

(12) 发明专利申请

(10) 申请公布号 CN 102595405 A

(43) 申请公布日 2012.07.18

(21) 申请号 201210019801.3

(22) 申请日 2012.01.21

(71) 申请人 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 刘启明

(74) 专利代理机构 深圳市深佳知识产权代理事  
务所（普通合伙）44285

代理人 唐华明

(51) Int. Cl.

H04W 12/06 (2009.01)

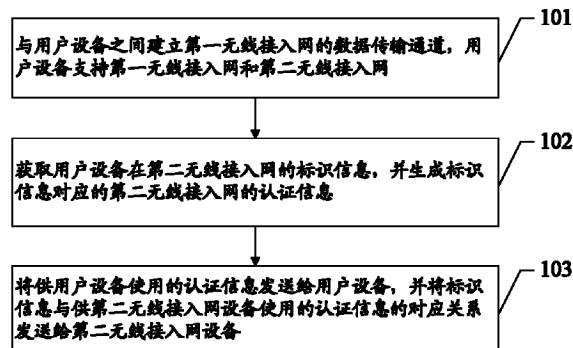
权利要求书 3 页 说明书 14 页 附图 4 页

(54) 发明名称

一种网络接入的认证方法、系统和设备

(57) 摘要

本发明实施例公开了网络接入的认证方法、系统及设备，应用于通信技术领域。本实施例的网络接入认证方法中，第一无线接入网设备建立与用户设备的第一无线接入网的数据传输通道，在获取了该用户设备在第二无线接入网的标识信息后，生成该标识信息对应的第二无线接入网的认证信息，该认证信息中包括供用户设备和第二无线接入网设备使用的第二无线接入网的认证信息；并将供用户设备使用的认证信息发送给用户设备，且将标识信息和供第二无线接入网设备使用的认证信息的对应关系发送给第二无线接入网设备。使得进行网络接入认证的认证信息不容易被泄露，提高了网络接入认证的安全性。



1. 一种网络接入的认证方法,其特征在于,包括:

与用户设备之间建立第一无线接入网的数据传输通道,所述用户设备支持所述第一无线接入网和第二无线接入网;

获取所述用户设备在所述第二无线接入网的标识信息,并生成所述标识信息对应的第二无线接入网的认证信息,所述认证信息包括供所述用户设备使用的第二无线接入网的认证信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息;

通过所述建立的第一无线接入网的数据传输通道将所述供所述用户设备使用的第二无线接入网的认证信息发送给所述用户设备,并将所述标识信息与供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给所述第二无线接入网设备。

2. 如权利要求1所述的方法,其特征在于,所述供所述用户设备使用的第二无线接入网的认证信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息相同或不同。

3. 如权利要求2所述的方法,其特征在于,所述生成所述标识信息对应的第二无线接入网的认证信息之前还包括:

如果预置的计时器超时或预置的定时器触发,则确定要生成所述认证信息,

所述预置的计时器的超时时间或所述定时器的定时时间根据所述用户设备和第二无线接入网设备更新储存的所述认证信息的周期设置。

4. 如权利要求1至3任一项所述的方法,其特征在于,所述将所述标识信息与供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给所述第二无线接入网设备,之后还包括:

所述第二无线接入网设备根据所述接收的对应关系对所述用户设备进行第二无线接入网的接入认证。

5. 如权利要求1至3任一项所述的方法,其特征在于,所述第一无线接入网是蜂窝网络,所述第二无线接入网是无线局域网 WLAN,其中所述第二无线接入网设备是接入点 AP 或接入控制器 AC 或基站。

6. 如权利要求1至3任一项所述的方法,其特征在于,所述将所述供所述用户设备使用的第二无线接入网的认证信息发送给所述用户设备,包括:

通过用户面消息、控制面消息或短消息,将所述供所述用户设备使用的第二无线接入网的认证信息发送给所述用户设备。

7. 一种网络接入的认证方法,其特征在于,包括:

与第一无线接入网设备之间建立第一无线接入网的数据传输通道;

将用户设备在第二无线接入网的标识信息发送给所述第一无线接入网设备;

接收所述第一无线接入网设备返回的供所述用户设备使用的与所述标识信息对应的第二无线接入网的认证信息;

根据所述接收的认证信息进行第二无线接入网的接入认证。

8. 如权利要求7所述的方法,其特征在于,所述接收所述第一无线接入网设备返回的供所述用户设备使用的与所述标识信息对应的认证信息之后还包括:

查询本地是否储存有供所述用户设备使用的认证信息,如果是,则用所述接收的认证信息更新本地储存的认证信息;如果不是,则将所述接收的认证信息进行储存。

9. 如权利要求 7 或 8 所述的方法, 其特征在于, 所述第一无线接入网是蜂窝网络, 所述第二无线接入网是无线局域网 WLAN, 且所述第二无线接入网设备为接入点 AP 或接入控制器 AC 或基站。

10. 一种无线接入网设备, 其特征在于, 包括:

通道建立单元, 用于与用户设备之间建立第一无线接入网的数据传输通道, 所述用户设备支持所述第一无线接入网和第二无线接入网;

认证生成单元, 用于获取所述用户设备在所述第二无线接入网的标识信息, 并生成所述标识信息对应的第二无线接入网的认证信息, 所述认证信息包括供所述用户设备使用的第二无线接入网的认证信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息;

认证发送单元, 用于通过所述通道建立单元建立的第一无线接入网的数据传输通道将所述供所述用户设备使用的第二无线接入网的认证信息发送给所述用户设备, 并将所述标识信息与供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给所述第二无线接入网设备。

11. 如权利要求 10 所述的无线接入网设备, 其特征在于, 还包括:

认证判断单元, 用于当预置的计时器超时或预置的定时器触发, 则确定要生成所述认证信息, 通知所述认证生成单元生成所述认证信息,

所述预置的计时器的超时时间或所述定时器的定时时间根据所述用户设备和第二无线接入网设备更新储存的所述认证信息的周期设置。

12. 一种用户设备, 其特征在于, 包括:

数据通道建立单元, 用于与第一无线接入网设备之间建立第一无线接入网的数据传输通道;

信息发送单元, 用于将用户设备在第二无线接入网的标识信息发送给所述第一无线接入网设备;

认证接收单元, 用于接收所述第一无线接入网设备返回的供所述用户设备使用的与所述标识信息对应的第二无线接入网的认证信息;

认证单元, 用于根据所述认证接收单元接收的认证信息进行第二无线接入网的接入认证。

13. 如权利要求 12 所述的用户设备, 其特征在于, 还包括:

认证查询单元, 用于查询本地是否储存有认证信息, 如果是, 则用所述认证接收单元接收的认证信息更新本地储存的认证信息; 如果不是, 则将所述认证接收单元接收的认证信息进行储存。

14. 一种网络接入的认证系统, 其特征在于, 包括第一无线接入网设备和第二无线接入网设备, 其中:

所述第一无线接入网设备, 用于与所述用户设备之间建立第一无线接入网的数据传输通道, 获取所述用户设备在第二无线接入网的标识信息, 并生成所述标识信息对应的第二无线接入网的认证信息, 所述认证信息包括供所述用户设备使用的第二无线接入网的认证信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息; 通过所述建立的第一无线接入网的数据传输通道将所述供所述用户设备使用的第二无线接入网的认证信息

发送给所述用户设备，并将所述标识信息与供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给所述第二无线接入网设备；

所述第二无线接入网设备，用于接收所述第一无线接入网设备发送的供所述第二无线接入网设备使用的第二无线接入网的认证信息和所述标识信息的对应关系，且根据所述接收的对应关系对所述用户设备进行第二无线接入网的接入认证。

15. 如权利要求 14 所述的系统，其特征在于，所述第一无线接入网设备是如权利要求 10 或 11 所述的无线接入网设备。

## 一种网络接入的认证方法、系统和设备

### 技术领域

[0001] 本发明涉及通信技术领域，特别涉及一种网络接入的认证方法、系统和设备。

### 背景技术

[0002] 在无线接入网比如无线局域网 (Wireless Local Area Network, WLAN) 中，为了解决网络安全的问题，一般采用统一认证的方法对无线接入网中的用户进行认证，这样用户设备就可以使用用户名和令牌登陆访问被允许登录的网络系统。现有的统一认证方法包括在可扩展的身份验证协议之上基于用户识别卡 (Extensible Authentication Protocol Method for GSM Subscriber Identity Module, EAP-SIM) 的认证方式，门户网站 (Portal) 认证方式，和基于无线保护接入的预共享密钥 (Wi-Fi Protected Access, Pre-Shared Key, WPA-PSK) 认证方法等。

