(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 105554747 B
(45)授权公告日 2018.09.04

(21)申请号 201610067787.2

(22)申请日 2016.01.29

(65)同一申请的已公布的文献号
申请公布号 CN 105554747 A

(43)申请公布日 2016.05.04

(73)专利权人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 朱戈 唐文宁 杨志伟 付火平 陈水明 徐森圣

(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 刘映东

(51)Int.Cl.
H04W 12/04(2009.01)
H04W 12/06(2009.01)
H04W 76/12(2018.01)
H04L 29/06(2006.01)

(56)对比文件
CN 103024743 A,2013.04.03,
CN 104244248 A,2014.12.24,
CN 104394533 A,2015.03.04,
CN 101212296 A,2008.07.02,
US 2009214036 A1,2009.08.27,

审查员 欧阳洁

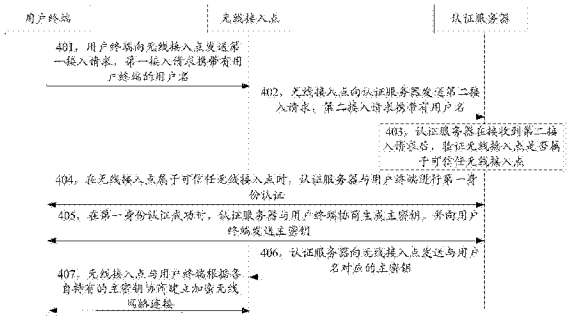
权利要求书7页 说明书20页 附图8页

(54)发明名称

无线网络连接方法、装置及系统

(57)摘要

本发明实施例公开了一种无线网络连接方法、装置及系统，属于网络安全领域。本发明通过向无线接入点发送第一接入请求；向认证服务器发送第二接入请求；验证无线接入点是否属于可信任无线接入点，属于可信任无线接入点时与用户终端进行第一身份认证，与用户终端协商生成主密钥；向无线接入点发送与用户名对应的主密钥；根据主密钥与用户终端协商建立加密无线网络连接；解决了用户终端向假冒的公众Wi-Fi所传输的数据以及用户终端内部的数据均会受到安全威胁的问题；达到了只有可信任无线接入点能获取与用户名对应的主密钥，从而与用户终端根据各自持有的主密钥协商建立加密无线网络连接，提高了用户终端传输的数据以及用户终端内部数据安全性的效果。



CN 105554747 B

1.一种无线网络连接方法,其特征在于,所述方法包括:

用户终端向无线接入点发送第一接入请求,所述第一接入请求携带有所述用户终端的用户名;

所述无线接入点向认证服务器发送第二接入请求,所述第二接入请求中携带第一密文和与所述无线接入点对应的第二公钥,所述第一密文包括所述用户名,所述第一密文是所述无线接入点通过与所述无线接入点对应的第二私钥对所述用户名进行加密的密文;

所述认证服务器在接收到所述第二接入请求后,验证所述无线接入点是否属于可信任无线接入点,在所述无线接入点属于所述可信任无线接入点时,使用与所述无线接入点对应的第二公钥对所述第二接入请求中携带的第一密文进行解密,得到所述用户名;查询与所述用户名对应的密钥信息;根据所述密钥信息与所述用户终端进行第一身份认证;

在所述第一身份认证成功时,所述认证服务器与所述用户终端协商生成主密钥,并向所述用户终端发送所述主密钥;

所述认证服务器向所述无线接入点发送与所述用户名对应的所述主密钥;

所述无线接入点与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接。

2.根据权利要求1所述的方法,其特征在于,所述认证服务器在接收到所述第二接入请求后,验证所述无线接入点是否属于可信任无线接入点,包括:

所述认证服务器获取所述第二接入请求中携带的第一密文和与所述无线接入点对应的第二公钥;

所述认证服务器验证与所述无线接入点对应的第二公钥是否存在于可信任公钥集合中;若与所述无线接入点对应的第二公钥存在于所述可信任公钥集合中,则将所述无线接入点验证为所述可信任无线接入点;

其中,所述可信任公钥集合存储有成功通过所述认证服务器的第二身份认证的无线接入点对应的第二公钥。

3.根据权利要求2所述的方法,其特征在于,所述认证服务器获取所述第二接入请求中携带的第一密文和与所述无线接入点对应的第二公钥,包括:

所述认证服务器通过与所述认证服务器对应的第一私钥对所述第二接入请求进行解密,得到第一密文和与所述无线接入点对应的第二公钥;

其中,所述第二接入请求是所述无线接入点通过与所述认证服务器对应的第一公钥对所述第一密文和与所述无线接入点对应的第二公钥进行加密的请求。

4.根据权利要求2或3所述的方法,其特征在于,所述认证服务器向所述无线接入点发送与所述用户名对应的所述主密钥,包括:

所述认证服务器使用与所述无线接入点对应的第二公钥对协商生成的所述主密钥进行第一加密,向所述无线接入点发送第一加密后的所述主密钥。

5.根据权利要求4所述的方法,其特征在于,所述向所述无线接入点发送第一加密后的所述主密钥,包括:

所述认证服务器使用与所述认证服务器对应的第一私钥对第一加密后的所述主密钥进行第二加密,向所述无线接入点发送第二加密后的所述主密钥。

6.根据权利要求1至3、5任一所述的方法,其特征在于,所述无线接入点向所述认证服

务器发送第二接入请求之前，还包括：

所述无线接入点生成与所述无线接入点对应的第二公钥和第二私钥；

所述无线接入点获取与所述认证服务器对应的第一公钥；

所述无线接入点向所述认证服务器发送身份认证请求，所述身份认证请求携带有认证信息和与所述无线接入点对应的第二公钥，所述认证信息和与所述无线接入点对应的第二公钥均使用与所述认证服务器对应的第一公钥进行加密，所述认证信息至少包括硬件信息和/或拥有者信息；

所述认证服务器通过与所述认证服务器对应的第一私钥对所述身份认证请求进行解密，得到所述认证信息和与所述无线接入点对应的第二公钥；

所述认证服务器对所述认证信息进行第二身份认证，在所述第二身份认证成功时，将与所述无线接入点对应的第二公钥添加至所述可信任公钥集合中。

7.根据权利要求6所述的方法，其特征在于，所述认证信息是所述无线接入点通过与所述无线接入点对应的第二私钥进行加密的信息；

所述认证服务器对所述认证信息进行第二身份认证，包括：

所述认证服务器通过与所述无线接入点对应的第二公钥对所述认证信息进行解密，得到所述硬件信息和/或所述拥有者信息；

所述认证服务器对所述硬件信息和/或所述拥有者信息进行第二身份认证，在所述第二身份认证成功时，将与所述无线接入点对应的第二公钥添加至所述可信任公钥集合中。

8.根据权利要求1至3、5任一所述的方法，其特征在于，所述无线接入点与所述用户终端通过各自持有的所述主密钥协商建立加密无线网络连接，包括：

所述无线接入点和所述用户终端使用各自持有的所述主密钥，协商生成本次连接所使用的临时密钥，使用所述临时密钥建立加密无线网络连接。

9.根据权利要求1至3、5任一所述的方法，其特征在于，所述用户终端向无线接入点发送第一接入请求之前，还包括：

所述用户终端通过独立通道向所述认证服务器注册所述用户名和与所述用户名对应的密钥信息，所述独立通道是不经过所述无线接入点的通信通道；

其中，所述密钥信息是密码或者证书。

10.一种无线网络连接方法，其特征在于，所述方法包括：

接收用户终端发送的第一接入请求，所述第一接入请求携带有所述用户终端的用户名；

向认证服务器发送第二接入请求，所述第二接入请求中携带第一密文和与无线接入点对应的第二公钥，所述第一密文包括所述用户名，所述第一密文是所述无线接入点通过与所述无线接入点对应的第二私钥对所述用户名进行加密的密文；

接收所述认证服务器发送的与所述用户名对应的主密钥，所述主密钥是所述认证服务器在接收到所述第二接入请求后，验证无线接入点属于可信任无线接入点时，与用户终端进行第一身份认证成功后使用与所述无线接入点对应的第二公钥对所述第二接入请求中携带的第一密文进行解密，得到所述用户名；查询与所述用户名对应的密钥信息；根据所述密钥信息协商生成的密钥；

