息或切换请求消息中获得;

或

所述安全验证实体中保存有非新鲜的NCC、NH及计算新鲜NH需要使用的输入参数KASME; 则所述安全验证实体根据所述非新鲜的NCC计算新鲜的NCC，以及根据所述非新鲜的NH以及KASME计算得到新鲜的NH; 所述保存的非新鲜的NCC及NH为所述安全验证实体在上次所述UE的切换过程中计算获得。

12、如权利要求5、7或9所述的方法，其特征在于，所述新鲜的安全参数从安全验证实体保存的{NCC，NH}列表中按照NCC值从小到大的顺序取用NCC值及对应的NH值，在所述{NCC，NH}列表中所有NCC，NH均被使用完后，或者所述安全验证实体内没有新鲜的NCC，NH时，所述安全验证实体获得所述{NCC，NH}列表，所述安全验证实体获取所述{NCC，NH}列表的方法包括:

安全验证实体向核心网节点发送UE安全上下文请求消息，所述消息中包含UE标识;

接收所述核心网节点发送的UE安全上下文响应消息，所述UE安全上下文响应消息中包含｛NCC，NH｝列表，所述｛NCC，NH｝列表中包含核心网节点当前的NCC及NH，以及核心网节点计算的下1跳至下n跳的NCC及对应的NH，n为大于1的自然数;

所述安全验证实体保存所述｛NCC，NH｝列表。

13、如权利要求12所述的方法，其特征在于，若所述安全验证实体保存的所述｛NCC，NH｝列表中存在未使用的新鲜的安全参数情况下，所述UE执行有核心网节点参与的正常切换，则所述核心网节点使用本地保存的最新的安全参数进行安全处理，以及通过切换命令实现与UE的所述最新的安全参数的同步。

14、如权利要求5、7或9所述的方法，其特征在于，所述安全验证实体获得所述新鲜的安全参数的方法包括:

所述安全验证实体在上次优化切换的安全处理过程中，从核心网节点发送给目标节点的路径修改确认消息中截取所述新鲜的安全参数。

15、如权利要求1或4所述的方法，其特征在于，所述安全验证实体本地保存的所述UE的安全能力信息通过如下方法获得:

所述安全验证实体从核心网实体发送给所述安全验证实体的切换消息中获得所述UE的安全能力信息；或

所述安全验证实体从核心网实体发送的初始上下文建立请求消息中获得所述UE的安全能力信息。

16、一种安全验证实体，其特征在于，所述安全验证实体为：基站下的用户设备UE切换场景中的网关或中继节点relay下的UE切换场景中的锚点基站；所述安全验证实体包括:

接收单元，用于接收目标节点发送的路径修改请求消息，所述路径修

改请求消息中携带源节点提供给目标节点的UE的安全能力信息;

验证单元，用于验证所述路径修改请求消息里携带的所述UE的安全能力信息与本地保存的UE的安全能力信息是否一致;

发送单元，用于在验证所述路径修改请求消息里携带的所述UE的安全能力信息与本地保存的UE的安全能力信息一致情况下发送路径修改确认消息给所述目标节点。

17、如权利要求16所述的安全验证实体，其特征在于，还包括:

安全参数获取单元，用于获取下次切换备用的新鲜的安全参数;

所述发送单元在发送的所述路径修改确认消息中携带所述下次切换备用的新鲜的安全参数。

18、如权利要求16所述的安全验证实体，其特征在于，还包括:

安全能力信息获取单元，用于从核心网实体发送的切换消息中或者初始上下文建立请求消息中获得UE的安全能力信息;

安全能力信息保存单元，用于保存所述UE的安全能力信息;

所述验证单元从所述安全能力信息保存单元中获得所述本地保存的UE的安全能力信息。

19、如权利要求16至18中任一项所述的安全验证实体，其特征在于，还包括:

报警单元，用于在所述验证单元验证所述路径修改请求消息里携带的所述UE的安全能力信息与安全验证实体本地保存的UE的安全能力信息不一致情况下启动报警过程。

20、一种安全验证实体，其特征在于，所述安全验证实体为：基站下的用户设备UE切换场景中的网关或中继节点relay下的UE切换场景中的锚点基站; 所述安全验证实体包括:

接收单元，用于接收源节点发送的切换请求消息;

转发单元，用于转发所述切换请求消息给目标节点，在转发的所述切

换请求消息中携带所述安全验证实体本地保存的UE的安全能力信息。

21、如权利要求20所述的安全验证实体，其特征在于，还包括:

安全能力信息获取单元，用于从核心网实体发送的切换消息中或者初始上下文建立请求消息中获得UE的安全能力信息;

安全能力信息保存单元，用于保存所述UE的安全能力信息;

所述转发单元从所述安全能力信息保存单元中获得所述本地保存的UE的安全能力信息。

22、如权利要求20或21所述的安全验证实体，其特征在于，还包括:

安全参数获取单元，用于获取新鲜的安全参数；所述新鲜的安全参数包括：新鲜的下跳链计数NCC及下一跳NH值;