[0003] 例如，在采用 WPA-PSK 方法进行认证时，需要首先在无线设备端（比如接入点）和用户设备上配置相同的共享密钥。无线设备端会广播消息发起认证过程，经过几次握手无线设备端与用户设备之间将计算消息完整性保护值 (MIC) 的必要信息进行交互，由无线设备端与用户设备分别使用同样的算法，根据接收的必要信息、预置的共享密钥和本地信息计算 MIC；最后用户设备将计算的 MIC 发送给无线设备端，如果用户设备和无线设备端分别计算的 MIC 一致，则通过验证，否则，不通过验证。

[0004] 上述现有认证的前提是，需要在认证端和用户设备都配置有认证信息，比如进行 WPA-PSK 认证的前提是，需要在无线设备端和用户设备上预先配置相同的共享密钥和相同的算法等认证信息，这样比较容易泄露认证信息；且如果认证信息泄露，就需要人工重新配置认证端和用户设备，比较繁琐。

### 发明内容

[0005] 本发明实施例提供一种网络接入的认证方法、系统和设备，以提高网络接入认证的安全性。

[0006] 一方面，提供一种网络接入的认证方法，包括：

[0007] 与用户设备之间建立第一无线接入网的数据传输通道，所述用户设备支持所述第一无线接入网和第二无线接入网；

[0008] 获取所述用户设备在所述第二无线接入网的标识信息，并生成所述标识信息对应的第二无线接入网的认证信息，所述认证信息包括供所述用户设备使用的第二无线接入网的认证信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息；

[0009] 通过所述建立的第一无线接入网的数据传输通道将所述供所述用户设备使用的第二无线接入网的认证信息发送给所述用户设备，并将所述标识信息与供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给所述第二无线接入网设备。

[0010] 另一方面，提供一种网络接入的认证方法，包括：

[0011] 与第一无线接入网设备之间建立第一无线接入网的数据传输通道；

- [0012] 将用户设备在第二无线接入网的标识信息发送给所述第一无线接入网设备；
- [0013] 接收所述第一无线接入网设备返回的供所述用户设备使用的与所述标识信息对应的第二无线接入网的认证信息；
- [0014] 根据所述接收的认证信息进行第二无线接入网的接入认证。
- [0015] 另一方面，提供一种无线接入网设备，包括：
- [0016] 通道建立单元，用于与用户设备之间建立第一无线接入网的数据传输通道，所述用户设备支持所述第一无线接入网和第二无线接入网；
- [0017] 认证生成单元，用于获取所述用户设备在所述第二无线接入网的标识信息，并生成所述标识信息对应的第二无线接入网的认证信息，所述认证信息包括供所述用户设备使用的第二无线接入网的认证信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息；
- [0018] 认证发送单元，用于通过所述通道建立单元建立的第一无线接入网的数据传输通道将所述供所述用户设备使用的第二无线接入网的认证信息发送给所述用户设备，并将所述标识信息与供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给所述第二无线接入网设备。
- [0019] 另一方面，提供一种用户设备，包括：
- [0020] 数据通道建立单元，用于与第一无线接入网设备之间建立第一无线接入网的数据传输通道；
- [0021] 信息发送单元，用于将用户设备在第二无线接入网的标识信息发送给所述第一无线接入网设备；
- [0022] 认证接收单元，用于接收所述第一无线接入网设备返回的供所述用户设备使用的与所述标识信息对应的第二无线接入网的认证信息；
- [0023] 认证单元，用于根据所述认证接收单元接收的认证信息进行第二无线接入网的接入认证。
- [0024] 再一方面，提供一种网络接入的认证系统，包括第一无线接入网设备和第二无线接入网设备，其中：
- [0025] 所述第一无线接入网设备，用于与所述用户设备之间建立第一无线接入网的数据传输通道，获取所述用户设备在第二无线接入网的标识信息，并生成所述标识信息对应的第二无线接入网的认证信息，所述认证信息包括供所述用户设备使用的第二无线接入网的认证信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息；通过所述建立的第一无线接入网的数据传输通道将所述供所述用户设备使用的第二无线接入网的认证信息发送给所述用户设备，并将所述标识信息与供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给所述第二无线接入网设备；
- [0026] 所述第二无线接入网设备，用于接收所述第一无线接入网设备发送的供所述第二无线接入网设备使用的第二无线接入网的认证信息和所述标识信息的对应关系，且根据所述接收的对应关系对所述用户设备进行第二无线接入网的接入认证。
- [0027] 本实施例的网络接入认证的技术方案中，第一无线接入网设备建立与用户设备之间的第一无线接入网的数据传输通道，在获取了该用户设备在第二无线接入网的标识信息后，生成该标识信息对应的第二无线接入网的认证信息，该认证信息中包括供用户设备和

第二无线接入网设备使用的第二无线接入网的认证信息；并通过建立的第一无线接入网的数据传输通道将供用户设备使用的第二无线接入网的认证信息发送给用户设备，且将所述标识信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给第二无线接入网设备，用户设备与第二无线接入网设备可以根据该认证信息进行第二无线接入网的认证。从而使得进行第二无线接入网认证的认证信息就不再需要固定保存在用户设备和第二无线接入网设备中，而是可以由第一无线接入网进行动态分配，使得进行网络接入认证的认证信息不容易被泄露，从而提高了网络接入认证的安全性。

## 附图说明

[0028] 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性的前提下，还可以根据这些附图获得其他的附图。

- [0029] 图 1 是本发明实施例中提供的一种网络接入的认证方法的流程图；
- [0030] 图 2 是本发明实施例中提供的另一种网络接入的认证方法的流程图；
- [0031] 图 3 是本发明实施例中提供的另一种网络接入的认证方法的流程图；
- [0032] 图 4 是本发明实施例中提供的一种具体应用中网络接入的认证方法的流程图；
- [0033] 图 5 是本发明实施例中提供的另一种具体应用中网络接入的认证方法的流程图；
- [0034] 图 6 是本发明实施例提供的一种无线接入网设备的结构示意图；
- [0035] 图 7 是本发明实施例提供的一种用户设备的结构示意图。

## 具体实施方式

[0036] 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，所描述的实施例仅仅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。

[0037] 本发明实施例提供一种网络接入的认证方法，可以对支持多种类型无线接入网的用户设备进行认证，其中多种类型无线接入网，例如，可以包括蜂窝网络和 WLAN 等类型的网络。所述蜂窝网络，例如，可以是通用移动通信系统 (Universal Mobile Telecommunications System, UMTS)、全球移动通信系统 (Global System of Mobile communication, GSM) 或长期演进 (Long Term Evolution, LTE) 等网络。

[0038] 本发明实施例的方法是第一无线接入网设备所执行的方法，流程图如图 1 所示，包括：

[0039] 步骤 101，与用户设备之间建立第一无线接入网的数据传输通道，所述用户设备支持所述第一无线接入网和第二无线接入网。

[0040] 具体地，本实施例中，当用户设备发起所述第二无线接入网的业务时，需要通过用户设备与第二无线接入网设备之间的鉴权和认证后，才能从第二无线接入网接入，而其中在认证时一般都采用密钥认证、口令认证、身份认证或证书认证等方法，这就需要在用户设备和第二无线接入网设备都配置有认证信息。比如对于 WPA-PSK 认证方法来说，需要在用

户设备和第二无线接入网设备（比如认证服务器）之间配置相同的共享密钥和认证算法等认证信息，从而根据该认证信息进行认证。

[0041] 其中所述认证信息是指在接入第二无线接入网的认证过程中，需要在用户设备和第二无线接入网设备上都需要配置的认证相关信息，具体地，可以是进行口令认证的口令，或是进行身份认证的身份号码，或是进行证书认证的证书，或计算认证文件比如消息完整性保护值的共享密钥或私有密钥，或用户设备和第二无线接入网设备计算认证文件的算法等信息。