与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接。

11.根据权利要求10所述的方法，其特征在于，所述接收所述认证服务器发送的与所述用户名对应的主密钥，包括：

接收所述认证服务器发送的第一加密后的主密钥，所述第一加密后的主密钥是所述认证服务器在所述无线接入点属于所述可信任无线接入点时，使用与所述无线接入点对应的第二公钥对所述主密钥进行加密后的主密钥。

12.根据权利要求10所述的方法，其特征在于，所述接收所述认证服务器发送的与所述用户名对应的主密钥，包括：

接收所述认证服务器发送的第二加密后的主密钥，所述第二加密后的主密钥是所述认证服务器在所述无线接入点属于所述可信任无线接入点时，使用与所述无线接入点对应的第二公钥对所述主密钥进行第一加密，再使用与所述认证服务器对应的第一私钥对第一加密后的所述主密钥进行第二加密后的主密钥。

13.根据权利要求11所述的方法，其特征在于，所述与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接，包括：

使用与所述无线接入点对应的第二私钥对所述第一加密后的主密钥进行解密，得到所述主密钥；

与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接。

14.根据权利要求12所述的方法，所述与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接，包括：

使用与所述认证服务器对应的第一公钥对第二加密后的所述主密钥进行解密，得到第二密文；

使用与所述无线接入点对应的第二私钥对所述第二密文进行解密，得到所述主密钥；

与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接；

其中，所述第二密文是所述认证服务器通过与所述无线接入点对应的第二公钥对所述主密钥进行加密的密文。

15.根据权利要求10所述的方法，其特征在于，向所述认证服务器发送第二接入请求之前，还包括：

生成与所述无线接入点对应的第二公钥和第二私钥；

获取与所述认证服务器对应的第一公钥；

向所述认证服务器发送身份认证请求，所述身份认证请求携带有认证信息和与所述无线接入点对应的第二公钥，所述认证信息和与所述无线接入点对应的第二公钥均使用与所述认证服务器对应的第一公钥进行加密，所述认证信息至少包括硬件信息和/或拥有者信息。

16.根据权利要求15所述的方法，其特征在于，所述认证信息是通过与所述无线接入点对应的第二私钥进行加密的信息。

17.根据权利要求10至16任一所述的方法，其特征在于，所述与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接，包括：

与所述用户终端使用各自持有的所述主密钥，协商生成本次连接所使用的临时密钥，根据所述临时密钥与所述用户终端建立加密无线网络连接。

18.一种无线网络连接方法，其特征在于，所述方法包括：

接收无线接入点发送的第二接入请求，所述第二接入请求中携带第一密文和与所述无线接入点对应的第二公钥，所述第一密文包括用户终端的用户名，所述第一密文是所述无线接入点通过与所述无线接入点对应的第二私钥对所述用户名进行加密的密文；

在接收到所述第二接入请求后，验证所述无线接入点是否属于可信任无线接入点；

在所述无线接入点属于所述可信任无线接入点时，使用与所述无线接入点对应的第二公钥对所述第二接入请求中携带的第一密文进行解密，得到所述用户名；查询与所述用户名对应的密钥信息；根据所述密钥信息与用户终端进行第一身份认证；

在所述第一身份认证成功时，与所述用户终端协商生成主密钥，并向所述用户终端发送所述主密钥；

向所述无线接入点发送与所述用户名对应的所述主密钥，以便所述无线接入点与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接。

19.根据权利要求18所述的方法，其特征在于，所述验证所述无线接入点是否属于可信任无线接入点，包括：

获取所述第二接入请求中携带的第一密文和与所述无线接入点对应的第二公钥；

验证与所述无线接入点对应的第二公钥是否存在于可信任公钥集合中；若与所述无线接入点对应的第二公钥存在于所述可信任公钥集合中，则将所述无线接入点验证为所述可信任无线接入点；

其中，所述可信任公钥集合存储有成功通过第二身份认证的无线接入点对应的第二公钥。

20.根据权利要求19所述的方法，其特征在于，所述获取所述第二接入请求中携带的第一密文和与所述无线接入点对应的第二公钥，包括：

通过与所述认证服务器对应的第一私钥对所述第二接入请求进行解密，得到第一密文和与所述无线接入点对应的第二公钥；

其中，所述第二接入请求是所述无线接入点通过与所述认证服务器对应的第一公钥对所述第一密文和与所述无线接入点对应的第二公钥进行加密的请求。

21.根据权利要求19或20所述的方法，其特征在于，所述向所述无线接入点发送与所述用户名对应的所述主密钥，包括：

使用与所述无线接入点对应的第二公钥对协商生成的所述主密钥进行第一加密，向所述无线接入点发送第一加密后的所述主密钥。

22.根据权利要求21所述的方法，其特征在于，所述向所述无线接入点发送第一加密后的所述主密钥，包括：

使用与所述认证服务器对应的第一私钥对第一加密后的所述主密钥进行第二加密，向所述无线接入点发送第二加密后的所述主密钥。

23.根据权利要求18至20、22任一所述的方法，其特征在于，所述接收无线接入点发送的第二接入请求之前，还包括：

接收所述无线接入点发送的身份认证请求，所述身份认证请求携带有认证信息和与所述无线接入点对应的第二公钥，所述认证信息和与所述无线接入点对应的第二公钥均使用与所述认证服务器对应的第一公钥进行加密，所述认证信息至少包括硬件信息和/或拥有者信息；

通过与所述认证服务器对应的第一私钥对所述身份认证请求进行解密，得到所述认证信息和与所述无线接入点对应的第二公钥；

对所述认证信息进行第二身份认证，在所述第二身份认证成功时，将与所述无线接入点对应的第二公钥添加至所述可信任公钥集合中。

24.根据权利要求23所述的方法，其特征在于，所述认证信息是所述无线接入点通过与所述无线接入点对应的第二私钥进行加密的信息；

所述对所述认证信息进行第二身份认证，包括：

通过与所述无线接入点对应的第二公钥对所述认证信息进行解密，得到所述硬件信息和/或所述拥有者信息；

对所述硬件信息和/或所述拥有者信息进行第二身份认证，在所述第二身份认证成功时，将与所述无线接入点对应的第二公钥添加至所述可信任公钥集合中。

25.一种无线网络连接装置，其特征在于，所述装置包括：

第一接收模块，用于接收用户终端发送的第一接入请求，所述第一接入请求携带有所述用户终端的用户名；

第二接收模块，用于向认证服务器发送第二接入请求，所述第二接入请求中携带第一密文和与无线接入点对应的第二公钥，所述第一密文包括所述用户名，所述第一密文是所述无线接入点通过与所述无线接入点对应的第二私钥对所述用户名进行加密的密文；

密钥接收模块，用于接收所述认证服务器发送的与所述用户名对应的主密钥，所述主密钥是所述认证服务器在接收到所述第二接入请求后，验证无线接入点属于可信任无线接入点时，使用与所述无线接入点对应的第二公钥对所述第二接入请求中携带的第一密文进行解密，得到所述用户名；查询与所述用户名对应的密钥信息；根据所述密钥信息与用户终端进行第一身份认证成功后协商生成的密钥；

网络连接模块，用于与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接。

26.根据权利要求25所述的装置，其特征在于，所述密钥接收模块，还用于接收所述认证服务器发送的第一加密后的主密钥，所述第一加密后的主密钥是所述认证服务器在所述无线接入点属于所述可信任无线接入点时，使用与所述无线接入点对应的第二公钥对所述主密钥进行加密后的主密钥。

27.根据权利要求25所述的装置，其特征在于，所述密钥接收模块，还用于接收所述认证服务器发送的第二加密后的主密钥，所述第二加密后的主密钥是所述认证服务器在所述无线接入点属于所述可信任无线接入点时，使用与所述无线接入点对应的第二公钥对所述主密钥进行第一加密，再使用与所述认证服务器对应的第一私钥对第一加密后的所述主密钥进行第二加密后的主密钥。

