

(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
2014年1月9日 (09.01.2014)



(10) 国际公布号
WO 2014/005482 A1

- (51) 国际专利分类号:
H04W 12/04 (2009.01) H04W 76/02 (2009.01)
- (21) 国际申请号: PCT/CN2013/077431
- (22) 国际申请日: 2013年6月19日 (19.06.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210226264.X 2012年7月3日 (03.07.2012) CN
- (71) 申请人: 华为终端有限公司 (HUAWEI DEVICE CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地B区2号楼, Guangdong 518129 (CN)。
- (72) 发明人: 陆苏 (LU, Su); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 丁志明 (DING, Zhiming); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 树贵明 (SHU, Guiming); 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, BN, 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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, 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, CG, CI, CM, GA, GN, GQ, GW, KM, 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))。

(54) Title: METHOD FOR ESTABLISHING DIRECT LINK, AND KEY UPDATING METHOD AND DEVICE

(54) 发明名称: 建立直接链路方法、密钥更新方法和设备

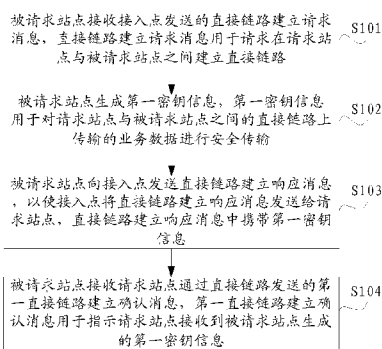


图 1/ Fig. 1

- S101 A REQUESTED STATION RECEIVING A DIRECT LINK SETUP REQUEST MESSAGE TRANSMITTED BY AN ACCESS POINT, THE DIRECT LINK SETUP REQUEST MESSAGE BEING USED FOR REQUESTING THE SETUP OF A DIRECT LINK BETWEEN A REQUESTING STATION AND THE REQUESTED STATION
- S102 THE REQUESTED STATION GENERATING FIRST KEY INFORMATION, THE FIRST KEY INFORMATION BEING USED FOR PERFORMING SECURE TRANSMISSION ON SERVICE DATA WHICH IS TRANSMITTED OVER THE DIRECT LINK BETWEEN THE REQUESTING STATION AND THE REQUESTED STATION
- S103 THE REQUESTED STATION TRANSMITTING A DIRECT LINK SETUP RESPONSE MESSAGE TO THE ACCESS POINT, SO AS TO ALLOW THE ACCESS POINT TO TRANSMIT THE DIRECT LINK SETUP RESPONSE MESSAGE TO THE REQUESTING STATION, THE DIRECT LINK SETUP RESPONSE MESSAGE CARRYING THE FIRST KEY INFORMATION
- S104 THE REQUESTED STATION RECEIVING A FIRST DIRECT LINK SETUP CONFIRMATION MESSAGE WHICH IS TRANSMITTED BY THE REQUESTING STATION THROUGH THE DIRECT LINK, THE FIRST DIRECT LINK SETUP CONFIRMATION MESSAGE BEING USED FOR INDICATING THAT THE REQUESTING STATION HAS RECEIVED THE FIRST KEY INFORMATION GENERATED BY THE REQUESTED STATION

(57) Abstract: Provided are a method for establishing a direct link, and a key updating method and device. The method includes: a requested station receiving a direct link setup request message transmitted by an access point, the direct link setup request message being used for requesting the setup of a direct link between a requesting station and the requested station; the requested station generating first key information, the first key information being used for performing secure transmission on service data which is transmitted over the direct link between the requesting station and the requested station; the requested station transmitting a direct link setup response message to the access point, the direct link setup response message carrying the first key information; and the requested station receiving a first direct link setup confirmation message which is transmitted by the requesting station through the direct link, the first direct link setup confirmation message being used for indicating that the requesting station has received the first key information generated by the requested station. The signalling overhead in the process of setting up a link between a requesting station and a requested station is saved.

(57) 摘要:

[见续页]

WO 2014/005482 A1



本发明实施例提供一种建立直接链路方法、密钥更新方法和设备。一种方法包括：被请求站点接收接入点发送的直接链路建立请求消息，直接链路建立请求消息用于请求在请求站点与被请求站点之间建立直接链路；被请求站点生成第一密钥信息，第一密钥信息用于对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输；被请求站点向接入点发送直接链路建立响应消息，直接链路建立响应消息中携带第一密钥信息；被请求站点接收请求站点通过直接链路发送的第一直接链路建立确认消息，第一直接链路建立确认消息用于指示请求站点接收到被请求站点生成的第一密钥信息。以节省请求站点与被请求站点建立链路过程中的信令开销。

建立直接链路方法、密钥更新方法和设备

本申请要求于 2012 年 7 月 3 日提交中国专利局、申请号为 201210226264.X、发明名称为“建立直接链路方法、密钥更新方法和设备”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。

5 技术领域

本发明涉及通信技术，尤其涉及一种建立直接链路方法、密钥更新方法和设备。

背景技术

10 站点 (Station, STA) 以与接入点 (Access Point, AP) 协商的功率与 AP 通信。由于一个 AP 覆盖范围内不同位置的 STA 与 AP 直接通信的速率是不同的，而与 AP 距离较远的 STA 在与 AP 通信时，需要通过中继设备 (Relay) 转发数据来缩短 STA 和 AP 的通信时间。

15 现有技术的 STA 与 Relay 之间直接链路的密钥产生方法为，STA 产生一个随机数，并在向 AP 发送的建立请求中携带该随机数，AP 通过建立请求将该随机数发送给 Relay。Relay 接收到 STA 产生的随机数后，产生一个随机数，通过 STA 产生的随机数、Relay 产生的随机数进行计算生成用于对 STA 向 Relay 发送的业务数据进行解密的密钥。Relay 通过向 AP 发送的建立响应携带自身产生的随机数，AP 通过建立响应将 Relay 产生的随机数发送给 STA，通过 STA 产生的随机数、Relay 产生的随机数进行计算生成用于对 STA 向 Relay 发送的
20 业务数据进行加密的密钥。从而导致信令开销大。

发明内容

本发明实施例提供一种建立直接链路方法、请求站点和被请求站点，以节省信令开销。

一方面，本发明实施例提供一种建立直接链路方法，包括：

25 请求站点向接入点发送直接链路建立请求消息，以使所述接入点将所述直接链路建立请求消息发送给所述被请求站点，所述直接链路建立请求消息用于

请求在所述请求站点与被请求站点之间建立直接链路;

所述请求站点接收所述接入点发送的直接链路建立响应消息, 所述直接链路建立响应消息中携带第一密钥信息, 所述第一密钥信息用于对所述请求站点与所述被请求站点之间的所述直接链路上传输的业务数据进行安全传输;

- 5 所述请求站点通过所述直接链路向所述被请求站点发送的第一直接链路建立确认消息, 所述第一直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的所述第一密钥信息。

本发明实施例提供另一种建立直接链路方法, 包括:

- 10 被请求站点接收接入点发送的直接链路建立请求消息, 所述直接链路建立请求消息用于请求在请求站点与所述被请求站点之间建立直接链路;

所述被请求站点生成第一密钥信息, 所述第一密钥信息用于对所述请求站点与所述被请求站点之间的所述直接链路上传输的业务数据进行安全传输;

- 15 所述被请求站点向所述接入点发送直接链路建立响应消息, 以使所述接入点将所述直接链路建立响应消息发送给所述请求站点, 所述直接链路建立响应消息中携带第一密钥信息;

所述被请求站点接收所述请求站点通过所述直接链路发送的第一直接链路建立确认消息, 所述第一直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的所述第一密钥信息。

本发明实施例提供一种请求站点, 包括:

- 20 发送器, 用于向接入点发送直接链路建立请求消息, 以使所述接入点将所述直接链路建立请求消息发送给所述被请求站点, 所述直接链路建立请求消息用于请求在所述请求站点与被请求站点之间建立直接链路;

- 25 接收器, 用于接收所述接入点发送的直接链路建立响应消息, 所述直接链路建立响应消息中携带第一密钥信息, 所述第一密钥信息用于对所述请求站点与所述被请求站点之间的所述直接链路上传输的业务数据进行安全传输;

所述发送器还用于: 通过所述直接链路向所述被请求站点发送的第一直接链路建立确认消息, 所述第一直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的所述第一密钥信息。

本发明实施例提供一种被请求站点, 包括:

- 30 接收器, 用于接收接入点发送的直接链路建立请求消息, 所述直接链路建立请求消息用于请求在请求站点与所述被请求站点之间建立直接链路;

处理器，用于生成第一密钥信息，所述第一密钥信息用于对所述请求站点与
所述被请求站点之间的所述直接链路上传输的业务数据进行安全传输；

发送器，用于向所述接入点发送直接链路建立响应消息，以使所述接入点
将所述直接链路建立响应消息发送给所述请求站点，所述直接链路建立响应消
5 息中携带第一密钥信息；

所述接收器还用于：接收所述请求站点通过所述直接链路发送的第一直接
链路建立确认消息，所述第一直接链路建立确认消息用于指示所述请求站点接
收到所述被请求站点生成的所述第一密钥信息。

本发明实施例提供的建立链路方法和设备，被请求站点接收到接入点转发
10 的直接链路建立请求消息之后，在返回给接入点的直接链路建立响应消息中携
带被请求站点生成的密钥信息，以使接入点将该直接链路建立响应消息返回给
请求站点后，请求站点能够根据该密钥对请求站点与被请求站点之间的直接链
路上传输的业务数据进行安全传输，实现节省请求站点与被请求站点建立链路
过程中的信令开销。

15 另一方面，本发明实施例提供一种密钥更新方法，包括：

被请求站点生成第二密钥信息，所述第二密钥信息用于替换所述被请求站
点生成的第一密钥信息，对请求站点与所述被请求站点之间的直接链路上传输
的业务数据进行安全传输；

所述被请求站点将第二密钥信息发送给接入点，以使所述接入点将所述第
20 二密钥信息发送给所述被请求站点。

本发明实施例还提供一种密钥更新方法，包括：

请求站点接收接入点发送的所述第二密钥信息，所述第二密钥信息由所述
被请求站点生成，用于替换所述被请求站点生成的第一密钥信息，对所述请求
站点与所述被请求站点之间的直接链路上传输的业务数据进行安全传输；

25 所述请求站点采用所述第二密钥信息替换所述第一密钥信息，对所述请求
站点与所述被请求站点之间的直接链路上传输的业务数据进行安全传输。

本发明实施例还提供一种被请求站点，包括：

处理器，用于生成第二密钥信息，所述第二密钥信息用于替换所述被请求
站点生成的第一密钥信息，对请求站点与所述被请求站点之间的直接链路上传
30 输的业务数据进行安全传输；

