(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107690138 B
(45)授权公告日 2020.08.14

(21)申请号 201610640221.4

(22)申请日 2016.08.05

(65)同一申请的已公布的文献号
申请公布号 CN 107690138 A

(43)申请公布日 2018.02.13

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 陈国海

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 罗振安

(51)Int.Cl.
H04W 12/02(2009.01)
H04W 12/04(2009.01)
H04W 12/06(2009.01)
H04W 36/00(2009.01)
H04W 36/08(2009.01)

(56)对比文件
CN 103888941 A,2014.06.25
CN 103888941 A,2014.06.25
US 7480939 B1,2009.01.20
CN 101111056 B,2010.05.12

审查员 贾斌

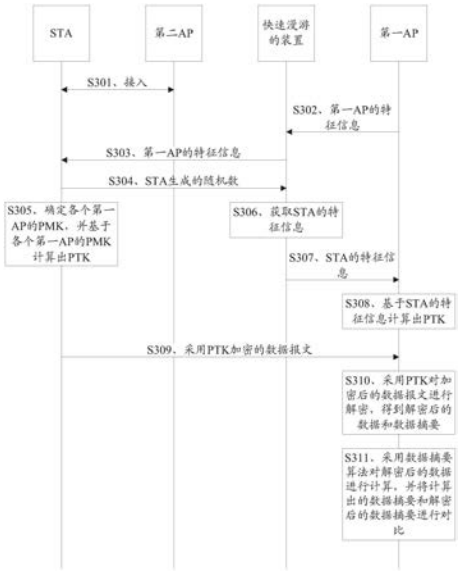
权利要求书4页 说明书18页 附图18页

(54)发明名称

一种快速漫游方法、装置、系统、接入点和移动站

(57)摘要

本发明公开了一种快速漫游方法、装置、系统、接入点和移动站，属于网络技术领域。所述方法包括：快速漫游装置获取第一AP的特征信息；快速漫游装置在确定STA接入第二AP之后，向STA发送第一AP的特征信息；STA生成、发送随机数，并生成PTK；快速漫游装置获取STA的特征信息；快速漫游装置向第一AP发送STA的特征信息；第一AP生成PTK，链路认证、接入认证、密钥协商完成；STA在确定切换到第一AP之后，向第一AP发送采用PTK加密后的数据报文；所述第一AP采用PTK对加密后的数据报文进行解密；第一AP根据解密后的数据报文的内部信息是否一致，完成关联。本发明可以将漫游切换的时间减至0。



CN 107690138 B

1.一种快速漫游方法,其特征在于,所述方法包括:

快速漫游装置获取第一接入点AP的特征信息,所述第一AP的特征信息包括所述第一AP的介质访问控制MAC地址和所述第一AP生成的随机数;

所述快速漫游装置在确定移动站STA接入第二AP之后,向所述STA发送所述第一AP的特征信息,所述第一AP为所述第二AP的邻居;

所述STA生成并发送随机数,基于所述STA生成的随机数、所述STA的MAC地址、成对主密钥PMK、以及所述第一AP的特征信息生成成对临时密钥PTK;

所述快速漫游装置获取所述STA的特征信息,所述STA的特征信息包括所述STA的MAC地址、所述STA生成的随机数、以及所述PMK的特征值;

所述快速漫游装置向所述第一AP发送所述STA的特征信息;

所述第一AP基于所述STA的特征信息和所述第一AP的特征信息生成所述PTK,所述STA和所述第一AP之间的链路认证、接入认证、以及密钥协商完成;

所述STA在确定切换到所述第一AP之后,向所述第一AP发送采用所述PTK加密后的数据报文,其中,所述数据报文包括数据和数据摘要;

所述第一AP采用所述PTK对加密后的所述数据报文进行解密;

所述第一AP采用数据摘要算法对解密后的所述数据进行计算,得到计算出的数据摘要;

所述第一AP将计算出的所述数据摘要与解密后的所述数据摘要进行对比;

当计算出的所述数据摘要与解密后的所述数据摘要一致时,所述STA和所述第一AP之间的关联完成。

2.根据权利要求1所述的方法,其特征在于,所述第一AP的特征信息还包括所述第一AP的加密方式、所述第一AP的频点、所述第一AP的带宽中的至少一种。

3.一种快速漫游方法,其特征在于,所述方法包括:

快速漫游装置获取第一接入点AP的特征信息,所述第一AP的特征信息包括所述第一AP的介质访问控制MAC地址和所述第一AP生成的随机数;

所述快速漫游装置在确定移动站STA接入第二AP之后,向所述STA发送所述第一AP的特征信息,所述第一AP为所述第二AP的邻居,使所述STA生成并发送随机数,基于所述STA生成的随机数、所述STA的MAC地址、成对主密钥PMK、以及所述第一AP的特征信息生成成对临时密钥PTK;

所述快速漫游装置获取所述STA的特征信息,所述STA的特征信息包括所述STA的MAC地址、所述STA生成的随机数、以及所述PMK的特征值;

所述快速漫游装置向所述第一AP发送所述STA的特征信息,使所述第一AP基于所述STA的特征信息和所述第一AP的特征信息生成所述PTK,所述STA和所述第一AP之间的链路认证、接入认证、以及密钥协商完成。

4.一种快速漫游方法,其特征在于,所述方法包括:

第一接入点AP基于移动站STA的特征信息和所述第一AP的特征信息生成成对临时密钥PTK,完成与所述STA之间的链路认证、接入认证、密钥协商,得到所述STA的MAC地址、成对主密钥PMK和所述PTK,其中,所述STA的特征信息是快速漫游装置发送的,所述STA的特征信息包括所述STA的MAC地址、所述STA生成并发送的随机数、以及所述PMK的特征值,所述PTK是

所述STA基于所述STA生成的随机数、所述STA的MAC地址、所述PMK以及所述第一AP的特征信息生成的，所述第一AP的特征信息是所述快速漫游装置在确定移动站STA接入第二AP之后向所述STA发送的，所述第一AP的特征信息包括所述第一AP的MAC地址和所述第一AP生成的随机数；

所述第一AP接收所述STA在确定从第二AP切换到所述第一AP之后发送的采用所述PTK加密后的数据报文，所述第一AP为所述第二AP的邻居，所述数据报文包括数据和数据摘要；

所述第一AP采用所述PTK对加密后的所述数据报文进行解密；

所述第一AP采用数据摘要算法对解密后的所述数据进行计算，得到计算出的数据摘要；

所述第一AP将计算出的所述数据摘要与解密后的所述数据摘要进行对比；

当计算出的所述数据摘要与解密后的所述数据摘要一致时，所述STA和所述第一AP之间的关联完成。

5.一种快速漫游系统，其特征在于，所述系统包括快速漫游装置、移动站STA、第一接入点AP、第二AP，所述第一AP为所述第二AP的邻居；

所述快速漫游装置，用于获取第一AP的特征信息，并在确定所述STA接入第二接入点AP之后发送给所述STA，所述第一AP的特征信息包括所述第一AP的介质访问控制MAC地址和所述第一AP生成的随机数；

所述STA，用于生成并发送随机数，基于所述STA生成的随机数、所述STA的MAC地址、成对主密钥PMK、以及所述第一AP的特征信息生成成对临时密钥PTK；

所述快速漫游装置，还用于获取所述STA的特征信息并发送给所述第一AP，所述STA的特征信息包括所述STA的MAC地址、所述STA生成的随机数、以及所述PMK的特征值；

所述第一AP，用于基于所述STA的特征信息和所述第一AP的特征信息生成所述PTK，所述STA和所述第一AP之间的链路认证、接入认证、以及密钥协商完成；

所述STA，还用于在确定切换到所述第一AP之后，向所述第一AP发送采用所述PTK加密后的数据报文，其中，所述数据报文包括数据和数据摘要；

所述第一AP，还用于采用所述PTK对加密后的所述数据报文进行解密；采用数据摘要算法对解密后的所述数据进行计算，得到计算出的数据摘要；将计算出的所述数据摘要与解密后的所述数据摘要进行对比；当计算出的所述数据摘要与解密后的所述数据摘要一致时，所述STA和所述第一AP之间的关联完成。

6.根据权利要求5所述的系统，其特征在于，所述第一AP的特征信息还包括所述第一AP的加密方式、所述第一AP的频点、所述第一AP的带宽中的至少一种。

7.一种快速漫游装置，其特征在于，所述装置包括：

AP信息获取单元，用于获取第一接入点AP的特征信息，所述第一AP的特征信息包括所述第一AP的介质访问控制MAC地址和所述第一AP生成的随机数；

AP信息发送单元，用于在确定移动站STA接入第二AP之后，向所述STA发送所述第一AP的特征信息，所述第一AP为所述第二AP的邻居，使所述STA生成并发送随机数，基于所述STA生成的随机数、所述STA的MAC地址、成对主密钥PMK、以及所述第一AP的特征信息生成成对临时密钥PTK；

STA信息获取单元，用于获取所述STA的特征信息，所述STA的特征信息包括所述STA的

MAC地址、所述STA生成的随机数、以及所述PMK的特征值；

STA信息发送单元，用于向所述第一AP发送所述STA的特征信息，使所述第一AP基于所述STA的特征信息和所述第一AP的特征信息生成所述PTK，所述STA和所述第一AP之间的链路认证、接入认证、以及密钥协商完成。

8.第一接入点AP，其特征在于，所述第一AP包括：

接入准备单元，用于基于移动站STA的特征信息和所述第一AP的特征信息生成成对临时密钥PTK，完成与所述STA之间的链路认证、接入认证、密钥协商，得到所述STA的MAC地址、成对主密钥PMK和所述PTK，其中，所述STA的特征信息是快速漫游装置发送的，所述STA的特征信息包括所述STA的MAC地址、所述STA生成并发送的随机数、以及所述PMK的特征值，所述PTK是所述STA基于所述STA生成的随机数、所述STA的MAC地址、所述PMK以及所述第一AP的特征信息生成的，所述第一AP的特征信息是所述快速漫游装置在确定移动站STA接入第二AP之后向所述STA发送的，所述第一AP的特征信息包括所述第一AP的MAC地址和所述第一AP生成的随机数；

报文接收单元，用于接收所述STA在确定从第二AP切换到所述第一AP之后发送的采用所述PTK加密后的数据报文，所述第一AP为所述第二AP的邻居，所述数据报文包括数据和数据摘要；

解密单元，用于采用所述PTK对加密后的所述数据报文进行解密；

确定单元，用于采用数据摘要算法对解密后的所述数据进行计算，得到计算出的数据摘要；将计算出的所述数据摘要与解密后的所述数据摘要进行对比；当计算出的所述数据摘要与解密后的所述数据摘要一致时，所述STA和所述第一AP之间的关联完成。

9.一种快速漫游装置，其特征在于，所述装置包括处理器、存储器以及通信接口；所述存储器用于存储软件程序，所述处理器通过运行或执行存储在所述存储器内的软件程序实现：

获取第一接入点AP的特征信息，所述第一AP的特征信息包括所述第一AP的介质访问控制MAC地址和所述第一AP生成的随机数；

在确定移动站STA接入第二AP之后，向所述STA发送所述第一AP的特征信息，所述第一AP为所述第二AP的邻居，使所述STA生成并发送随机数，基于所述STA生成的随机数、所述STA的MAC地址、成对主密钥PMK、以及所述第一AP的特征信息生成成对临时密钥PTK；

获取所述STA的特征信息，所述STA的特征信息包括所述STA的MAC地址、所述STA生成的随机数、以及所述PMK的特征值；

向所述第一AP发送所述STA的特征信息，使所述第一AP基于所述STA的特征信息和所述第一AP的特征信息生成所述PTK，所述STA和所述第一AP之间的链路认证、接入认证、以及密钥协商完成。

10.第一接入点AP，其特征在于，所述第一AP包括处理器、存储器以及通信接口；所述存储器用于存储软件程序，所述处理器通过运行或执行存储在所述存储器内的软件程序实现：

基于移动站STA的特征信息和所述第一AP的特征信息生成成对临时密钥PTK，完成与所述STA之间的链路认证、接入认证、密钥协商，得到所述STA的MAC地址、成对主密钥PMK和所述PTK，其中，所述STA的特征信息是快速漫游装置发送的，所述STA的特征信息包括所述STA

的MAC地址、所述STA生成并发送的随机数、以及所述PMK的特征值，所述PTK是所述STA基于所述STA生成的随机数、所述STA的MAC地址、所述PMK以及所述第一AP的特征信息生成的，所述第一AP的特征信息是所述快速漫游装置在确定移动站STA接入第二AP之后向所述STA发送的，所述第一AP的特征信息包括所述第一AP的MAC地址和所述第一AP生成的随机数；

接收所述STA在确定从第二AP切换到所述第一AP之后发送的采用所述PTK加密后的数据报文，所述第一AP为所述第二AP的邻居，所述数据报文包括数据和数据摘要；

采用所述PTK对加密后的所述数据报文进行解密；

采用数据摘要算法对解密后的所述数据进行计算，得到计算出的数据摘要；

将计算出的所述数据摘要与解密后的所述数据摘要进行对比；

当计算出的所述数据摘要与解密后的所述数据摘要一致时，所述STA和所述第一AP之间的关联完成。

一种快速漫游方法、装置、系统、接入点和移动站

技术领域

[0001] 本发明涉及网络技术领域，特别涉及一种快速漫游方法、装置、系统、接入点和移动站。

背景技术

[0002] 漫游(英文:roaming)指移动台(英文:station，简称:STA)从无线局域网(英文:Wireless Local Area Networks，简称:WLAN)的一个无线接入点(英文:Access Point，简称:AP)切换到另一个AP，WLAN仍可向其提供服务的功能。

[0003] 目前AP的切换需要STA与AP之间通过多次交互实现链路认证、关联(英文:Association)、接入认证、密钥协商四个过程。如果上述四个过程分别进行，则整个漫游过程耗费的时间将达到几百毫秒。电气电子工程师学会(英文:Institute of Electrical and Electronics Engineers，简称:IEEE)为无线局域网(英文:Wireless Local Area Networks，简称:WLAN)制定的标准802.11r中，采用增加信息负载的方式减少交互流程，在关联和认证的过程中进行密钥协商，将漫游耗费的时间减少到100毫秒内，实现快速漫游。

[0004] 在实现本发明的过程中，发明人发现现有技术至少存在以下问题：

[0005] 国际电信联盟(英文:International Telecommunication Union，简称:国际电信联盟)定义的标准中，以互联网协议语音通话(英文:Voice over Internet Protocol，简称:VoIP)为例，要求单向时延小于200ms，抖动小于40ms。802.11r中漫游耗费的时间通常为50ms～80ms，如果通信网络由于流量的突发性导致时延为160ms左右，抖动为30ms左右，则漫游中单向最大时延为160ms+80ms＝240ms＞200ms，抖动为30ms+80ms＝110ms＞40ms，无法满足VoIP等业务需求。

发明内容

[0006] 为了解决现有技术无法满足VoIP等业务需求的问题，本发明实施例提供了一种快速漫游方法、装置、系统、接入点和移动站。所述技术方案如下：

[0007] 第一方面，本发明实施例提供了一种快速漫游方法，所述方法包括：

[0008] 快速漫游装置获取第一接入点AP的特征信息，所述第一AP的特征信息包括所述第一AP的介质访问控制MAC地址和所述第一AP生成的随机数；

[0009] 所述快速漫游装置在确定移动站STA接入第二AP之后，向所述STA发送所述第一AP的特征信息，所述第一AP为所述第二AP的邻居；

[0010] 所述STA生成并发送随机数，基于所述STA生成的随机数、所述STA的MAC地址、成对主密钥PMK、以及所述第一AP的特征信息生成成对临时密钥PTK；