所述转发单元在转发的所述切换请求消息中携带所述新鲜的安全参数。

23、如权利要求20或21所述的安全验证实体，其特征在于，还包括:

安全参数获取单元，用于获取新鲜的安全参数;

计算单元，用于根据所述新鲜的安全参数计算接入层根密钥;

所述转发单元在转发的所述切换请求消息中携带所述计算单元计算的接入层根密钥以及对应的NCC。

24、一种切换过程中安全处理系统，其特征在于，包括：源节点、目标节点及如权利要求16至19任一项所述的安全验证实体;

所述目标节点在切换准备及切换执行过程中获得由所述源节点提供的UE的安全能力信息;

所述安全验证实体通过将所述源节点提供的所述UE的安全能力信息与本地保存的UE的安全能力信息比较，以验证所述源节点提供的所述UE的安全能力信息是否安全。

25、一种切换过程中的安全处理系统，其特征在于，包括：源节点、目标节点及如权利要求20至23中任一项所述的安全验证实体;

所述安全验证实体在切换准备过程中提供UE的安全能力信息给所述目标节点。

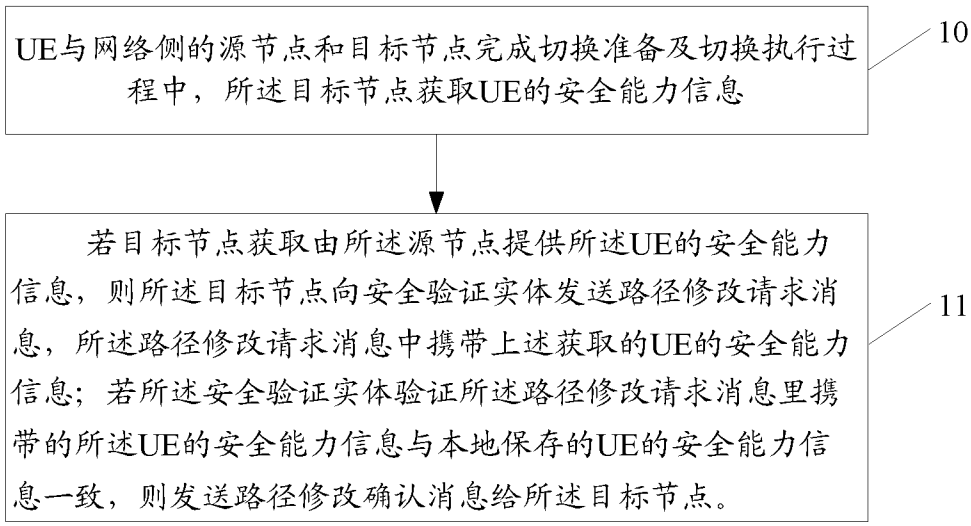
UE与网络侧的源节点和目标节点完成切换准备及切换执行过程中，所述目标节点获取UE的安全能力信息
10
若目标节点获取由所述源节点提供所述UE的安全能力信息，则所述目标节点向安全验证实体发送路径修改请求消息，所述路径修改请求消息中携带上述获取的UE的安全能力信息；若所述安全验证实体验证所述路径修改请求消息里携带的所述UE的安全能力信息与本地保存的UE的安全能力信息一致，则发送路径修改确认消息给所述目标节点。
11