发送器，用于将第二密钥信息发送给接入点，以使所述接入点将所述第二

密钥信息发送给所述被请求站点。

本发明实施例还提供一种请求站点，包括：

接收器，用于接收接入点发送的所述第二密钥信息，所述第二密钥信息由所述被请求站点生成，用于替换所述被请求站点生成的第一密钥信息，对所述
5 请求站点与所述被请求站点之间的直接链路上传输的业务数据进行安全传输；

处理器，用于采用所述第二密钥信息替换所述第一密钥信息，对所述请求站点与所述被请求站点之间的直接链路上传输的业务数据进行安全传输。

本发明实施例提供的密钥更新方法和设备，被请求站点产生用于替换第一
10 密钥的第二密钥后，可以将第二密钥信息通过接入点返回给请求站点，以使请
求站点采用第二密钥替换第一密钥对请求站点与被请求站点之间的直接链路上
传输的业务数据进行安全传输，实现节省密钥更新过程的信令开销。

附图说明

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
15 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
造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明的建立直接链路方法一个实施例的流程图；

图 2 为本发明的建立直接链路方法又一个实施例的流程图；

20 图 3 为本发明的建立直接链路方法另一个实施例的流程图；

图 4 为本发明的建立直接链路方法另一个实施例的流程图；

图 5 为本发明提供的被请求站点一个实施例的结构示意图；

图 6 为本发明提供的接入点一个实施例的结构示意图；

图 7 为本发明提供的请求站点一个实施例的结构示意图；

25 图 8 为本发明提供的请求站点又一个实施例的结构示意图；

图 9 为本发明提供的被请求站点一个实施例的结构示意图；

图 10 为本发明提供的请求站点一个实施例的结构示意图；

图 11 为本发明提供的被请求站点又一个实施例的结构示意图；

图 12 为本发明提供的被请求站点又一个实施例的结构示意图；

30 图 13 为本发明提供的请求站点又一个实施例的结构示意图；

图 14 为本发明提供的请求站点又一个实施例的结构示意图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，
5 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做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。

本文中描述的技术可用于各种通信系统，例如当前 2G，3G 通信系统和下一代通信系统，例如全球移动通信系统（GSM，Global System for Mobile
10 communications），码分多址（CDMA，Code Division Multiple Access）系统，时分多址（TDMA，Time Division Multiple Access）系统，宽带码分多址（WCDMA，Wideband Code Division Multiple Access），频分多址（FDMA，Frequency Division Multiple Access）系统，正交频分多址（OFDMA，Orthogonal Frequency-Division Multiple Access）系统，单载波 FDMA（SC-FDMA）系统，
15 通用分组无线业务（GPRS，General Packet Radio Service）系统，长期演进（LTE，Long Term Evolution）系统，以及其他此类通信系统。

图 1 为本发明的建立直接链路方法一个实施例的流程图，如图 1 所示，本实施例从被请求站点侧在建立直接链路过程中执行的操作为例，对本发明提供的建立链路方法进行说明。该方法包括：

20 S101、被请求站点接收接入点发送的直接链路建立请求消息，直接链路建立请求消息用于请求在请求站点与被请求站点之间建立直接链路。

S102、被请求站点生成第一密钥信息，第一密钥信息用于对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输。

25 S103、被请求站点向接入点发送直接链路建立响应消息，以使接入点将直接链路建立响应消息发送给请求站点，直接链路建立响应消息中携带第一密钥信息。

S104、被请求站点接收请求站点通过直接链路发送的第一直接链路建立确认消息，第一直接链路建立确认消息用于指示请求站点接收到被请求站点生成的第一密钥信息。

30 本申请中涉及的请求站点，可以是无线请求站点也可以是有线请求站点，

举例来说，可以是各种网络，例如：无线保真（Wireless Fidelity，WiFi）网络或蜂窝网络中的站点，例如：传感器、电表等站点（STA）。被请求站点具备生成第一密钥信息的能力，可以是无线请求站点也可以是有线请求站点，例如，可以是传感器、电表等站点。同时，请求站点和被请求站点位于同一个网络中，

5 例如，位于同一个接入点下的 WiFi 网络中。接入点可以是无线局域网（Wireless Local Area Networks，WLAN）中的接入点（Access Point，AP），也可以是 WiFi 网络中的接入点，也可以是 GSM 网络、GPRS 网络或 CDMA 网络、蜂窝网络中的基站（Base Transceiver Station，BTS），还可以是 CDMA2000 网络或 WCDMA 网络中的基站（NodeB），还可以是 LTE 网络中的演进型基站

10 （Evolved NodeB，eNB），还可以是 WiMAX 网络中的接入服务网络的基站（Access Service Network Base Station，ASN BS）等网元；或也可以是以上接入点、基站后面的控制器或认证器等网元。

本申请可以适用于多种实施场景，例如：在 WiFi 网络中，作为请求站点的电表向接入点上报电表读数的实施场景；作为请求站点的温湿度传感器向接入

15 点上报测量的温湿度等实施场景，在此不一一列举。在这种实施场景下，如果请求站点与接入点之间的距离较远，则请求站点可以通过被请求站点转发向接入点上报的业务数据，来缩短请求站点和接入点的通信时间。请求站点与被请求站点之间需要建立直接链路来传输业务数据。

在请求站点与被请求站点建立直接链路的过程中，需要接入点转发直接链

20 路建立请求消息和直接链路建立响应消息。

本发明实施例中，被请求站点接收到接入点转发的直接链路建立请求消息后，可以在本地生成用于对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输的第一密钥信息。其中，安全传输可以包括：对传输数据进行加/解密，和/或，完整性验证等操作。被请求站点可以将第一密钥信息携带

25 在直接链路建立响应消息中发送给接入点，以使接入点将携带第一密钥信息的直接链路建立响应消息发送给请求站点。从而请求站点在与被请求站点之间的直接链路（即空口）上发送业务数据，例如：电表读数，传感器的检测数据时，在第一密钥的生命周期内，请求站点可以采用该第一密钥信息对业务数据进行加密，被请求站点接收到请求站点发送的业务数据后，可以采用第一密钥信息

30 对接收到的业务数据进行解密。

可选的，第一密钥信息可以包括第一密钥，或者可以包括第一密钥和第一

密钥的生命周期信息。在第一密钥信息包括第一密钥和第一密钥的生命周期信息的场景下，被请求站点在生成第一密钥后，还可以确定第一密钥的生命周期，并将第一密钥的生命周期信息包括在第一密钥信息中发送给接入点。

进一步的，被请求站点向接入点发送携带第一密钥信息的直接链路建立响应消息之后，可以接收到请求站点通过直接链路发送的第一直接链路建立确认消息（**Confirm** 消息），该第一直接链路建立确认消息用于指示请求站点接收到被请求站点生成的第一密钥信息，该第一确认消息中可以携带用于完整性验证的消息完整性码（**Message Integrity Code, MIC**）。

由于被请求站点可以从直接链路上直接收到请求站点发送的第一直接链路建立确认消息，而不必通过接入点转发该第一直接链路建立确认消息，因此，减少了请求站点直接向接入点发送消息的次数，可以有效降低请求站点的能耗。

被请求站点能够从直接链路上接收到请求站点发送的第一直接链路建立确认消息。请求站点可以根据其中携带的 **MIC**，对请求站点接收的第一直接链路建立确认消息进行完整性验证。若验证通过，则被请求站点可以通过直接链路向请求站点发送确认消息（**Acknowledgement, ACK**），用于指示通过完整性验证，即请求站点正确接收第一密钥信息。

由于第一密钥具有一定的生命周期，在生命周期结束后，第一密钥将失效，无法再用于对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输。据此，可选的，被请求站点可以在第一密钥的生命周期结束之前，或者被请求站点的计时器溢出，或者请求站点请求更新第一密钥信息等实施场景下，生成第二密钥信息，将第二密钥信息发送给接入点，以使接入点将该第二密钥信息转发给请求站点，从而请求站点可以在第一密钥的生命周期结束之后，采用第二密钥信息替换第一密钥信息，对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输。

可选的，第二密钥信息可以包括第二密钥，或者可以包括第二密钥和第二密钥的生命周期信息。在第二密钥信息包括第二密钥和第二密钥的生命周期信息的场景下，被请求站点在生成第二密钥后，还可以确定第二密钥的生命周期，并将第二密钥的生命周期信息包括在第二密钥信息中发送给接入点。

其中，被请求站点可以将第二密钥信息携带在现有的与接入点之间交互的各种格式的消息中发送给接入点，举例来说，可以将第二密钥信息携带在直接链路建立响应格式的消息中发送给接入点。

由于被请求站点可以在第一密钥的生命周期结束之前，产生第二密钥信息并发送给请求站点，从而避免了由于第一密钥过期而导致的请求站点与被请求站点之间的直接链路重新建立，从而增加了传输吞吐率。

与向请求站点发送第一密钥信息相类似的，被请求站点将第二密钥信息发送给接入点之后，可以接收到请求站点通过直接链路发送的第二直接链路建立确认消息（**Confirm** 消息），该第二直接链路建立确认消息用于指示请求站点接收到被请求站点生成的第二密钥信息，该第二直接链路建立确认消息中也可以携带用于完整性验证的 **MIC**。

被请求站点可以通过直接链路接收请求站点发送的第二直接链路建立确认消息，可以根据其中携带的 **MIC** 进行完整性验证。若验证通过，则被请求站点可以通过直接链路向请求站点发送 **ACK**。

需要说明的是，本发明实施例涉及的直接链路建立请求消息、直接链路建立响应消息、以及第一直接链路建立确认消息（**Confirm** 消息）和第二直接链路建立确认消息（**Confirm** 消息）中，除了携带本发明实施例中涉及的信息之外，保留了上述消息中现有的各种信息，例如：请求站点的地址信息、被请求站点的地址信息、请求站点或被请求站点支持的速率集合以及能力（**Capacities**）参数等信息，对于上述消息中携带的这些现有信息，可以参见电子电器工程师学会（**Institute of Electrical and Electronics Engineers, IEEE**）标准组织制定的例如 **802.11** 等现有协议中的相关描述，在此不一一赘述。

本实施例提供的建立链路方法，被请求站点接收到接入点转发的直接链路建立请求消息之后，在返回给接入点的直接链路建立响应消息中携带被请求站点生成的密钥信息，以使接入点将该直接链路建立响应消息返回给请求站点后，请求站点能够根据该密钥对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输，实现节省请求站点与被请求站点建立链路过程中的信令开销。

图 2 为本发明的建立直接链路方法又一个实施例的流程图，如图 2 所示，本实施例从接入点侧在建立直接链路过程中执行的操作为例，对本发明提供的建立链路方法进行说明。该方法包括：