[0011] 所述快速漫游装置获取所述STA的特征信息，所述STA的特征信息包括所述STA的MAC地址、所述STA生成的随机数、以及所述PMK的特征值；

[0012] 所述快速漫游装置向所述第一AP发送所述STA的特征信息；

[0013] 所述第一AP基于所述STA的特征信息和所述第一AP的特征信息生成所述PTK，所述

STA和所述第一AP之间的链路认证、接入认证、以及密钥协商完成；

[0014] 所述STA在确定切换到所述第一AP之后，向所述第一AP发送采用所述PTK加密后的数据报文；

[0015] 所述第一AP采用所述PTK对加密后的所述数据报文进行解密；

[0016] 所述第一AP根据解密后的所述数据报文的内部信息是否一致，完成所述STA和所述第一AP之间的关联。

[0017] 在确定STA已接入第二AP的情况下，考虑到STA只有通过第二AP的链路认证、接入认证等过程才能接入第二AP，因此此时可以确定STA已经通过认证，其合法性得到了初步保证。为了避免由于进行多次报文协商实现接入认证而耗费大量的时间，本发明对STA从第二AP切换到第一AP的过程进行了简化：在STA切换到第一AP之前，实现STA和第一AP之间的信息交互，STA和第一AP均获取到对方的MAC地址、配置好PMK、以及生成PTK，完成STA和第一AP之间的链路认证、接入认证、以及密钥协商；在STA确定切换到第一AP之后，第一AP根据STA向第一AP发送的第一个数据报文的内部信息是否一致，完成STA和第一AP之间的关联。

[0018] 通过在STA接入第二AP之后，在STA和作为第二AP的邻居的第一AP之间交互建立无线链接的MAC地址、PMK、PTK等信息，完成STA接入第一AP过程中的链路认证、接入认证、密钥协商，大大减少STA漫游过程中交互信息所耗费的时间。同时当STA确定切换到第一AP时，AP根据STA向AP发送的第一个数据报文的内部信息是否一致，完成STA和第一AP之间的关联，使得STA的漫游过程中没有时间的消耗(即漫游切换的时间减至0)，切换过程快，完全可以满足VoIP等业务需求，有效保障用户体验。

[0019] 在第一方面一种可能的实现方式中，所述数据报文包括数据和数据摘要，所述第一AP根据解密后的所述数据报文的内部信息是否一致，完成所述STA和所述第一AP之间的关联，包括：

[0020] 所述第一AP采用数据摘要算法对解密后的所述数据进行计算，得到计算出的数据摘要；

[0021] 所述第一AP将计算出的所述数据摘要与解密后的所述数据摘要进行对比；

[0022] 当计算出的所述数据摘要与解密后的所述数据摘要一致时，所述STA和所述第一AP之间的关联完成。

[0023] 第一AP利用现有的数据摘要算法检测数据报文中的数据和数据摘要是否一致，并将其应用于关联过程：通过验证首个数据报文中的摘要的正确性完成STA和AP间的关联，没有独立的关联报文，在通过两次交互完成链路认证、接入认证和密钥协商的基础上，将AP和STA间漫游时间减为0，保障用户体验。

[0024] 在第一方面另一种可能的实现方式中，所述快速漫游装置设置在AP上或者接入控制器AC上，所述AC用于控制和管理所述AP。

[0025] 通过对现有设备进行改进实现快速漫游装置，实现成本低。

[0026] 在第一方面又一种可能的实现方式中，所述第一AP的特征信息还包括所述第一AP的加密方式、所述第一AP的频点、所述第一AP的带宽中的至少一种。

[0027] 可以根据接入AP所需信息，对第一AP的特征信息进行适应性调整。

[0028] 第二方面，本发明实施例提供了一种快速漫游方法，所述方法包括：

[0029] 快速漫游装置获取第一接入点AP的特征信息，所述第一AP的特征信息包括所述第

一AP的介质访问控制MAC地址和所述第一AP生成的随机数；

[0030] 所述快速漫游装置在确定移动站STA接入第二AP之后，向所述STA发送所述第一AP的特征信息，所述第一AP为所述第二AP的邻居，使所述STA生成并发送随机数，基于所述STA生成的随机数、所述STA的MAC地址、成对主密钥PMK、以及所述第一AP的特征信息生成成对临时密钥PTK；

[0031] 所述快速漫游装置获取所述STA的特征信息，所述STA的特征信息包括所述STA的MAC地址、所述STA生成的随机数、以及所述PMK的特征值；

[0032] 所述快速漫游装置向所述第一AP发送所述STA的特征信息，使所述第一AP基于所述STA的特征信息和所述第一AP的特征信息生成所述PTK，所述STA和所述第一AP之间的链路认证、接入认证、以及密钥协商完成。

[0033] 通过在STA接入第二AP之后，在STA和作为第二AP的邻居的第一AP之间交互建立无线链接的MAC地址、PMK、PTK等信息，完成STA接入第一AP过程中的链路认证、接入认证、密钥协商，大大减少STA漫游过程中交互信息所耗费的时间。

[0034] 在第二方面一种可能的实现方式中，所述快速漫游装置设置在AP上或者接入控制器AC上，所述AC用于控制和管理所述AP。

[0035] 通过对现有设备进行改进实现快速漫游装置，实现成本低。

[0036] 第三方面，本发明实施例提供了一种快速漫游方法，所述方法包括：

[0037] 第一接入点AP完成与移动站STA之间的链路认证、接入认证、密钥协商，得到所述STA的MAC地址、成对主密钥PMK和成对临时密钥PTK；

[0038] 所述第一AP接收所述STA在确定从第二AP切换到所述第一AP之后发送的采用所述PTK加密后的数据报文，所述第一AP为所述第二AP的邻居；

[0039] 所述第一AP采用所述PTK对加密后的所述数据报文进行解密；

[0040] 所述第一AP根据解密后的所述数据报文的内部信息是否一致，完成所述STA和所述第一AP之间的关联。

[0041] 通过在STA确定从第二AP切换到该AP之前，完成与STA之间的链路认证、接入认证、密钥协商，得到STA的MAC地址、PMK和PTK，在STA确定从第二AP切换到该AP之后，接收STA采用PTK加密后发送的数据报文，采用PTK对加密后的数据报文进行解密，并根据解密后的数据报文的内部信息是否一致，完成STA和第一AP之间的关联，使得STA的漫游过程中没有时间的消耗(即漫游切换的时间减至0)，切换过程快，完全可以满足VoIP等业务需求，有效保障用户体验。

[0042] 在第三方面一种可能的实现方式中，所述数据报文包括数据和数据摘要，所述第一AP根据解密后的所述数据报文的内部信息是否一致，完成所述STA和所述第一AP之间的关联，包括：

[0043] 所述第一AP采用数据摘要算法对解密后的所述数据进行计算，得到计算出的数据摘要；

[0044] 所述第一AP将计算出的所述数据摘要与解密后的所述数据摘要进行对比；

[0045] 当计算出的所述数据摘要与解密后的所述数据摘要一致时，所述STA和所述第一AP之间的关联完成。

[0046] 第一AP通过验证首个数据报文中的摘要的正确性完成STA和AP间的关联，没有独

立的关联报文，在通过两次交互完成链路认证、接入认证和密钥协商的基础上，将AP和STA间漫游时间减为0，保障用户体验。

[0047] 第四方面，本发明实施例提供了一种快速漫游方法，所述方法包括：

[0048] 移动站STA在接入第二接入点AP之后，完成与第一AP之间的链路认证、接入认证、密钥协商，得到所述第一AP的MAC地址、成对主密钥PMK和成对临时密钥PTK，所述第一AP为所述第二AP的邻居；

[0049] 所述STA在确定切换到所述第一AP之后，向所述第一AP发送采用所述PTK加密后的数据报文。

[0050] 通过在STA确定从第二AP切换到第一AP之前，完成与第一AP之间的链路认证、接入认证、密钥协商，得到第一AP的MAC地址、PMK和PTK，在STA确定从第二AP切换到该AP之后，向STA发送采用PTK加密后的数据报文，使第一AP采用PTK对加密后的数据报文进行解密，并根据解密后数据报文的内部信息是否一致，完成STA和第一AP之间的关联，使得STA的漫游过程中没有时间的消耗(即漫游切换的时间减至0)，切换过程快，完全可以满足VoIP等业务需求，有效保障用户体验。

[0051] 第五方面，本发明实施例提供了一种快速漫游系统，所述系统包括用于实现上述第一方面所述的方法的设备，例如快速漫游装置、移动站STA、第二接入点AP、第一AP。

[0052] 第六方面，本发明实施例提供了一种快速漫游装置，所述装置包括用于实现上述第二方面所述的方法的单元，例如AP信息获取单元、AP信息发送单元、STA信息获取单元、STA信息发送单元。

[0053] 第七方面，本发明实施例提供了一种接入点AP，所述AP包括用于实现上述第三方面所述的方法的单元，例如接入准备单元、报文接收单元、解密单元、确定单元。

[0054] 第八方面，本发明实施例提供了一种移动站STA，所述STA包括用于实现上述第四方面所述的方法的单元，例如接入准备单元、接入完成单元。

[0055] 第九方面，本发明实施例提供了一种快速漫游装置，所述装置包括：存储器、与存储器连接的处理器，所述存储器用于存储软件程序以及模块，当所述处理器用于运行或执行存储在所述存储器内的软件程序以及模块时，可以执行第二方面所述的方法。

[0056] 第十方面，本发明实施例还提供了一种计算机可读介质，用于存储供终端执行的程序代码，所述程序代码包括执行第二方面所述的方法的指令。

[0057] 第十一方面，本发明实施例提供了一种接入点AP，所述AP包括：存储器、与存储器连接的处理器，所述存储器用于存储软件程序以及模块，当所述处理器用于运行或执行存储在所述存储器内的软件程序以及模块时，可以执行第三方面所述的方法。

[0058] 第十二方面，本发明实施例还提供了一种计算机可读介质，用于存储供终端执行的程序代码，所述程序代码包括执行第三方面所述的方法的指令。

[0059] 第十三方面，本发明实施例提供了一种移动站STA，所述STA包括：存储器、与存储器连接的处理器，所述存储器用于存储软件程序以及模块，当所述处理器用于运行或执行存储在所述存储器内的软件程序以及模块时，可以执行第四方面所述的方法。

[0060] 第十四方面，本发明实施例还提供了一种计算机可读介质，用于存储供终端执行的程序代码，所述程序代码包括执行第四方面所述的方法的指令。

[0061] 本发明实施例提供的技术方案带来的有益效果是：

[0062] 通过在STA接入第二AP之后，在STA和作为第二AP的邻居的第一AP之间交互建立无线链接的MAC地址、PMK、PTK等信息，完成STA接入第一AP过程中的链路认证、接入认证、密钥协商，大大减少STA漫游过程中交互信息所耗费的时间。同时当STA确定切换到第一AP时，AP根据STA向AP发送的第一个数据报文的内部信息是否一致，完成STA和第一AP之间的关联，使得STA的漫游过程中没有时间的消耗(即漫游切换的时间减至0)，切换过程快，完全可以满足VoIP等业务需求，有效保障用户体验。

附图说明

[0063] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例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。

[0064] 图1是本发明实施例提供的快速漫游方法的应用场景图；

[0065] 图2是本发明实施例提供的实现AP切换的网络架构图；

[0066] 图3是本发明实施例提供的快速漫游装置的硬件结构图；

[0067] 图4是本发明实施例提供的第一AP的硬件结构图；

[0068] 图5是本发明实施例提供的STA的硬件结构图；

[0069] 图6是本发明实施例提供的一种快速漫游方法的流程图；

[0070] 图7是本发明实施例提供的STA接入第二AP的交互过程图；

[0071] 图8a和图8b是本发明实施例提供的STA发现第二AP的过程示意图；

[0072] 图9a和图9b是本发明实施例提供的STA和第二AP进行链路认证的示意图；

[0073] 图10是本发明实施例提供的STA和第二AP进行关联的示意图；

[0074] 图11a和图11b是本发明实施例提供的STA与AC、RADIUS服务器进行接入认证的示意图；

[0075] 图12a和图12b是本发明实施例提供的STA和第二AP进行密钥协商的示意图；

[0076] 图13是本发明实施例提供的PTK的结构示意图；

[0077] 图14a和图14b是本发明实施例提供的另一种快速漫游方法的交互过程图；

[0078] 图15是本发明实施例提供的AP的特征信息的结构示意图；

[0079] 图16是本发明实施例提供的承载STA生成的随机数的消息的结构示意图；

[0080] 图17是本发明实施例提供的802.11r中密钥的结构示意图；

[0081] 图18是本发明实施例提供的数据报文生成过程的示意图；

[0082] 图19是本发明实施例提供的一种快速漫游装置的结构示意图；

[0083] 图20是本发明实施例提供的一种接入点的结构示意图；

[0084] 图21是本发明实施例提供的一种移动站的结构示意图；

[0085] 图22a和图22b是本发明实施例提供的一种快速漫游系统的结构示意图。

具体实施方式

[0086] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0087] 移动办公是办公人员在任何时间(英文:Anytime)、任何地点(英文:Anywhere)处理与业务相关的任何事情(英文:Anything),也称为“3A办公”。这种全新的办公模式让办公人员摆脱时间和空间的束缚,可以在任意位置接入企业网络完成工作。

[0088] 图1为本发明实施例提供的快速漫游方法应用在移动办公场景的示意图。参见图1,第一AP 10和第二AP 20接入同一个企业网络30,企业网络30实质上是一个无线局域网(英文:Wireless Local Are Networks,简称:WLAN)。企业网络30、客户所在网络41和数据中心42分别接入运营商网络50。STA60当前位于第二AP 20的服务区域(图1中用椭圆表示各个AP的服务区域)内,STA 60接入第二AP 20(第二AP 20称为STA60的当前AP),第二AP 20接入企业网络30,通过运营商网络50可以实现对客户所在网络41、以及数据中心42的访问;之后STA 60移动到第一AP 10的服务区域内(图1用带箭头的直线表示STA的移动方向),STA 60切换到第一AP 10(第一AP 10称为STA 60的目标AP),第一AP 10也接入企业网络30,STA60可以继续访问客户所在网络41、以及数据中心42,实现移动办公。STA60从第二AP 20切换到第一AP 10的过程中,采用本发明实施例提供的方法实现快速漫游。

[0089] 图2为在图1所示的应用场景下具体实现AP切换的网络架构图。如图2所示,三个第一AP 10和第二AP 20布置在不同位置,三个第一AP 10为第二AP20的邻居。其中,两个互为邻居的AP由同一个接入控制器(英文:Access Controller,简称:AC)控制且服务集标识(英文:Service Set Identifier,简称:SSID)相同。STA可以在互为邻居的AP之间漫游,即从一个AP切换到另一个AP。图2所示第一AP的数量仅为举例,本发明实施例对此不做限制。

[0090] 在图2中,STA60当前接入第二AP 20,STA60移动后可能切换到某个第一AP 10。第二AP 20和所有第一AP 10均与接入控制器(英文:Access Controller,简称:AC)70连接(通常采用有线连接),AC 70对各个AP的配置、射频、用户接入等进行管理和控制。AC 70还与远程认证拨号用户服务(英文:Remote Authentication Dial-In User Service,简称:RADIUS)服务器80连接(通常采用有线连接),RADIUS服务器80被用作认证、授权和记账(英文:Authentication、Authorization、Accounting,简称:AAA)服务器,实现用户接入认证。

[0091] 本发明在上述网络架构增设一个快速漫游装置90,主要在STA 60切换到第一AP 10之前实现STA60和第一AP 10之间的信息交互。具体地,快速漫游装置可以设置在AC 70上,也可以设置在各个AP上,还可以独立于AC 70和AP设置。图2中以快速漫游装置90独立于AC和AP设置进行示例性说明,在实际应用中,快速漫游装置90也可以设置在AC或者各个AP上。

[0092] 在具体实现中,STA 60一般为客户端,可以是装有无线网卡的计算机,也可以是配置有的无线保真(英文:Wireless-Fidelity,简称:Wi-Fi)模块的智能手机、平板电脑等。第一AP 10、第二AP 20、AC 70均为网络设备,如路由器。

[0093] 需要说明的是,图1和图2所示的架构仅为示例,本发明并不限制于此。

[0094] 下面结合具体的硬件结构对实现本发明实施例提供的快速漫游装置、第一AP和STA进行说明。

[0095] 参见图3,快速漫游装置90可以为路由器等网络设备。快速漫游装置9可以包括一个或者一个以上处理核心的处理器91、一个或一个以上计算机可读存储介质的存储器92、以及通信接口93等部件,处理器91可以用总线94与存储器92和通信接口93相连。本领域技术人员可以理解,图3中示出的结构并不构成对装置的限定,可以包括比图示更多或更少的