28.根据权利要求26所述的装置，其特征在于，所述网络连接模块，包括：

第一解密单元，用于使用与所述无线接入点对应的第二私钥对所述第一加密后的主密钥进行解密，得到所述主密钥；

第一连接单元，用于与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接。

29.根据权利要求27所述的装置，其特征在于，所述网络连接模块，包括：

第二解密单元，用于使用与所述认证服务器对应的第一公钥对第二加密后的所述主密钥进行解密，得到第二密文；

第三解密单元，用于使用与所述无线接入点对应的第二私钥对所述第二密文进行解密，得到所述主密钥；

第二连接单元，用于与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接；

其中，所述第二密文是所述认证服务器通过与所述无线接入点对应的第二公钥对所述主密钥进行加密的密文。

30.根据权利要求25所述的装置，其特征在于，所述装置还包括：

密钥生成模块，用于生成与所述无线接入点对应的第二公钥和第二私钥；

公钥获取模块，用于获取与所述认证服务器对应的第一公钥；

信息发送模块，用于向所述认证服务器发送身份认证请求，所述身份认证请求携带有认证信息和与所述无线接入点对应的第二公钥，所述认证信息和与所述无线接入点对应的第二公钥均使用与所述认证服务器对应的第一公钥进行加密，所述认证信息至少包括硬件信息和/或拥有者信息。

31.根据权利要求30所述的装置，其特征在于，所述认证信息是通过与所述无线接入点对应的第二私钥进行加密的信息。

32.根据权利要求25至31任一所述的装置，其特征在于，所述网络连接模块，还用于与所述用户终端使用各自持有的所述主密钥，协商生成本次连接所使用的临时密钥，使用所述临时密钥与所述用户终端建立加密无线网络连接。

33.一种无线网络连接装置，其特征在于，所述装置包括：

请求接收模块，用于接收无线接入点发送的第二接入请求，所述第二接入请求中携带第一密文和与所述无线接入点对应的第二公钥，所述第一密文包括用户终端的用户名，所述第一密文是所述无线接入点通过与所述无线接入点对应的第二私钥对所述用户名进行加密的密文；

信任验证模块，用于在接收到所述第二接入请求后，验证所述无线接入点是否属于可信任无线接入点；

用户认证模块，用于在所述无线接入点属于所述可信任无线接入点时与用户终端进行第一身份认证；

密钥生成模块，用于在所述第一身份认证成功时，使用与所述无线接入点对应的第二公钥对所述第二接入请求中携带的第一密文进行解密，得到所述用户名；查询与所述用户名对应的密钥信息；根据所述密钥信息与所述用户终端协商生成主密钥，并向所述用户终端发送所述主密钥；

密钥发送模块，用于向所述无线接入点发送与所述用户名对应的所述主密钥，以便所述无线接入点与用户终端根据各自持有的所述主密钥与用户终端协商建立加密无线网络连接。

34.根据权利要求33所述的装置，其特征在于，所述信任验证模块，包括：

公钥获取单元，用于获取所述第二接入请求中携带的第一密文和与所述无线接入点对应的第二公钥；

第一验证单元，用于验证与所述无线接入点对应的第二公钥是否存在于可信任公钥集合中；若与所述无线接入点对应的第二公钥存在于所述可信任公钥集合中，则将所述无线接入点验证为所述可信任无线接入点；

其中，所述可信任公钥集合存储有成功通过身份认证的无线接入点对应的第二公钥。

35.根据权利要求34所述的装置，其特征在于，所述公钥获取单元，还用于通过与所述认证服务器对应的第一私钥对所述第二接入请求进行解密，得到第一密文和与所述无线接入点对应的第二公钥；

其中，所述第二接入请求是所述无线接入点通过与所述认证服务器对应的第一公钥对所述第一密文和与所述无线接入点对应的第二公钥进行加密的请求。

36.根据权利要求34或35所述的装置，其特征在于，所述密钥发送模块，还用于使用与所述无线接入点对应的第二公钥对协商生成的所述主密钥进行第一加密，向所述无线接入点发送第一加密后的所述主密钥。

37.根据权利要求36所述的装置，其特征在于，所述密钥发送模块，还用于使用与所述认证服务器对应的第一私钥对第一加密后的所述主密钥进行第二加密，向所述无线接入点发送第二加密后的所述主密钥。

38.根据权利要求33至35、37任一所述的装置，其特征在于，所述装置，还包括：

认证接收模块，用于接收所述无线接入点发送的身份认证请求，所述身份认证请求携带有认证信息和与所述无线接入点对应的第二公钥，所述认证信息和与所述无线接入点对应的第二公钥均使用与所述认证服务器对应的第一公钥进行加密，所述认证信息至少包括硬件信息和/或拥有者信息；

信息解密模块，用于通过与所述认证服务器对应的第一私钥对所述身份认证请求进行解密，得到所述认证信息和与所述无线接入点对应的第二公钥；

信息认证模块，用于对所述认证信息进行第二身份认证，在所述第二身份认证成功时，将与所述无线接入点对应的第二公钥添加至所述可信任公钥集合中。

39.根据权利要求38所述的装置，其特征在于，所述认证信息是所述无线接入点通过与所述无线接入点对应的第二私钥进行加密的信息；

所述信息认证模块，包括：

第一解密单元，用于通过与所述无线接入点对应的第二公钥对所述认证信息进行解密，得到所述硬件信息和/或所述拥有者信息；

第一认证单元，用于对所述硬件信息和/或所述拥有者信息进行第二身份认证，在所述第二身份认证成功时，将与所述无线接入点对应的第二公钥添加至所述可信任公钥集合中。

40.一种无线网络连接系统，其特征在于，所述系统包括：用户终端、无线接入点和认证服务器；

所述用户终端，用于向无线接入点发送第一接入请求，以及与所述认证服务器进行第一身份认证；

所述无线接入点包括如权利要求25至32任一所述的无线网络连接装置；

所述认证服务器包括如权利要求33至39任一所述的无线网络连接装置。

无线网络连接方法、装置及系统

技术领域

[0001] 本发明实施例涉及网络安全领域，特别涉及一种无线网络连接方法、装置及系统。

背景技术

[0002] 随着用户终端的广泛使用，无线网络成为用户终端接入互联网的一种重要形式。常见的无线网络是Wi-Fi(Wireless-Fidelity，无线保真)网络。目前的大部分商业场所均提供有公众Wi-Fi，供用户免费使用。

[0003] 现有技术中，用户终端接入公众Wi-Fi的方式主要包括：无密码接入、验证码接入和单一密码接入三种方式。其中：无密码接入是指用户终端在获取到公众Wi-Fi的SSID(Service Set Identifier，服务集标识)后，向无线接入点发送接入请求，无线接入点无需验证，直接允许用户终端接入该公众Wi-Fi；验证码接入是指用户终端在接入公众Wi-Fi时需要获取公众Wi-Fi的SSID和验证码，通过将验证码和SSID向无线接入点发送接入请求，无线接入点对验证码和SSID进行验证，在验证成功后，允许用户终端接入该公众Wi-Fi，验证码通常具有有效期，比如60s；单一密码接入是指用户终端在接入公众Wi-Fi时，预先获取该公众Wi-Fi的SSID和连接密码，通过将该SSID和连接密码向无线接入点发送接入请求；无线接入点对SSID和连接密码进行验证；在无线接入点验证成功后，允许用户终端接入该公众Wi-Fi，连接密码通常是长期有效的。

[0004] 在实现本发明实施例的过程中，发明人发现现有技术至少存在以下问题：由于黑客可以设置假冒的公众Wi-Fi，该假冒的公众Wi-Fi与真实的公众Wi-Fi具有完全相同的硬件信息，比如SSID。当用户使用上述三种接入方式中的任意一种方式将用户终端接入假冒的公众Wi-Fi后，用户终端向假冒的公众Wi-Fi所传输的数据以及用户终端内部的数据均会受到安全威胁。

发明内容

[0005] 为了解决用户使用现有的接入方法使得用户终端接入假冒的公众Wi-Fi后，导致用户终端向假冒的公众Wi-Fi所传输的数据以及用户终端内部的数据均会受到安全威胁的问题，本发明实施例提供了一种无线网络连接方法、装置及系统。所述技术方案如下：