S201、接入点接收请求站点发送的直接链路建立请求消息，直接链路建立请求消息用于请求在请求站点与被请求站点之间建立直接链路。

S202、接入点将直接链路建立请求消息发送给被请求站点。

S203、接入点接收被请求站点发送的直接链路建立响应消息，直接链路建立响应消息中携带第一密钥信息，第一密钥信息用于对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输。

5 S204、接入点将直接链路建立响应消息发送给请求站点。

接入点接收到请求站点发送的直接链路建立请求消息后，可以将该直接链路建立的请求消息转发给被请求站点。

被请求站点接收到接入点转发的直接链路建立请求消息后，可以在本地生成用于对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输的第一密钥信息。被请求站点可以将第一密钥信息携带在直接链路建立响应消息中发送给接入点。接入点接收到携带第一密钥信息的直接链路建立响应消息之后，可以将该直接链路建立响应消息转发给请求站点。

10 可选的，被请求站点可以在第一密钥的生命周期结束之前，生成第二密钥信息，将第二密钥信息发送给接入点。接入点可以将该第二密钥信息转发给请求站点，从而请求站点可以在第一密钥的生命周期结束之后，采用第二密钥信息替换第一密钥信息对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输。

需要说明的是，作为一种可行的实施方式，直接链路建立请求消息和直接链路建立响应消息可以封装成数据帧格式经由接入点转发。在这种实施场景下，接入点可以不对上述消息进行解析，而仅执行消息转发操作，这种场景即为隧道式直接链路建立过程。

20 作为另一种可行的实施方式，直接链路建立请求消息和直接链路建立响应消息也可以以管理帧的格式经由接入点转发，在该实施场景下，接入点可以对上述消息解析，以便于对请求站点与哪个中继通信进行管理，这种实施场景即为非隧道式直接链路建立过程。

本实施例提供的建立链路方法，接入点将请求站点发送的直接链路建立请求消息转发给被请求站点之后，接入点接收的被请求站点返回的直接链路建立响应消息中携带被请求站点生成的密钥信息，接入点将该直接链路建立响应消息返回给请求站点后，请求站点能够根据该密钥对请求站点与被请求站点之间的直接链路上传输的业务数据进行加/解密，实现节省请求站点与被请求站点建

30

立链路过程中的信令开销。

图 3 为本发明的建立直接链路方法另一个实施例的流程图，如图 3 所示，本实施例从请求站点侧在建立直接链路过程中执行的操作为例，对本发明提供
5 的建立直接链路方法进行说明。该方法包括：

S301、请求站点向接入点发送直接链路建立请求消息，以使接入点将直接链路建立请求消息发送给被请求站点，直接链路建立请求消息用于请求在请求站点与被请求站点之间建立直接链路。

S302、请求站点接收接入点发送的直接链路建立响应消息，直接链路建立
10 响应消息中携带第一密钥信息，第一密钥信息用于对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输。

S303、请求站点通过直接链路向被请求站点发送的第一直接链路建立确认消息，第一直接链路建立确认消息用于指示请求站点接收到被请求站点生成的第一密钥信息。

15 当请求站点与接入点距离较远，需要被请求站点转发业务数据的实施场景下，请求站点可以发起到被请求站点的直接链路建立。而在请求站点与被请求站点直接链路建立的过程中，需要接入点转发直接链路建立请求消息和直接链路建立响应消息。

被请求站点接收到接入点转发的直接链路建立请求消息后，可以在本地生
20 成用于对请求站点与被请求站点之间的直接链路上传输的业务数据进行加/解密的第一密钥信息。并将第一密钥信息携带在直接链路建立响应消息中发送给接入点。请求站点可以接收到接入点转发的携带第一密钥信息的直接链路建立响应消息。

其中，第一密钥信息中可以包括第一密钥，或者可以包括第一密钥和第一
25 密钥的生命周期信息。

请求站点与被请求站点之间的直接链路建立之后，请求站点可以该上采用该第一密钥信息对业务数据，例如：电表读数，传感器的检测数据等进行加密。

需要说明的是，请求站点接收接入点发送的直接链路建立响应消息之后，可以通过直接链路向被请求站点返回第一直接链路建立确认消息，以指示接收
30 到被请求站点生成的第一密钥信息。

进一步的，在第一密钥的生命周期结束之前，请求站点还可以接收到接入

点转发的第二密钥信息，该第二密钥信息由被请求站点在第一密钥的生命周期结束之前生成。从而请求站点可以在第一密钥的生命周期结束之后，采用第二密钥信息对请求站点与被请求站点之间的直接链路上传输的业务数据进行加密。

- 5 其中，第二密钥信息中可以包括第二密钥，或者，可以包括第二密钥和第二密钥的生命周期信息。

类似的，请求站点接收接入点发送的第二密钥信息之后，可以通过直接链路向被请求站点发送的第二直接链路建立确认消息，用于指示接收到被请求站点生成的第二密钥信息。

- 10 本实施例提供的建立链路方法，请求站点向接入点发送直接链路建立请求消息之后，可以接收到接入点返回的携带被请求站点生成的密钥信息的直接链路建立响应消息，请求站点能够根据该密钥对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输，实现节省请求站点与被请求站点建立链路过程中的信令开销。

15

图 4 为本发明提供的密钥更新方法又一个实施例的流程图，如图 4 所示，该方法包括：

- S401、被请求站点生成第二密钥信息，第二密钥信息用于替换被请求站点生成的第一密钥信息，对请求站点与被请求站点之间的直接链路上传输的业务数据 20 数据进行安全传输；

S402、被请求站点将第二密钥信息发送给接入点，以使接入点将第二密钥信息发送给请求站点。

- 第一密钥信息可以为被请求站点生成的任一密钥信息，举例来说，可以是被请求站点与请求站点建立直接链路过程中生成的密钥信息，也可以是被请求 25 站点在与请求站点通过直接链路进行业务传输的过程中生成的密钥信息。

- 由于第一密钥具有一定的生命周期，在生命周期结束后，第一密钥将失效，无法再用于对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输。据此，被请求站点可以在第一密钥的生命周期结束之前，或者被请求站点的计时器溢出，或者请求站点请求更新第一密钥等实施场景下，生成第二 30 密钥信息，将包括第二密钥信息发送给接入点，以使接入点将该第二密钥信息转发给请求站点，从而请求站点可以在第一密钥的生命周期结束之后，采用第

二密钥信息替换第一密钥信息，对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输。

可选的，第二密钥信息中可以包括第二密钥，或者可以包括第二密钥和第二密钥的生命周期，在第二密钥信息中包括第二密钥和第二密钥的生命周期
5 时，被请求站点在生成第二密钥后，还可以确定第二密钥的生命周期，并将第二密钥的生命周期信息包括在第二密钥信息中发送给接入点。

其中，被请求站点可以将第二密钥信息携带在现有的与接入点之间交互的各种格式的消息中发送给接入点，举例来说，可以将第二密钥信息携带在直接链路建立响应格式的消息中发送给接入点。

10 由于被请求站点可以在第一密钥的生命周期结束之前，产生第二密钥信息并发送给请求站点，从而避免了由于第一密钥过期而导致的请求站点与被请求站点之间的直接链路重新建立，从而增加了传输吞吐率。

被请求站点将第二密钥信息发送给接入点之后，可以接收到请求站点通过直接链路发送的第二直接链路建立确认消息（**Confirm** 消息），该第二直接链路
15 建立确认消息用于指示请求站点接收到被请求站点生成的第二密钥信息，该第二直接链路建立确认消息中也可以携带用于完整性验证的 **MIC**。

被请求站点可以通过直接链路接收请求站点发送的第二直接链路建立确认消息，可以根据其中携带的 **MIC** 进行完整性验证。若验证通过，则被请求站点可以通过直接链路向请求站点发送 **ACK**。

20 本实施例提供的密钥更新方法，被请求站点产生用于替换第一密钥信息的第二密钥信息后，可以将第二密钥信息通过接入点返回给请求站点，以使请求站点采用第二密钥信息替换第一密钥信息对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输，实现节省密钥更新过程的信令开销。

25 图 5 为本发明提供的密钥更新方法又一个实施例的流程图，如图 5 所示，该方法包括：

S501、接入点接收被请求站点发送的第二密钥信息，第二密钥信息由被请求站点生成，用于替换被请求站点生成的第一密钥信息，对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输；

30 **S502**、接入点将第二密钥信息发送给请求站点。

被请求站点在第一密钥的生命周期结束之前，生成第二密钥信息，将第二

密钥信息发送给接入点。接入点可以将该第二密钥信息转发给请求站点，从而请求站点可以在第一密钥的生命周期结束之后，采用第二密钥信息替换第一密钥信息对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输。

5 本实施例提供的密钥更新方法，接入点接收到被请求站点产生用于替换第一密钥的第二密钥信息后，可以将第二密钥信息转发给请求站点，以使请求站点采用第二密钥信息替换第一密钥信息对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输，实现节省密钥更新过程的信令开销。

10 图 6 为本发明提供的密钥更新方法又一个实施例的流程图，如图 6 所示，该方法包括：

S601、请求站点接收接入点发送的第二密钥信息，第二密钥信息由被请求站点生成，用于替换被请求站点生成的第一密钥信息，对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输；

15 S602、请求站点采用第二密钥信息替换第一密钥信息，对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输。

在第一密钥的生命周期结束之前，请求站点还可以接收到接入点转发的第二密钥信息，该第二密钥信息由被请求站点在第一密钥的生命周期结束之前生成。从而请求站点可以在第一密钥的生命周期结束之后，采用第二密钥信息对
20 请求站点与被请求站点之间的直接链路上传输的业务数据进行加密。

其中，第二密钥信息中包括用于替换被请求站点生成的第一密钥信息，对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输第二密钥信息。可选的，第二密钥信息中还可以包括第二密钥的生命周期信息。

请求站点接收接入点发送的第二密钥信息之后，可以通过直接链路向被请
25 求站点发送的第二直接链路建立确认消息，用于指示接收到被请求站点生成的第二密钥信息。

本实施例提供的密钥更新方法，请求站点可以接收到接入点转发的被请求站点产生用于替换第一密钥信息的第二密钥信息，从而采用第二密钥信息替换第一密钥信息对请求站点与被请求站点之间的直接链路上传输的业务数据进行
30 安全传输，实现节省密钥更新过程的信令开销。

图 7 为本发明的建立链路方法另一个实施例的流程图，如图 7 所示，本实施例提供了请求站点（STA1）、接入点（AP）和被请求站点（STA2）在建立链路过程中交互过程。