部件，或者组合某些部件，或者不同的部件布置。其中：

[0096] 处理器91是快速漫游装置90的控制中心，利用各种接口和线路连接整个快速漫游装置90的各个部分，通过运行或执行存储在存储器92内的软件程序和/或模块，以及调用存储在存储器92内的数据，执行快速漫游装置90的各种功能和处理数据，从而对快速漫游装置90进行整体监控。可选地，处理器91可以包括一个或者一个以上处理单元，该处理单元可以是中央处理单元(英文:Central Processing Unit，简称:CPU)或者网络处理器(英文:Network Processor，简称:NP)等。

[0097] 存储器92可用于存储软件程序，该软件程序可以由处理器91执行。存储器92可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、AP信息获取模块、AP信息发送模块、STA信息获取模块、STA信息发送模块；存储数据区可存储根据快速漫游装置90的使用所创建的数据，例如成对主密钥、成对临时密钥等。此外，存储器92可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地，存储器92还可以包括存储器控制器，以提供处理器91对存储器92的访问。

[0098] 通信接口93可以包括有线网络接口(比如以太网接口)和无线网络接口(比如WLAN接口)中的至少一种。当快速漫游装置90增设在AC上或者独立于AC和AP时，通信接口93包括有线网络接口；当快速漫游装置90增设在AP上时，通信接口包括有线网络接口和无线网络接口。通信接口93由处理器91控制。

[0099] 可选地，快速漫游装置90还可以包括输出设备95以及输入设备96。输出设备95和输入设备96与处理器91相连。输出设备95可以是用于显示信息的显示器、播放声音的功放设备或者打印机等，输出设备95还可以包括输出控制器，用以提供输出到显示屏、功放设备或者打印机。输入设备96可以是用于用户输入信息的诸如鼠标、键盘、电子触控笔、或者触控面板之类的设备，输入设备96还可以包括输出控制器以用于接收和处理来自鼠标、键盘、电子触控笔、或者触控面板等设备的输入。

[0100] 参见图4，第一AP 10可以为路由器等网络设备。第一AP 10可以包括一个或者一个以上处理核心的处理器11、一个或一个以上计算机可读存储介质的存储器12、以及通信接口13等部件，处理器11可以用总线14与存储器12和通信接口13相连。本领域技术人员可以理解，图4中示出的结构并不构成对装置的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。其中：

[0101] 处理器11是第一AP 10的控制中心，利用各种接口和线路连接整个第一AP 10的各个部分，通过运行或执行存储在存储器12内的软件程序和/或模块，以及调用存储在存储器12内的数据，执行第一AP 10的各种功能和处理数据，从而对第一AP 10进行整体监控。可选地，处理器11可以包括一个或者一个以上处理单元，该处理单元可以是中央处理单元(英文:Central Processing Unit，简称:CPU)或者网络处理器(英文:Network Processor，简称:NP)等。

[0102] 存储器12可用于存储软件程序，该软件程序可以由处理器11执行。存储器12可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、接入准备模块、报文接收模块、解密模块、确定模块；存储数据区可存储根据第一AP 10的使用所创建的数据，例如成对主密钥、成对临时密钥等。此外，存储器12可以包括高速随机存取存储器，还可以包

括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地，存储器12还可以包括存储器控制器，以提供处理器11对存储器12的访问。

[0103] 通信接口13可以包括有线网络接口(比如以太网接口)和无线网络接口(比如WLAN接口)。通信接口13由处理器11控制。

[0104] 可选地，第一AP 10还可以包括输出设备15以及输入设备16。输出设备15和输入设备16与处理器11相连。输出设备15可以是用于显示信息的显示器、播放声音的功放设备或者打印机等，输出设备15还可以包括输出控制器，用以提供输出到显示屏、功放设备或者打印机。输入设备16可以是用于用户输入信息的诸如鼠标、键盘、电子触控笔、或者触控面板之类的设备，输入设备16还可以包括输出控制器以用于接收和处理来自鼠标、键盘、电子触控笔、或者触控面板等设备的输入。

[0105] 图5示出了实现本发明实施例提供的STA的硬件结构。STA60可以为智能手机、平板电脑、笔记本电脑等。以智能手机为例，STA60可以包括射频(Radio Frequency，简称RF)电路61、包括有一个或一个以上计算机可读存储介质的存储器62、输入单元63、显示单元64、传感器65、音频电路66、无线保真(wireless fidelity，简称WiFi)模块67、包括有一个或者一个以上处理核心的处理器68、以及电源69等部件。本领域技术人员可以理解，图5中示出的硬件结构并不构成对STA的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。其中：

[0106] 处理器68是STA60的控制中心，利用各种接口和线路连接整个STA60的各个部分，通过运行或执行存储在存储器62内的软件程序和/或模块，以及调用存储在存储器62内的数据，执行STA60的各种功能和处理数据，从而对STA 60进行整体监控。可选的，处理器68可包括一个或多个处理核心；优选的，处理器68可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器68中。

[0107] 存储器62可用于存储各种数据，例如各种配置参数、存储软件程序以及模块，处理器68通过运行存储在存储器62的软件程序以及模块，从而执行各种功能应用以及数据处理。存储器62可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、接入准备模块、接入完成模块；存储数据区可存储根据STA 60的使用所创建的数据，例如成对主密钥、成对临时密钥等。此外，存储器62可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地，存储器62还可以包括存储器控制器，以提供处理器68和输入单元63对存储器62的访问。

[0108] RF电路61可用于收发信息或通话过程中，信号的接收和发送，特别地，将基站的下行信息接收后，交由一个或者一个以上处理器68处理。通常，RF电路61包括但不限于天线、至少一个放大器、调谐器、一个或多个振荡器、用户身份模块(Subscriber Identity Module，简称SIM)卡、收发信机、耦合器、低噪声放大器(Low Noise Amplifier，简称LNA)、双工器等。此外，RF电路61还可以通过无线通信与网络和其他设备通信。所述无线通信可以使用任一通信标准或协议，包括但不限于全球移动通讯系统(Global System of Mobile communication，简称GSM)、通用分组无线服务(General Packet Radio Service，简称GPRS)、码分多址(Code Division Multiple Access，简称CDMA)、宽带码分多址(Wideband Code Division Multiple Access，简称WCDMA)、长期演进(Long Term Evolution，简称

LTE)、电子邮件、短消息服务(Short Messaging Service,简称SMS)等。

[0109] 参见图6,其示出了本发明实施例提供的一种快速漫游方法,该方法在图1所示的应用场景下,采用图2所示的网络架构实现快速漫游。如图6所示,该方法包括:

[0110] 步骤S301:STA接入第二AP。

[0111] 在本实施例中,参见图7,该步骤S301可以包括:

[0112] 步骤S301a,STA发现第二AP;

[0113] 步骤S301b,STA和第二AP进行链路认证;

[0114] 步骤S301c,在链路认证通过之后,STA和第二AP进行关联;

[0115] 步骤S301d,AC利用RADIUS服务器对STA进行接入认证;

[0116] 步骤S301e,在接入认证通过之后,STA和第二AP进行密钥协商。

[0117] 其中,AC用于管理和控制AP。

[0118] 链路认证是AP许可STA使用两者之间的无线链路。

[0119] 关联是协商无线链路的配置参数,建立满足数据传输要求的无线链路。

[0120] 接入认证是对STA的身份进行验证,得到STA和AP共同对应的成对主密钥(英文:Pairwise Master Key,简称:PMK),PMK为STA和AP之间通信使用的所有密钥的来源。例如,STA1和AP1使用PMK1生成相互通信的密钥,STA1和AP2使用PMK2生成相互通信的密钥,STA2和AP1使用PMK3生成相互通信的密钥,STA2和AP2使用PMK4生成相互通信的密钥。

[0121] 密钥协商是基于STA和AP交互的信息、以及PMK得到成对临时密钥(英文:Pairwise Temporal Key,简称:PTK),PTK用于对STA和AP之间传输的数据加密。

[0122] 在本实施例的一种实现方式中,参见图8a,该步骤S301a可以包括:

[0123] 1、STA在支持的信道上依次发送探测请求(英文:Probe Request);

[0124] 2、第二AP接收到探测请求,向STA发送探测响应(英文:Probe Response)。

[0125] 在此种实现方式中,STA主动扫描周围可接入的AP,以确定周围可接入的AP,发现AP的速度较快。

[0126] 进一步地,探测请求可以包括AP的服务集标识(英文:Service Set Identifier,简称:SSID),各个接收到探测请求的AP会将探测请求中的SSID与自身的SSID进行比较,如果两个SSDI相同则向STA发送探测响应,因此此时只有SSID与探测请求中的SSID相同的AP会向STA发送响应,便于STA发现所需AP。

[0127] 在本实施例的另一种实现方式中,参见图8b,该步骤S301a可以包括:

[0128] 1、第二AP每隔设定周期发送信标(英文:Beacon)帧;

[0129] 2、STA接收到第二AP发送的信标帧。

[0130] 在此种实现方式中,STA被动等待周围可接入的AP发送的信标帧,以确定周围可接入的AP,与主动发送探测请求相比,被动接收信标帧可以大大节省STA消耗的电能,节电的特点也使此种实现方式应用广泛。

[0131] 在具体实现中,设定周期可以为100ms,信标帧可以包括AP的SSID、支持速率等。

[0132] 在本实施例的一种实现方式中,参见图9a,该步骤S301b可以包括:

[0133] 1、STA向第二AP发送链路认证请求;

[0134] 2、第二AP向STA发送链路认证响应。

[0135] 此种实现方式称为开放系统认证(英文:Open System Authentication),只要STA

发送认证请求，AP都会允许其认证成功，目前被广泛应用。

[0136] 在本实施例的另一种实现方式中，参见图9b，该步骤S301b可以包括：

[0137] 1、STA向第二AP发送链路认证请求；

[0138] 2、第二AP生成挑战短语，并发送给STA；

[0139] 3、STA采用预先配置的密钥对挑战短语进行加密，并将加密后的挑战短语发送给第二AP；

[0140] 4、第二AP采用预先配置的密钥对发送给STA的挑战短语进行加密，并将得到的加密后的挑战短语与接收的加密后的挑战短语进行对比；

[0141] 5、当两个挑战短语相同时，第二AP向STA发送链路认证响应。

[0142] 在实际应用中，在预先配置的密钥为对称密钥(发送和接收数据的双方必使用相同的密钥对明文进行加密和解密运算)的情况下，第二AP在第4步中也可以采用预先配置的密钥对加密后的挑战短语进行解密，并将解密后的挑战短语与发送给STA的挑战短语进行对比，同样可以实现链路认证。

[0143] 此种实现方式称为共享密钥认证(英文：Shared-key Authentication)，只有STA和第二AP中预先配置的密钥相同，才能通过链路认证，安全性较高。

[0144] 可选地，参见图10，该步骤S301c可以包括：

[0145] 1、STA向第二AP发送关联请求；

[0146] 2、第二AP接收到关联请求，向STA发送关联响应。

[0147] 其中，关联请求包括STA的支持速率、信道、服务质量(英文：Quality of Service，简称：QoS)、接入认证方式、加密算法等。通常如果AP可以满足STA在关联请求中的要求，则向STA发送关联响应，并按照STA在关联请求中的要求传输数据，以确保数据能够准确安全地传输。可以理解地，在关联之后，STA和AP之间的无线链路建立完成。

[0148] 在本实施例的一种实现方式中，参见图11a，该步骤S301d可以包括：

[0149] 1、STA向AC发送接入认证请求；

[0150] 2、AC接收到认证请求，向STA发送身份请求；

[0151] 3、STA接收到身份请求，向AC发送STA的身份信息，身份信息包括用户标识；

[0152] 4、AC将STA的身份信息转发给RADIUS服务器；

[0153] 5、RADIUS服务器接收到身份信息，向AC发送包括公钥的服务器的证书；

[0154] 6、AC将包括公钥的服务器的证书转发给STA；

[0155] 7、STA接收到包括公钥的服务器的证书，对服务器的证书进行验证，验证成功后产生一个随机密码串(又称为预主密钥(英文：pre-master-secret))，并采用公钥对随机密码串进行加密，并基于随机密码串生成PMK；

[0156] 8、STA向AC发送STA的证书和加密后的随机密码串；

[0157] 9、AC将STA的证书和加密后的随机密码串转发给RADIUS服务器；

[0158] 10、RADIUS服务器验证STA的证书，验证成功后采用私钥对加密后的随机密码串进行解密，并基于随机密码串生成PMK；

[0159] 11、RADIUS服务器向AC发送接入认证响应和PMK，AC得到PMK；

[0160] 12、AC向STA转发接入认证响应。

[0161] 在本实施例的另一种实现方式中，参见图11b，该步骤S301d可以包括：

[0162] 1、STA向AC发送接入认证请求；

[0163] 2、AC接收到认证请求，向STA发送身份请求；

[0164] 3、STA接收到身份请求，向AC发送STA的身份信息，身份信息包括用户标识；

[0165] 4、AC将STA的身份信息转发给RADIUS服务器；

[0166] 5、RADIUS服务器接收到身份信息，向AC发送认证开始消息；

[0167] 6、AC将认证开始消息转发给STA；

[0168] 7、STA接收到认证开始消息，向AC发送认证消息，认证消息包括加密算法列表、安全传输层(英文:Transport Layer Security，简称:TLS)协议版本、会话标识等；

[0169] 8、AC向RADIUS服务器转发认证消息；

[0170] 9、RADIUS服务器接收到认证信息，向AC发送包括公钥的服务器的证书；

[0171] 10、AC将包括公钥的服务器的证书转发给STA；

[0172] 11、STA接收到包括公钥的服务器的证书，对服务器的证书进行验证，验证成功后产生一个随机密码串，并采用公钥对随机密码串进行加密，并基于随机密码串生成PMK；

[0173] 12、STA向AC发送STA的证书和加密后的随机密码串；

[0174] 13、AC将STA的证书和加密后的随机密码串转发给RADIUS服务器；

[0175] 14、RADIUS服务器验证STA的证书，验证成功后采用私钥对加密后的随机密码串进行解密，并基于随机密码串生成PMK；

[0176] 15、RADIUS服务器向AC发送接入认证响应和PMK，AC得到PMK；

[0177] 16、AC向STA转发接入认证响应。

[0178] 需要说明的是，AC得到PMK之后，即可将PMK告知相应的AP，因此最终AP和STA上均设置好PMK。

[0179] 进一步地，以验证服务器的证书为例，验证证书可以采用如下方式实现：

[0180] RADIUS服务器采用私钥对说明信息进行加密，得到签名，说明信息包括颁发机构、过期时间等；

[0181] RADIUS将说明信息、与私钥匹配的公钥和签名组成数字证书发送给STA；

[0182] STA接收到数字证书，采用数字证书中的公钥对数字证书中的签名进行解密，并将解密结果与数字证书中的说明信息进行对比；

[0183] 当解密结果与数字证书中的说明信息一致时，验证成功；

[0184] 当解密结果与数字证书中的说明信息不同时，验证失败。

[0185] 可以理解地，验证STA的证书可以与上述过程类似，在此不再详述。

[0186] 可选地，参见图12a，该步骤S301e可以包括：

[0187] 1、STA和第二AP分别生成随机数；

[0188] 2、第二AP将第二AP生成的随机数发送给STA；

[0189] 3、STA基于第二AP生成的随机数、第二AP的介质访问控制(英文:Media Access Control，简称:MAC)地址、STA生成的随机数、STA的MAC地址、PMK，采用哈希(英文:Hash)算法生成PTK；