图1

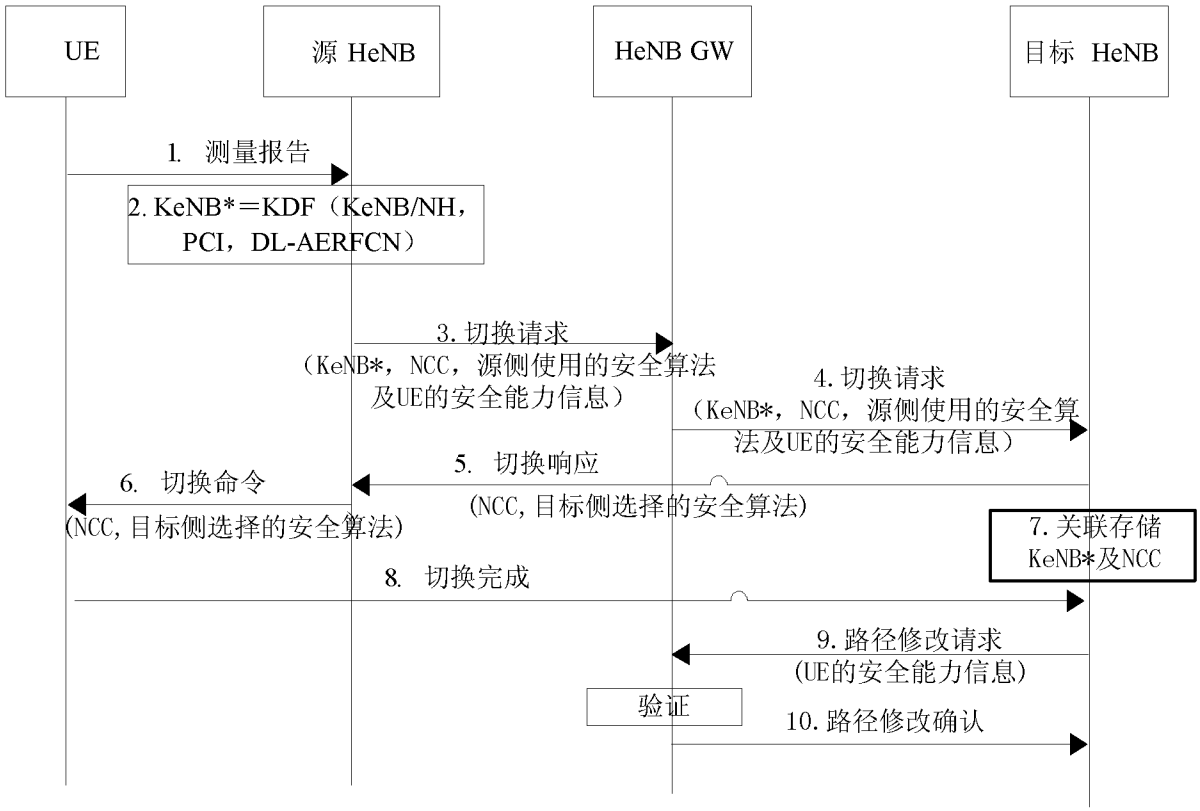
UE
源 HeNB
HeNB GW
目标 HeNB
1. 测量报告
2. KeNB*＝KDF（KeNB/NH，PCI，DL-AERFCN）
3. 切换请求
（KeNB*，NCC，源侧使用的安全算法及UE的安全能力信息）
4. 切换请求
（KeNB*，NCC，源侧使用的安全算法及UE的安全能力信息）
5. 切换响应
(NCC, 目标侧选择的安全算法)
6. 切换命令
(NCC, 目标侧选择的安全算法)
7. 关联存储KeNB*及NCC
8. 切换完成
9. 路径修改请求
(UE的安全能力信息)
验证
10. 路径修改确认

图 2

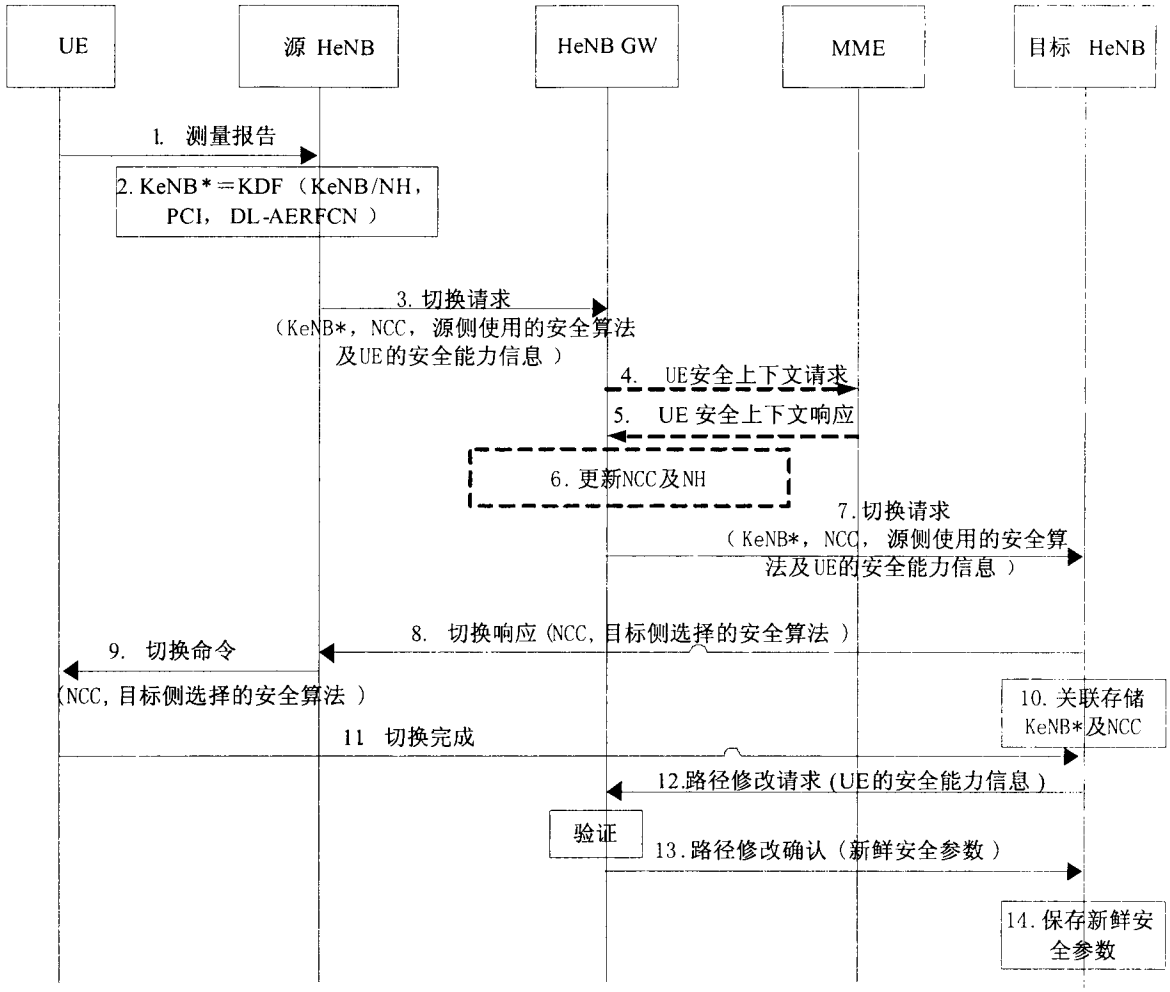
UE
源 HeNB
HeNB GW
MME
目标 HeNB
1. 测量报告
2. KeNB*＝KDF（KeNB/NH，PCI，DL-AERFCN）
3. 切换请求
（KeNB*，NCC，源侧使用的安全算法及UE的安全能力信息）
4. UE安全上下文请求
5. UE 安全上下文响应
6. 更新NCC及NH
7. 切换请求
（KeNB*，NCC，源侧使用的安全算法及UE的安全能力信息）
8. 切换响应（NCC，目标侧选择的安全算法）
9. 切换命令
（NCC，目标侧选择的安全算法）
10. 关联存储KeNB*及NCC
11 切换完成
12.路径修改请求（UE的安全能力信息）
验证
13.路径修改确认（新鲜安全参数）
14. 保存新鲜安全参数