需要说明的是，STA1 已经确定需要通过 STA2 传输业务数据到达 AP，STA1 已选定 STA2（即获得 STA2 地址信息）。在建立 STA1 与 STA2 之间的直接链路之前，STA1 和 STA2 分别与同一个 AP 关联，并建立了对应的鲁棒安全网络关联（Robust Security Network Association, RSNA），即 STA1 与 AP 之间，AP 与 STA2 之间均建立了安全的双向的链路。

该方法包括：

S701、STA1 向 AP 发送直接链路建立请求消息，直接链路建立请求消息用于请求在请求站点与被请求站点之间建立直接链路。

其中，STA1 向 AP 发送的直接链路建立请求消息（Setup Request）中包括：STA1 的地址信息，STA2 的地址信息，STA1 支持的速率集合和能力 Capacities 参数等。该直接链路建立请求消息利用 STA1 与 AP 进行关联时产生的 PTK 进行加密。STA1 与 AP 进行关联时产生密钥 1（PTK1）的过程为现有技术，在此不再赘述。

可选的，直接链路建立请求消息中携带的 STA1 的地址信息和 STA2 的地址信息，可以采用关联标识（Association Identifier, AID），AID 可以是在 STA1 与 AP 进行关联时 AP 为 STA1 分配的关联标识，该关联标识的长度通常为 16 比特，相对于使用 48 比特媒体接入控制（Media Access Control, MAC）地址，在 STA2 传输时使用长度短的关联标识可以降低传输的负担，缩短链路建立后数据帧的帧头，从而可以提高有效负载的吞吐率。

需要说明的是，STA1 与 STA2 建立直连链路过程中，可以采用 AID 作为各自的地址信息。STA1 与 STA2 直连链路建立后，当 STA1 需要向 STA2 发送业务数据时，可以采用如下表一所示的两地址的短 MAC 帧头格式。

Octets: 2	2	2	2
Frame Control	AID (A1 for STA1)	AID (A2 for STA2)	Sequence Control

表一

表一中：Frame Control 表示帧控制字，占用 2 个字节；A1 for STA1 为 STA1 的 AID，占用 2 个字节；A2 for STA2 为 STA2 的 AID，占用 2 个字节；Sequence

Control 携带数据单元的编号和数据单元片段的编号，占用 2 个字节。

S702、AP 将直接链路建立请求消息发送给 STA2。

其中，AP 可以根据业务需要选择是否需要解析直接链路建立请求消息。例如：为了管理 AP 范围内的各 STA1，以保证业务传输质量，AP 可以解析建立请求消息，以获知 STA1 通过哪个 STA2 转发业务数据。

AP 向 STA2 转发的直接链路建立请求消息采用 STA2 与 AP 关联时产生的密钥 2 (PTK2) 进行加密。

S703、STA2 生成第一密钥信息，第一密钥信息用于对 STA1 与 STA2 之间的直接链路上传输的业务数据进行安全传输。

其中，STA2 可以生成一个唯一的不与其他密钥重复的随机数作为第一密钥，也可以通过其他密钥生成方式生成第一密钥，在此并不做出限制。

可选的，STA2 还可以确定第一密钥的生命周期。

S704、STA2 向 AP 发送直接链路建立响应消息，直接链路建立响应消息中携带第一密钥信息。

其中，第一密钥信息中包括第一密钥，或者，可以包括第一密钥和第一密钥的生命周期信息。

与直接链路建立请求消息类似的，STA2 向 AP 发送 TDLS 建立响应消息中包括：STA1 的地址信息，STA2 的地址信息，STA2 支持的速率集合和能力 Capacities 参数等。可选的，该 STA1 的地址信息和 STA2 的地址信息也可以采用 AID。此外，该直接链路建立响应消息中还携带 STA2 生成的第一密钥信息。

STA2 向 AP 方式的直接链路建立响应消息同样采用 STA2 与 AP 关联时产生的密钥 2 (PTK2) 进行加密。

STA2 在向 AP 发送直接链路建立响应消息之后，可以一直处于 active 状态，直到收到 S707 中的第一确认消息或是 STA2 的定时器溢出。

S705、AP 将直接链路建立响应消息发送给请求站点。

AP 向 STA1 转发的直接链路建立响应消息可以采用 STA1 与 AP 进行关联时产生密钥 1 (PTK1) 进行加密。

S706、STA1 采用第一密钥信息对第一直接链路建立确认消息进行加密，生成第一消息完整性码 MIC。

S707、STA1 通过直接链路向 STA2 发送第一直接链路建立确认消息，第

一直接链路建立确认消息中携带第一 MIC。

其中，第一直接链路建立确认消息（Confirm 消息）至少包括：STA1 的地址信息、STA2 的地址信息和第一 MIC 等。

可选的，STA1 的地址信息和 STA2 的地址信息，可以采用 AID。

- 5 S708、STA2 根据第一 MIC 对请求站点接收的第一密钥进行完整性验证。若验证通过，则执行 S709，否则流程结束。

S709、STA2 通过直接链路向 STA1 发送第一确认消息，第一确认消息用于指示 STA1 接收的第一密钥信息通过完整性验证。

- 10 其中，STA1 根据第一密钥信息生成第一 MIC 的过程，以及 STA2 根据第一 MIC 对 STA1 接收的第一密钥信息进行完整性验证的过程均为现有技术，在此不再赘述。如果 STA2 进行完整性验证失败，则 STA2 不向 STA1 发送第一确认消息，则 STA1 与 STA2 的直接链路建立失败。

- 15 STA1 与 STA2 之间的直接链路建立完毕后，STA1 可以采用第一密钥信息对在直接链路向 STA2 发送的业务数据进行加密，再由 STA2 将业务数据传输至 AP。其中，STA2 向 AP 转发的业务数据可以由 STA2 与 AP 进行关联时产生密钥 2（PTK2）进行加密。

- 20 可选的，STA1 在向 AP 发送业务数据的过程中，也可以选择是否通过 STA2 转发业务数据。STA1 可以在业务数据的物理层（Physical Layer，PHY 层）的帧头的信号或信号 A 或信号 B（Signal 或 Signal A 或 Signal B，SIGA）单元内添加一个比特的指示位，通过该指示位指示 STA2 是否转发数据包。例如：STA1 可以通过该指示位置 1，表示数据包由 STA2 转发；置 0，表示数据包不由 STA2 转发，若 STA2 接收到 STA1 发送的数据包，可以做丢弃处理。需要说明的是，由于 11ah 规范中物理层的循环冗余校验（Cyclical Redundancy Check，CRC）校验只有 4 个比特，物理头内的指示位较易受到干扰，因此，
- 25 STA2 可以进一步分析数据帧 MAC 头内的地址信息来确认是否需要向 AP 转发数据帧。

- 30 本实施例提供的建立链路方法，请求站点向接入点发送直接链路建立请求消息之后，接入点可以将该建立请求消息发送给被请求站点，被请求站点接收到接入点转发的直接链路建立请求消息之后，在返回给接入点的直接链路建立响应消息中携带被请求站点生成的密钥信息，以使接入点将该建立响应消息返回给请求站点后，请求站点能够根据该密钥对请求站点与被请求站点之间的直

接链路上传输的业务数据进行安全传输，实现节省请求站点与被请求站点建立链路过程中的信令开销。被请求站点可以从直接链路上直接收到请求站点发送的直接链路建立确认消息，而不必通过接入点转发该确认消息，因此，减少了请求站点直接向接入点发送消息的次数，可以有效降低请求站点的能耗。

5

图 8 为本发明提供的密钥更新方法又一个实施例的流程图，如图 8 所示，该方法包括：

S801、STA2 生成第二密钥信息，第二密钥信息用于替换第一密钥信息，对 STA1 与 STA2 之间的直接链路上传输的业务数据进行安全传输。

10 可选的，STA2 还可以确定第二密钥的生命周期。

与生成第一密钥类似的，STA2 可以生成一个唯一的不与其他密钥（包括第一密钥）重复的随机数作为第二密钥，也可以通过其他密钥生成方式生成第二密钥，在此并不做出限制。

S802、STA2 将第二密钥信息发送给 AP。

15 其中，第二密钥信息中包括第二密钥，或者，可以包括第二密钥和第二密钥的生命周期信息。

其中，STA2 向 AP 发送的第二密钥信息可以采用现有的各种消息格式。可选的，可以采用直接链路建立响应消息（Setup Response）的消息格式。该新消息中可以包括：STA1 的地址信息、STA2 的地址信息，STA2 支持的速率集合和能力（Capacities）参数，以及第二密钥信息。该消息可以通过 STA2 与 AP 之间的 RSNA 传递，可以采用 STA2 与 AP 之间关联时产生的密钥 2（PTK2）进行加密。

可选的，STA1 的地址信息和 STA2 的地址信息可以采用 AID。

S803、AP 将第二密钥信息发送给 STA1。

25 与 S802 类似的，AP 可以根据业务需要选择是否需要解析携带第二密钥及第二密钥的生命周期信息的消息。AP 可以通过 STA1 与 AP 关联时产生的密钥 1（PTK1）对携带第二密钥信息的消息进行加密。

S804、STA1 采用第二密钥信息对第二直接链路建立确认消息进行加密，生成第二 MIC。

30 S805、STA1 通过直接链路向 STA2 发送第二直接链路建立确认消息，第二直接链路建立确认消息中携带第二 MIC。

S806、STA2 根据第二 MIC 对第三确认消息进行完整性验证。若验证通过，则执行 S417，否则流程结束。

S807、STA2 通过直接链路向 STA1 发送第二确认消息，第二确认消息用于指示 STA1 接收的第二密钥通过完整性验证。

5 其中，S804-S807 的过程与 S706-S709 的过程相类似，可参见 S706-S709 的相关描述。

本实施例提供的密钥更新方法，被请求站点可以在密钥的生命周期结束之前，产生新的密钥并发送给请求站点，从而避免了由于密钥过期而导致的请求站点与被请求站点之间的直接链路重新建立，从而增加了传输吞吐率。

10

图 9 为本发明提供的被请求站点一个实施例的结构示意图，如图 9 所示，该被请求站点包括：接收器 11、处理器 12 和发送器 13；

接收器 11，用于接收接入点发送的直接链路建立请求消息，直接链路建立请求消息用于请求在请求站点与被请求站点之间建立直接链路；

15 处理器 12，用于生成第一密钥信息，第一密钥信息用于对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输；

发送器 13，用于向接入点发送直接链路建立响应消息，以使接入点将直接链路建立响应消息发送给请求站点，直接链路建立响应消息中携带第一密钥信息；

20 接收器 11 还可以用于：接收请求站点通过直接链路发送的第一直接链路建立确认消息，第一直接链路建立确认消息用于指示请求站点接收到被请求站点生成的第一密钥信息。