[0190] 4、STA向第二AP发送STA生成的随机数；

[0191] 5、第二AP基于STA生成的随机数、STA的MAC地址、第二AP生成的随机数、第二AP的MAC地址、PMK，采用哈希算法生成PTK；

[0192] 6、第二AP向STA发送安装PTK的通知；

[0193] 7、STA接收到安装PTK的通知，安装PTK并向第二AP发送安装PTK的通知；

[0194] 8、第二AP接收到安装PTK的通知，安装PTK。

[0195] 图13为PTK的结构示意图。如图13所示，当采用计数器模式密码块消息完整码协议(英文:Counter Cipher Block Chaining Message Authentication Code Protocol，简称:CCMP)时，PTK的0～127比特(英文:bit)为密钥确认密钥(英文:Key Confirmation Key，简称:KCK)，128～255比特为密钥加密密钥(英文:Key Encryption Key，简称:KEK)，256～383比特为临时加密密钥(英文:Temporal Encryption Key，简称:TEK)；当采用临时密钥完整性协议(英文:Temporal Key Integrity Protocol，简称:TKIP)时，PTK的0～127比特为KCK，128～255比特为KEK，256～383比特为TEK，384～511比特为临时消息完整性检查密钥(英文:Temporal Message Integrity Check Key，简称:TMK)。

[0196] 优选地，参见图12b，该步骤S301e还可以包括：

[0197] 1、第二AP生成组主密钥(英文:Group Master Key，简称:GMK)，基于GMK计算出组临时密钥(英文:Group Transient Key，简称:GTK)，并采用PTK对GTK进行加密；

[0198] 2、第二AP向STA发送加密后的GTK；

[0199] 3、STA采用PTK对加密后的GTK进行解密，得到GTK并进行安装；

[0200] 4、STA向第二AP发送指示安装GTK的通知；

[0201] 5、第二AP接收到指示安装GTK的通知，安装GTK。

[0202] 其中，GMK为一组随机数，用来生成GTK；GTK用来加密组播和广播报文；PTK用来加密单播报文。

[0203] 需要说明的是，在STA和AP中，PTK、GTK等密钥的安装是指将密钥存储在设备内，以供随时使用。

[0204] 由于STA接入第二AP经历了完整的服务发现、链路认证、关联、接入认证、密钥协商五个过程，因此第二AP通常为STA在WLAN中首次接入的AP。

[0205] 在步骤S301之后，STA已接入WLAN中的一个AP(本实施例中为第二AP)，说明STA已经通过WLAN的接入认证，STA的合法性得到了初步保证。为了避免由于进行多次报文协商实现接入认证而耗费大量的时间，因此当STA由于位置的移动切换到该WLAN中的其它AP时，STA接入的过程会进行简化，主要是在STA和切换到的AP之间建立安全准确地传输数据的无线链路。具体地，本实施例在漫游过程中，利用快速漫游装置在STA切换到AP之前，实现STA和AP之间的信息交互，STA和AP均获取到对方的MAC地址、配置好PMK、以及生成PTK，完成STA和AP之间的链路认证、接入认证、以及密钥协商；另外，在STA确定切换到AP之后，AP根据STA向AP发送的第一个数据报文的内部信息是否一致，完成STA和AP之间的关联。具体见下文：

[0206] 步骤S302：第一AP将第一AP的特征信息发送给快速漫游装置。该步骤S302与步骤S301的执行没有先后顺序。

[0207] 在本实施例中，第一AP为第二AP的邻居。第一AP的特征信息包括第一AP的MAC地址和第一AP生成的随机数(英文:Nonce)。其中，随机数是第一AP为下一个接入的STA生成的。

[0208] 可选地，第一AP的特征信息还可以包括第一AP采用的加密算法、带宽、频点，具体可以根据STA接入AP所需交互的信息设置。

[0209] 在具体实现中，该步骤S302可以包括：

[0210] 快速漫游装置确定STA接入第二AP；

[0211] 快速漫游装置根据各个AP的位置确定所有第一AP，并向所有第一AP发送特征信息获取请求；

[0212] 第一AP接收到特征信息获取请求，将自己的特征信息发送给快速漫游装置。

[0213] 具体地，当快速漫游装置增设在AC上时，AC与第二AP有线连接，可以对第二AP进行控制和管理，因此AC可以通过主动询问第二AP的方式确定STA接入第二AP，也可以通过接收第二AP上报的信息确定STA接入第二AP。

[0214] 同时由于AC是控制和管理AP的，因此AC已知各个AP的位置，进而确定出作为第二AP的邻居的所有第一AP，分别向各个第一AP发送特征信息获取请求，并接收第一AP接收到特征信息获取请求之后回复的特征信息。

[0215] 当快速漫游装置增设在AP上时，第二AP上增设的快速漫游装置当然可以确定STA接入第二AP。

[0216] 同时由于第二AP与AC有线连接，AC可以对各个AP进行控制和管理，了解所有AP的位置，因此第二AP可以通过向AC发送请求的方式获取到作为第二AP的邻居的所有第一AP，加上各个AP之间也是有线连接，进而可以向各个第一AP发送特征信息获取请求，并接收第一AP接收到特征信息获取请求之后回复的特征信息。

[0217] 当快速漫游装置独立于AC和AP设置时，快速漫游装置可以与AC、各个AP有线连接，通过向AC发送请求的方式确定STA接入第二AP、以及获取到作为第二AP的邻居的所有第一AP，也可以通过向各个AP发送的方式确定STA接入第二AP、以及获取到作为第二AP的邻居的所有第一AP，进而再向各个第一AP发送特征信息获取请求，并接收第一AP接收到特征信息获取请求之后回复的特征信息。

[0218] 图6为在快速漫游装置独立于AC和AP的情况下，实现STA从第二AP快速漫游到第一AP的过程的示意图；在快速漫游装置设置在AC上的情况下，实现快速漫游的过程可以参见图14a；在快速漫游装置设置在各个AP上的情况下，实现快速漫游的过程可以参见图14b。

[0219] 步骤S303：快速漫游装置将第一AP的特征信息转发给STA。该步骤S303在步骤S301之后执行。

[0220] 具体地，当快速漫游装置增设在AC上或者独立于AC和AP设置时，AC将第一AP的特征信息发送给第二AP，由第二AP发送给STA；当快速漫游装置增设在AP上时，第二AP上的快速漫游装置直接将第一AP的特征信息发送给STA。

[0221] 在具体实现中，快速漫游装置发送的第一AP的特征信息可以包括AP标识、物理特征、安全特征、射频特征、随机数。例如，参见图15，快速漫游装置发送的一个第一AP的特征信息为AP ID1(AP标识)、MAC1(物理特征)、高级加密标准(英文：Advanced Encryption Standard，简称：AES)加密(安全特征)、频点2.418G(射频特征)、Nounce1(随机数)；快速漫游装置发送的另一个第一AP的特征信息包括AP ID2(AP标识)、MAC2(物理特征)、AES加密(安全特征)、频点2.438G(射频特征)、Nounce2(随机数)。

[0222] 步骤S304：STA生成随机数并发送给快速漫游装置。

[0223] 具体地，当快速漫游装置增设在AC上或者独立于AC和AP设置时，STA将STA生成的随机数发送给第二AP，由第二AP将STA生成的随机数转发给AC；当快速漫游装置增设在AP上时，STA直接将STA生成的随机数发送给第二AP上增设的快速漫游装置。

[0224] 需要说明的是，作为第二AP的邻居的第一AP可能有多个，此时STA会针对每一个第一AP，生成一个随机数，并发给对应的第一AP。其中，各个第一AP对应的随机数可能相同，也可能不同。实现时，由于将STA生成的随机数发送给第一AP时会携带第一AP的MAC地址，因此快速漫游装置可以根据携带的第一AP的MAC地址，区分各个随机数对应的第一AP。

[0225] 在具体实现中，针对各个第一AP发送的消息可以包括AP标识、随机数。例如，参见图16，针对一个第一AP发送的消息为AP ID1(AP标识)、Nounce1(随机数)；针对另一个第一AP发送的消息为AP ID2(AP标识)、Nounce2(随机数)。

[0226] 步骤S305:STA确定各个第一AP的PMK，并基于各个第一AP的PMK计算出PTK。

[0227] 如前所述，PMK与STA和AP共同对应，由于本实施例中只涉及到一个STA，因此直接采用AP区分各个PMK。

[0228] 可选地，STA确定第一AP的PMK，可以包括：

[0229] STA根据第一AP的MAC地址，确定是否缓存有第一AP的PMK安全关联(英文:PMK Security Association，简称:PMKSA)；

[0230] 当STA缓存有第一AP的PMKSA时，获取到缓存的第一AP的PMKID；

[0231] 当STA没有缓存第一AP的PMKSA时，通过802.1X协商步骤确定第一AP的PMK。

[0232] 在实际应用中，由于通过802.1X协商步骤获取PMK涉及多次帧交换，花费时间较长，因此STA会对得到的PMK进行缓存避免再次进行802.1X协商步骤，STA具体缓存的就是PMKSA。PMKSA包括AP的MAC地址、PMK的生命周期、以及PMK标识(英文:PMK Identifier，简称:PMKID)，PMKID由PMK、AP的MAC地址、STA的MAC地址等信息进行哈希计算得到。

[0233] 在802.11r标准中，参见图17，将密钥分成三层，三层密钥分别为PMK_R0、PMK_R1、PTK。PMK_R0为第二层密钥，各个AP的PMK_R0是相同的；PMK_R1为第一层密钥，PMK_R1基于PMK_R0和各个AP数值不同的信息(如AP的标识)计算得到，各个AP的PMK_R1各不相同；PTK为第二层密钥，PTK基于PMK_R1计算得到。这样一方面在STA漫游时，传递的是PMK_R1，由于各个AP的PMK_R1各不相同，因此即使PMK_R1被破解，也只对一个AP造成影响，安全性较高；另一方面，在已知一个AP的PMK_R1的情况下，可以得到PMK_R0，再基于PMK_R0和另一个AP的信息，即可得到该AP的PMK_R1，进而基于PMK_R1协商出PTK，避免再进行耗时的802.1x认证，缩短切换时间。

[0234] 在上述情形下，STA确定第一AP的PMK，可以包括：

[0235] STA基于PMK_R0和第一AP的标识，计算出第一AP的PMK_R1。

[0236] 例如，可以采用802.11r中定义的密钥生成函数(英文:Key Derivation Function，简称:KDF)，基于接入的服务集标识(英文:Service Set Identifier，简称:SSID)的长度、SSID、消息摘要算法标识(英文:Message Digest Algorithm Identifier，简称:MDID)、PMK_R0承载容器的长度、PMK_R0承载容器的标识等信息，计算出PMK_R0；进而采用802.11r中定义的KDF，基于PMK_R0、承载PMK_R1的容器的标识等信息，计算出PMK_R1。

[0237] 具体地，基于各个第一AP的PMK计算出PTK，可以包括：

[0238] STA基于第一AP的MAC地址、第一AP生成的随机数、STA的MAC地址、STA生成的随机数、以及第一AP的PMK，利用哈希算法计算出PTK。

[0239] 如前所述，当从已接入的AP切换到其它AP时，可以简化流程，只需要获取一些必要的参数建立安全准确传输数据的无线链路即可，在实际应用中，STA中会建立缓存列表记录

建立无线链路所需的参数，如下表一所示：

[0240] 表一

[0241]

AP 的 MAC 地址	STA 生成的随机数	AP 生成的随机数	PMKID	PMK_R1	加密密钥	摘要密钥	有效时间

[0242] 表中列有各个第一AP的MAC地址、STA生成的随机数、第一AP生成的随机数、PMKID、PMK_R1、加密密钥、摘要密钥、有效时间。其中，加密密钥为PTK中的TEK，摘要密钥为PTK中的TMK。需要说明的是，表中的项目可以根据接入AP实际所需的参数进行删减。

[0243] 步骤S306：快速漫游装置获取STA的特征信息。

[0244] 在本实施例中，STA的特征信息包括STA的MAC地址、STA生成的随机数、以及STA为第一AP生成的PMK的特征值。

[0245] 在具体实现中，STA生成的随机数由STA发送给快速漫游装置，同时承载STA生成的随机数的报文中会携带STA的MAC地址，快速漫游装置可以从报文中获取STA的MAC地址。另外，快速漫游装置也可以通过第二AP确定STA的MAC地址。STA为第一AP生成的PMK的特征值通常为第一AP的PMKID或第一AP的PMK_R1，RADIUS服务器可以采用与步骤S305中STA确定第一AP的PMK相同的方式确定STA为第一AP生成的PMK的特征值，再将PMK的特征值发送给AC。如果快速装置增设在AC上，则可以直接获取到STA为第一AP生成的PMK的特征值；如果快速漫游装置增设在AP或独立于AC和AP设置时，则可以通过与AC的交互获取STA为第一AP生成的PMK的特征值。

[0246] 步骤S307：快速漫游装置将STA的特征信息发送给第一AP。

[0247] 具体地，各个AP之间有线连接，各个AP和AC之间有线连接，快速漫游装置设置在AC或者AP上，均可以直接将STA的特征信息发送给AP。快速漫游装置独立于AC和AP设置时，快速漫游装置与AC和各个AP有线连接，可以直接将STA的特征信息发送给AP。

[0248] 步骤S308：第一AP接收到STA的特征信息，基于STA的特征信息计算出PTK。

[0249] 具体地，该步骤S308可以包括：

[0250] 第一AP基于第一AP的MAC地址、第一AP生成的随机数、STA的MAC地址、STA生成的随机数、以及STA和第一AP的PMK，利用哈希算法计算出PTK。

[0251] 在实际应用中，AP中也建有缓存列表，如下表二所示：

[0252] 表二

[0253]

STA 的 MAC 地址	STA 生成的随机数	AP 生成的随机数	PMKID	PMK_R1	加密密钥	摘要密钥	有效时间

[0254] 表中列有STA的MAC地址、STA生成的随机数、第一AP生成的随机数、PMKID、PMK_R1、加密密钥、摘要密钥、有效时间。其中，加密密钥为PTK中的TEK，摘要密钥为PTK中的TMK。需要说明的是，表中的项目可以根据接入AP实际所需的参数进行删减。

[0255] 在实际应用中，若缓存列表中各个表项均有记录，则标志STA和AP之间的链路认证、接入认证和密钥协商完成。也可以由快速漫游装置通知STA和AP链路认证、接入认证和

密钥协商完成。

[0256] 如前所述，本实施例在漫游过程中，对接入过程进行简化，利用快速漫游装置实现STA和AP之间的信息交互，得到对方的MAC地址、配置PMK、生成PTK。容易知道，通过上述步骤S302-步骤S308中快速漫游装置与STA、各个AP之间的信息交互，已完成链路认证、接入认证、以及密钥协商。

[0257] 步骤S309：在STA确定从第二AP切换到第一AP之后，STA采用PTK对数据报文进行加密，并向第一AP发送加密后的数据报文。

[0258] 在本实施例中，数据报文包括数据摘要和数据。数据摘要是通过对所有数据提取指纹信息以实现数据签名、数据完整性校验等功能。数据摘要算法被称为哈希算法、散列算法，常见的算法有循环冗余校验(英文：Cyclic Redundancy Check，简称：CRC)、消息摘要算法版本5(英文：Message-Digest Algorithm 5，简称：MD5)、安全散列算法(英文：Secure Hash Algorithm，简称：SHA)。

[0259] 具体地，在高级加密标准(英文：Advanced Encryption Standard，简称：AES)中，可以采用密码块消息完整码协议(英文：Cipher Block Chaining Message Authentication Code，简称：CBC-MAC)作为摘要。

[0260] 进一步地，参见图18，数据报文的生成过程如下：

[0261] 采用数据摘要算法对数据进行计算，得到数据摘要并加在数据的后面；

[0262] 在数据的前面加上802.11头部；

[0263] 在数据摘要的后面加上帧校验序列(英文：Frame Check Sequence，简称：FCS)。

[0264] 在实际应用中，STA可以基于信号强度或者信道的繁忙程度，确定是否进行AP的切换、以及切换到的AP。

[0265] 具体地，STA采用PTK对数据报文进行加密，可以包括：

[0266] 采用确定切换到的第一AP的PTK对数据报文进行加密。

[0267] 步骤S310：第一AP接收到加密后的数据报文，采用PTK对加密后的数据报文进行解密，得到解密后的数据和数据摘要。

[0268] 具体地，该步骤S310可以包括：

[0269] 根据STA的MAC地址选择PTK对加密后的数据报文进行解密，得到解密后的数据摘要和数据。

[0270] 步骤S311：第一AP采用数据摘要算法对解密后的数据进行计算，并将计算出的数据摘要和解密后的数据摘要进行对比。

[0271] 如前所述，本实施例在漫游过程中，将关联简化为STA和AP之间传输的数据准确即可。当计算出的数据摘要和解密后的数据摘要一致时，可以说明STA和第一AP之间的无线链路能够安全准确地传输数据，因此STA和第一AP之间完成关联，STA接入第一AP。