[0006] 根据本发明实施例的第一方面，提供了一种无线网络连接方法，所述方法包括：

[0007] 用户终端向无线接入点发送第一接入请求，所述第一接入请求携带有所述用户终端的用户名；

[0008] 所述无线接入点向所述认证服务器发送第二接入请求，所述第二接入请求携带有所述用户名；

[0009] 所述认证服务器在接收到所述第二接入请求后，验证所述无线接入点是否属于可信任无线接入点，在所述无线接入点属于所述可信任无线接入点时与所述用户终端进行第一身份认证；

[0010] 在所述第一身份认证成功时，所述认证服务器与所述用户终端协商生成主密钥，

并向所述用户终端发送所述主密钥；

[0011] 所述认证服务器向所述无线接入点发送与所述用户名对应的所述主密钥；

[0012] 所述无线接入点与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接。

[0013] 根据本发明实施例的第二方面，提供了一种无线网络连接方法，所述方法包括：

[0014] 接收用户终端发送的第一接入请求，所述第一接入请求携带有所述用户终端的用户名；

[0015] 向所述认证服务器发送第二接入请求，所述第二接入请求携带有所述用户名；

[0016] 接收所述认证服务器发送的与所述用户名对应的主密钥，所述主密钥是所述认证服务器在接收到所述第二接入请求后，验证无线接入点属于可信任无线接入点时，与用户终端进行第一身份认证成功后协商生成的密钥；

[0017] 与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接。

[0018] 根据本发明实施例的第三方面，提供了一种无线网络连接方法，所述方法包括：

[0019] 接收无线接入点发送的第二接入请求，所述第二接入请求携带有所述用户名；

[0020] 在接收到所述第二接入请求后，验证所述无线接入点是否属于可信任无线接入点；

[0021] 在所述无线接入点属于所述可信任无线接入点时与用户终端进行第一身份认证；

[0022] 在所述第一身份认证成功时，与所述用户终端协商生成主密钥，并向所述用户终端发送所述主密钥；

[0023] 向所述无线接入点发送与所述用户名对应的所述主密钥，以便所述无线接入点与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接。

[0024] 根据本发明实施例的第四方面，提供了一种无线网络连接装置，所述装置包括：

[0025] 第一接收模块，用于接收用户终端发送的第一接入请求，所述第一接入请求携带有所述用户终端的用户名；

[0026] 第二接收模块，用于向所述认证服务器发送第二接入请求，所述第二接入请求携带有所述用户名；

[0027] 密钥接收模块，用于接收所述认证服务器发送的与所述用户名对应的主密钥，所述主密钥是所述认证服务器在接收到所述第二接入请求后，验证无线接入点属于可信任无线接入点时，与用户终端进行第一身份认证成功后协商生成的密钥；

[0028] 网络连接模块，用于与所述用户终端根据各自持有的所述主密钥协商建立加密无线网络连接。

[0029] 根据本发明实施例的第五方面，提供了一种无线网络连接装置，所述装置包括：

[0030] 请求接收模块，用于接收无线接入点发送的第二接入请求，所述第二接入请求携带有所述用户名；

[0031] 信任验证模块，用于在接收到所述第二接入请求后，验证所述无线接入点是否属于可信任无线接入点；

[0032] 用户认证模块，用于在所述无线接入点属于所述可信任无线接入点时与用户终端进行第一身份认证；

[0033] 密钥生成模块，用于在所述第一身份认证成功时，与所述用户终端协商生成主密

钥，并向所述用户终端发送所述主密钥；

[0034] 密钥发送模块，用于向所述无线接入点发送与所述用户名对应的所述主密钥，以便所述无线接入点与用户终端根据各自持有的所述主密钥与用户终端协商建立加密无线网络连接。

[0035] 根据本发明实施例的第六方面，提供了一种无线网络连接系统，所述系统包括：用户终端、无线接入点和认证服务器；

[0036] 所述用户终端，用于向无线接入点发送第一接入请求，以及与所述认证服务器进行第一身份认证；

[0037] 所述无线接入点包括如上述第四方面所述的无线网络连接装置；

[0038] 所述认证服务器包括如上述第五方面所述的无线网络连接装置。

[0039] 本发明实施例提供的技术方案带来的有益效果是：

[0040] 通过用户终端向无线接入点发送第一接入请求；无线接入点向认证服务器发送第二接入请求；认证服务器在接收到第二接入请求后，验证无线接入点是否属于可信任无线接入点，在无线接入点属于可信任无线接入点时与用户终端进行第一身份认证，在第一身份认证成功时，与用户终端协商生成主密钥，并向用户终端发送主密钥；认证服务器向无线接入点发送与用户名对应的主密钥；无线接入点根据主密钥与用户终端协商建立加密无线网络连接；解决了用户使用现有的接入方法使得用户终端接入假冒的公众Wi-Fi时，导致用户终端向假冒的公众Wi-Fi所传输的数据以及用户终端内部的数据均会受到安全威胁的问题；达到了通过认证服务器对无线接入点进行身份认证，只有可信任无线接入点才能获取与用户名对应的主密钥，从而根据主密钥与用户终端建立加密无线网络连接，提高了用户终端传输的数据以及用户终端内部的数据安全性的效果。

附图说明

[0041] 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。

[0042] 图1是本发明一个示例性实施例提供的无线网络连接系统的结构示意图；

[0043] 图2是本发明一个实施例提供的无线网络连接方法的流程图；

[0044] 图3是本发明另一个实施例提供的无线网络连接方法的流程图；

[0045] 图4是本发明再一个实施例提供的无线网络连接方法的流程图；

[0046] 图5A是本发明还一个实施例提供的无线网络接入方法的流程图；

[0047] 图5B是本发明一个实施例提供的认证服务器对无线接入点的身份认证过程的示意图；

[0048] 图5C是本发明一个实施例提供的用户终端向认证服务器注册用户名和密钥信息过程的示意图；

[0049] 图5D是本发明一个实施例提供的用户终端接入无线接入点过程的示意图；

[0050] 图6是本发明一个实施例提供的无线网络连接装置的结构方框图；

[0051] 图7是本发明另一个实施例提供的无线网络连接装置的结构方框图；

[0052] 图8是本发明一个实施例提供的无线网络连接装置的结构方框图；

[0053] 图9是本发明另一个实施例提供的无线网络连接装置的结构方框图；

[0054] 图10是本发明一个实施例提供的一种无线网络连接系统的结构方框图。

具体实施方式

[0055] 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。

[0056] 为了便于理解，首先介绍一些本发明实施例所涉及的技术概念。

[0057] 公钥和私钥

[0058] 公钥是指公开的密钥，不需要进行保密，解密方可以通过各种渠道获取；而私钥是指仅由加密方自身持有的密钥，需要进行保密。一个公钥对应一个私钥；公钥和私钥共同组成了一种不对称加密方式。不对称加密方式是指用公钥加密的信息只能用对应的私钥进行解密，使用私钥加密的信息也只能用对应的公钥进行解密。也即，加密和解密使用的密钥是不相同的。

[0059] 比如：假定A要向B发送加密信息，则A首先要获取与B对应的公钥，然后使用与B对应的公钥对需要发送的信息进行加密后，将加密后的信息发送给B，B在接收到A发送的加密的信息后，必须使用与B对应的私钥才可以对加密的信息进行解密，获取加密的信息中的内容。由于与B对应的私钥只有B自己拥有，因此A发送的加密的信息是安全的。

[0060] 请参考图1，其示出了本发明一个示例性实施例提供的无线网络连接系统的结构示意图。该无线网络连接系统包括：无线接入点120、用户终端140和认证服务器160。

[0061] 无线接入点120可以是路由器、Wi-Fi热点和无线网关等提供无线网络接入服务的设备的统称。本发明实施例中，以无线接入点120是路由器来举例说明。无线接入点120在与用户终端140建立无线网络连接之前，需要通过认证服务器160对该无线接入点120的身份认证。无线接入点120与认证服务器160之间通过无线网络或有线网络建立连接。本发明实施例对无线接入点120和认证服务器160之间的通信方式不做限定。

[0062] 用户终端140可以是手机、平板电脑、电子书阅读器、MP3(Moving Picture Experts Group Audio Layer III，动态影像专家压缩标准音频层面3)播放器、MP4(Moving Picture Experts Group Audio Layer IV，动态影像专家压缩标准音频层面4)播放器、膝上型便携计算机和台式计算机等等。可选的，用户终端140中安装有具有扫码功能的应用程序，比如，腾讯QQ、微信、QQ浏览器、无线上网程序等。