可选的，发送器 13 发送的第一密钥信息中包括第一密钥，或包括第一密钥和第一密钥的生命周期；当第一密钥信息中包括第一密钥和第一密钥的生命周
25 期时，处理器 12 还可以用于：确定第一密钥的生命周期。

可选的，处理器 12 还可以用于：生成第二密钥信息，第二密钥信息用于替换第一密钥信息，对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输；

30 相应的，发送器 13 还可以用于：将第二密钥信息发送给接入点，以使接入点将第二密钥信息发送给被请求站点。

可选的，发送器 13 发送的第二密钥信息中包括第二密钥，或第二密钥和第

二密钥的生命周期；当第二密钥信息中包括第二密钥和第二密钥的生命周期时，处理器 12 还可以用于：确定第二密钥的生命周期。

可选的，接收器 11 还可以用于：接收请求站点通过直接链路发送的第二直接链路建立确认消息，第二直接链路建立确认消息用于指示请求站点接收到被
5 请求站点生成的第二密钥信息。

本发明实例提供的被请求站点为本发明实施例提供的建立直接链路方法的执行设备，其执行建立直接链路方法的具体过程可参见图 3 和图 7 所示的方法实施例中的相关描述，在此不再赘述。

本实施例被请求站点，接收到接入点转发的直接链路建立请求消息之后，
10 在返回给接入点的直接链路建立响应消息中携带被请求站点生成的密钥信息，以使接入点将该直接链路建立响应消息返回给请求站点后，请求站点能够根据该密钥对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输，实现节省请求站点与被请求站点建立链路过程中的信令开销。

15 图 10 为本发明提供的请求站点一个实施例的结构示意图，如图 10 所示，该请求站点包括：发送器 21、接收器 22；

发送器 21，用于向接入点发送直接链路建立请求消息，以使接入点将直接链路建立请求消息发送给被请求站点，直接链路建立请求消息用于请求在请求站点与被请求站点之间建立直接链路；

20 接收器 22，用于接收接入点发送的直接链路建立响应消息，直接链路建立响应消息中携带第一密钥信息，第一密钥信息用于对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输；

发送器 21 还用于：通过直接链路向被请求站点发送的第一直接链路建立确认消息，第一直接链路建立确认消息用于指示请求站点接收到被请求站点生成
25 的第一密钥信息。

可选的，接收器 22 接收的第一密钥信息可以包括第一密钥，或者包括第一密钥和第一密钥的生命周期信息。

可选的，接收器 22 还可以用于：接收接入点发送的第二密钥信息，第二密钥信息由被请求站点生成，第二密钥信息用于替换第一密钥，对请求站点与被
30 请求站点之间的直接链路上传输的业务数据进行安全传输。

可选的，接收器 22 接收的第二密钥信息可以包括第二密钥，或包括第二密

钥和第二密钥的生命周期信息。

可选的，发送器 21 还可以用于：通过直接链路向被请求站点发送的第二直接链路建立确认消息，第二直接链路建立确认消息用于指示请求站点接收到被请求站点生成的第二密钥信息。

5 本发明实例提供的请求站点为本发明实施例提供的建立直接链路方法的执行设备，其执行建立直接链路方法的具体过程可参见图 1 和图 7 所示的方法实施例中的相关描述，在此不再赘述。

本实施例提供的请求站点，向接入点发送直接链路建立请求消息之后，可以接收到接入点返回的携带被请求站点生成的密钥信息的直接链路建立响应消息，请求站点能够根据该密钥对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输，实现节省请求站点与被请求站点建立链路过程中的信令开销。

图 11 为本发明提供的被请求站点又一个实施例的结构示意图，如图 11 所示，该被请求站点可以包括：处理器 31 和发送器 32；

处理器 31，用于生成第二密钥信息，第二密钥信息用于替换被请求站点生成的第一密钥信息，对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输；

发送器 32，用于将第二密钥信息发送给接入点，以使接入点将第二密钥信息发送给被请求站点。

可选的，发送器 32 发送的第二密钥信息中包括可以第二密钥，或第二密钥和第二密钥的生命周期；当第二密钥信息中包括第二密钥和第二密钥的生命周期时，处理器 31 还可以用于：确定第二密钥的生命周期。

图 12 为本发明提供的被请求站点又一个实施例的结构示意图，如图 12 所示，可选的，在图 11 所示实施例的基础上，被请求站点还可以包括：

接收器 33，可以用于接收请求站点通过直接链路发送的直接链路建立确认消息，直接链路建立确认消息用于指示请求站点接收到被请求站点生成的第二密钥信息。

本发明实例提供的被请求站点为本发明实施例提供的密钥更新方法的执行设备，其执行密钥更新方法的具体过程可参见图 4 和图 8 所示的方法实施例中的相关描述，在此不再赘述。

本实施例提供的被请求站点，产生用于替换第一密钥信息的第二密钥信息后，可以将第二密钥信息通过接入点返回给请求站点，以使请求站点采用第二密钥信息替换第一密钥信息对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输，实现节省密钥更新过程的信令开销。

5

图 13 为本发明提供的请求站点又一个实施例的结构示意图，如图 13 所示，该请求站点包括：接收器 41 和处理器 42；

接收器 41，用于接收接入点发送的第二密钥信息，第二密钥信息由被请求站点生成，用于替换被请求站点生成的第一密钥信息，对请求站点与被请求站
10 点之间的直接链路上传输的业务数据进行安全传输；

处理器 42，用于采用第二密信息钥替换第一密钥信息，对请求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输。

可选的，接收器 41 接收的第二密钥信息可以包括第二密钥，或包括第一密钥和第二密钥的生命周期信息。

15 图 14 为本发明提供的请求站点又一个实施例的结构示意图，如图 14 所示，在图 13 所示实施例的基础上，该请求站点还可以包括：

发送器 43，用于通过直接链路向被请求站点发送直接链路建立确认消息，直接链路建立确认消息用于指示请求站点接收到被请求站点生成的第二密钥信息。

20 本发明实例提供的请求站点为本发明实施例提供的密钥更新方法的执行设备，其执行密钥更新方法的具体过程可参见图 6 和图 8 所示的方法实施例中的相关描述，在此不再赘述。

本实施例提供的请求站点，可以接收到接入点转发的被请求站点产生用于替换第一密钥的第二密钥信息，从而采用第二密钥信息替换第一密钥信息对请
25 求站点与被请求站点之间的直接链路上传输的业务数据进行安全传输，实现节省密钥更新过程的信令开销。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完
30 成以上描述的全部或者部分功能。上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，模块或单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，
5 或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。
10

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。
15

集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用
时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分
20 可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，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）或处理器（processor）执行本申请各个实施例方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM, Read-Only
Memory）、随机存取存储器（RAM, Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

25 以上，以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案
的本质脱离本申请各实施例技术方案的范围。

权利要求

1、一种建立直接链路方法，其特征在于，包括：

请求站点向接入点发送直接链路建立请求消息，以使所述接入点将所述直接链路建立请求消息发送给所述被请求站点，所述直接链路建立请求消息用于
5 请求在所述请求站点与被请求站点之间建立直接链路；

所述请求站点接收所述接入点发送的直接链路建立响应消息，所述直接链路建立响应消息中携带第一密钥信息，所述第一密钥信息用于对所述请求站点与
所述被请求站点之间的所述直接链路上传输的业务数据进行安全传输；

所述请求站点通过所述直接链路向所述被请求站点发送的第一直接链路建
10 立确认消息，所述第一直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的所述第一密钥信息。

2、根据权利要求 1 所述的方法，其特征在于，所述第一密钥信息包括第一密钥，或者包括所述第一密钥和所述第一密钥的生命周期信息。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述请求站点接收所述
15 接入点发送的直接链路建立响应消息之后，还包括：

所述请求站点接收所述接入点发送的第二密钥信息，所述第二密钥信息由所述被请求站点生成，所述第二密钥信息用于替换所述第一密钥信息，对所述
请求站点与所述被请求站点之间的所述直接链路上传输的业务数据进行安全传
输。

20 4、根据权利要求 3 所述的方法，其特征在于，所述第二密钥信息包括第二密钥，或包括所述第二密钥和所述第二密钥的生命周期信息。

5、根据权利要求 3 或 4 所述的方法，其特征在于，所述请求站点接收所述
接入点发送的第二密钥信息之后，还包括：

所述请求站点通过所述直接链路向所述被请求站点发送的第二直接链路建
25 立确认消息，所述第二直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的所述第二密钥信息。

6、一种建立直接链路方法，其特征在于，包括：

被请求站点接收接入点发送的直接链路建立请求消息，所述直接链路建立
请求消息用于请求在请求站点与所述被请求站点之间建立直接链路；

30 所述被请求站点生成第一密钥信息，所述第一密钥信息用于对所述请求站

点与所述被请求站点之间的所述直接链路上传输的业务数据进行安全传输；

所述被请求站点向所述接入点发送直接链路建立响应消息，以使所述接入点将所述直接链路建立响应消息发送给所述请求站点，所述直接链路建立响应消息中携带第一密钥信息；

- 5 所述被请求站点接收所述请求站点通过所述直接链路发送的第一直接链路建立确认消息，所述第一直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的所述第一密钥信息。

7、根据权利要求 6 所述的方法，其特征在于，所述第一密钥信息中包括第一密钥，或包括所述第一密钥和所述第一密钥的生命周期；

- 10 当所述第一密钥信息中包括所述第一密钥和所述第一密钥的生命周期时，所述被请求站点向所述接入点发送直接链路建立响应消息之前，还包括：

所述被请求站点确定所述第一密钥的生命周期。

8、根据权利要求 6 或 7 所述的方法，其特征在于，所述被请求站点向所述接入点发送直接链路建立响应消息之后，还包括：

- 15 所述被请求站点生成第二密钥信息，所述第二密钥信息用于替换所述第一密钥信息，对所述请求站点与所述被请求站点之间的所述直接链路上传输的业务数据进行安全传输；