图 3

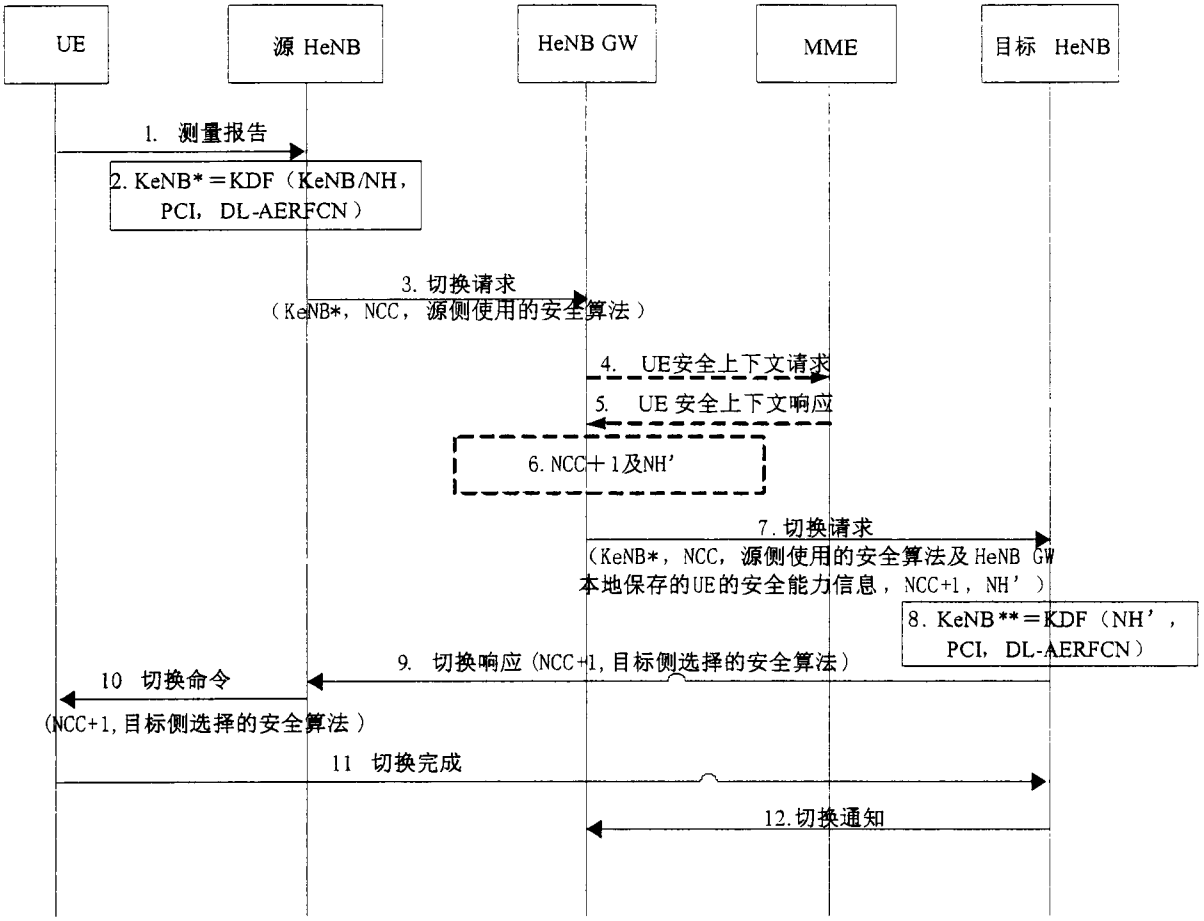
UE
源 HeNB
HeNB GW
MME
目标 HeNB
1. 测量报告
2. KeNB*＝KDF（KeNB/NH，PCI，DL-AERFCN）
3. 切换请求
（KeNB*，NCC，源侧使用的安全算法）
4. UE安全上下文请求
5. UE 安全上下文响应
6. NCC＋1及NH'
7. 切换请求
（KeNB*，NCC，源侧使用的安全算法及HeNB GW本地保存的UE的安全能力信息，NCC+1，NH'）
8. KeNB**＝KDF（NH'，PCI，DL-AERFCN）
9. 切换响应（NCC+1，目标侧选择的安全算法）
10 切换命令
（NCC+1，目标侧选择的安全算法）
11 切换完成
12. 切换通知