[0042] 在本实施例中，该认证信息是通过用户设备所支持的第一无线接入网的设备动态分配的，需要第一无线接入网设备先与用户设备之间建立数据传输通道，具体地，可以通过用户设备发送连接建立请求到第一无线接入网设备，并相互之间完成认证鉴权的过程后，当用户设备发起第一无线接入网的业务时，即可建立数据传输通道，具体可以为用户面传输通道。

[0043] 步骤 102，获取所述用户设备在所述第二无线接入网的标识信息，并生成所述标识信息对应的第二无线接入网的认证信息，该认证信息可以包括供所述用户设备使用的第二无线接入网的认证信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息，且所述供用户设备使用的认证信息和所述供第二无线接入网设备使用的认证信息可以相同，也可以不同。

[0044] 具体地，所述第一无线接入网设备与所述用户设备之间建立第一无线接入网的数据传输通道后，如果该用户设备又要发起所述第二无线接入网的接入时，可以通过与所述第一无线接入网设备之间的交互来上报该用户设备在所述第二无线接入网的标识信息。

[0045] 比如所述用户设备可以向所述第一无线接入网设备发起请求消息来获取进行第二无线接入网的认证的信息，并在该请求消息中可以携带该用户设备在所述第二无线接入网中的标识信息，比如用户标识，或第二无线接入网的介质访问控制 (Media Access Control, MAC) 地址等可以唯一标识该用户设备的信息；当所述第一无线接入网设备接收到该请求消息后，可以解析得到该用户设备在所述第二无线接入网中的标识信息，就可以根据预置的策略生成所述标识信息对应的第二无线接入网的认证信息，比如可以随机生成一个认证信息并与该标识信息关联起来，或按照一定的算法对该标识信息进行计算生成等，这里如何生成认证信息并不构成对本发明的限制。

[0046] 本实施例中所述第一无线接入网设备生成的所述认证信息可以包括供所述用户设备使用的第二无线接入网的认证信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息，其中，供所述用户设备使用的认证信息和供所述第二无线接入网设备使用的认证信息可以相同，比如共享密钥、证书、身份号码或口令等信息；或者，供所述用户设备使用的认证信息和供所述第二无线接入网设备使用的认证信息也可以不同，比如私有密钥等信息。

[0047] 步骤 103，通过步骤 101 中建立的第一无线接入网的数据传输通道将所述供用户设备使用的第二无线接入网的认证信息发送给所述用户设备，并将所述标识信息与所述供第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给所述第二无线接入网设备。

[0048] 具体地，所述第一无线接入网设备可以将步骤 102 中生成的所述认证信息相应地

发送给所述用户设备和第二无线接入网设备，使得所述用户设备和第二无线接入网设备上保存所述第一无线接入网设备动态分配的第二无线接入网的认证信息，从而进行第二无线接入网的接入认证。例如，所述第一无线接入网设备可以通过步骤 101 中建立的数据传输通道向所述用户设备发送生成的供所述用户设备使用的第二无线接入网的认证信息，比如可以通过将该生成的供所述用户设备使用的第二无线接入网的认证信息携带在用户面消息、控制面消息或短消息中发送给所述用户设备进行储存；而在本实施例中，无线接入网设备之间有进行通信的接口，所述第一无线接入网设备可以通过与所述第二无线接入网设备之间的接口，将生成的供第二无线接入网设备使用的认证信息和所述标识信息的对应关系发送给所述第二无线接入网设备进行储存。

[0049] 这样如果所述用户设备要通过所述第二无线接入网接入时，第二无线接入网设备可以找到其储存的该用户设备的标识信息对应的第二无线接入网的认证信息，并与该用户设备之间根据找到的所述认证信息进行第二无线接入网的接入认证，比如口令认证、证书认证、密钥认证或身份认证等。具体地，对于密钥认证来说，由所述用户设备和第二无线接入网设备分别根据各自储存的所述认证信息计算 MIC，如果所述用户设备计算得到的 MIC 与所述第二无线接入网设备计算的 MIC 一致，则认证通过，否则认证不通过。

[0050] 本实施例中，上述第一无线接入网、第二无线接入网并不表示顺序关系，而是为了指示无线接入网的不同。例如，所述第一无线接入网可以是 UMTS，GSM 或 LTE 等蜂窝网络，所述第二无线接入网可以是 WLAN；而其中所述第一无线接入网设备，例如，可以是 UMTS 网络中的无线网络控制器 (Radio Network Controller, RNC)，所述第二无线接入网设备，例如，可以是 WLAN 中的接入点 (Access Point, AP) 或接入控制器 (Access Controller, AC) 或基站等设备。当然，第一无线接入网和第二无线接入网可以是其它任意的两个无线接入网络。

[0051] 可见，本实施例的网络接入认证的方法中，第一无线接入网设备建立与用户设备之间的第一无线接入网的数据传输通道，在获取了该用户设备在第二无线接入网的标识信息后，生成该标识信息对应的第二无线接入网的认证信息，该认证信息中包括供用户设备和第二无线接入网设备使用的第二无线接入网的认证信息；并通过建立的第一无线接入网的数据传输通道将供用户设备使用的第二无线接入网的认证信息发送给用户设备，且将所述标识信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给第二无线接入网设备，用户设备与第二无线接入网设备可以根据该认证信息进行第二无线接入网的认证。这样进行第二无线接入网认证的认证信息就不再需要固定保存在用户设备和第二无线接入网设备中，而是可以由第一无线接入网进行动态分配，使得进行网络接入认证的认证信息不容易被泄露，从而提高了网络接入认证的安全性。

[0052] 需要说明的是，上述实施例中，可选的，在所述用户设备和第二无线接入网设备上可以预先不保存所述第二无线接入网的认证信息，比如共享密钥、私有密钥或认证文件的算法等，当用户设备每次从第二无线接入网接入时，第一无线接入网设备就会为所述用户设备和第二无线接入网设备动态分配认证信息，从而进行第二无线接入网的认证的过程；或者，可选的，在所述用户设备和第二无线接入网设备上也可以预先保存有所述第二无线接入网的认证信息，而该认证信息可以周期性地更新，这就需要第一无线接入网设备在执行步骤 102 的生成认证信息之前，先判断所述用户设备和第二无线接入网设备预先保存的

所述认证信息是否需要更新,如果是,则执行步骤 102 的生成认证信息,如果不是,则结束流程。

[0053] 具体地,例如,在所述第一无线接入网设备启动时,或与所述用户设备建立数据传输通道时,可以启动一个定时器,该定时器的定时时间可以根据所述用户设备和第二无线接入网设备更新储存的认证信息的周期设置,或也可以根据实际需要设置。所述第一无线接入网设备获取到所述标识信息后,则会先判断预置的定时器是否触发,如果是,则说明所述用户设备和第二无线接入网设备上储存的认证信息需要更新,则会动态分配所述认证信息给所述用户设备和第二无线接入网设备进行储存,如果不是,则结束流程。又例如,在所述第一无线接入网设备启动时,或与所述用户设备建立数据传输通道时,也可以启动一个计时器,所述计时器的超时时间可以根据所述用户设备和第二无线接入网设备更新储存的所述认证信息的周期设置,当然,也可以根据实际需要来设置。所述第一无线接入网设备获取到所述标识信息后,可以先判断预置的计时器是否超时,如果是,则可以动态分配所述认证信息给所述用户设备和第二无线接入网设备进行储存,如果不是,则结束流程。

[0054] 本发明实施例还提供另一种网络接入的认证方法,可以对支持多种类型无线接入网的用户设备进行认证,其中多种类型无线接入网,例如,可以包括蜂窝网络和 WLAN 等类型的网络。所述蜂窝网络,例如,可以是 UMTS、GSM 或 LTE 等网络。本实施例的方法是用户设备所执行的方法,所述用户设备支持第一无线接入网和第二无线接入网,流程图如图 2 所示,包括:

[0055] 步骤 201,与第一无线接入网设备之间建立第一无线接入网的数据传输通道。

[0056] 具体地,本实施例中,当用户设备发起第二无线接入网的业务时,需要通过与第二无线接入网设备之间的鉴权和认证后,才能从第二无线接入网接入,而其中认证的过程一般采用口令认证、身份认证、证书认证或密钥认证等方法,具体地,例如对于 WPA-PSK 认证方法来说,需要在用户设备和第二无线接入网设备之间配置相同的认证信息,从而根据该认证信息进行认证。

[0057] 其中认证信息是指在接入第二无线接入网的认证过程中,需要在用户设备和第二无线接入网设备配置的认证相关信息,具体地,可以是进行口令认证的口令,或是进行身份认证的身份号码,或是进行证书认证的证书,或计算认证文件比如计算认证文件比如消息完整性保护值的共享密钥或私有密钥,或用户设备和第二无线接入网设备计算认证文件的算法等信息。

[0058] 在本实施例中,该认证信息是通过用户设备所支持的第一无线接入网的设备分配的,需要用户设备先与第一无线接入网设备之间建立数据传输通道,具体地,用户设备发送连接建立请求到第一无线接入网设备,并相互之间完成认证鉴权的过程后,当用户设备发起第一无线接入网的业务时,即可建立数据传输通道,具体可以为用户面传输通道。

[0059] 步骤 202,将所述用户设备在所述第二无线接入网的标识信息发送给所述第一无线接入网设备。

[0060] 具体地,所述用户设备可以通过与所述第二无线接入网设备之间的交互发送所述标识信息,比如所述用户设备可以主动向所述第一无线接入网设备发起请求消息来上报所述标识信息,并在所述请求消息中可以携带该用户设备在所述第二无线接入网中的标识信息,比如用户标识,或第二无线接入网的 MAC 地址等可以唯一标识用户设备的信息。

[0061] 步骤 203，接收所述第一无线接入网设备返回的供所述用户设备使用的，且与所述标识信息对应的第二无线接入网的认证信息。

[0062] 具体地，当所述第一无线接入网设备接收到所述用户设备发送的所述标识信息后，会生成所述标识信息对应的第二无线接入网的认证信息，该认证信息可以包括供所述用户设备使用的第二无线接入网的认证信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息，并通过建立的数据传输通道将所述供该用户设备使用的认证信息发送给该用户设备，则该用户设备会接收所述发送的认证信息。其中，所述第一无线接入网设备生成认证信息和发送认证信息的具体过程如图 1 对应实施例所述，不再赘述。

[0063] 步骤 204，在从所述第二无线接入网接入时，与所述第二无线接入网设备之间根据步骤 203 中接收的认证信息进行第二无线接入网的接入认证，比如口令认证、身份认证、密钥认证或证书认证等，第二无线接入网设备上储存着第一无线接入网设备发送的所述标识信息与供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系。

[0064] 具体地，可以理解，本实施例中所述供所述用户设备使用的认证信息和供所述第二无线接入网设备使用的认证信息可以相同，比如共享密钥、证书、身份号码或口令等信息；或者，所述供所述用户设备使用的认证信息和供所述第二无线接入网设备使用的认证信息也可以不同，比如私有密钥等信息。

[0065] 具体的，例如，对于密钥认证来说，由所述用户设备和第二无线接入网设备可以根据该认证信息分别计算 MIC，如果所述用户设备计算的 MIC 与所述第二无线接入网设备计算的 MIC 一致，则认证通过，否则认证不通过。

[0066] 本实施例中，上述第一无线接入网、第二无线接入网并不表示顺序关系，而是为了指示无线接入网的不同。例如，所述第一无线接入网可以是 UMTS，GSM 或 LTE 等蜂窝网络，所述第二无线接入网可以是 WLAN；而其中所述第一无线接入网设备，例如，可以是 UMTS 网络中的无线网络控制器，所述第二无线接入网设备，例如，可以是 WLAN 中的接入点或接入控制器或基站等设备。当然，第一无线接入网和第二无线接入网可以是其它任意的两个无线接入网络。

[0067] 可见，本实施例的网络接入认证的方法中，第一无线接入网设备建立与用户设备之间的第一无线接入网的数据传输通道，在获取了该用户设备在第二无线接入网的标识信息后，生成该标识信息对应的第二无线接入网的认证信息，该认证信息中包括供用户设备和第二无线接入网设备使用的第二无线接入网的认证信息；并通过建立的第一无线接入网的数据传输通道将供用户设备使用的第二无线接入网的认证信息发送给用户设备，且将所述标识信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给第二无线接入网设备，用户设备与第二无线接入网设备可以根据该认证信息进行第二无线接入网的认证。这样进行第二无线接入网认证的认证信息就不再需要固定保存在用户设备和第二无线接入网设备中，而是可以由第一无线接入网进行动态分配，使得进行网络接入认证的认证信息不容易被泄露，从而提高了网络接入认证的安全性。

[0068] 需要说明的是，上述实施例中，可选的，在所述用户设备和第二无线接入网设备上可以预先不保存所述第二无线接入网的认证信息，比如共享密钥、私有密钥或认证文件的算法等，当用户设备每次从第二无线接入网接入时，第一无线接入网设备就会为所述用户设备和第二无线接入网设备动态分配认证信息，从而进行第二无线接入网的认证的过程；

或者,可选的,在所述用户设备和第二无线接入网设备上也可以预先保存有所述第二无线接入网的认证信息,而该认证信息可以周期性地更新,这就需要第一无线接入网设备在生成所述认证信息之前,先判断所述用户设备和第二无线接入网设备预先保存的所述认证信息是否需要更新,如果是,则生成所述认证信息,如果不是,则结束流程。具体地,例如,可以通过定时器或计时器来确定是否需要更新,具体过程如图 1 对应实施例所述,不再赘述。

[0069] 本发明实施例还提供另一种网络接入的认证方法,可以对支持多种类型无线接入网的用户设备进行认证,其中多种类型无线接入网,例如,可以包括蜂窝网络和 WLAN 等类型的网络。所述蜂窝网络,例如,可以是 UMTS、GSM 或 LTE 等网络。本实施例的方法是第二无线接入网设备所执行的方法,流程图如图 3 所示,包括:

[0070] 步骤 301,接收第一无线接入网设备发送的供所述第二无线接入网设备使用的第二无线接入网的认证信息和用户设备在第二无线接入网的标识信息的对应关系。

[0071] 具体地,可以理解,当所述第一无线接入网设备与所述用户设备之间建立了数据传输通道后,可以获取所述用户设备在所述第二无线接入网的标识信息,比如在第二无线接入网的 MAC 地址等信息,生成该获取的标识信息对应的第二无线接入网的认证信息,所述认证信息可以包括供所述用户设备使用的第二无线接入网的认证信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息;所述第一无线接入网设备通过与所述第二无线接入网设备之间的接口,将供第二无线接入网设备使用的认证信息与所述标识信息的对应关系发送给第二无线接入网设备。第一无线接入网设备生成所述认证信息和发送所述认证信息的具体过程如图 1 对应实施例所述,不再赘述。

[0072] 其中所述认证信息是指在接入第二无线接入网的认证过程中,需要在用户设备和第二无线接入网设备都配置的认证相关信息,具体地,可以是进行口令认证的口令,或是进行身份认证的身份号码,或是进行证书认证的证书,或计算认证文件比如计算认证文件比如消息完整性保护值的共享密钥或私有密钥,或用户设备和第二无线接入网设备计算认证文件的算法等信息。所述供所述用户设备使用的认证信息和供所述第二无线接入网设备使用的认证信息可以相同,比如共享密钥、证书、身份号码或口令等信息;或者,所述供所述用户设备使用的认证信息和供所述第二无线接入网设备使用的认证信息也可以不同,比如私有密钥等信息。

[0073] 步骤 302,根据步骤 301 中接收的所述认证信息与所述标识信息的对应关系,对所述用户设备进行第二无线接入网的接入认证,比如进行口令认证、身份认证、密钥认证或证书认证等。

[0074] 具体地,当所述用户设备从所述第二无线接入网接入时,所述第二无线接入网设备可以根据接收的所述对应关系,找到该用户设备的标识信息对应的供所述第二无线接入网设备使用的第二无线接入网的认证信息,并根据找到的所述认证信息对所述用户设备进行第二无线接入网的接入认证,比如口令认证、证书认证、密钥认证或身份认证等。具体地认证过程如图 1 和图 2 对应实施例所述,不再赘述。