所述被请求站点将第二密钥信息发送给所述接入点，以使所述接入点将所述第二密钥信息发送给所述被请求站点。

- 20 9、根据权利要求 8 所述的方法，其特征在于，所述第二密钥信息中包括第二密钥，或所述第二密钥和所述第二密钥的生命周期；

当所述第二密钥信息中包括所述第二密钥和所述第二密钥的生命周期时，所述被请求站点向所述接入点发送直接链路建立响应消息之后，还包括：

所述被请求站点确定所述第二密钥的生命周期

- 25 。

10、根据权利要求 8 或 9 所述的方法，其特征在于，所述被请求站点将所述第二密钥信息发送给所述接入点之后，还包括：

所述被请求站点接收所述请求站点通过所述直接链路发送的第二直接链路建立确认消息，所述第二直接链路建立确认消息用于指示所述请求站点接收到

- 30 所述被请求站点生成的第二密钥信息。

11、一种密钥更新方法，其特征在于，包括：

被请求站点生成第二密钥信息，所述第二密钥信息用于替换所述被请求站点生成的第一密钥信息，对请求站点与所述被请求站点之间的直接链路上传输的业务数据进行安全传输；

5 所述被请求站点将第二密钥信息发送给接入点，以使所述接入点将所述第二密钥信息发送给所述被请求站点。

12、根据权利要求 11 所述的方法，其特征在于，所述第二密钥信息中包括第二密钥，或所述第二密钥和所述第二密钥的生命周期；

10 当所述第二密钥信息中包括所述第二密钥和所述第二密钥的生命周期时，所述被请求站点将第二密钥信息发送给接入点之前，还包括：

所述被请求站点确定所述第二密钥的生命周期。

13、根据权利要求 11 或 12 所述的方法，其特征在于，所述被请求站点将所述第二密钥信息发送给接入点之后，还包括：

15 所述被请求站点接收所述请求站点通过所述直接链路发送的直接链路建立确认消息，所述直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的第二密钥信息。

14、一种密钥更新方法，其特征在于，包括：

20 请求站点接收接入点发送的所述第二密钥信息，所述第二密钥信息由所述被请求站点生成，用于替换所述被请求站点生成的第一密钥信息，对所述请求站点与所述被请求站点之间的直接链路上传输的业务数据进行安全传输；

所述请求站点采用所述第二密钥信息替换所述第一密钥信息，对所述请求站点与所述被请求站点之间的直接链路上传输的业务数据进行安全传输。

15、根据权利要求 14 所述的方法，其特征在于，所述第二密钥信息包括第二密钥，或包括所述第一密钥和所述第二密钥的生命周期信息。

25 16、根据权利要求 14 或 15 所述的方法，其特征在于，所述请求站点接收接入点发送的所述第二密钥信息之后，还包括：

所述请求站点通过所述直接链路向所述被请求站点发送直接链路建立确认消息，所述直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的第二密钥信息。

30 17、一种请求站点，其特征在于，包括：

发送器，用于向接入点发送直接链路建立请求消息，以使所述接入点将所

述直接链路建立请求消息发送给所述被请求站点，所述直接链路建立请求消息用于请求在所述请求站点与被请求站点之间建立直接链路；

接收器，用于接收所述接入点发送的直接链路建立响应消息，所述直接链路建立响应消息中携带第一密钥信息，所述第一密钥信息用于对所述请求站点
5 与所述被请求站点之间的所述直接链路上传输的业务数据进行安全传输；

所述发送器还用于：通过所述直接链路向所述被请求站点发送的第一直接链路建立确认消息，所述第一直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的所述第一密钥信息。

18、根据权利要求 17 所述的请求站点，其特征在于，所述接收器接收的所述
10 述第一密钥信息包括第一密钥，或者包括所述第一密钥和所述第一密钥的生命周期信息。

19、根据权利要求 17 或 18 所述的请求站点，其特征在于，所述接收器还用于：接收所述接入点发送的第二密钥信息，所述第二密钥信息由所述被请求
15 站点生成，所述第二密钥信息用于替换所述第一密钥信息，对所述请求站点与所述被请求站点之间的所述直接链路上传输的业务数据进行安全传输。

20、根据权利要求 19 所述的请求站点，其特征在于，所述接收器接收的所述
述第二密钥信息包括第二密钥，或包括所述第二密钥和所述第二密钥的生命周期信息。

21、根据权利要求 19 或 20 所述的请求站点，其特征在于，所述发送器还
20 用于：通过所述直接链路向所述被请求站点发送的第二直接链路建立确认消息，所述第二直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的所述第二密钥信息。

22、一种被请求站点，其特征在于，包括：

接收器，用于接收接入点发送的直接链路建立请求消息，所述直接链路建
25 立请求消息用于请求在请求站点与所述被请求站点之间建立直接链路；

处理器，用于生成第一密钥信息，所述第一密钥信息用于对所述请求站点
与所述被请求站点之间的所述直接链路上传输的业务数据进行安全传输；

发送器，用于向所述接入点发送直接链路建立响应消息，以使所述接入点
30 将所述直接链路建立响应消息发送给所述请求站点，所述直接链路建立响应消息中携带第一密钥信息；

所述接收器还用于：接收所述请求站点通过所述直接链路发送的第一直接

链路建立确认消息，所述第一直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的所述第一密钥信息。

23、根据权利要求 22 所述的被请求站点，其特征在于，所述发送器发送的所述第一密钥信息中包括第一密钥，或包括所述第一密钥和所述第一密钥的生命周期；当所述第一密钥信息中包括所述第一密钥和所述第一密钥的生命周期时，所述处理器还用于：确定所述第一密钥的生命周期。

24、根据权利要求 22 或 23 所述的被请求站点，其特征在于，所述处理器还用于：生成第二密钥信息，所述第二密钥信息用于替换所述第一密钥信息，对所述请求站点与所述被请求站点之间的所述直接链路上传输的业务数据进行安全传输；

所述发送器还用于：将第二密钥信息发送给所述接入点，以使所述接入点将所述第二密钥信息发送给所述被请求站点。

25、根据权利要求 24 所述的请求站点，其特征在于，所述发送器发送的所述第二密钥信息中包括第二密钥，或所述第二密钥和所述第二密钥的生命周期；当所述第二密钥信息中包括所述第二密钥和所述第二密钥的生命周期时，所述处理器还用于：确定所述第二密钥的生命周期。

26、根据权利要求 24 或 25 所述的被请求站点，其特征在于，所述接收器还用于：接收所述请求站点通过所述直接链路发送的第二直接链路建立确认消息，所述第二直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的第二密钥信息。

27、一种被请求站点，其特征在于，包括：

处理器，用于生成第二密钥信息，所述第二密钥信息用于替换所述被请求站点生成的第一密钥信息，对请求站点与所述被请求站点之间的直接链路上传输的业务数据进行安全传输；

发送器，用于将第二密钥信息发送给接入点，以使所述接入点将所述第二密钥信息发送给所述被请求站点。

28、根据权利要求 27 所述的被请求站点，其特征在于，所述发送器发送的所述第二密钥信息中包括第二密钥，或所述第二密钥和所述第二密钥的生命周期；当所述第二密钥信息中包括所述第二密钥和所述第二密钥的生命周期时，所述处理器还用于：确定所述第二密钥的生命周期。

29、根据权利要求 27 或 28 所述的被请求站点，其特征在于，还包括：

接收器，用于接收所述请求站点通过所述直接链路发送的直接链路建立确认消息，所述直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的第二密钥信息。

5

30、一种请求站点，其特征在于，包括：

接收器，用于接收接入点发送的所述第二密钥信息，所述第二密钥信息由所述被请求站点生成，用于替换所述被请求站点生成的第一密钥信息，对所述请求站点与所述被请求站点之间的直接链路上传输的业务数据进行安全传输；