图 4

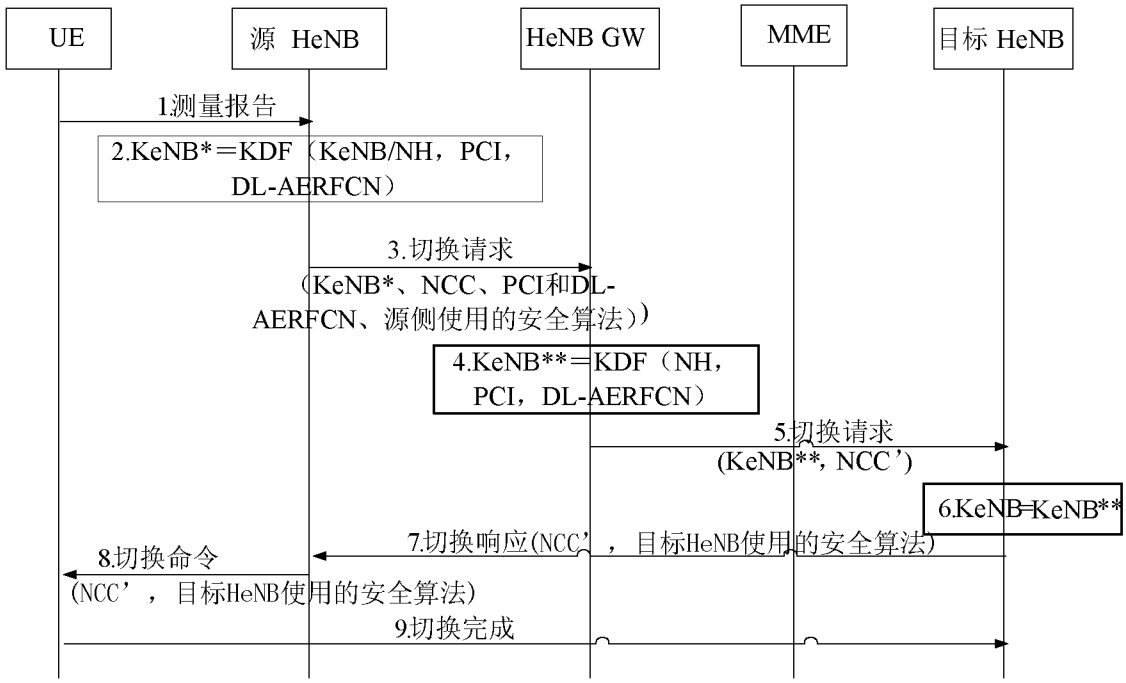
UE
源 HeNB
HeNB GW
MME
目标 HeNB
1.测量报告
2.KeNB*＝KDF（KeNB/NH，PCI，DL-AERFCN）
3.切换请求
（KeNB*、NCC、PCI和DL-AERFCN、源侧使用的安全算法））
4.KeNB**＝KDF（NH，PCI，DL-AERFCN）
5.切换请求
(KeNB**, NCC’)
6.KeNB=KeNB**
7.切换响应(NCC’，目标HeNB使用的安全算法)
8.切换命令
(NCC’，目标HeNB使用的安全算法)
9.切换完成