[0063] 用户终端140与认证服务器160之间通过无线网络或有线网络建立连接。可选的，用户终端140通过独立通道向认证服务器160注册用户名和密钥信息，其中，独立通道是指不经过无线接入点的通信通道，比如：2G网络、3G网络等。本发明实施例对用户终端140和认证服务器160之间的通信方式不做限定。

[0064] 认证服务器160中存储有可信任公钥集合、每个用户终端140对应的用户名和密钥信息。认证服务器160可以是一台服务器、多台服务器组成的服务器集群或云计算中心。

[0065] 请参考图2，其示出了本发明一个实施例提供的无线网络连接方法的流程图。本实施例以该无线网络连接方法应用于图1所示的无线接入点120中来举例说明。该方法包括：

[0066] 步骤201，接收用户终端发送的第一接入请求，第一接入请求携带有用户终端的用

户名；

[0067] 步骤202，向认证服务器发送第二接入请求，第二接入请求携带有用户名；

[0068] 步骤203，接收认证服务器发送的与用户名对应的主密钥，主密钥是认证服务器在接收到第二接入请求后，验证无线接入点属于可信任无线接入点时，与用户终端进行第一身份认证成功后协商生成的密钥；

[0069] 步骤204，与用户终端根据各自持有的主密钥协商建立加密无线网络连接。

[0070] 综上所述，本实施例提供的无线网络接入方法，接收用户终端发送的第一接入请求；向认证服务器发送第二接入请求；接收认证服务器发送的与用户名对应的主密钥；根据主密钥与用户终端协商建立加密无线网络连接；解决了用户使用现有的接入方法使得用户终端接入假冒的公众Wi-Fi时，导致用户终端向假冒的公众Wi-Fi所传输的数据以及用户终端内部的数据均会受到安全威胁的问题；达到了通过认证服务器对无线接入点进行身份认证，只有可信任无线接入点才能获取与用户名对应的主密钥，从而根据主密钥与用户终端建立加密无线网络连接，提高了用户终端传输的数据以及用户终端内部的数据安全性的效果。

[0071] 请参考图3，其示出了本发明一个实施例提供的无线网络连接方法的流程图。本实施例以该无线网络连接方法应用于图1所示的认证服务器160中来举例说明。该方法包括：

[0072] 步骤301，接收无线接入点发送的第二接入请求，第二接入请求携带有用户名。

[0073] 步骤302，在接收到第二接入请求后，验证无线接入点是否属于可信任无线接入点。

[0074] 步骤303，在无线接入点属于可信任无线接入点时与用户终端进行第一身份认证。

[0075] 步骤304，在第一身份认证成功时，与用户终端协商生成主密钥，并向用户终端发送主密钥。

[0076] 步骤305，向无线接入点发送与用户名对应的主密钥，以便无线接入点与用户终端根据各自持有的主密钥协商建立加密无线网络连接。

[0077] 综上所述，本实施例提供的无线网络接入方法，通过接收无线接入点发送的第二接入请求；在接收到第二接入请求后，验证无线接入点是否属于可信任无线接入点；在无线接入点属于可信任无线接入点时与用户终端进行第一身份认证；在第一身份认证成功时，与用户终端协商生成主密钥，并向用户终端发送主密钥；向无线接入点发送与用户名对应的主密钥；解决了用户使用现有的接入方法使得用户终端接入假冒的公众Wi-Fi时，导致用户终端向假冒的公众Wi-Fi所传输的数据以及用户终端内部的数据均会受到安全威胁的问题；达到了通过认证服务器对无线接入点进行身份认证，只有可信任无线接入点才能获取与用户名对应的主密钥，从而根据主密钥与用户终端建立加密无线网络连接，提高了用户终端传输的数据以及用户终端内部的数据安全性的效果。

[0078] 请参考图4，其示出了本发明一个实施例提供的无线网络连接方法的流程图。本实施例以该无线网络连接方法应用于图1所示的无线网络接入系统中来举例说明。该方法包括：

[0079] 步骤401，用户终端向无线接入点发送第一接入请求，第一接入请求携带有用户终端的用户名。

[0080] 用户终端存储有预先在认证服务器中注册的用户名和密钥信息。

[0081] 对应地，无线接入点接收用户终端发送的第一接入请求。

[0082] 步骤402，无线接入点向认证服务器发送第二接入请求，第二接入请求携带有用户名。

[0083] 第二接入请求中携带有与无线接入点对应的第二公钥。

[0084] 对应地，认证服务器接收无线接入点发送的第二接入请求。

[0085] 步骤403，认证服务器在接收到第二接入请求后，验证无线接入点是否属于可信任无线接入点。

[0086] 步骤404，在无线接入点属于可信任无线接入点时，认证服务器与用户终端进行第一身份认证。

[0087] 在无线接入点属于可信任无线接入点时，认证服务器与用户终端进行双向身份认证，认证服务器对用户终端进行身份认证，认证用户终端是否可信；同时用户终端对认证服务器也进行认证。

[0088] 步骤405，在第一身份认证成功时，认证服务器与用户终端协商生成主密钥，并向用户终端发送主密钥。

[0089] 对应地，用户终端接收认证服务器发送的与用户名对应的主密钥。

[0090] 步骤406，认证服务器向无线接入点发送与用户名对应的主密钥。

[0091] 对应地，无线接入点接收认证服务器发送的与用户名对应的主密钥。

[0092] 步骤407，无线接入点与用户终端根据各自持有的主密钥协商建立加密无线网络连接。

[0093] 综上所述，本实施例提供的无线网络接入方法，通过用户终端向无线接入点发送第一接入请求；无线接入点向认证服务器发送第二接入请求；认证服务器在接收到第二接入请求后，验证无线接入点是否属于可信任无线接入点，在无线接入点属于可信任无线接入点时，认证服务器与用户终端进行第一身份认证；在第一身份认证成功时，认证服务器与用户终端协商生成主密钥，并向用户终端发送主密钥；认证服务器向无线接入点发送与用户名对应的主密钥；无线接入点与用户终端根据各自持有的主密钥协商建立加密无线网络连接；解决了用户使用现有的接入方法使得用户终端接入假冒的公众Wi-Fi时，导致用户终端向假冒的公众Wi-Fi所传输的数据以及用户终端内部的数据均会受到安全威胁的问题；达到了通过认证服务器对无线接入点进行身份认证，只有可信任无线接入点才能获取与用户名对应的主密钥，从而根据主密钥与用户终端建立加密无线网络连接，提高了用户终端传输的数据以及用户终端内部的数据安全性的效果。

[0094] 在一个具体的例子中，本发明实施例的整个过程包括四个阶段：

[0095] 第一、无线接入点根据与无线接入点对应的第二公钥和第二私钥，在认证服务器中完成身份认证，认证服务器将完成身份认证的无线接入点对应的第二公钥添加至可信任公钥集合中；

[0096] 第二、用户终端通过独立通道在认证服务器中注册用户名和密钥信息，认证服务器将用户终端注册的用户名和密钥信息反馈给用户终端；可选地，密钥信息是密码或者证书。

[0097] 第三、用户终端向无线接入点发送第一接入请求，第一接入请求中携带有用户名，无线接入点向认证服务器发送第二接入请求，第二接入请求携带有用户名和与无线接入点

对应的第二公钥。

[0098] 第四、认证服务器对无线接入点进行验证，在无线接入点是可信任无线接入点时，与用户终端进行第一身份认证；在第一身份认证成功时，与用户终端根据各自持有的密钥信息协商生成主密钥，并将与用户名对应的主密钥分别发送给用户终端和无线接入点；无线接入点与用户终端根据各自持有的主密钥协商建立加密无线网络连接。

[0099] 请参考图5A，其示出了本发明另一个实施例提供的无线网络接入方法的流程图。本实施例以该无线网络接入方法应用于图1所示的无线网络接入系统中来举例说明。该方法包括：