[0272] 本发明实施例通过在STA接入第二AP之后，在STA和作为第二AP的邻居的第一AP之间交互建立无线链接的MAC地址、PMK、PTK等信息，完成STA接入第一AP过程中的链路认证、接入认证、密钥协商，大大减少STA漫游过程中交互信息所耗费的时间。同时当STA确定切换到第一AP时，AP根据STA向AP发送的第一个数据报文的内部信息是否一致，完成STA和第一AP之间的关联，使得STA的漫游过程中没有时间的消耗(即漫游切换的时间减至0)，切换过程快，完全可以满足VoIP等业务需求，有效保障用户体验。

[0273] 上述步骤的执行可以通过基站根据前述软件程序执行。例如，步骤S302由快速漫游装置根据图3中的AP信息获取模块执行，步骤S303由快速漫游装置根据图3中的AP信息发送模块执行，步骤S304和步骤S305由STA根据图6中的接入准备模块执行，步骤S306由快速漫游装置根据图3中的STA信息获取模块执行，步骤S307由快速漫游装置根据图3中的STA信息发送模块执行，步骤S308由第一AP根据图4中的接入准备模块执行，步骤S309由STA根据图5中的接入完成模块执行，步骤S310由第一AP根据图4中的报文接收模块和解密模块执行，步骤S311由第一AP根据图4中的确定模块执行。

[0274] 参见图19，本发明实施例提供了一种快速漫游装置，该装置可以通过软件、硬件或者两者的结合实现成为基站的全部或者一部分。该装置包括：AP信息获取单元602、AP信息发送单元603、STA信息获取单元604和STA信息发送单元605。

[0275] 其中，AP信息获取单元602用于获取第一AP的特征信息，第一AP的特征信息包括第一AP的MAC地址和第一AP生成的随机数。AP信息发送单元603用于在确定STA接入第二AP之后，向STA发送第一AP的特征信息，第一AP为第二AP的邻居，使STA生成并发送随机数，基于STA生成的随机数、STA的MAC地址、PMK、以及第一AP的特征信息生成PTK。STA信息获取单元604用于获取STA的特征信息，STA的特征信息包括STA的MAC地址、STA生成的随机数、以及PMK的特征值。STA信息发送单元605用于向第一AP发送STA的特征信息，使第一AP基于STA的特征信息和第一AP的特征信息生成PTK，STA和第一AP之间的链路认证、接入认证、以及密钥协商完成。

[0276] 可选地，该装置可以设置在AP上或者接入控制器AC上，AC用于控制和管理AP。

[0277] 本发明实施例通过在STA接入第二AP之后，在STA和作为第二AP的邻居的第一AP之间交互建立无线链接的MAC地址、PMK、PTK等信息，完成STA接入第一AP过程中的链路认证、接入认证、密钥协商，大大减少STA漫游过程中交互信息所耗费的时间。

[0278] 参见图20，本发明实施例提供了一种AP，该AP可以通过软件、硬件或者两者的结合实现成为基站的全部或者一部分。该AP包括：接入准备单元701、报文接收单元702、解密单元703和确定单元704。

[0279] 其中，接入准备单元701用于完成与STA之间的链路认证、接入认证、密钥协商，得到STA的MAC地址、PMK和PTK。报文接收单元702用于接收STA在确定从第二AP切换到该AP之后发送的采用PTK加密后的数据报文，该AP为第二AP的邻居。解密单元703用于采用PTK对加密后的数据报文进行解密。确定单元704用于根据解密后的所述数据报文的内部信息是否一致，完成所述STA和所述AP之间的关联。

[0280] 可选地，确定单元704可以用于采用数据摘要算法对解密后的数据进行计算，得到计算出的数据摘要；将计算出的数据摘要与解密后的数据摘要进行对比；当计算出的数据摘要与解密后的数据摘要一致时，STA和第一AP之间的关联完成。

[0281] 本发明实施例通过在STA确定从第二AP切换到该AP之前，完成与STA之间的链路认证、接入认证、密钥协商，得到STA的MAC地址、PMK和PTK，在STA确定从第二AP切换到该AP之后，接收STA采用PTK加密后发送的数据报文，采用PTK对加密后的数据报文进行解密，并根据解密后的数据报文的内部信息是否一致，完成STA和第一AP之间的关联，使得STA的漫游过程中没有时间的消耗(即漫游切换的时间减至0)，切换过程快，完全可以满足VoIP等业务需求，有效保障用户体验。

[0282] 参见图21，本发明实施例提供了一种STA，该STA可以通过软件、硬件或者两者的结合实现成为基站的全部或者一部分。该STA包括：接入准备单元801和接入完成单元803。

[0283] 其中，接入准备单元801用于在接入第二AP之后，完成与第一AP之间的链路认证、接入认证、密钥协商，得到第一AP的MAC地址、PMK和PTK，第一AP为第二AP的邻居。接入完成单元803用于在确定切换到第一AP之后，向第一AP发送采用所述PTK加密后的数据报文。

[0284] 本发明实施例通过在STA确定从第二AP切换到第一AP之前，完成与第一AP之间的链路认证、接入认证、密钥协商，得到第一AP的MAC地址、PMK和PTK，在STA确定从第二AP切换到该AP之后，向STA发送采用PTK加密后的数据报文，使第一AP采用PTK对加密后的数据报文进行解密，并根据解密后数据报文的内部信息是否一致，完成STA和第一AP之间的关联，使得STA的漫游过程中没有时间的消耗(即漫游切换的时间减至0)，切换过程快，完全可以满足VoIP等业务需求，有效保障用户体验。

[0285] 参见图22a和图22b，其示出了本发明实施例提供的快速漫游系统，该系统包括快速漫游装置901、STA 902、至少一个第一AP 904、第二AP 903，第一AP 904为第二AP 903的邻居。

[0286] 具体地，快速漫游装置901可以与图19所示实施例提供的快速漫游装置相同，STA902可以与图21所示实施例提供的STA相同，第一AP 904可以与图20所示实施例提供的AP相同，在此不再详述。

[0287] 可选地，当快速漫游装置901设置在AC上或独立于AC和AP时，快速漫游装置901与第一AP 904和第二AP 903有线连接，第一AP 904与第二AP 903有线连接，STA902与第一AP 904无线连接；当快速漫游装置901设置在AP上时，第一AP 904与第二AP 903有线连接，STA902与第一AP 904无线连接。

[0288] 本发明实施例通过在STA接入第二AP之后，在STA和作为第二AP的邻居的第一AP之间交互建立无线链接的MAC地址、PMK、PTK等信息，完成STA接入第一AP过程中的链路认证、接入认证、密钥协商，大大减少STA漫游过程中交互信息所耗费的时间。同时当STA确定切换到第一AP时，AP根据STA向AP发送的第一个数据报文的内部信息是否一致，完成STA和第一AP之间的关联，使得STA的漫游过程中没有时间的消耗(即漫游切换的时间减至0)，切换过程快，完全可以满足VoIP等业务需求，有效保障用户体验。

[0289] 需要说明的是：上述实施例提供的快速漫游装置、快速漫游系统在快速漫游时，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，即将装置和系统的内部信息结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的快速漫游装置、快速漫游系统与快速漫游方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0290] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0291] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0292] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

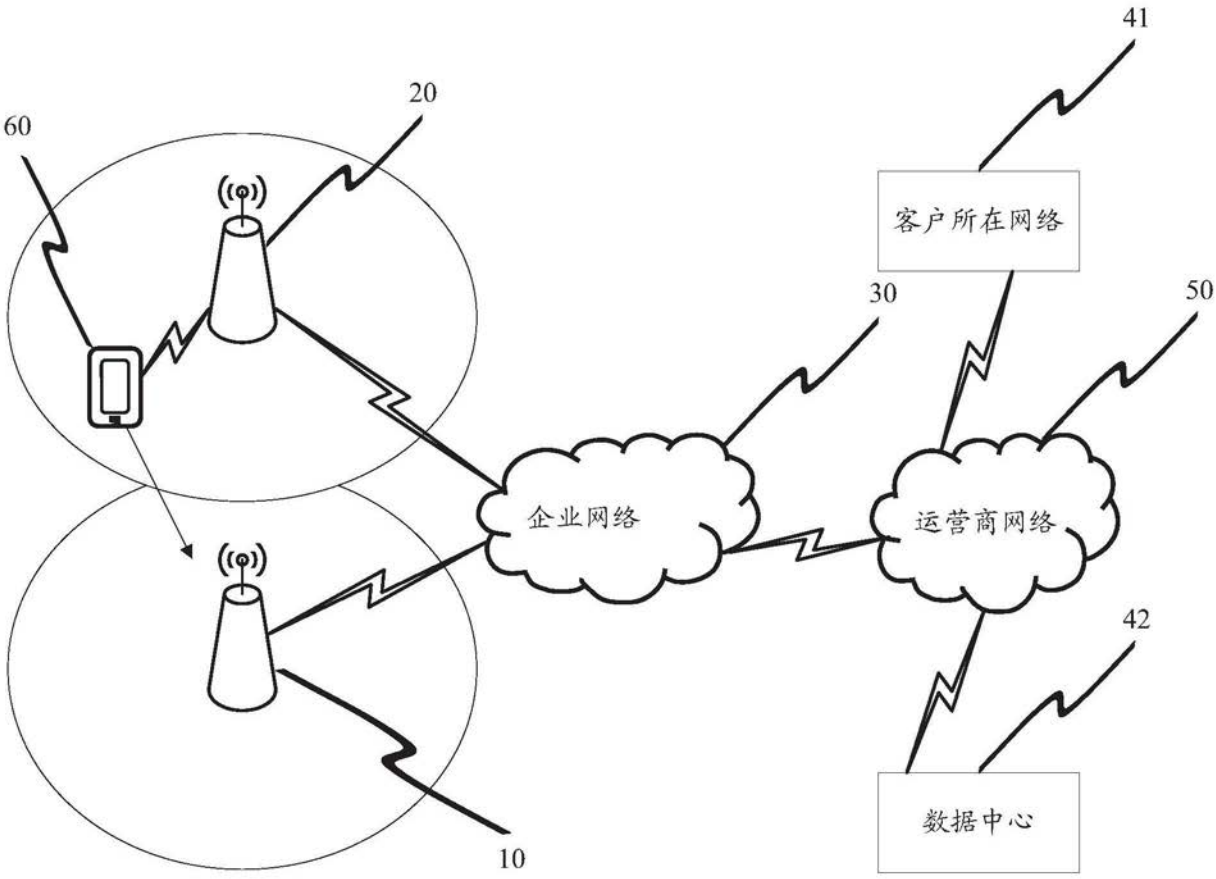


图1

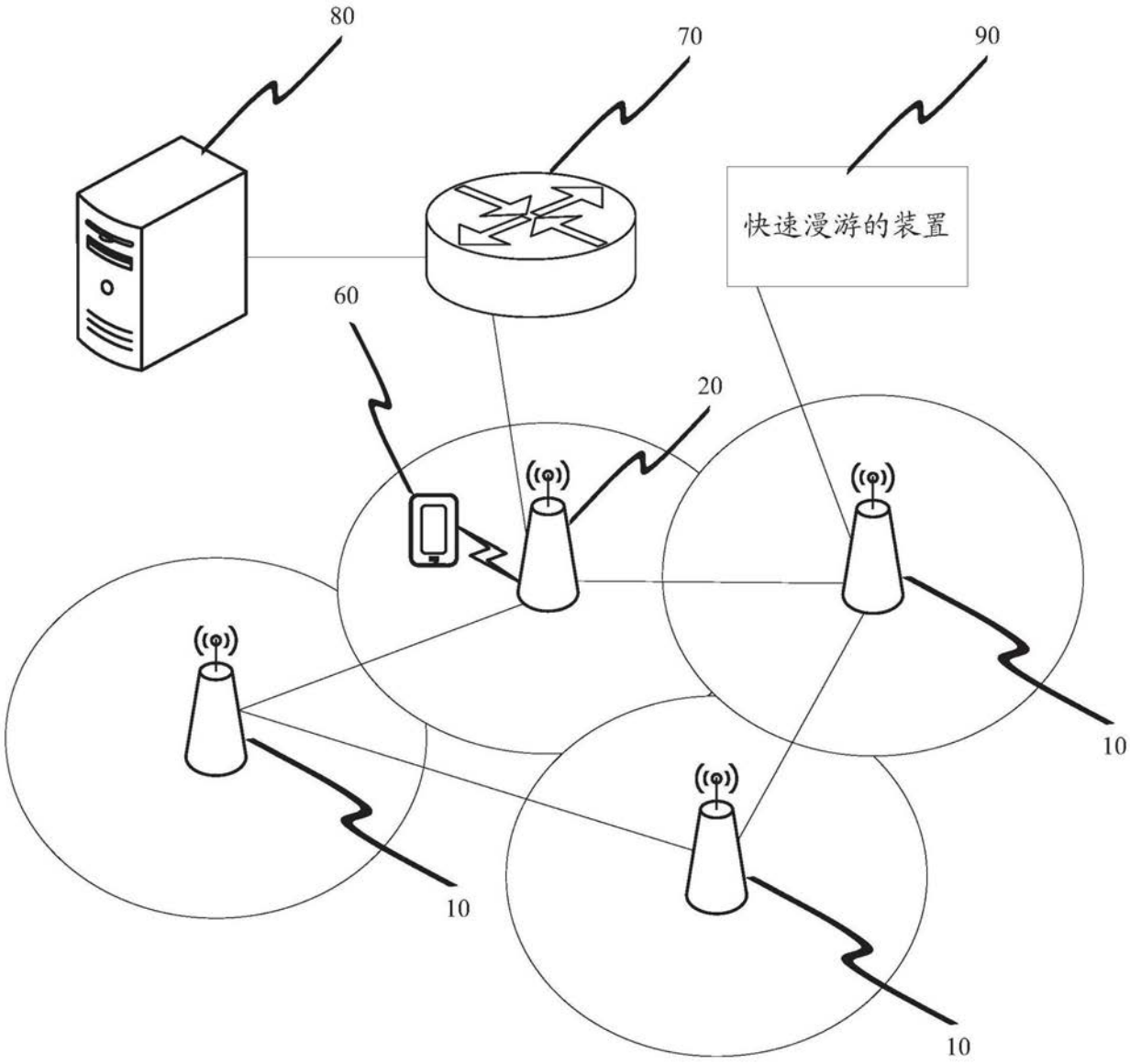


图2

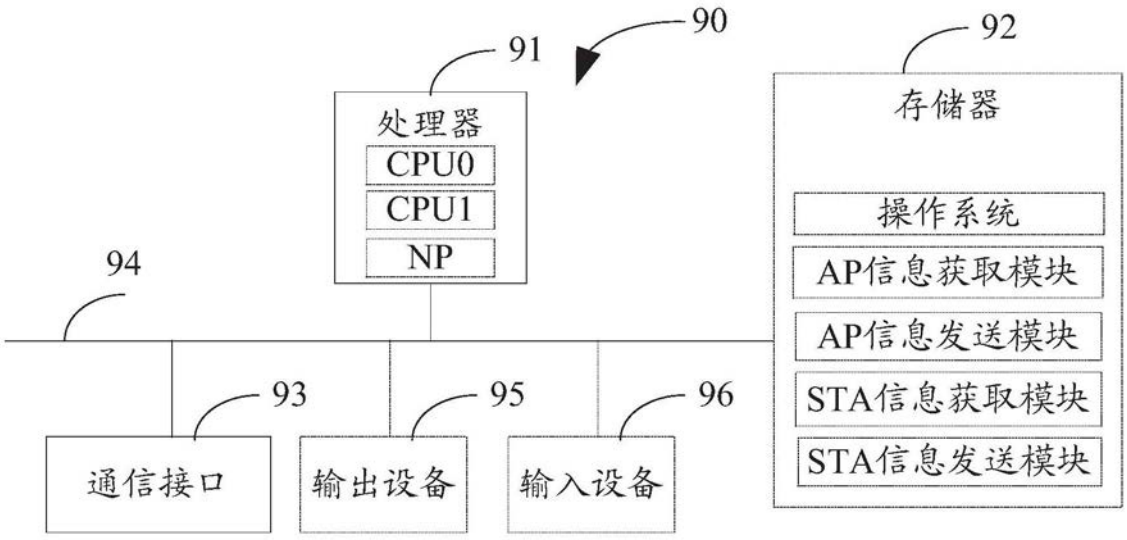

90
91
处理器
CPU0
CPU1
NP
92
存储器
操作系统
AP信息获取模块
AP信息发送模块
STA信息获取模块
STA信息发送模块
94
93
95
96
通信接口
输出设备
输入设备