[0075] 本实施例中,上述第一无线接入网、第二无线接入网并不表示顺序关系,而是为了指示无线接入网的不同。例如,所述第一无线接入网可以是 UMTS、GSM 或 LTE 等蜂窝网络,所述第二无线接入网可以是 WLAN;而其中所述第一无线接入网设备,例如,可以是 UMTS 网络中的无线网络控制器,所述第二无线接入网设备,例如,可以是 WLAN 中的接入点或接入

控制器或基站等设备。当然,第一无线接入网和第二无线接入网可以是其它任意的两个无线接入网络。

[0076] 可见,本实施例的网络接入认证的方法中,第一无线接入网设备建立与用户设备之间的第一无线接入网的数据传输通道,在获取了该用户设备在第二无线接入网的标识信息后,生成该标识信息对应的第二无线接入网的认证信息,该认证信息中包括供用户设备和第二无线接入网设备使用的第二无线接入网的认证信息;并通过建立的第一无线接入网的数据传输通道将供用户设备使用的第二无线接入网的认证信息发送给用户设备,且将所述标识信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给第二无线接入网设备,用户设备与第二无线接入网设备可以根据该认证信息进行第二无线接入网的认证。这样进行第二无线接入网认证的认证信息就不再需要固定保存在用户设备和第二无线接入网设备中,而是可以由第一无线接入网进行动态分配,使得进行网络接入认证的认证信息不容易被泄露,从而提高了网络接入认证的安全性。

[0077] 以下以一个具体应用例来说明本发明实施例的方法,在本实施例中,第一无线接入网是UTMS 网络,第二无线接入网是 WLAN,且在用户设备和 WLAN 设备上预先并没有储存认证信息。具体地,参考图 4 所示,本实施例中网络接入的认证方法包括:

[0078] 步骤 401,用户设备 (User Equipment, UE) 与 RNC 之间建立 UMTS 网络的数据传输通道。

[0079] 具体地,例如,UE 可以向 UMTS 网络的 RNC 发送无线资源控制协议 (Radio Resource Control, RRC) 连接建立请求,通过 RNC 与 UE 之间的信令交互建立 RRC 连接,接着完成 UMTS 网络的认证和鉴权,当 UE 发起 UMTS 网络业务时, RNC 与 UE 之间通过信令交互完成用户面数据传输通道的建立。UE 向 RNC 发送 RRC 连接建立请求时,例如,可以通过运营商提供的客户端软件发送。

[0080] 步骤 402,UE 与 RNC 进行通信,传输 UE 在 WLAN 中的标识信息。

[0081] 具体地,例如,UE 可以创建一个用于描述网络协议 (IP) 地址和端口号的套接字 (Socket),并通过对应的端口发送请求消息给 RNC,其中在请求消息中包括 UE 在 WLAN 中的标识信息,比如 WLAN MAC 地址等。

[0082] 步骤 403,RNC 接收到 UE 上报的标识信息,生成标识信息对应的 WLAN 网络的认证信息。

[0083] 具体地,本实施例中,可以生成供 UE 使用的 WLAN 网络认证信息和供 WLAN 设备使用的 WLAN 网络认证信息,供 UE 使用的 WLAN 网络认证信息和供 WLAN 设备使用的 WLAN 网络认证信息可以相同,比如共享密钥或认证算法等。其中 WLAN 设备可以是接入控制器 (Access Controller, AC) 或是 AP 或是基站等设备。

[0084] 步骤 404,RNC 通过与 WLAN 设备之间的接口,将步骤 403 生成的供 WLAN 设备使用的 WLAN 网络认证信息和所述标识信息的对应关系发送给所述 WLAN 设备进行储存。

[0085] 具体地,例如,RNC 可以通过与 AP 之间的接口将对应关系直接发送给 AP,RNC 也可以通过与 AC 之间的接口先将对应关系发送给 AC,然后由 AC 转发给 AP,这种情况下,由 UE 与 AP 进行 WLAN 网络接入的认证;RNC 也可以将对应关系发送给 AC,由 AC 与 UE 进行 WLAN 网络接入的认证。

[0086] 步骤 405,RNC 通过步骤 401 中建立的数据传输通道将步骤 403 生成的供 UE 使用

的 WLAN 网络认证信息发送给 UE 进行储存。

[0087] 具体地,例如,认证信息可以携带在用户面消息、控制面消息或短消息中发送给 UE。

[0088] 步骤 406, UE 收到 RNC 发送的认证信息后配置 WLAN 的认证文件,启动 WLAN 功能,并进行用户设备接入 WLAN 网络的认证。

[0089] 具体地,例如,如果供 UE 使用的 WLAN 网络认证信息和供 WLAN 设备使用的 WLAN 网络认证信息相同,例如是相同的共享密钥,或是相同的计算 MIC 的算法信息等,则在进行认证时,可以由 WLAN 设备发起 WPA-PSK 认证过程,经过几次握手,在 WLAN 设备与 UE 之间交互计算 MIC 的必要信息,WLAN 设备与 UE 分别使用同样的算法,根据获取的计算 MIC 的必要信息、共享密钥和本地信息计算 MIC;最后 UE 将计算的 MIC 发送给 WLAN 设备,如果确定 UE 和 WLAN 设备分别计算的 MIC 是一致的,则通过验证,否则,不通过验证。

[0090] 本实施例中 UE 通过先接入 UMTS 网络中,由 RNC 为 UE 和 WLAN 设备动态分配相同的认证信息,进行 WLAN 网络接入的认证,比如 WPA-PSK 认证,使得认证信息不容易泄露,提高了安全性。

[0091] 可以理解,可选的,上述实施例中 RNC 分配的供 UE 使用的 WLAN 网络认证信息和供 WLAN 设备使用的 WLAN 网络认证信息也可以不相同。

[0092] 以下以一个具体应用例来说明本发明实施例的方法,在本实施例中,第一无线接入网是 UMTS 网络,第二无线接入网是 WLAN,且在用户设备和 WLAN 设备上预先储存认证信息,可选的,该认证信息可以周期性地更新。具体地,参考图 5 所示,本实施例中网络接入的认证方法包括:

[0093] 步骤 501,UE 与 RNC 之间建立 UMTS 网络的数据传输通道。

[0094] 具体地,建立过程如上述步骤 401 中所述,不再赘述。

[0095] 步骤 502,RNC 可以启动一个定时器或计时器,其中定时器的定时时间或计时器的超时时间可以根据 UE 更新储存的认证信息的周期设置。可以理解,在其他具体实施例中,RNC 可以在启动时即可启动定时器或计时器。

[0096] 步骤 503,UE 与 RNC 之间通信,将 UE 在 WLAN 中的标识信息发送给 RNC。

[0097] 具体地,UR 会创建一个用于描述 IP 地址和端口号的套接字,并通过对应的端口发送请求消息给 RNC,其中在请求消息中包括 UE 在 WLAN 中的标识信息,比如 WLAN MAC 地址等。

[0098] 步骤 504,RNC 接收到 WLAN 中标识信息后,判断启动的定时器是否触发,或计时器是否超过预置的时间,该预置的时间可以根据 UE 更新储存的认证信息的周期设置,如果定时器触发或计时器超时,则执行步骤 505,如果定时器未触发或计时器未超时,则结束流程。

[0099] 步骤 505,RNC 生成所述标识信息对应的 WLAN 网络认证信息。

[0100] 具体地,例如,本实施例中可以生成供 UE 使用的 WLAN 网络认证信息和供 WLAN 设备使用的 WLAN 网络认证信息,供 UE 使用的 WLAN 网络认证信息和供 WLAN 设备使用的 WLAN 网络认证信息可以不同,比如私有密钥等。其中 WLAN 中的网络设备可以是 AC 或是 AP 或是基站等设备。

[0101] 步骤 506,RNC 通过与 WLAN 中的网络设备之间的接口,将生成的供 WLAN 中的网络设备使用的 WLAN 网络认证信息和标识信息的对应关系发送给 WLAN 设备,更新该 WLAN 中的