[0100] 第一阶段，包括步骤501至步骤506；

[0101] 步骤501，无线接入点生成与无线接入点对应的第二公钥和第二私钥。

[0102] 无线接入点在使用之前，首先生成与无线接入点对应的第二公钥和第二私钥。第二私钥由无线接入点自身来保存。

[0103] 步骤502，无线接入点获取与认证服务器对应的第一公钥。

[0104] 无线接入点在生成第二公钥和第二私钥后，获取认证服务器对应的第一公钥。

[0105] 可选的，无线接入点首先获取认证服务器对应的第一公钥后，再生成与无线接入点对应的第二公钥和第二私钥。

[0106] 可选的，与认证服务器对应的第一公钥存储在无线接入点的固件中，无线接入点直接从固件中获取与认证服务器对应的第一公钥。

[0107] 本实施例中，对无线接入点获取认证服务器对应的第一公钥和生成与无线接入点对应的第二公钥和第二私钥的先后顺序不作具体限定。

[0108] 步骤503，无线接入点向认证服务器发送身份认证请求。

[0109] 身份认证请求携带有认证信息和与无线接入点对应的第二公钥，认证信息和与无线接入点对应的第二公钥均使用与认证服务器对应的第一公钥进行加密，认证信息至少包括硬件信息和/或拥有者信息。

[0110] 可选地，认证信息是无线接入点通过与无线接入点对应的第二私钥进行加密的信息。

[0111] 可选的，无线接入点直接将硬件信息和拥有者信息发送给认证服务器；或者，无线接入点只将硬件信息发送给认证服务器，拥有者信息有管理终端间接发送给认证服务器。

[0112] 本实施例中，对向认证服务器发送认证信息的方式不作具体限定。本实施例中以无线接入点向认证服务器发送硬件信息和拥有者信息为例进行举例说明。

[0113] 无线接入点在获取到认证服务器对应的第一公钥后，与认证服务器建立加密通道。无线接入点通过加密通道将认证信息和与无线接入点对应的第二公钥携带在身份认证请求中发送给认证服务器。

[0114] 加密通道是指：将无线接入点向认证服务器发送的信息均使用与认证服务器对应的第一公钥进行加密，认证服务器在接收到无线接入点发送的加密信息后，需要使用认证服务器的第一私钥进行解密后获取其中的信息；认证服务器向无线接入点发送的信息均使用与无线接入点对应的第二公钥进行加密，无线接入点在接收到认证服务器发送的加密信息后，必须使用与无线接入点对应的第二私钥进行解密后才能获取其中的信息。

[0115] 可选的，与无线接入点对应的硬件信息可以包括：无线接入点的服务集标识、无线

接入点的BSSID(Basic Service Set Identifier,基本服务集标识)、无线接入点的MAC(Media Access Control,设备的物理地址)、无线接入点的网络地址和无线接入点的网关IP(Internet Protocol,互联网协议)等。

[0116] 本实施例中,对无线接入点将第二公钥提供给认证服务器的方式不作具体限定。

[0117] 与无线接入点对应的拥有者信息可以包括:管理员帐号、商家名称、注册公司、商家地址和商家电话等信息。

[0118] 可选的,无线接入点可以将认证信息和与无线接入点对应的第二公钥分别单独发送给认证服务器;比如:无线接入点先通过与认证服务器对应的第一公钥对与无线接入点对应的第二公钥进行加密后发送给认证服务器,再通过与无线接入点对应的第二公钥对认证信息进行加密后发送给认证服务器;认证服务器首先根据与认证服务器对应的第一私钥解密得到与无线接入点对应的第二公钥;再使用与无线接入点对应的第二公钥对加密后的认证信息进行解密得到认证信息。

[0119] 作为第一种可能的实现方式,无线接入点直接将身份认证请求发送给认证服务器,身份认证请求中携带有与无线接入点对应的第二公钥、硬件信息和/或拥有者信息;

[0120] 作为第二种可能的实现方式,无线接入点使用与认证服务器对应的第一公钥对身份认证请求进行加密,身份认证请求中携带有与无线接入点对应的第二公钥、硬件信息和/或拥有者信息;

[0121] 作为第三种可能的实现方式,无线接入点使用与认证服务器对应的第一公钥对身份认证请求进行加密,身份认证请求包括认证信息和与无线接入点对应的第二公钥;认证信息是无线接入点使用与无线接入点对应的第二私钥进行加密的信息;认证信息携带有硬件信息和/或拥有者信息。

[0122] 对应地,认证服务器接收无线接入点发送的身份认证请求。

[0123] 本实施例中以无线接入点使用与认证服务器对应的第一公钥对身份认证请求进行加密,身份认证请求包括认证信息和与无线接入点对应的第二公钥;并使用与无线接入点对应的第二私钥对认证信息进行加密为例进行举例说明。

[0124] 步骤504,认证服务器通过与认证服务器对应的第一私钥对身份认证请求进行解密,得到认证信息和与无线接入点对应的第二公钥。

[0125] 认证服务器在接收到无线接入点发送的身份认证请求后,通过与认证服务器对应的第一私钥对身份认证请求进行解密,得到身份认证请求携带的认证信息和与无线接入点对应的第二公钥。

[0126] 步骤505,认证服务器通过与无线接入点对应的第二公钥对认证信息进行解密,得到硬件信息和/或拥有者信息。

[0127] 认证服务器通过与认证服务器对应的第一私钥解密得到认证信息和与无线接入点对应的第二公钥后,通过与无线接入点对应的第二公钥对认证信息进行解密,得到认证信息包括的硬件信息和/或拥有者信息。

[0128] 步骤506,认证服务器对硬件信息和/或拥有者信息进行第二身份认证,在第二身份认证成功时,将与无线接入点对应的第二公钥添加至可信任公钥集合中。

[0129] 认证服务器在解密得到认证信息中携带的硬件信息和/或拥有者信息后,对硬件信息和/或拥有者信息进行第二身份认证。可选地,该第二身份认证过程是人工审核过程。

[0130] 其中，第二身份认证是指核实认证信息中携带的硬件信息和/或拥有者信息是否正确或完整。在第二身份认证成功后，认证服务器将与无线接入点对应的第二公钥添加至可信任公钥集合中，并保存与无线接入点对应的第二公钥。可信任公钥集合是认证服务器存储的成功通过第二身份认证的无线接入点对应的第二公钥的列表。也即，可信任公钥集合中对应的无线接入点都是经过认证服务器第二身份认证成功的无线接入点。

[0131] 可选的，在第二身份认证成功后，认证服务器将无线接入点对应的第二公钥与无线接入点的对应关系添加至可信任公钥集合中，允许用户终端向认证服务器查询该无线接入点，并认证该无线接入点是否为可信任无线接入点；同时，认证服务器允许该无线接入点向认证服务器查询用户终端的用户名对应的主密钥。

[0132] 示例性地，可信任公钥集合如下表一所示：

[0133]

无线接入点	第二公钥
接入点A	公钥1
接入点B	公钥2
接入点C	公钥3
接入点D	公钥4

[0134] 表一

[0135] 如表一所示，无线接入点A对应的第二公钥为“公钥1”；无线接入点B对应的第二公钥为“公钥2”；无线接入点C对应的第二公钥为“公钥3”；无线接入点D对应的第二公钥为“公钥4”。

[0136] 认证服务器对无线接入点的第二身份认证过程如图5B所示。在图5B中，无线接入点120向认证服务器160发送硬件信息，注册该无线接入点120的商家终端180向认证服务器160发送拥有者信息和管理员信息，认证服务器160对接收到的硬件信息、拥有者信息和管理员信息进行身份认证，在第二身份认证成功后，批准该无线接入点120加入可信任无线接入点中。

[0137] 第二阶段，包括步骤507；

[0138] 步骤507，用户终端通过独立通道向认证服务器注册用户名和与用户名对应的密钥信息。

[0139] 独立通道是不经过无线接入点的通信通道。

[0140] 可选的，密钥信息包括密码和证书中的至少一种。

[0141] 认证服务器在生成与用户终端对应的用户名和密钥信息时，将用户终端与用户名和密钥信息之间的对应关系存储至认证服务器中，并将用户名和密钥信息发送给用户终端。

[0142] 可选的，认证服务器将用户终端注册的用户名和密钥信息以用户名密码对的形式进行存储，或者认证服务器将用户终端注册的用户名和密钥信息以用户名证书对的形式进行存储。