10 处理器，用于采用所述第二密钥信息替换所述第一密钥信息，对所述请求站点与所述被请求站点之间的直接链路上传输的业务数据进行安全传输。

31、根据权利要求 30 所述的请求站点，其特征在于，所述接收器接收的所述第二密钥信息包括第二密钥，或包括所述第一密钥和所述第二密钥的生命周期信息。

15 32、根据权利要求 30 或 31 所述的请求站点，其特征在于，还包括：

发送器，用于通过所述直接链路向所述被请求站点发送直接链路建立确认消息，所述直接链路建立确认消息用于指示所述请求站点接收到所述被请求站点生成的第二密钥信息。

20

25

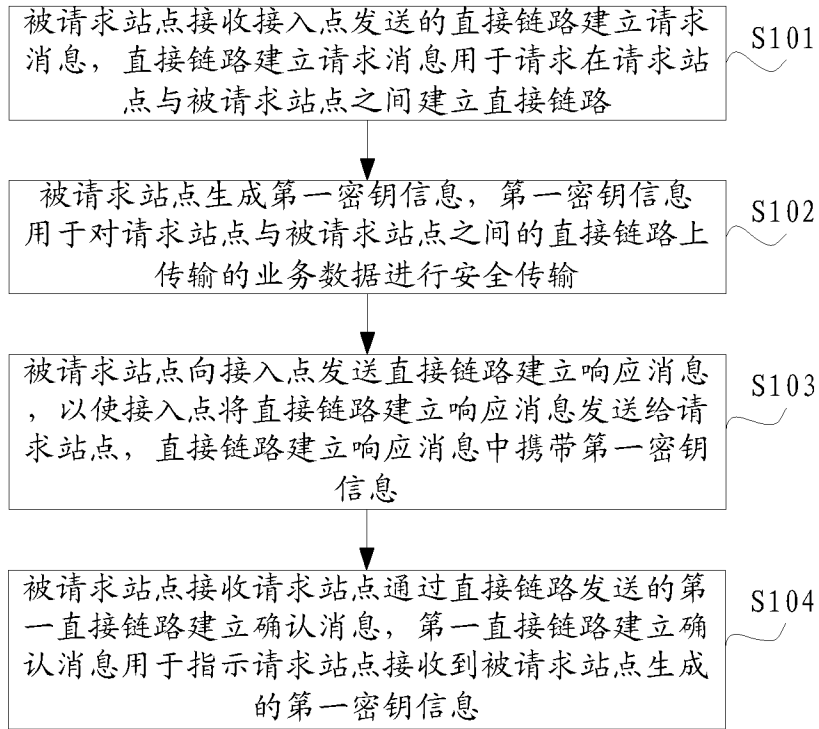


图 1

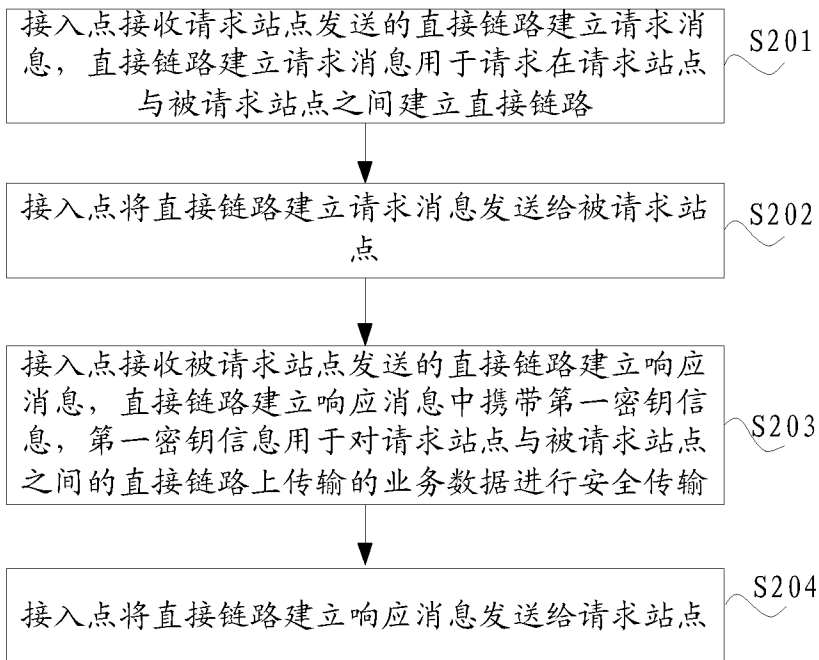


图 2

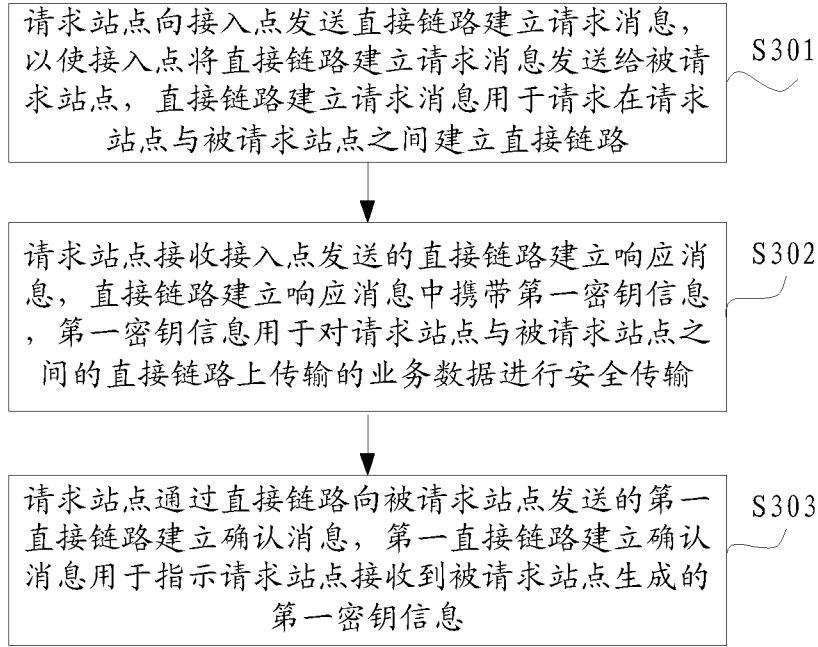


图 3

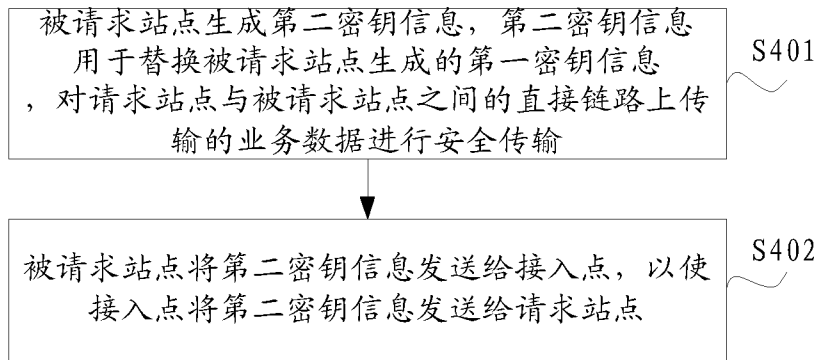


图 4

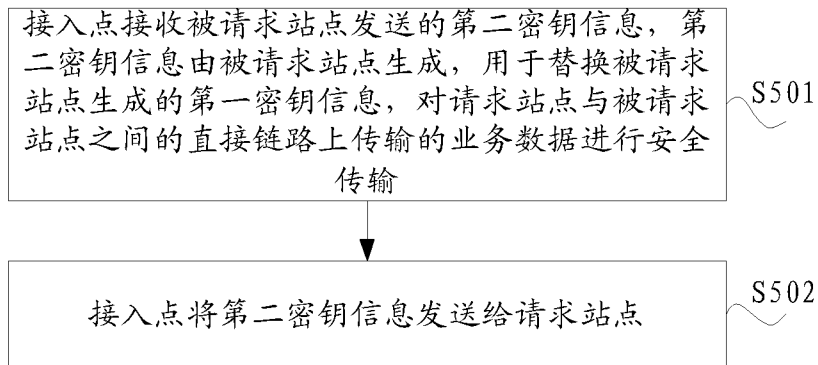


图 5

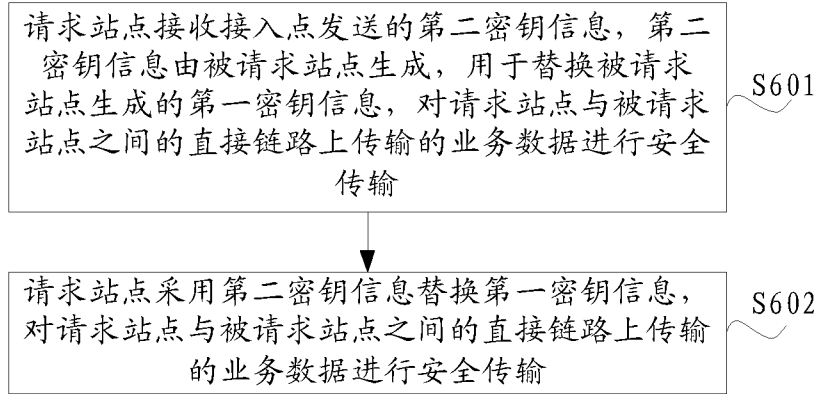


图 6

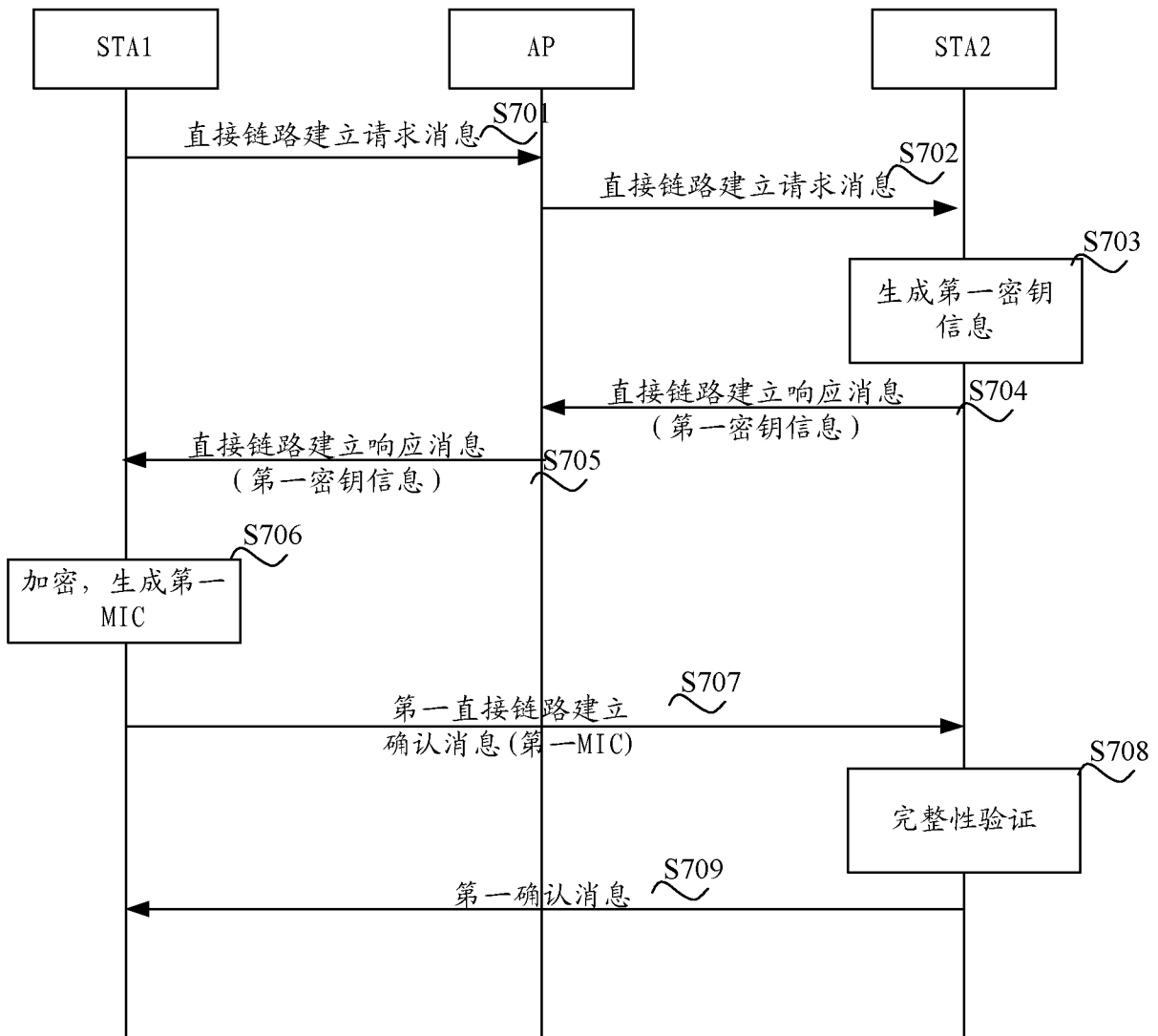


图 7

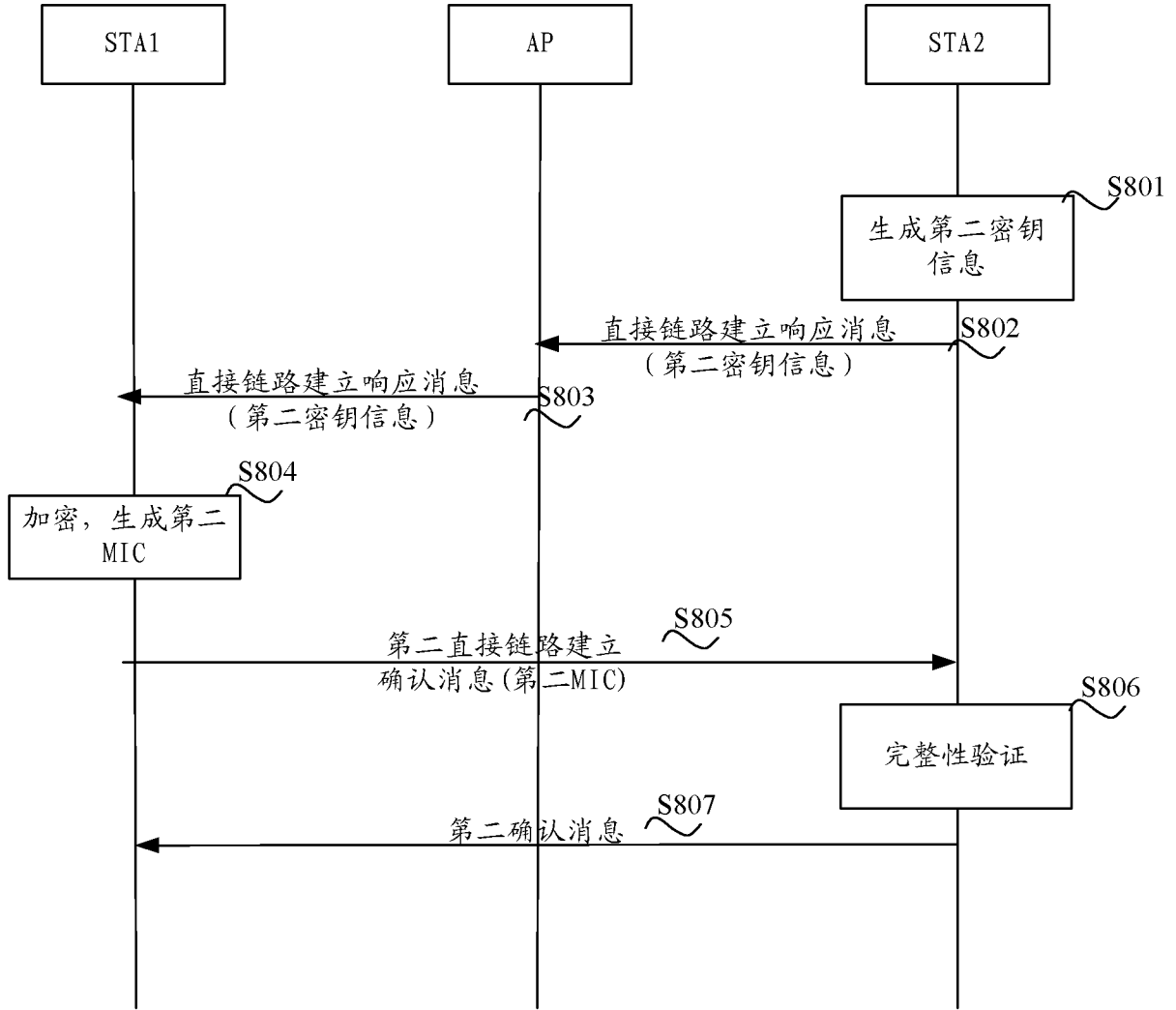


图 8

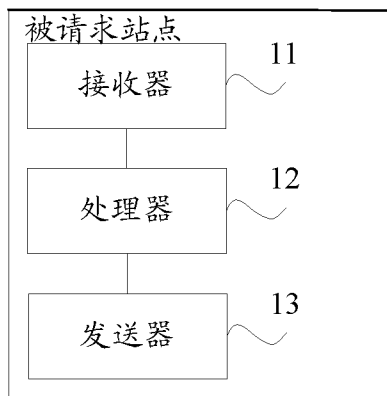


图 9

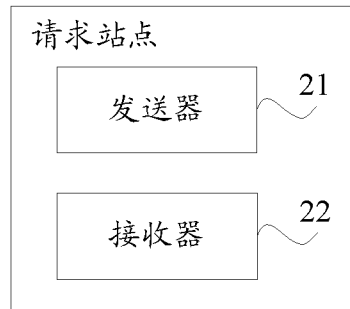


图 10

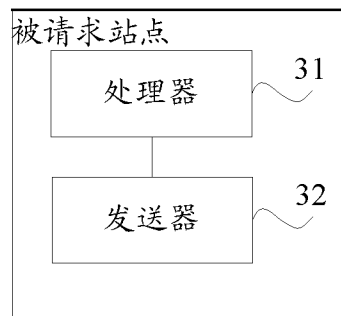


图 11

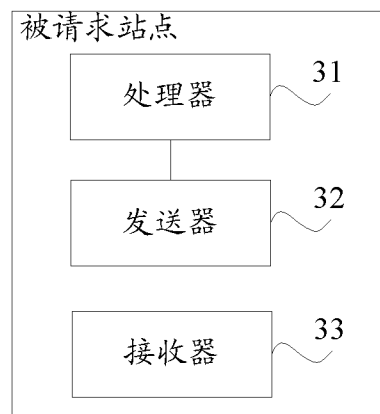


图 12

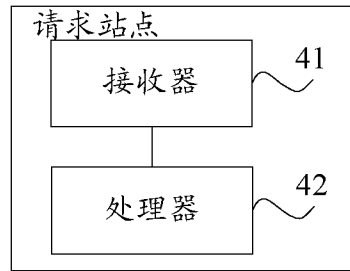


图 13

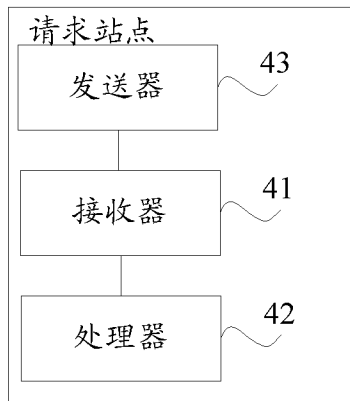


图 14

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/077431

A. CLASSIFICATION OF SUBJECT MATTER

See the 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, H04L, H04Q

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)

CNABS, CNTXT, CNKI: direct link, DLS, establish, key, response, replace, update

VEN: direct link, setup, establish, DLS, key, response, replace, update

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102461317 A (INTEL CORP.), 16 May 2012 (16.05.2012), see claims, and description, pages 2-3	1-2, 6-7, 17-18, 22-23
Y		3-5, 8-16, 19-21, 24-32
Y	CN 102255723 A (CHUNGHWA TELECOM CO., LTD.), 23 November 2011 (23.11.2011), see abstract	3-5, 8-16, 19-21, 24-32
A	CN 101594578 A (SHENZHEN HUAWEI COMMUNICATION TECHNOLOGIES CO., LTD.), 02 December 2009 (02.12.2009), see abstract, description, pages 3-5, and figure 2	1-32
A	CN 101471829 A (HUAWEI TECHNOLOGIES CO., LTD.), 01 July 2009 (01.07.2009), see the whole document	1-32
A	US 2012087356 A1 (QUALCOMM INC.), 12 April 2012 (12.04.2012), see the whole document	1-32

Further documents are listed in the continuation of Box C.

See patent family annex.

<p>* Special categories of cited documents:</p> <p>“A” document defining the general state of the art which is not considered to be of particular relevance</p> <p>“E” earlier application or patent but published on or after the international filing date</p> <p>“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)</p> <p>“O” document referring to an oral disclosure, use, exhibition or other means</p> <p>“P” document published prior to the international filing date but later than the priority date claimed</p>	<p>“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</p> <p>“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</p> <p>“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</p> <p>“&” document member of the same patent family</p>