图 5

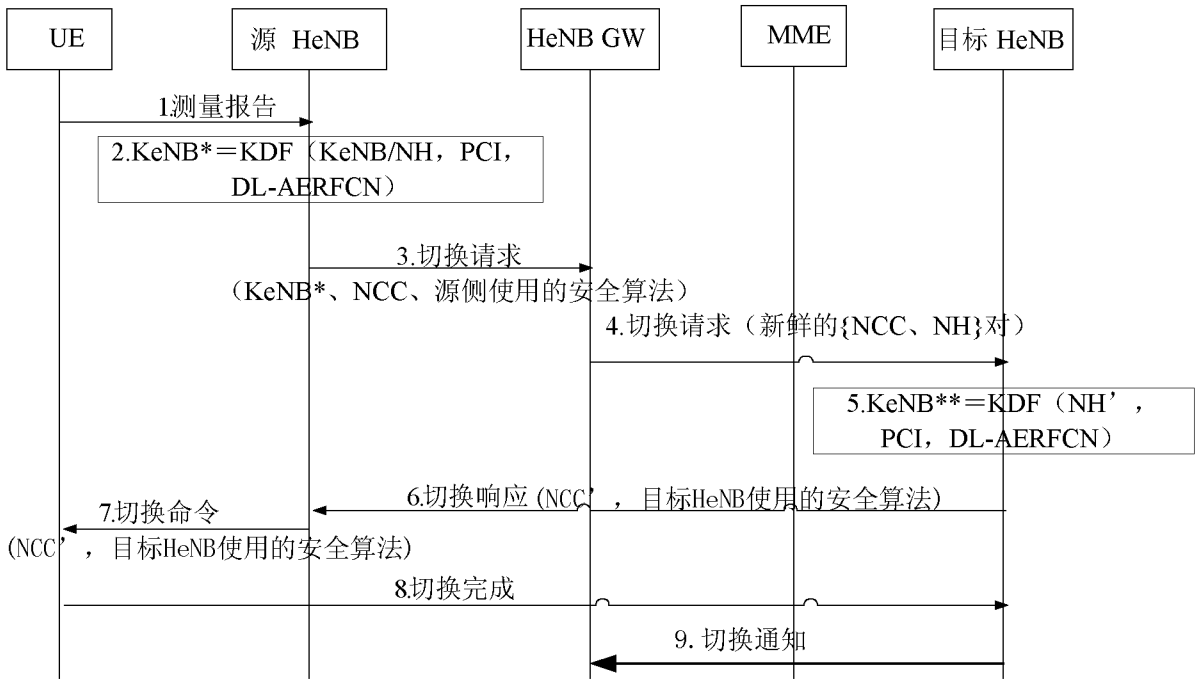
UE
源 HeNB
HeNB GW
MME
目标 HeNB
1.测量报告
2.KeNB*＝KDF（KeNB/NH，PCI，DL-AERFCN）
3.切换请求
（KeNB*、NCC、源侧使用的安全算法）
4.切换请求（新鲜的{NCC、NH}对）
5.KeNB**＝KDF（NH’，PCI，DL-AERFCN）
6.切换响应 (NCC’，目标HeNB使用的安全算法)
7.切换命令
(NCC’，目标HeNB使用的安全算法)
8.切换完成
9. 切换通知

图 6

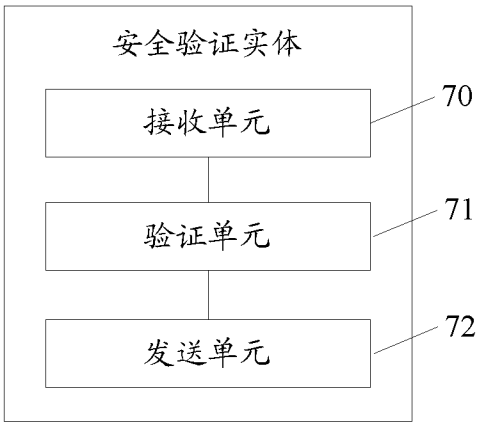
安全验证实体
接收单元
70
验证单元
71
发送单元
72

图 7

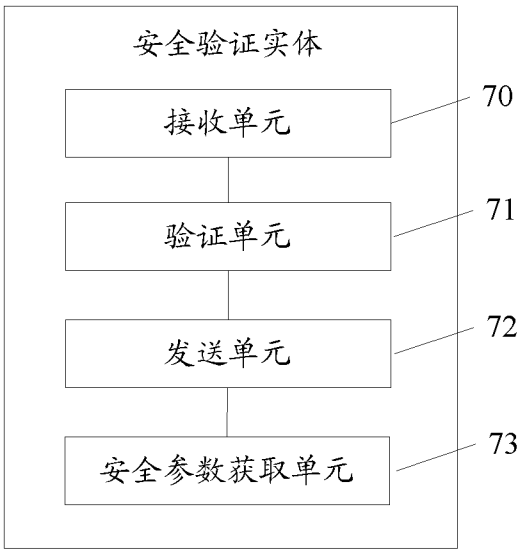
安全验证实体
接收单元
70
验证单元
71
发送单元
72
安全参数获取单元
73

图 8

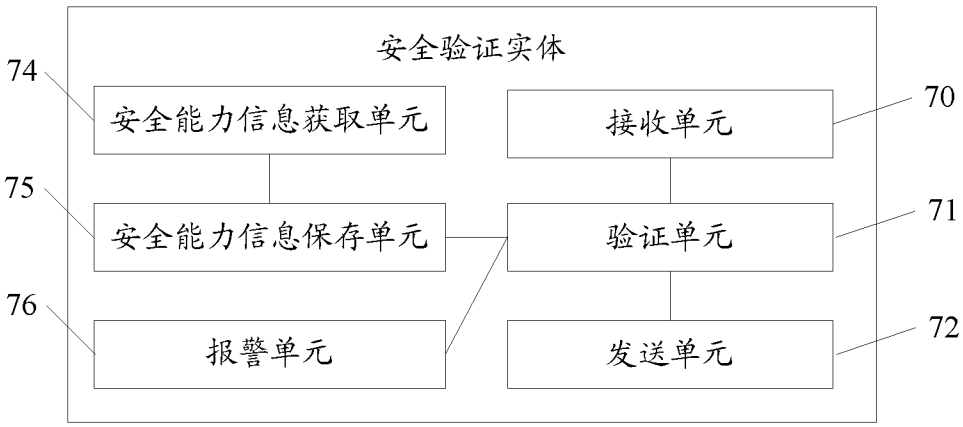
安全验证实体
74
安全能力信息获取单元
70
接收单元
75
安全能力信息保存单元
71
验证单元
76
报警单元
72
发送单元