网络设备储存的对应关系。

[0102] 具体地, RNC 可以通过与 AP 之间的接口将对应关系直接发送给 AP 进行更新储存的对应关系, RNC 也可以通过与 AC 之间的接口先将对应关系发送给 AC, 然后由 AC 转发给 AP 进行更新储存的对应关系, 这种情况下, 由 UE 与 AP 进行 WLAN 网络接入的认证; RNC 也可以将对应关系发送给 AC 进行更新储存的对应关系, 由 AC 与 UE 进行 WLAN 网络接入的认证。

[0103] 步骤 507, RNC 通过步骤 501 中建立的数据传输通道将生成的供 UE 使用的 WLAN 网络认证信息发送给 UE。

[0104] 具体地, 例如, 认证信息可以携带在用户面消息、控制面消息或短消息中发送给 UE; 当 UE 接收到供 UE 使用的 WLAN 网络认证信息后, 用接收的认证信息更新已储存的认证信息。

[0105] 步骤 508, UE 收到认证信息后配置 WLAN 的认证文件, 启动 WLAN 功能, 并与 WLAN 设备之间进行非对称密钥认证的过程。

[0106] 具体地, 在认证过程中, UE 进行加密(或解密)的私有密钥与 WLAN 设备进行解密(或加密)的私有密钥不相同。

[0107] 本实施例中 UE 通过先接入 UMTS 网络中, 由 RNC 为 UE 和 WLAN 设备动态分配不同的认证信息, 进行非对称密钥认证, 使得在网络接入的认证中认证信息不容易泄露, 提高了安全性。

[0108] 本发明实施例还提供一种无线接入网设备, 即上述方法实施例中所说的第一无线接入网设备, 其结构示意图如图 6 所示, 包括:

[0109] 通道建立单元 10, 用于与用户设备之间建立第一无线接入网的数据传输通道, 所述用户设备支持第一无线接入网和第二无线接入网;

[0110] 认证生成单元 11, 用于获取所述用户设备在所述第二无线接入网的标识信息, 并生成所述标识信息对应的第二无线接入网的认证信息, 所述认证信息包括供所述用户设备使用的第二无线接入网的认证信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息;

[0111] 认证发送单元 12, 用于通过所述通道建立单元 10 建立的第一无线接入网的数据传输通道将所述供所述用户设备使用的第二无线接入网的认证信息发送给所述用户设备, 并将所述标识信息与供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给所述第二无线接入网设备。

[0112] 具体地, 认证发送单元 12 可以通过用户面消息、控制面消息或短消息, 将所述生成的供用户设备使用的第二无线接入网的认证信息发送给所述用户设备。

[0113] 本实施例中, 上述第一无线接入网、第二无线接入网并不表示顺序关系, 而是为了指示无线接入网的不同。例如, 所述第一无线接入网可以是 UMTS, GSM 或 LTE 等蜂窝网络, 所述第二无线接入网可以是 WLAN; 而其中所述第一无线接入网设备, 例如, 可以是 UMTS 网络中的无线网络控制器, 所述第二无线接入网设备, 例如, 可以是 WLAN 中的接入点或接入控制器或基站等设备。当然, 第一无线接入网和第二无线接入网可以是其它任意的两个无线接入网络。

[0114] 可见, 在本实施例的无线接入网设备中, 通道建立单元 10 会建立与用户设备的第一无线接入网的数据传输通道, 在认证生成单元 11 获取了该用户设备在第二无线接入网

的标识信息后，生成该标识信息对应的第二无线接入网的认证信息，并由认证发送单元 12 通过建立的第一无线接入网的数据传输通道将供用户设备使用的第二无线接入网的认证信息发送给用户设备，且将标识信息和供第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给第二无线接入网设备，当用户设备从第二无线接入网接入时，用户设备与第二无线接入网设备就可以根据该认证信息进行认证。这样进行第二无线接入网认证的认证信息就不再需要固定保存在用户设备和第二无线接入网设备中，而是可以由第一无线接入网进行动态分配，使得进行网络接入认证的认证信息不容易被泄露，从而提高了网络接入认证的安全性。

[0115] 在一个具体地实施例中，无线接入网设备除了包括如图 6 所示的结构外，还可以包括认证判断单元，用于判断是否要生成标识信息对应的认证信息，如果是，则会通知认证生成单元 11 生成认证信息，并由认证发送单元 12 发送认证信息。具体地，认证判断单元可以判断预置的计时器是否超时或判断预置的定时器是否触发，如果是，则确定要为用户设备生成认证信息，所述预置的计时器的超时时间或所述定时器的定时时间可以根据所述用户设备和第二无线接入网设备更新储存的认证信息的周期设置。

[0116] 应用本发明实施例中的无线接入网设备进行认证的具体过程可以参考前述方法实施例，此处不再赘述。

[0117] 本发明实施例还提供一种用户设备，其结构示意图如图 7 所示，包括：

[0118] 数据通道建立单元 20，用于与第一无线接入网设备之间建立第一无线接入网的数据传输通道；

[0119] 信息发送单元 21，用于将用户设备在第二无线接入网的标识信息发送给所述第一无线接入网设备；

[0120] 认证接收单元 22，用于接收所述第一无线接入网设备返回的供所述用户设备使用的与所述标识信息对应的第二无线接入网的认证信息；

[0121] 认证单元 23，用于根据所述认证接收单元 22 接收的认证信息进行第二无线接入网的接入认证，比如口令认证、密钥认证、证书认证或身份认证等。

[0122] 所述第一无线接入网设备可以生成供用户设备使用的第二无线接入网的认证信息与供所述第二无线接入网设备使用的第二无线接入网的认证信息，所述供用户设备使用的认证信息与供所述第二无线接入网设备使用的认证信息可以相同，比如共享密钥、证书、身份号码或口令等信息；所述供用户设备使用的认证信息与供所述第二无线接入网设备使用的认证信息也可以不同，比如私有密钥等信息。

[0123] 在一个具体地实施例中，无线接入网设备除了包括如图 7 所示的结构外，还可以包括认证查询单元，用于查询本地是否储存有认证信息，如果是，则用认证接收单元 22 接收的认证信息更新本地储存的认证信息；如果不是，则将认证接收单元 22 接收的认证信息进行储存。具体地，当认证接收单元 22 接收到所述认证信息后，认证查询单元会进行查询及相应处理。

[0124] 本实施例中，上述第一无线接入网、第二无线接入网并不表示顺序关系，而是为了指示无线接入网的不同。例如，所述第一无线接入网可以是 UMTS、GSM 或 LTE 等蜂窝网络，所述第二无线接入网可以是 WLAN；而其中所述第一无线接入网设备，例如，可以是 UMTS 网络中的无线网络控制器，所述第二无线接入网设备，例如，可以是 WLAN 中的接入点或接入

控制器或基站等设备。当然,第一无线接入网和第二无线接入网可以是其它任意的两个无线接入网络。

[0125] 本实施例的用户设备中,数据通道建立单元 20 会与第一无线接入网设备建立第一无线接入网的数据传输通道,并由信息发送单元 21 发送用户设备在第二无线接入网的标识信息给第一无线接入网设备;当认证接收单元 22 接收到返回的标识信息对应的供所述用户设备使用的第二无线接入网的认证信息后,认证单元 23 会根据接收的认证信息进行第二无线接入网的接入认证。这样进行第二无线接入网认证的认证信息就不再需要固定保存在用户设备和第二无线接入网设备中,而是可以由第一无线接入网进行动态分配,使得进行网络接入认证的认证信息不容易被泄露,从而提高了网络接入认证的安全性。

[0126] 应用本发明实施例中的用户设备进行认证的具体过程可以参考前述方法实施例,此处不再赘述。

[0127] 本发明实施例还提供一种网络接入的认证系统,包括:第一无线接入网设备、第二无线接入网设备,其中:

[0128] 所述第一无线接入网设备,用于与所述用户设备之间建立第一无线接入网的数据传输通道,获取所述用户设备在第二无线接入网的标识信息,并生成所述标识信息对应的第二无线接入网的认证信息,所述认证信息包括供所述用户设备使用的第二无线接入网的认证信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息;通过所述建立的第一无线接入网的数据传输通道将所述供所述用户设备使用的第二无线接入网的认证信息发送给所述用户设备,并将所述标识信息与供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给所述第二无线接入网设备;