---	---

Date of the actual completion of the international search
16 September 2013 (16.09.2013)

Date of mailing of the international search report
26 September 2013 (26.09.2013)

Name and mailing address of the ISA/CN:
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No.: (86-10) 62019451

Authorized officer
CHEN, Junru
Telephone No.: (86-10) **62411493**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/077431

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102461317 A	16.05.2012	TW 201129185 A US 2010255869 A1 WO 2010117894 A3 JP 2012523202 A WO 2010117894 A2 EP 2417826 A2 KR 20110134931 A	16.08.2011 07.10.2010 13.01.2011 27.09.2012 14.10.2010 15.02.2012 15.12.2011
CN 102255723 A	23.11.2011	None	
CN 101594578 A	02.12.2009	None	
CN 101471829 A	01.07.2009	None	
US 2012087356 A1	12.04.2012	WO 2012048210 A1	12.04.2012

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/077431

CONTINUATION OF SECOND SHEET

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04 (2009.01) i

H04W 76/02 (2009.01) i

A. 主题的分类 <p style="text-align: center;">参见附加页</p> 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) <p style="text-align: center;">IPC: H04W, H04L, H04Q</p>		
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)) CNABS, CNTXT, CNKI: 直接链路, 直连链路, DLS, 建立, 密钥, 响应, 替换, 更新, 代替, 替代 VEN: direct link, setup, establish, DLS, key, response, replace, update		
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	CN 102461317 A (英特尔公司) 16.5 月 2012 (16.05.2012) 参见权利要求书, 说明书第 2-3 页	1-2, 6-7, 17-18, 22-23
Y		3-5, 8-16, 19-21, 24-32
Y	CN 102255723 A (中华电信股份有限公司) 23.11 月 2011 (23.11.2011) 参见摘要	3-5, 8-16, 19-21, 24-32
A	CN 101594578 A (深圳华为通信技术有限公司) 02.12 月 2009 (02.12.2009) 参见摘要, 说明书第 3-5 页, 图 2	1-32
A	CN 101471829 A (华为技术有限公司) 01.7 月 2009 (01.07.2009) 参见全文	1-32
A	US 2012087356 A1 (QUALCOMM INC) 12.4 月 2012 (12.04.2012) 参见全文	1-32
<input type="checkbox"/> 其余文件在 C 栏的续页中列出。 <input checked="" type="checkbox"/> 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 16.9 月 2013 (16.09.2013)	国际检索报告邮寄日期 26.9 月 2013 (26.09.2013)	
ISA/CN 的名称和邮寄地址: 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10) 62019451	受权官员 <p style="text-align: center;">陈俊茹</p> 电话号码: (86-10) 62411493	

国际检索报告

关于同族专利的信息

国际申请号

PCT/CN2013/077431

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN 102461317 A	16.05.2012	TW 201129185 A US 2010255869 A1 WO 2010117894 A3 JP 2012523202 A WO 2010117894 A2 EP 2417826 A2 KR 20110134931 A	16.08.2011 07.10.2010 13.01.2011 27.09.2012 14.10.2010 15.02.2012 15.12.2011
CN 102255723 A	23.11.2011	无	
CN 101594578 A	02.12.2009	无	
CN 101471829 A	01.07.2009	无	
US 2012087356 A1	12.04.2012	WO 2012048210 A1	12.04.2012

续：第 2 页

A. 主题的分类

H04W 12/04 (2009.01) ;

H04W 76/02 (2009.01) ;