[0143] 示例性地，认证服务器以用户名密码对的形式进行存储的对应关系如下表二所示：

[0144]

用户名	密码
用户A	密码1
用户B	密码2
用户C	密码3

[0145] 表二

[0146] 可选的，用户终端向认证服务器注册的用户名和密钥信息是唯一的。也即，每一个用户终端对应唯一一个用户名和密钥信息，用户终端与用户名之间是一一对应的关系。

[0147] 用户终端向认证服务器注册用户名和密钥信息的过程如图5C所示，以用户终端向认证服务器注册用户名和密码为例进行举例说明。在图5C中，用户终端140与认证服务器160之间通过独立通道完成用户名和密码的注册，也即，用户名和密码的注册过程在不经过无线接入点的通信通道中完成的。

[0148] 可选的，用户终端向认证服务器注册用户名和密钥信息时，可以通过用户终端中的通信类客户端或浏览器客户端等向认证服务器注册用户名和密钥信息。

[0149] 第三阶段，包括步骤508和步骤509；

[0150] 步骤508，用户终端向无线接入点发送第一接入请求。第一接入请求携带有用户终端的用户名。

[0151] 用户终端存储有预先在认证服务器中注册的用户名和密钥信息。

[0152] 在存在待接入的无线接入点时，用户终端向该无线接入点发送第一接入请求，该第一接入请求中携带有与用户终端对应的用户名。

[0153] 用户终端向无线接入点发送第一接入请求的方式包括：

[0154] 可选的，用户终端通过应用程序中的扫码功能扫描商家提供的携带有无线接入点的硬件信息的二维码，则用户终端通过扫描二维码向无线接入点发送第一接入请求。

[0155] 可选的，用户终端根据商家提供的携带有无线接入点的硬件信息的公众号向该无线接入点发送第一接入请求。

[0156] 可选的，用户终端根据商家提供的携带有无线接入点的硬件信息的单独的无线网络客户端向该无线接入点发送第一接入请求。

[0157] 比如：用户终端利用微信中的扫一扫功能，扫描商家提供的携带有无线接入点的硬件信息的二维码，通过微信向无线接入点发送第一接入请求。又比如：用户终端直接利用浏览器中的扫一扫功能，扫描商家提供的携带有无线接入点的硬件信息的二维码，通过浏览器直接向无线接入点发送第一接入请求。

[0158] 又比如：用户终端利用微信中的关注功能，对商家提供的公众号进行关注，并通过公众号向无线接入点发送第一接入请求。还比如：用户终端安装商家提供的携带有无线接入点的硬件信息的单独的无线网络客户端，通过单独的无线网络客户端向无线接入点发送第一接入请求。

[0159] 对应地，无线接入点接收用户终端发送的第一接入请求。

[0160] 步骤509，无线接入点向认证服务器发送第二接入请求，第二接入请求携带有用户名。

[0161] 无线接入点在接收到用户终端发送的第一接入请求后，向认证服务器发送第二接

入请求，第二接入请求中携带有用户名。

[0162] 可选的，第二接入请求中还携带有与无线接入点对应的第二公钥。

[0163] 无线接入点在接收到用户终端发送的第一接入请求后，将与无线接入点对应的第二公钥和第一接入请求中携带的用户名发送给认证服务器。

[0164] 作为第一种可能的实现方式，无线接入点向认证服务器发送第二接入请求，第二接入请求中携带有用户名和与无线接入点对应的第二公钥；

[0165] 作为第二种可能的实现方式，无线接入点向认证服务器发送第二接入请求，第二接入请求携带有用户名和与无线接入点对应的第二公钥；第二接入请求是无线接入点使用与认证服务器对应的第一公钥进行加密的请求；

[0166] 作为第三种可能的实现方式，无线接入点向认证服务器发送第二接入请求，第二接入请求携带有第一密文和与无线接入点对应的第二公钥；第二接入请求是无线接入点使用与认证服务器对应的第一公钥进行加密的请求，第一密文是无线接入点使用与无线接入点对应的第二私钥对用户名进行加密的密文。

[0167] 本实施例中以第三种可能的实现方式进行举例说明。

[0168] 对应地，认证服务器接收无线接入点发送的第二接入请求。

[0169] 第四阶段，包括步骤510至步骤519；

[0170] 步骤510，认证服务器获取查询密钥请求中携带的第一密文和与无线接入点对应的第二公钥。

[0171] 认证服务器在接收到无线接入点发送的第二接入请求后，获取第二接入请求中携带的第一密文和与无线接入点对应的第二公钥。

[0172] 针对第一种可能的实现方式，认证服务器接收到第二接入请求后，直接获取第二接入请求中携带的用户名和与无线接入点对应的第二公钥；

[0173] 针对第二种可能的实现方式，认证服务器接收到第二接入请求后，使用与认证服务器对应的第一私钥对第二接入请求进行解密，获取第二接入请求携带的用户名和与无线接入点对应的第二公钥；

[0174] 其中，第二接入请求是无线接入点通过与认证服务器对应的第一公钥对第一密文和与无线接入点对应的第二公钥进行加密的请求。

[0175] 步骤511，认证服务器验证与无线接入点对应的第二公钥是否存在于可信任公钥集合中；若与无线接入点对应的第二公钥存在于可信任公钥集合中，则将无线接入点验证为可信任无线接入点。

[0176] 其中，可信任公钥集合存储有成功通过认证服务器的身份认证的无线接入点对应的第二公钥，第一密文包括用户名。

[0177] 认证服务器在获取到与无线接入点对应的第二公钥后，验证与无线接入点对应的第二公钥是否存在于可信任公钥集合中，若存在于可信任公钥集合中，则认证服务器确定该无线接入点为可信任无线接入点。

[0178] 比如：如表一中示例性的可信任公钥集合为例，假定认证服务器获取到的与无线接入点对应的第二公钥为公钥2，则认证服务器将获取到的公钥2与表一中所示的可信任公钥集合中的第二公钥进行匹配，结果发现公钥2是属于可信任公钥集合中，则认证服务器确定该无线接入点为可信任无线接入点。

[0179] 可选的，当认证服务器验证该无线接入点不属于可信任无线接入点时，则不执行后续步骤。

[0180] 步骤512，认证服务器在无线接入点属于可信任无线接入点时，使用与无线接入点对应的第二公钥对第二接入请求中携带的第一密文进行解密，得到用户名。

[0181] 认证服务器在确定该无线接入点为可信任无线接入点后，使用获取到的与无线接入点对应的第二公钥对获取到的第一密文进行解密，解密后得到第一密文中携带的用户名。

[0182] 第一密文是无线接入点通过与无线接入点对应的第二私钥对用户名进行加密的密文，

[0183] 步骤513，认证服务器根据用户名查询与用户名对应的密钥信息。

[0184] 认证服务器在对第一密文解密得到第一密文携带的用户名后，查询与用户名对应的密钥信息。

[0185] 比如：如表二中示例性的用户名和密码之间的对应关系为例，假定认证服务器获取到的第二接入请求中携带的用户名为“用户B”，则认证服务器到用户名和密码之间的对应关系中查询与“用户B”对应的密码，则如表二所示，查询到的密码为“密码2”。

[0186] 步骤514，认证服务器使用密钥信息与用户终端进行第一身份认证。

[0187] 认证服务器在查询到与用户名对应的密钥信息后，使用该密钥信息与用户终端进行第一身份认证。可选的，第一身份认证是指认证服务器与用户终端之间的双向认证。也即，认证服务器需要根据密钥信息对用户终端进行身份认证；用户终端也需要根据密钥信息对认证服务器进行身份认证。

[0188] 可选的，第一身份认证为单向认证。也即认证服务器根据密钥信息对用户终端进行身份认证；或，用户终端需要根据密钥信息对认证服务器进行身份认证。

[0189] 认证服务器与用户终端进行第一身份认证和协商生成主密钥的过程是通过建立TLS(Transport Layer Security，安全传输层协议)通道，通过无线接入点的转发进行第一身份认证和协商生成主密钥。

[0190] 可选的，认证服务器与用户终端进行第一身份认证的过程符合PEAP(Protected Extensible Authentication Protocol，基于保护信道的认证协议)对用户接入的协议。