[0129] 所述第二无线接入网设备,用于接收所述第一无线接入网设备发送的供所述第二无线接入网设备使用的第二无线接入网的认证信息和所述标识信息的对应关系,且根据所述接收的对应关系对所述用户设备进行第二无线接入网的接入认证。

[0130] 而上述第一无线接入网设备的结构可以如图 6 对应实施例的设备结构,不再赘述。

[0131] 本实施例中,上述第一无线接入网、第二无线接入网并不表示顺序关系,而是为了指示无线接入网的不同。例如,所述第一无线接入网可以是 UMTS, GSM 或 LTE 等蜂窝网络,所述第二无线接入网可以是 WLAN;而其中所述第一无线接入网设备,例如,可以是 UMTS 网络中的无线网络控制器,所述第二无线接入网设备,例如,可以是 WLAN 中的接入点或接入控制器或基站等设备。当然,第一无线接入网和第二无线接入网可以是其它任意的两个无线接入网络。

[0132] 本实施例的认证系统中,第一无线接入网设备建立与用户设备之间的第一无线接入网的数据传输通道,在获取了该用户设备在第二无线接入网的标识信息后,生成该标识信息对应的第二无线接入网的认证信息,该认证信息中包括供用户设备和第二无线接入网设备使用的第二无线接入网的认证信息;并通过建立的第一无线接入网的数据传输通道将供用户设备使用的第二无线接入网的认证信息发送给用户设备,且将所述标识信息和供所述第二无线接入网设备使用的第二无线接入网的认证信息的对应关系发送给第二无线接入网设备,用户设备与第二无线接入网设备可以根据该认证信息进行第二无线接入网的认证。这样使得进行第二无线接入网认证的认证信息就不再需要固定保存在用户设备和第二

无线接入网设备中,而是可以由第一无线接入网进行动态分配,使得进行网络接入认证的认证信息不容易被泄露,从而提高了网络接入认证的安全性。

[0133] 应用本发明实施例中的认证系统进行认证的具体过程可以参考前述方法实施例,此处不再赘述。

[0134] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成,该程序可以存储于一计算机可读存储介质中,存储介质可以包括:只读存储器(ROM)、随机存取存储器(RAM)、磁盘或光盘等。

[0135] 以上对本发明实施例所提供的网络接入的认证方法、系统及设备,进行了详细介绍,本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想;同时,对于本领域的一般技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