图3

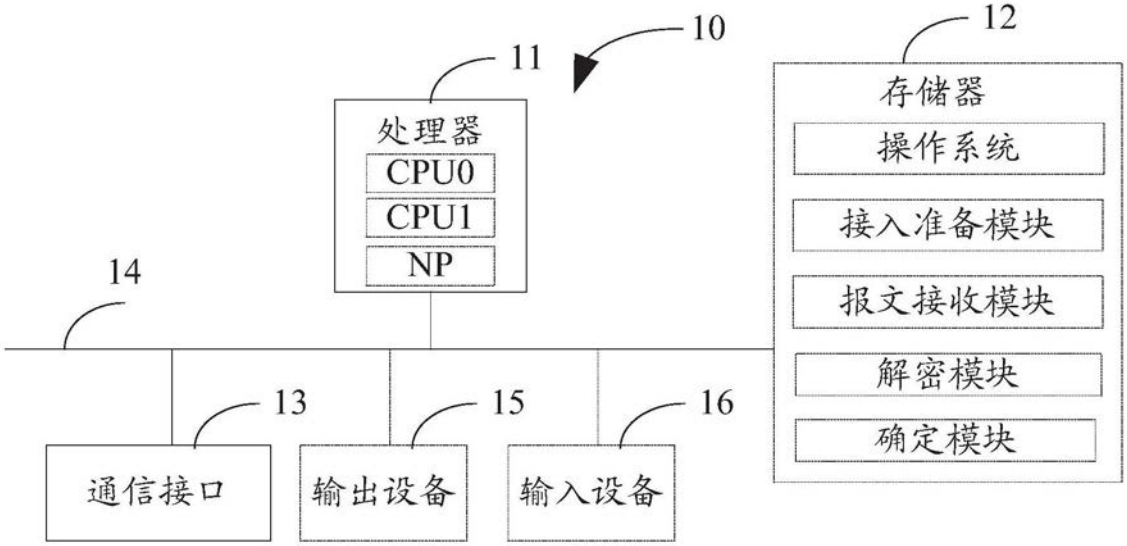

10
11
处理器
CPU0
CPU1
NP
12
存储器
操作系统
接入准备模块
报文接收模块
解密模块
确定模块
14
13
15
16
通信接口
输出设备
输入设备

图4

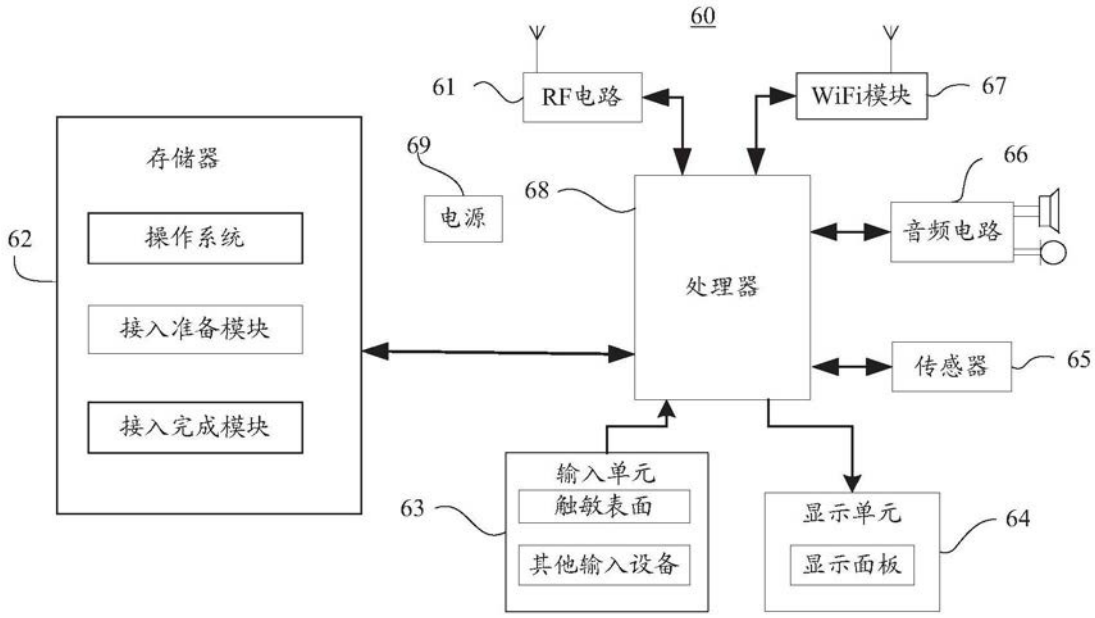

60
61
RF电路
WiFi模块
67
存储器
69
电源
68
66
62
操作系统
处理器
音频电路
接入准备模块
传感器
65
接入完成模块
输入单元
63
触敏表面
显示单元
64
其他输入设备
显示面板

图5

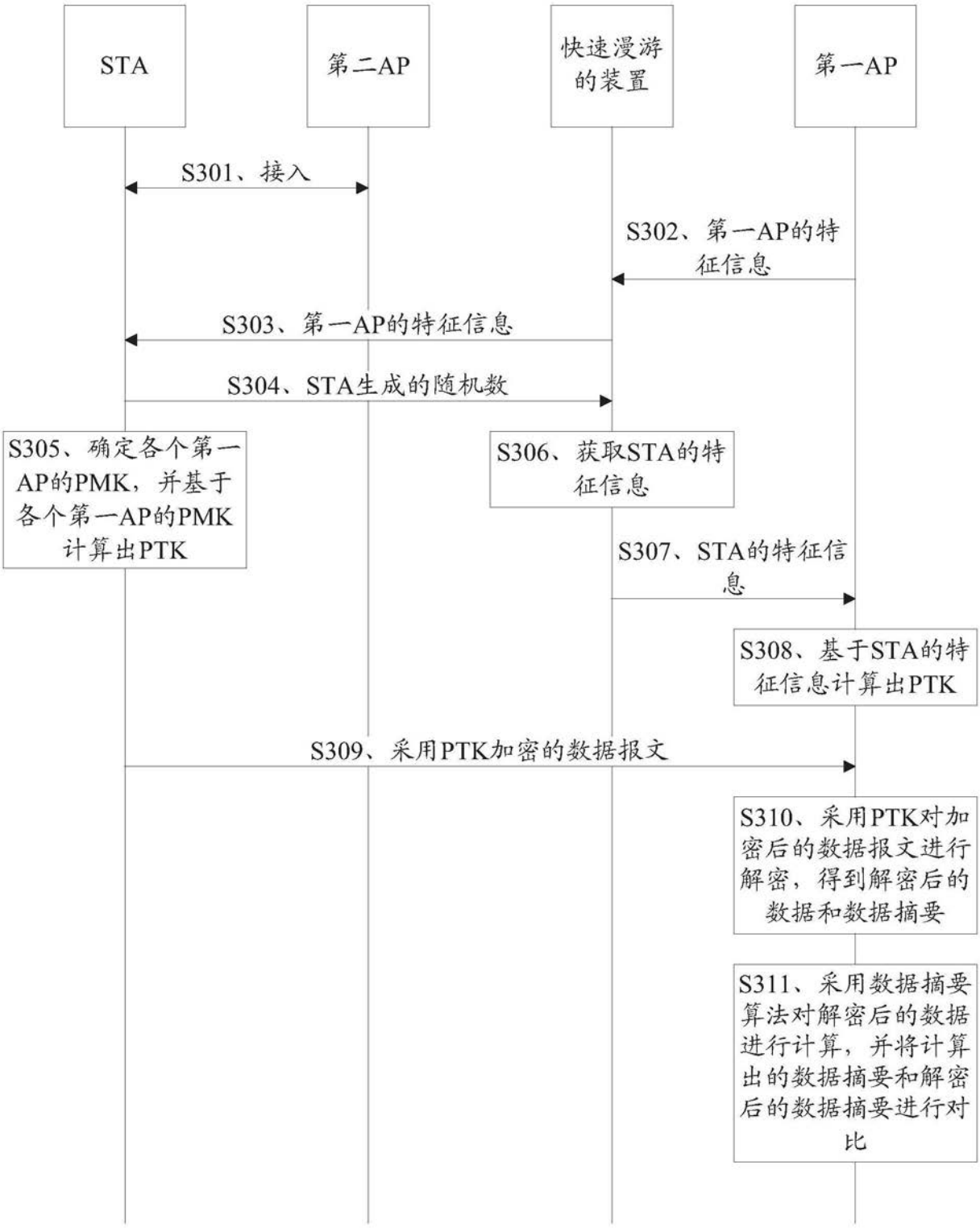

STA
第二AP
快速漫游的装置
第一AP
S301、接入
S302、第一AP的特征信息
S303、第一AP的特征信息
S304、STA生成的随机数
S305、确定各个第一AP的PMK，并基于各个第一AP的PMK计算出PTK
S306、获取STA的特征信息
S307、STA的特征信息
S308、基于STA的特征信息计算出PTK
S309、采用PTK加密的数据报文
S310、采用PTK对加密后的数据报文进行解密，得到解密后的数据和数据摘要
S311、采用数据摘要算法对解密后的数据进行计算，并将计算出的数据摘要和解密后的数据摘要进行对比

图6

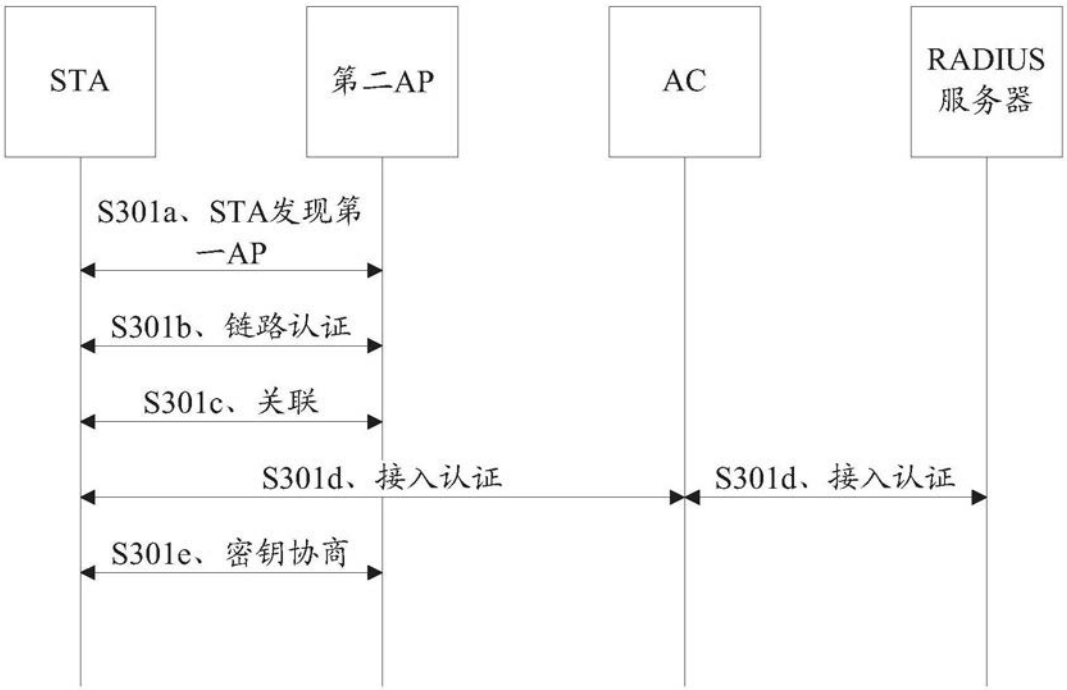

STA
第二AP
AC
RADIUS
服务器
S301a、STA发现第一AP
S301b、链路认证
S301c、关联
S301d、接入认证
S301d、接入认证
S301e、密钥协商

图7

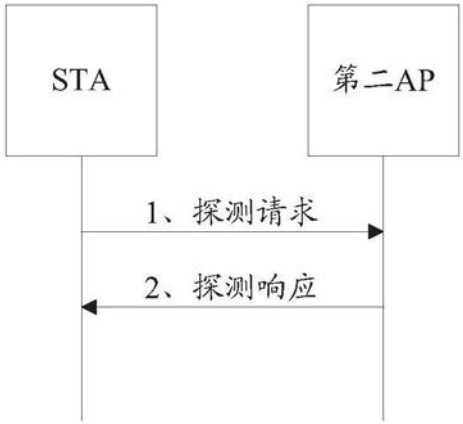

STA
第二AP
1、探测请求
2、探测响应

图8a

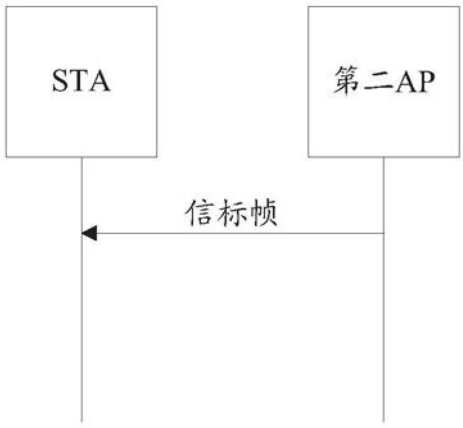


图8b

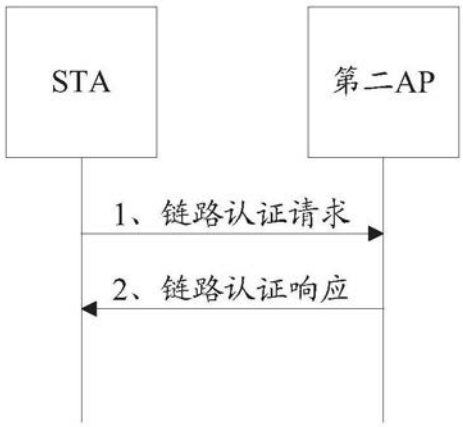


图9a

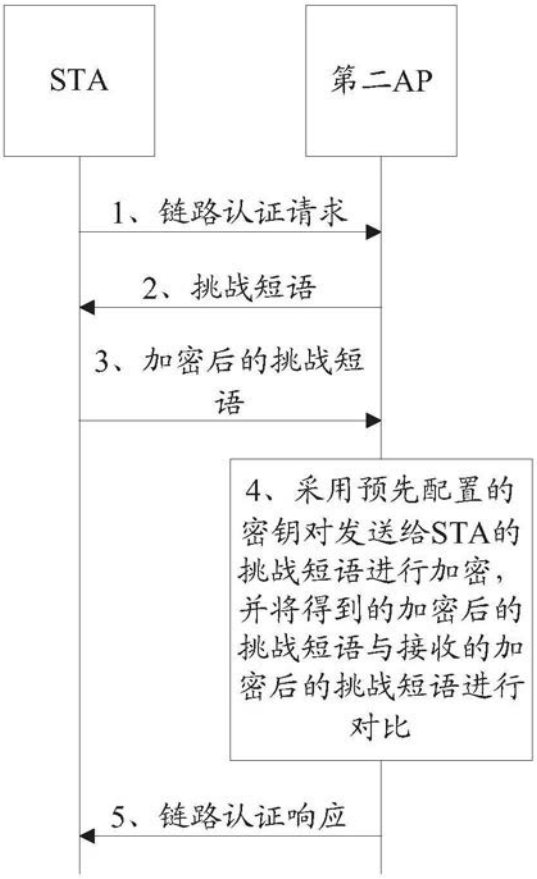

STA
第二AP
1、链路认证请求
2、挑战短语
3、加密后的挑战短语
4、采用预先配置的密钥对发送给STA的挑战短语进行加密，并将得到的加密后的挑战短语与接收的加密后的挑战短语进行对比
5、链路认证响应