图 9

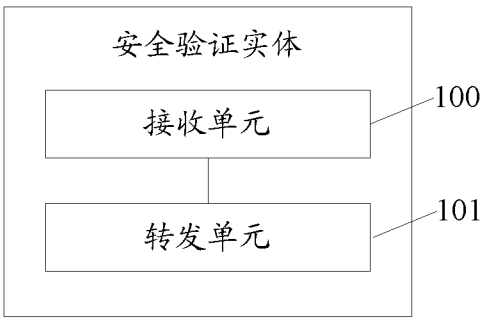
安全验证实体
接收单元
100
转发单元
101

图 10

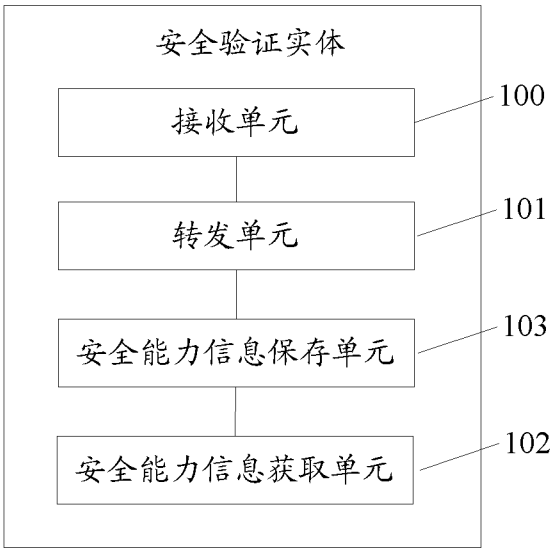
安全验证实体
接收单元
100
转发单元
101
安全能力信息保存单元
103
安全能力信息获取单元
102

图 11

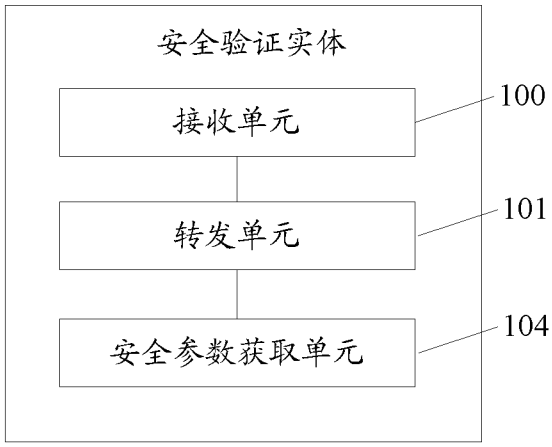
安全验证实体
接收单元
100
转发单元
101
安全参数获取单元
104

图 12

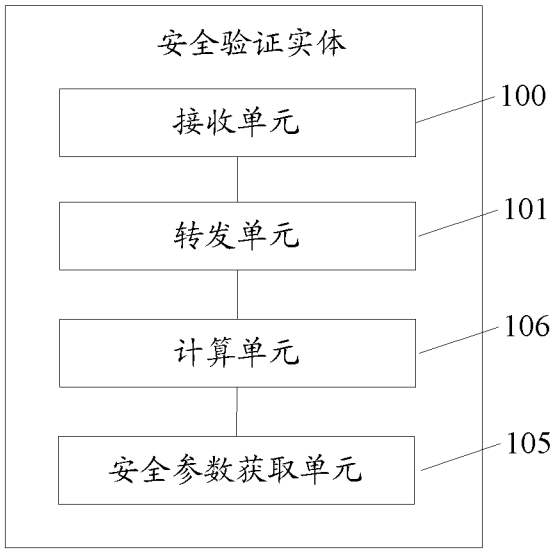
安全验证实体
接收单元
100
转发单元
101
计算单元
106
安全参数获取单元
105

图 13

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/074418

**A. CLASSIFICATION OF SUBJECT MATTER**

See extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC:H04W,H04M,H04L,H04Q,H04B,H04H,H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