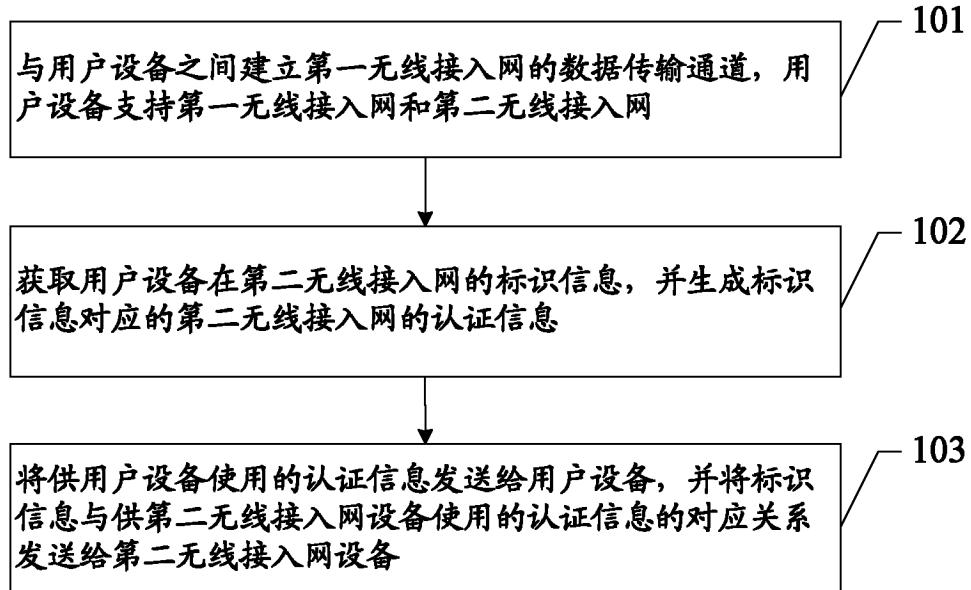


图 1

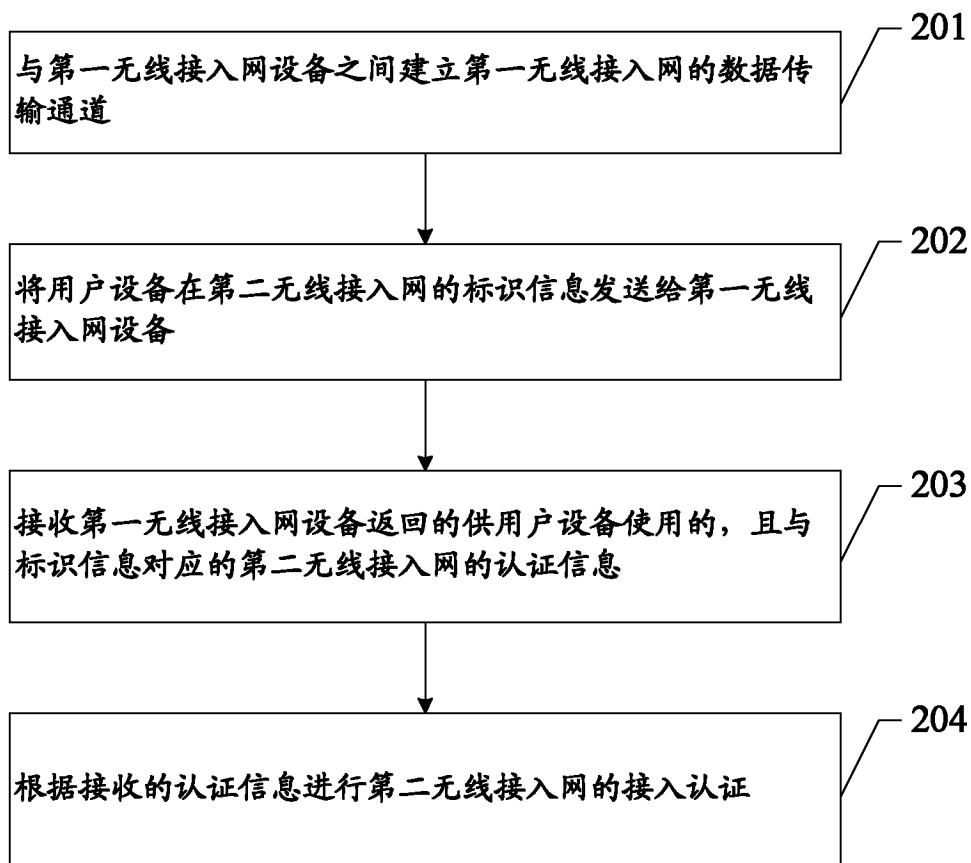


图 2

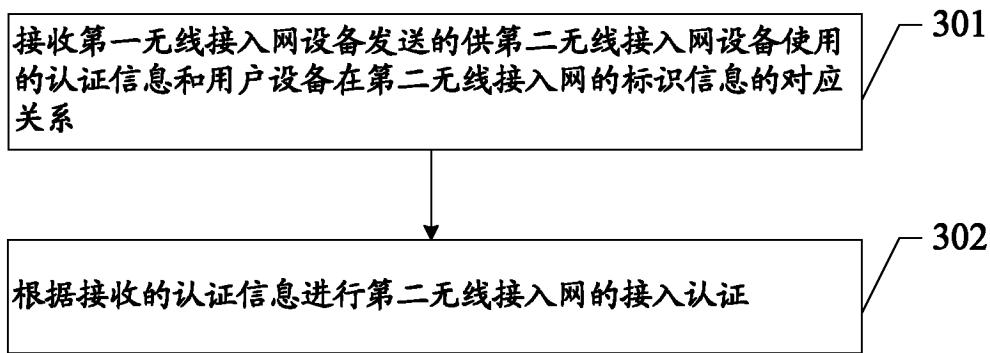


图 3

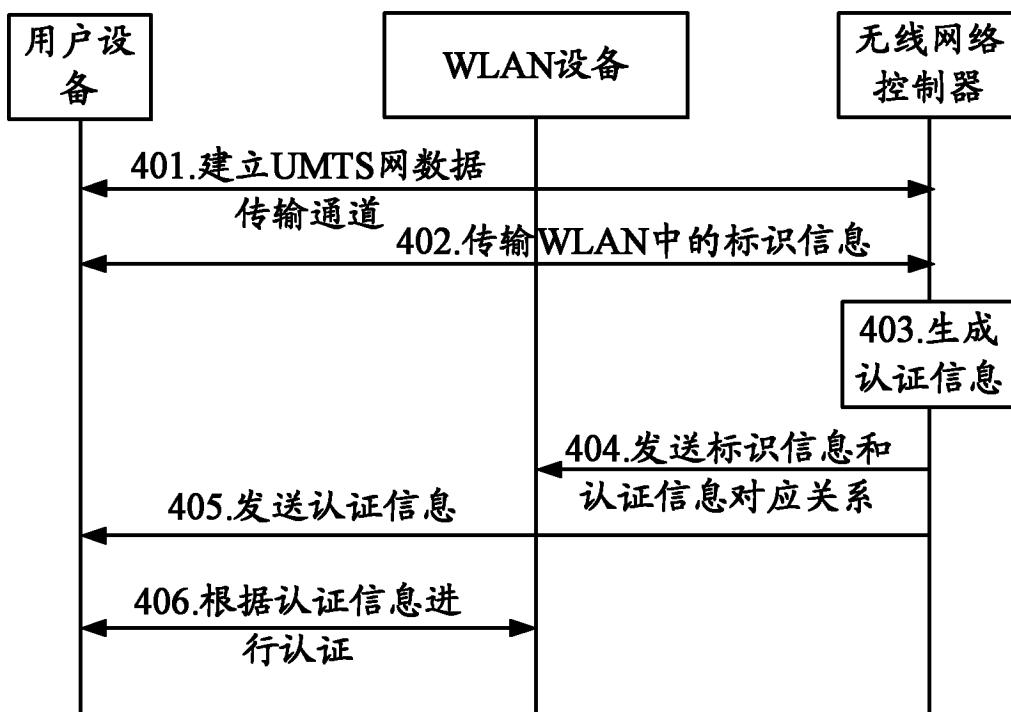


图 4

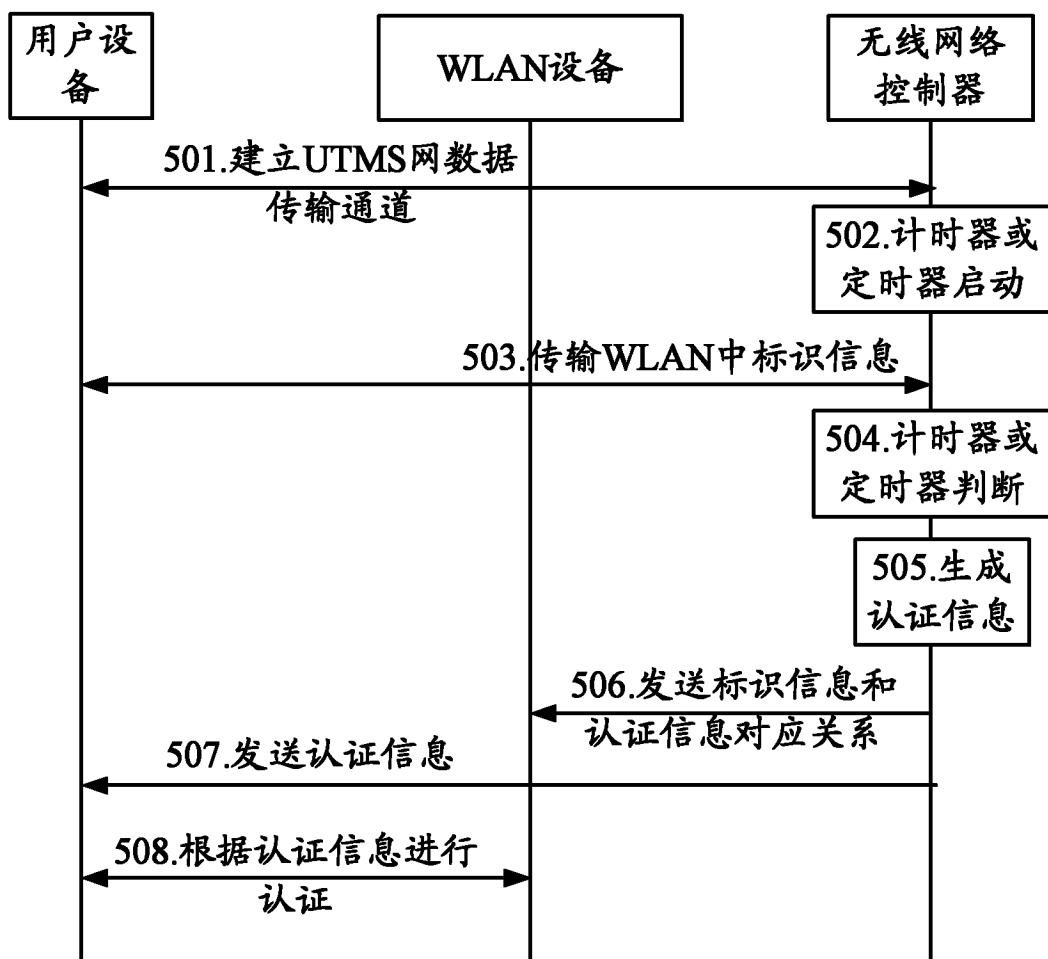


图 5

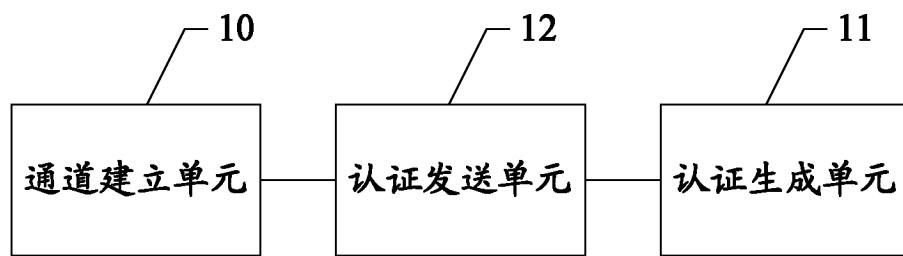


图 6

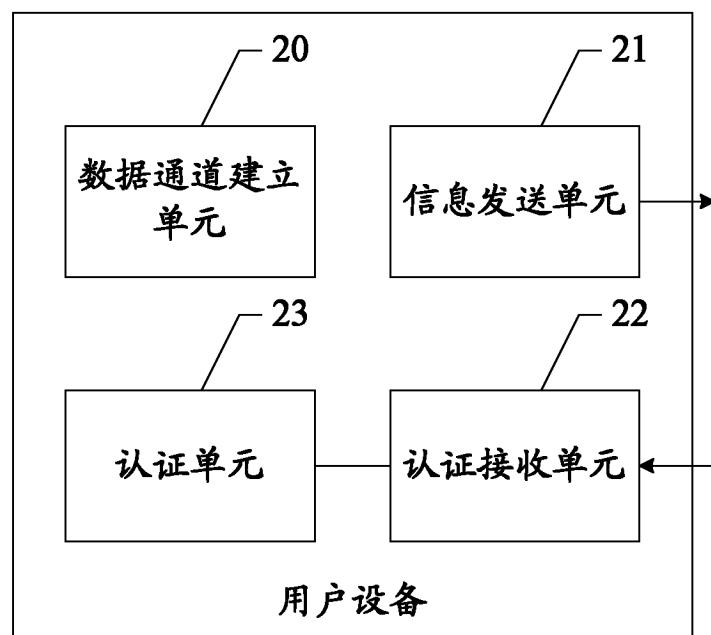


图 7