图9b

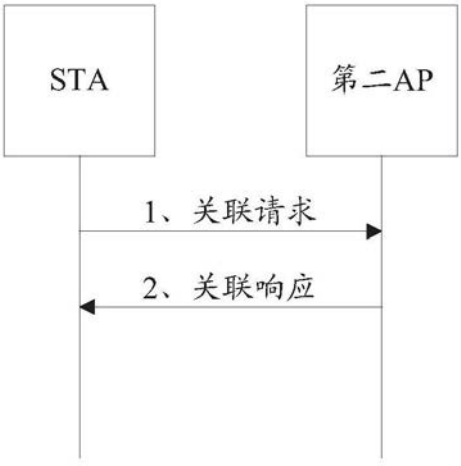

STA
第二AP
1、关联请求
2、关联响应

图10


STA
AC
RADIUS
服务器
1、接入认证请求
2、身份请求
3、STA的身份信息
4、STA的身份信息
5、包括公钥的服务器的证书
6、包括公钥的服务器的证书
7、对服务器的证书进行验证，验证成功后产生一个随机密码串，并采用公钥对随机密码串进行加密，并基于随机密码串生成PMK
8、STA的证书和加密后的随机密码串
9、STA的证书和加密后的随机密码串
10、验证STA的证书，验证成功后采用私钥对加密后的随机密码串进行解密，并基于随机密码串生成PMK
11、接入认证响应和PMK
12、接入认证响应

图11a

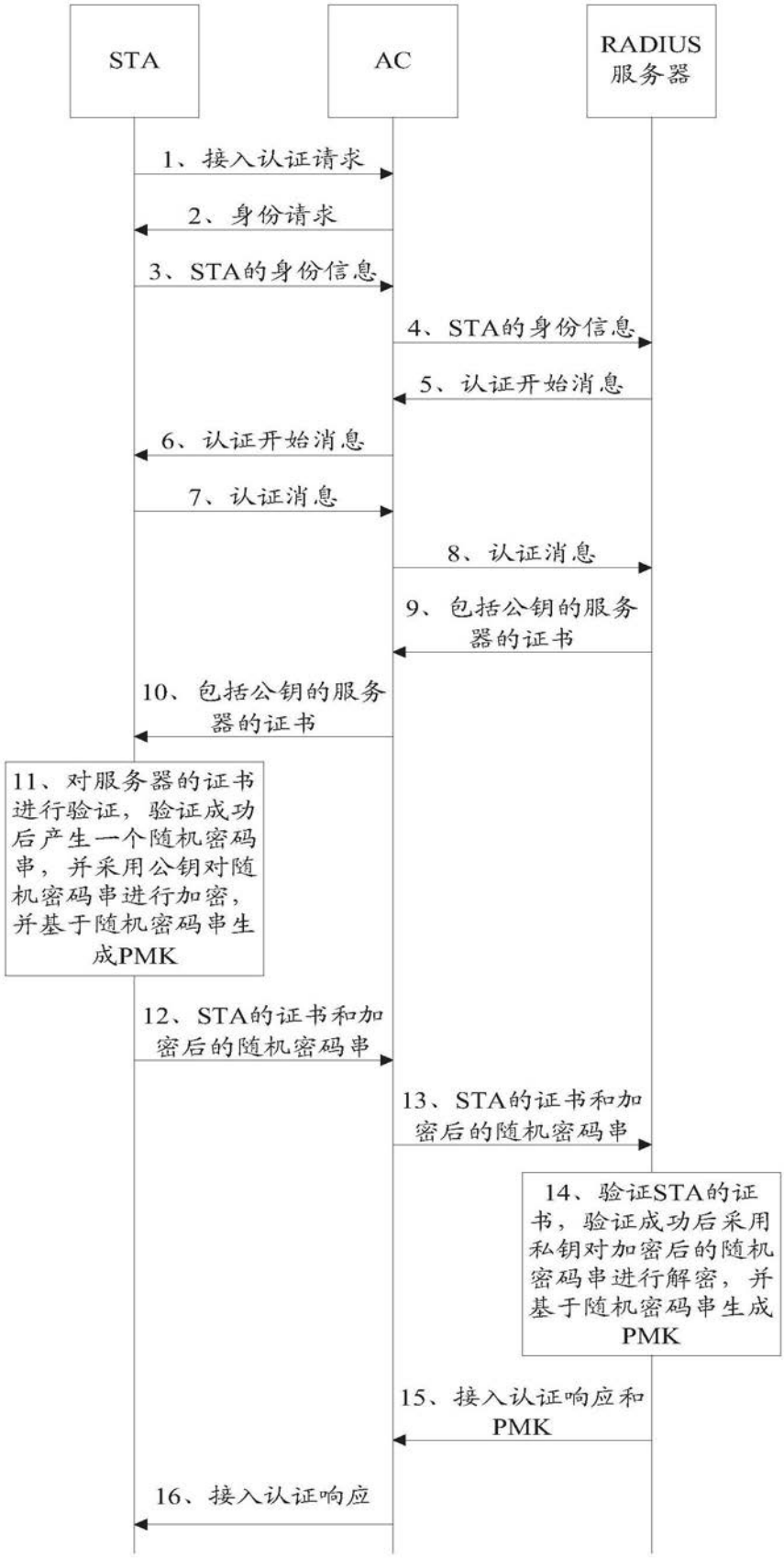

STA
AC
RADIUS
服务器
1、接入认证请求
2、身份请求
3、STA的身份信息
4、STA的身份信息
5、认证开始消息
6、认证开始消息
7、认证消息
8、认证消息
9、包括公钥的服务器的证书
10、包括公钥的服务器的证书
11、对服务器的证书进行验证，验证成功后产生一个随机密码串，并采用公钥对随机密码串进行加密，并基于随机密码串生成PMK
12、STA的证书和加密后的随机密码串
13、STA的证书和加密后的随机密码串
14、验证STA的证书，验证成功后采用私钥对加密后的随机密码串进行解密，并基于随机密码串生成PMK
15、接入认证响应和PMK
16、接入认证响应

图11b

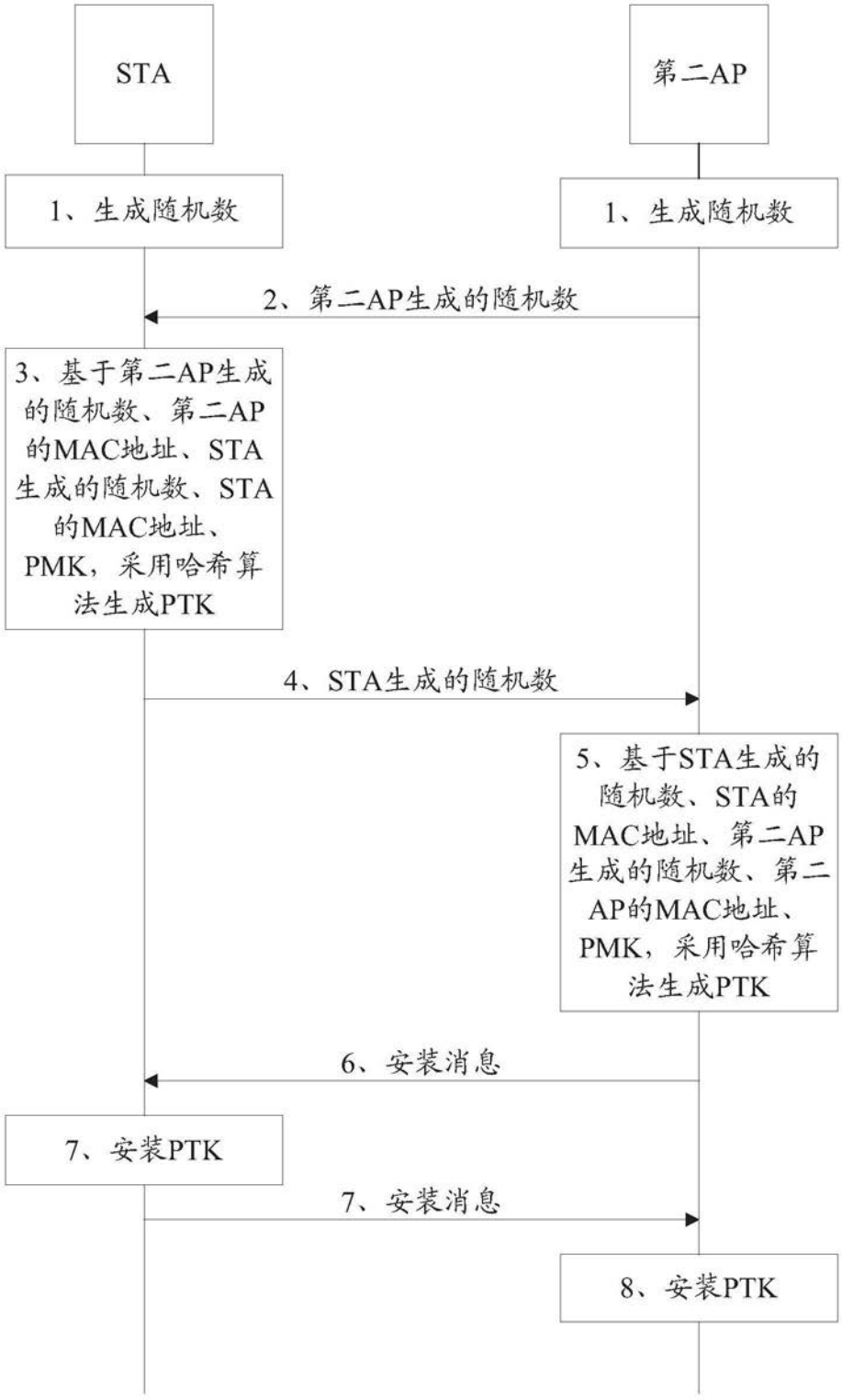

STA
第二AP
1、生成随机数
1、生成随机数
2、第二AP生成的随机数
3、基于第二AP生成的随机数、第二AP的MAC地址、STA生成的随机数、STA的MAC地址、PMK，采用哈希算法生成PTK
4、STA生成的随机数
5、基于STA生成的随机数、STA的MAC地址、第二AP生成的随机数、第二AP的MAC地址、PMK，采用哈希算法生成PTK
6、安装消息
7、安装PTK
7、安装消息
8、安装PTK

图12a

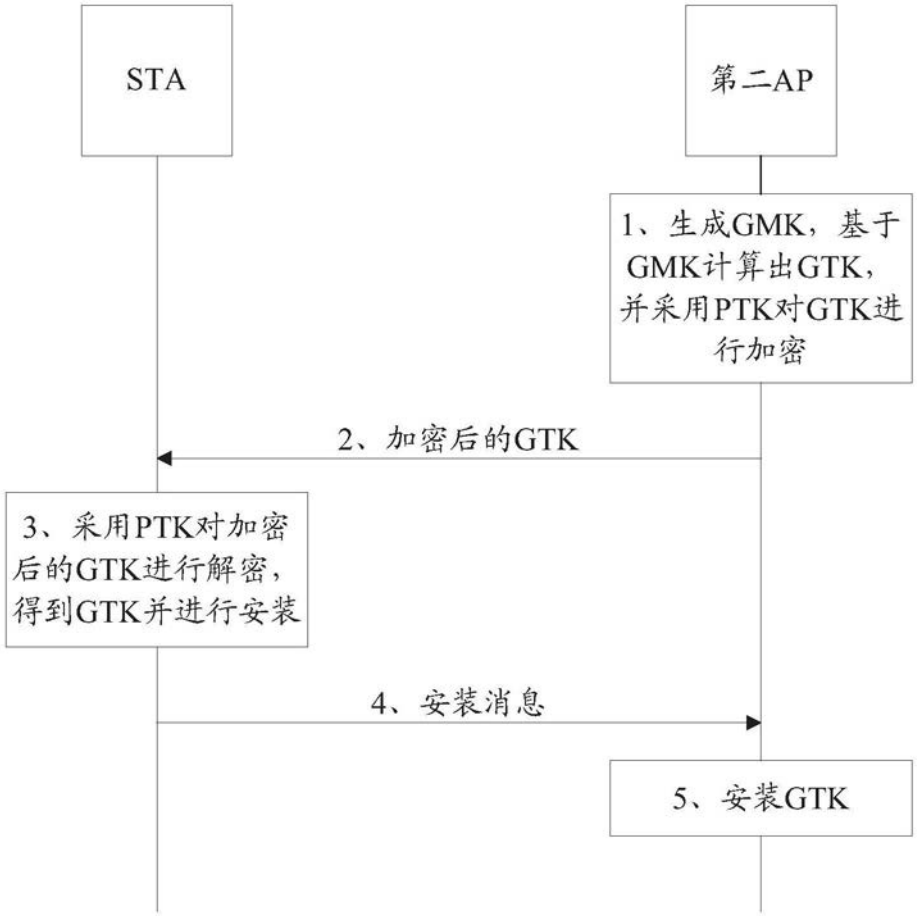

STA
第二AP
1、生成GMK，基于GMK计算出GTK，并采用PTK对GTK进行加密
2、加密后的GTK
3、采用PTK对加密后的GTK进行解密，得到GTK并进行安装
4、安装消息
5、安装GTK

图12b


PTK
KCK
0~127比特
KEK
128~255比特
TEK
256~383比特
TMK
384~511比特

图13

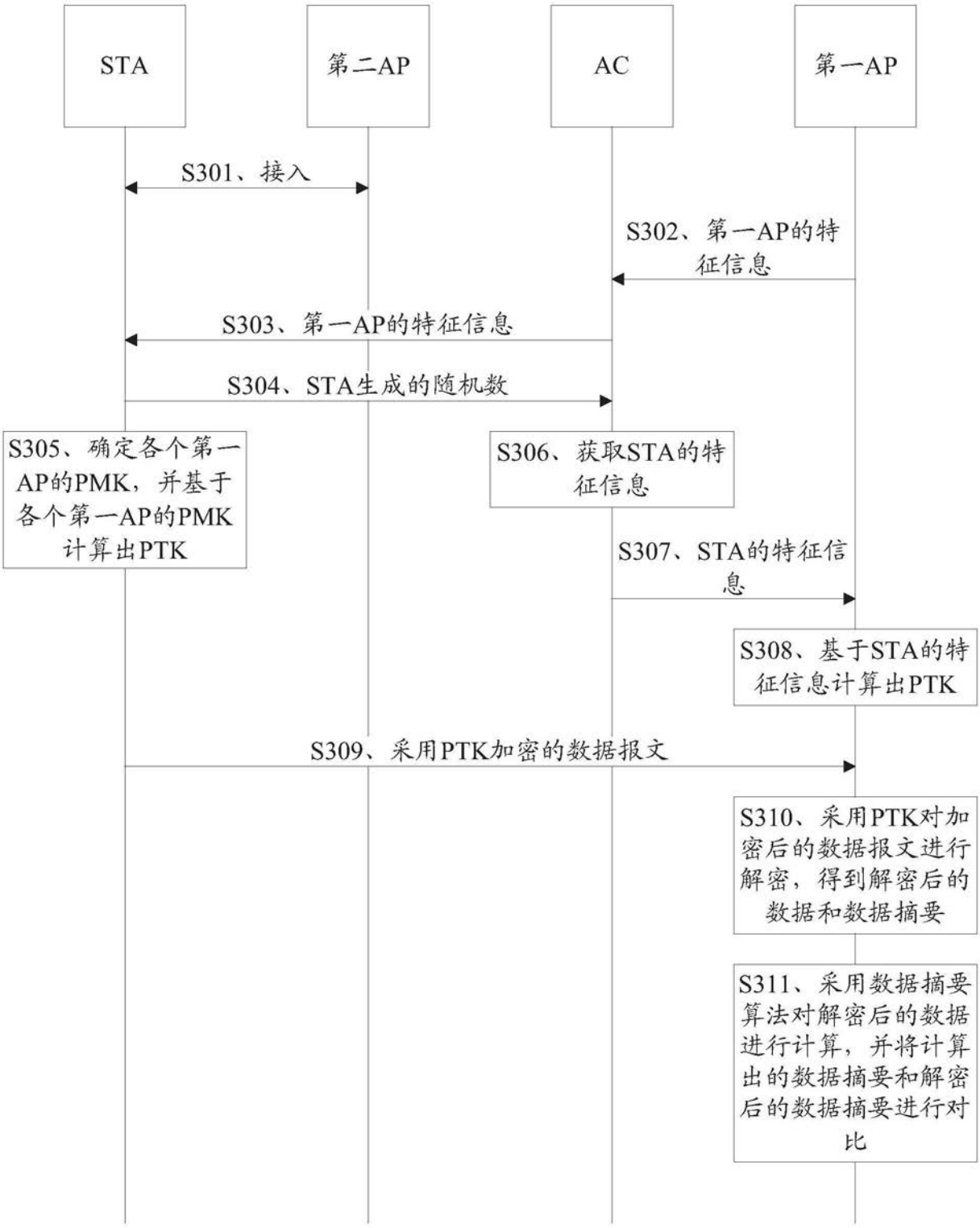

STA
第二AP
AC
第一AP
S301、接入
S302、第一AP的特征信息
S303、第一AP的特征信息
S304、STA生成的随机数
S305、确定各个第一AP的PMK，并基于各个第一AP的PMK计算出PTK
S306、获取STA的特征信息
S307、STA的特征信息
S308、基于STA的特征信息计算出PTK
S309、采用PTK加密的数据报文
S310、采用PTK对加密后的数据报文进行解密，得到解密后的数据和数据摘要
S311、采用数据摘要算法对解密后的数据进行计算，并将计算出的数据摘要和解密后的数据摘要进行对比