VEN,CPRSABS,CNABS,CNTXT,CNKI: switch+, security, process+, MME, gateway, home, donor, base w station, eNB, DeNB, HeNB, source, original, target, authentication, validat+, capability, alarm+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | CN101730060A (DATANG MOBILE COMMUNICATIONS EQUIP CO LT) 09 Jun. 2010 (09.06.2010) description page 1; figures 1-2 | 1-9，14-25 |
| A | CN101651950A (NEW POST COMMUNICATION EQUIP CO LTD) 17 Feb. 2010 (17.02.2010) the whole document | 1-25 |
| A | WO2010032845A1 (NTT DOCOMO INC) 25 Mar. 2010 (25.03.2010) the whole document | 1-25 |
| A | CN101730032A (NEW POST COMMUNICATION EQUIP CO LTD) 09 Jun. 2010 (09.06.2010) the whole document | 1-25 |
| A | CN101772100A (CHINA MOBILE COMMUNICATION CORP) 07 Jul. 2010 (07.07.2010) the whole document | 1-25 |

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 25 Jul. 2011 （25.07.2011） | **01 Sep. 2011 (01.09.2011)** |
| Name and mailing address of the ISA/CN<br>The State Intellectual Property Office, the P.R.China<br>6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088<br>Facsimile No. 86-10-62019451 | Authorized officer<br>HAN, Zheng<br>Telephone No. (86-10)62411998 |

Form PCT/ISA /210 (second sheet) (July 2009)

# INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2011/074418

| Patent Documents referred in the Report | Publication Date | Patent Family | Publication Date |
|---|---|---|---|
| CN101730060A | 09.06.2010 | None | |
| CN101651950A | 17.02.2010 | None | |
| WO2010032845A1 | 25.03.2010 | CN102027769A | 20.04.2011 |
| | | CA2725473A1 | 25.03.2010 |
| | | KR20100126843A | 02.12.2010 |
| | | AU2009292864A1 | 25.03.2010 |
| | | EP2271145A1 | 05.01.2011 |
| | | MX2010012140A | 01.12.2010 |
| CN101730032A | 09.06.2010 | None | |
| CN101772100A | 07.07.2010 | None | |

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/074418

**A. CLASSIFICATION OF SUBJECT MATTER**

H04W 8/24 (2009.01) i
H04W 12/04 (2009.01) n
H04W 88/16 (2009.01) n
H04W 88/08 (2009.01) n

# 国际检索报告

国际申请号
**PCT/CN2011/074418**

**A. 主题的分类**

参见附加页

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

**B. 检索领域**

检索的最低限度文献(标明分类系统和分类号)

IPC:H04W,H04M,H04L,H04Q,H04B,H04H,H04N

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

VEN: switch+, security, process+, MME, gateway, home, donor, base w station, eNB, DeNB, HeNB, source, original, target, authentication, validat+, capability, alarm+

CPRSABS,CNABS,CNTXT,CNKI: 切换，安全，处理，MME，网关，家庭，锚点，基站，eNB，DeNB，HeNB，源，目标，验证，能力，报警

**C. 相关文件**

| 类　型* | 引用文件，必要时，指明相关段落 | 相关的权利要求 |
|---|---|---|
| X | CN101730060A (大唐移动通信设备有限公司) 09.6 月 2010 (09.06.2010) 说明书第 1 页，附图 1-2 | 1-9，14-25 |
| A | CN101651950A (新邮通信设备有限公司) 17. 2 月 2010 (17.02.2010) 全文 | 1-25 |
| A | WO2010032845A1 (株式会社 NTT 都科摩) 25. 3 月 2010 (25.03.2010) 全文 | 1-25 |
| A | CN101730032A (新邮通信设备有限公司) 09. 6 月 2010 (09.06.2010) 全文 | 1-25 |
| A | CN101772100A (中国移动通信集团公司) 07. 7 月 2010 (07.07.2010) 全文 | 1-25 |

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

| 国际检索实际完成的日期 | 国际检索报告邮寄日期 |
|---|---|
| 25.7 月 2011（25.07.2011） | **01.9 月 2011 (01.09.2011)** |
| ISA/CN 的名称和邮寄地址：<br>中华人民共和国国家知识产权局<br>中国北京市海淀区蓟门桥西土城路 6 号 100088<br>传真号：　(86-10)62019451 | 受权官员<br>**韩峥**<br>电话号码：(86-10) **62411998** |

# 国际检索报告

关于同族专利的信息

国际申请号
**PCT/CN2011/074418**

| 检索报告中引用的专利文件 | 公布日期 | 同族专利 | 公布日期 |
|---|---|---|---|
| CN101730060A | 09.06.2010 | 无 | |
| CN101651950A | 17.02.2010 | 无 | |
| WO2010032845A1 | 25.03.2010 | CN102027769A | 20.04.2011 |
| | | CA2725473A1 | 25.03.2010 |
| | | KR20100126843A | 02.12.2010 |
| | | AU2009292864A1 | 25.03.2010 |
| | | EP2271145A1 | 05.01.2011 |
| | | MX2010012140A | 01.12.2010 |
| CN101730032A | 09.06.2010 | 无 | |
| CN101772100A | 07.07.2010 | 无 | |

A.主题的分类

H04W 8/24 (2009.01) i

H04W 12/04 (2009.01) n

H04W 88/16 (2009.01) n

H04W 88/08 (2009.01) n