图14a

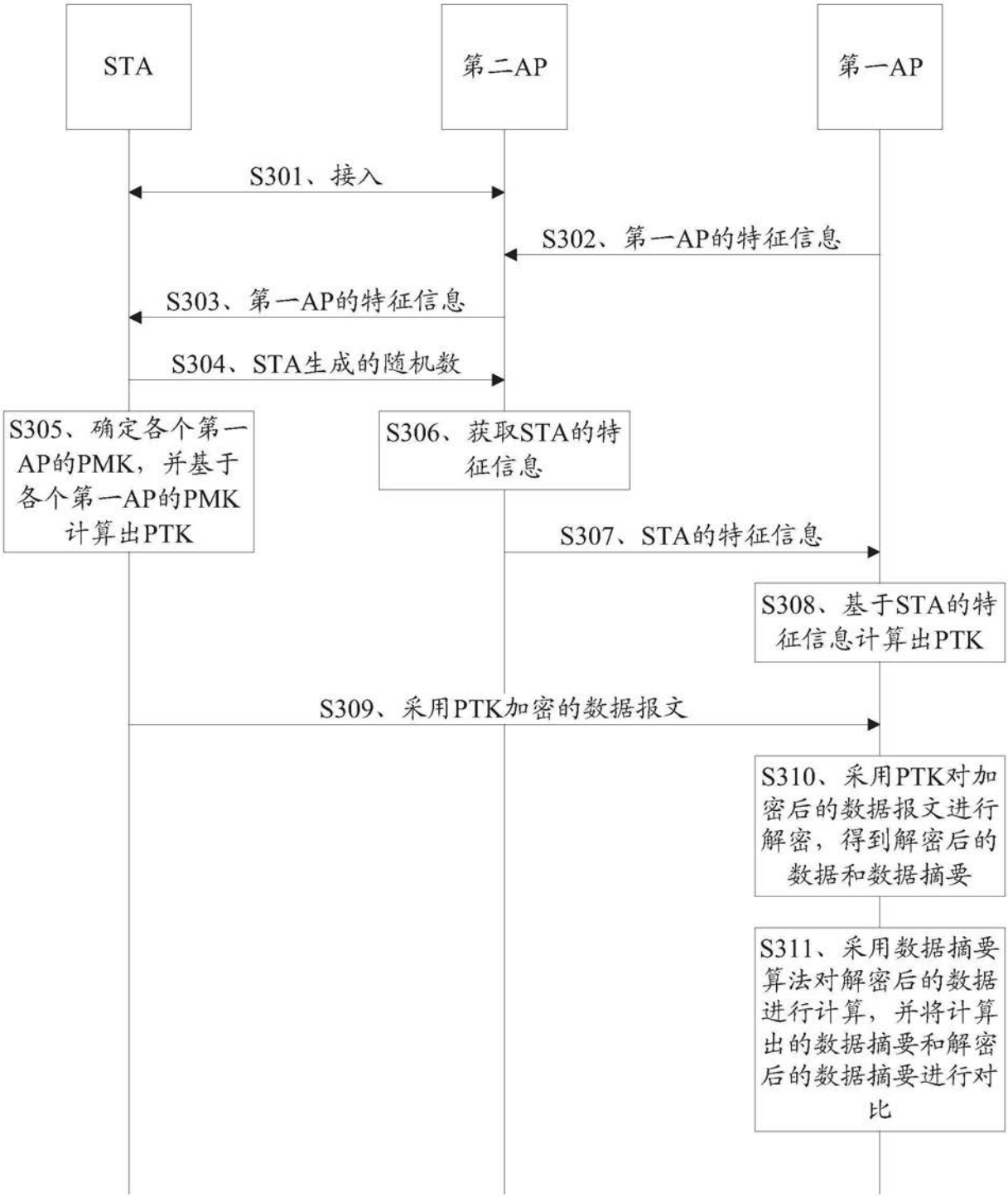

STA
第二AP
第一AP
S301、接入
S302、第一AP的特征信息
S303、第一AP的特征信息
S304、STA生成的随机数
S305、确定各个第一AP的PMK，并基于各个第一AP的PMK计算出PTK
S306、获取STA的特征信息
S307、STA的特征信息
S308、基于STA的特征信息计算出PTK
S309、采用PTK加密的数据报文
S310、采用PTK对加密后的数据报文进行解密，得到解密后的数据和数据摘要
S311、采用数据摘要算法对解密后的数据进行计算，并将计算出的数据摘要和解密后的数据摘要进行对比

图14b


AP ID1
MAC1
AES加密
频点2.418G
随机数1
AP ID2
MAC2
AES加密
频点2.438G
随机数2

图15


AP ID1
随机数1
AP ID2
随机数2

图16

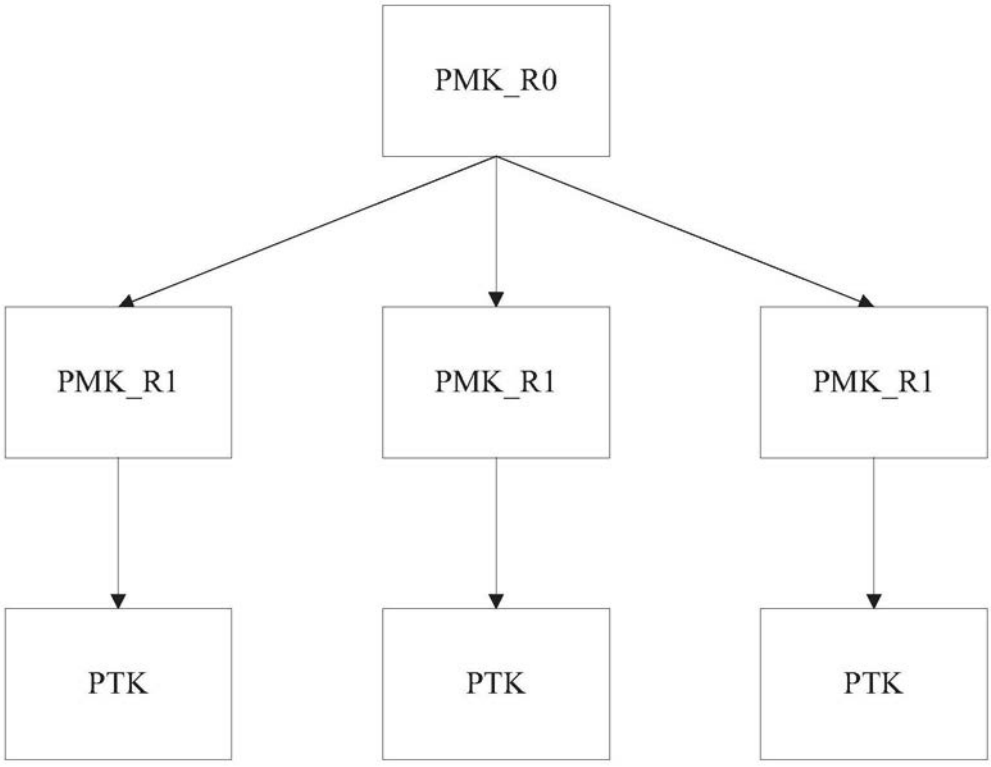

PMK_R0
PMK_R1
PMK_R1
PMK_R1
PTK
PTK
PTK

图17

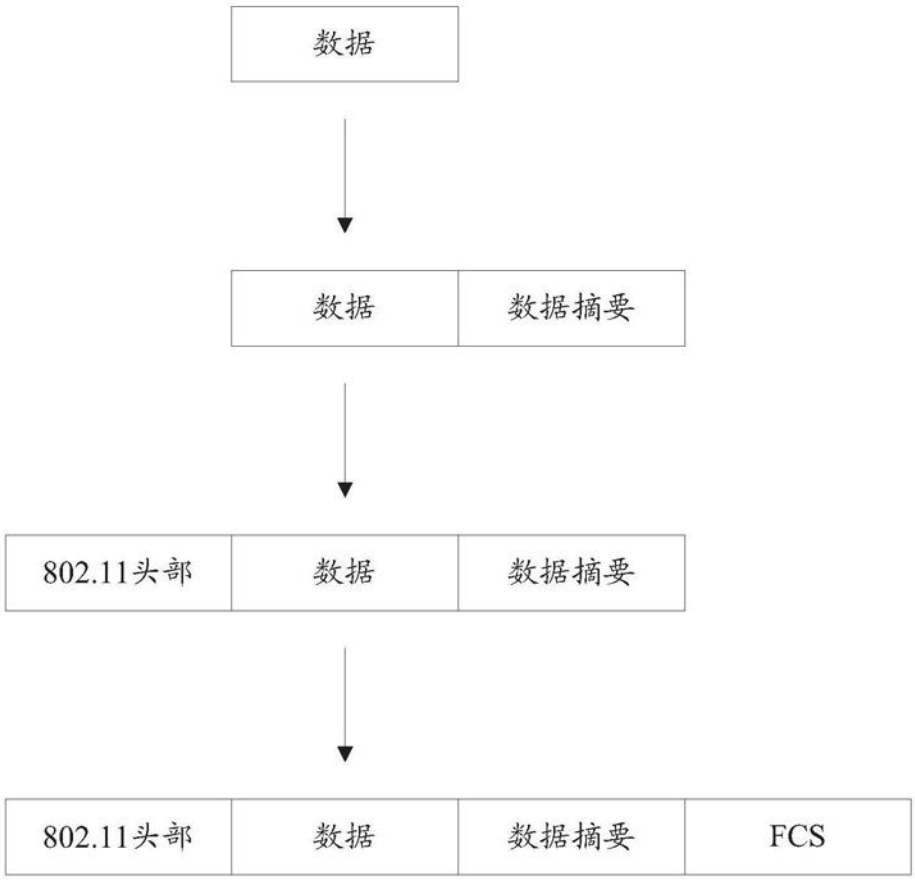

数据
数据
数据摘要
802.11头部
数据
数据摘要
802.11头部
数据
数据摘要
FCS

图18

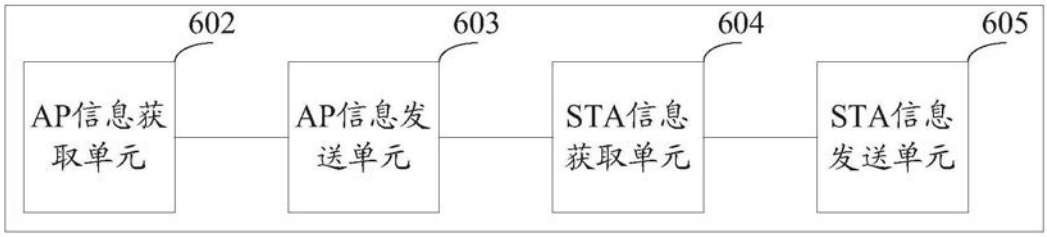

602
603
604
605
AP信息获取单元
AP信息发送单元
STA信息获取单元
STA信息发送单元

图19

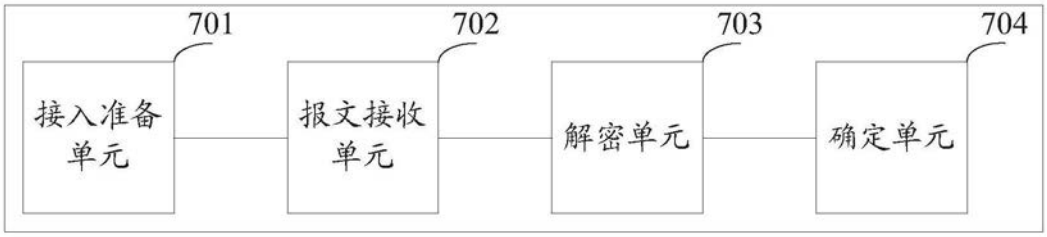

701
702
703
704
接入准备单元
报文接收单元
解密单元
确定单元

图20

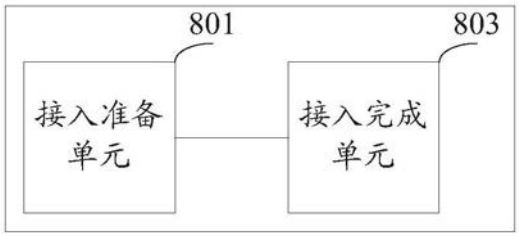


图21

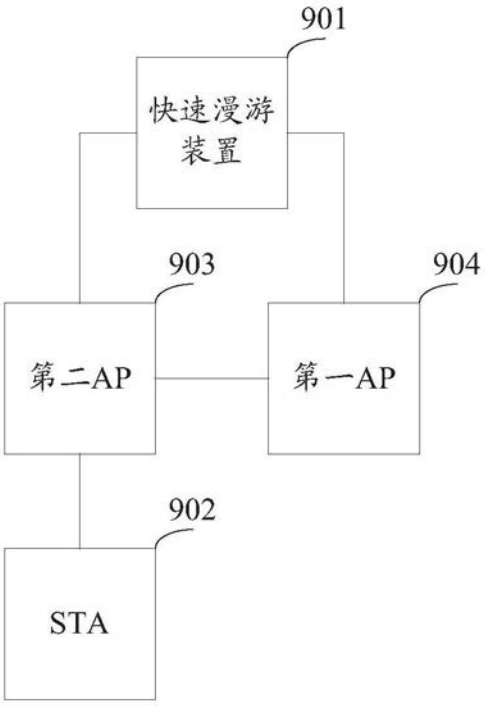


图22a

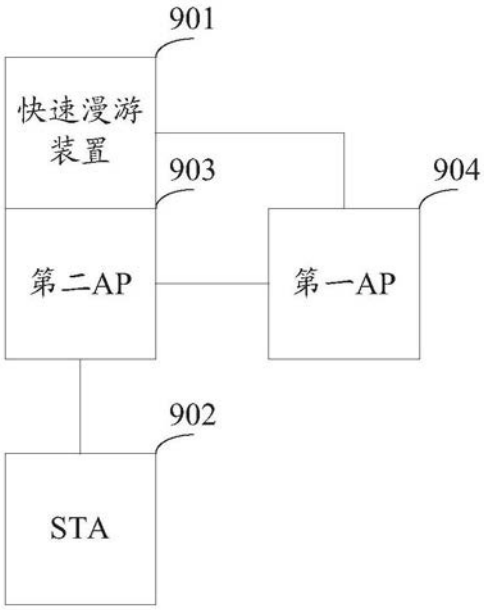


图22b