[0191] 步骤515，在第一身份认证成功时，认证服务器与用户终端协商生成主密钥，并向用户终端发送主密钥。

[0192] 在第一身份认证成功时，认证服务器与用户终端根据密钥信息协商生成主密钥。

[0193] 可选的，认证服务器与用户终端协商生成的主密钥为PMK(Pairwise Master Key，主成对密钥)。

[0194] 认证服务器与用户终端协商生成主密钥后，认证服务器将协商生成的主密钥通过TLS通道发送给用户终端。

[0195] 步骤516，认证服务器使用与无线接入点对应的第二公钥对协商生成的主密钥进行第一加密。

[0196] 认证服务器将主密钥发送给无线接入点的方式包括三种：

[0197] 作为第一种可能的实现方式，认证服务器直接通过加密通道将主密钥发送给无线接入点；

[0198] 作为第二种可能的实现方式，认证服务器使用与认证服务器对应的第一私钥对主密钥进行加密，将加密后的主密钥发送给无线接入点；

[0199] 作为第三种可能的实现方式，认证服务器首先使用与无线接入点对应的第二公钥对主密钥进行第一加密；再使用与认证服务器对应的第一私钥对第一加密后的主密钥进行第二加密；将第二加密后的主密钥发送给无线接入点。

[0200] 本实施例中，以第三种可能的实现方式进行举例说明。

[0201] 其中，与无线接入点对应的第二公钥是认证服务器对无线接入点的身份认证成功时保存的。

[0202] 认证服务器在与用户终端协商生成主密钥后，使用与无线接入点对应的第二公钥对主密钥进行第一加密。

[0203] 步骤517，认证服务器使用与认证服务器对应的第一私钥对第一加密后的主密钥进行第二加密，向无线接入点发送第二加密后的主密钥。

[0204] 认证服务器在使用与无线接入点对应的第二公钥对主密钥进行第一加密后，再使用与认证服务器对应的第一私钥对第一加密后的主密钥进行第二加密。将两次加密后的主密钥发送给无线接入点。

[0205] 可选的，本实施例中，仅以先使用与无线接入点对应的第二公钥对主密钥进行第一加密，再使用与认证服务器对应的第一私钥对第一加密后的主密钥进行第二加密进行举例说明。本实施例中，对主密钥的加密顺序不作具体限定，可以先使用与认证服务器对应的第一私钥对主密钥进行第一加密，再使用与无线接入点对应的第二公钥对第一加密后的主密钥进行第二加密。本实施例中认证服务器对主密钥的加密方式不作具体限定。

[0206] 对应地，无线接入点接收认证服务器发送的加密的主密钥。

[0207] 可选的，无线接入点接收认证服务发送的第一加密后的主密钥，第一加密后的主密钥是认证服务器在无线接入点属于可信任无线接入点时，使用与无线接入点对应的第二公钥对主密钥进行加密后的主密钥。

[0208] 可选的，无线接入点接收认证服务器发送的第二加密后的主密钥，第二加密后的主密钥是认证服务器在无线接入点属于可信任无线接入点时，使用与无线接入点对应的第二公钥对主密钥进行第一加密，再使用与认证服务器对应的第一私钥对第一加密后的主密钥进行第二加密后的主密钥。

[0209] 步骤518，无线接入点使用与认证服务器对应的第一公钥对第二加密后的主密钥进行解密，得到第二密文。

[0210] 无线接入点在接收到认证服务器发送的加密的主密钥后，使用与认证服务器对应的第一公钥对第二加密后的主密钥进行解密，得到第二密文。

[0211] 其中，第二密文是认证服务器通过与无线接入点对应的第二公钥对主密钥进行加密的密文。

[0212] 步骤519，无线接入点使用与无线接入点对应的第二私钥对第二密文进行解密，得到主密钥。

[0213] 无线接入点通过与认证服务器对应的第一公钥解密得到第二密文后，使用与无线接入点对应的第二私钥对第二密文进行解密，得到主密钥。

[0214] 可选的，若认证服务器仅使用与无线接入点对应的第二公钥对与用户名对应的主

密钥进行加密，则无线接入点仅需要使用与无线接入点对应的第二私钥对加密后的主密钥进行解密，即可得到主密钥。

[0215] 步骤520，无线接入点与用户终端根据各自持有的主密钥协商生成本次连接所使用的临时密钥，使用临时密钥建立加密无线网络连接。

[0216] 可选的，无线接入点和用户终端使用PMK协商生成本次连接所使用的PTK(Pairwise Temporary Key，临时成对密钥)，无线接入点和用户终端使用PTK建立加密无线网络连接。

[0217] 无线接入点在获取到认证服务器发送的主密钥后，无线接入点和用户终端使用各自获取到的主密钥作为PMK，完成WPA2(Wi-Fi Protected Access II，Wi-Fi联盟推出的无线网络安全认证协议)加密协议。利用主密钥作为PMK，协商生成本次连接使用的PTK，用户终端与无线接入点使用协商生成的PTK建立加密无线网络连接。

[0218] 无线接入点与用户终端之间通过PTK建立加密无线网络连接的具体过程如下：

[0219] 第一、无线接入点生成一个随机数A，无线接入点向用户终端发送消息M1，消息M1种携带有随机数A；

[0220] 第二、用户终端生成一个随机数B，用户终端根据主密钥、随机数A和随机数B计算得到本次连接所使用的PTK；用户终端向无线接入点发送消息M2，消息M2中携带有随机数B；且使用计算得到的PTK中的确认密钥部分对消息M2进行MIC(Message Integrity Code，消息完整性)认证；

[0221] 第三、无线接入点得到随机数B，并根据主密钥、随机数A和随机数B计算得到本次连接所使用的PTK，并使用计算得到的PTK中的确认密钥部分对消息M2进行MIC校验。若校验失败则丢弃消息M2，若校验正确则向用户终端发送消息M3，消息M3中包含一个MIC校验，使得用户终端核实无线接入点拥有主密钥。

[0222] 第四、用户终端收到消息M3后，对消息M3进行MIC校验，校验成功后装入PTK，并向无线接入点发送消息M4，消息M4用于表明用户终端已装入PTK。无线接入点在接收到消息M4后，也装入PTK即完成建立加密无线网络连接的过程。

[0223] 本实施例中无线接入点与用户终端之间完成WPA2加密协议的核心加密算法以WPE2-PEAP(WPE2-PEAP，基于保护信道的认证协议)进行举例说明，但完成WPA2加密协议的核心加密算法还可以包括但不限于：EAP-TLS(Extensible Authentication Protocol-Transport Layer Security，基于信道的认证协议和传输层加密协议)、EAP-TTLS/MSCHAPv2、PEAPv0/EAP-MSCHAPv2、PEAPv1/EAP-GTC、PEAP-TLS(Protected Extensible Authentication Protocol-Transport Layer Security，基于传输层安全的受保护的可扩展身份验证协议)、EAP-SIM(EPA-Subscriber Identity Module，基于客户身份识别卡的认证协议)、EAP-AKA(EAP-Authentication and Key Agreement，认证与密钥协商)和EAP-FAST(EAP-Flexible Authentication via Secure Tunneling，基于安全隧道的灵活认证协议)。

[0224] 可选地，用户终端接入无线接入点的过程如图5D所示。用户终端140向无线接入点120发送用户名，无线接入点120将用户名转发给认证服务器160，认证服务器160在确认无线接入点属于可信任无线接入点后与用户终端140进行第一身份认证，在第一身份认证成功时，分别向用户终端140和无线接入点120发送与用户名对应的主密钥，用户终端140与无

线接入点120以获取到的主密钥为PMK，协商建立加密无线网络连接。

[0225] 综上所述，本实施例提供的无线网络接入方法，通过用户终端向无线接入点发送第一接入请求；无线接入点向认证服务器发送第二接入请求；认证服务器在接收到第二接入请求后，验证无线接入点是否属于可信任无线接入点，在无线接入点属于可信任无线接入点时与用户终端进行第一身份认证，在第一身份认证成功时与用户终端协商生成主密钥；认证服务器向无线接入点发送与用户名对应的主密钥；无线接入点与用户终端根据各自持有的主密钥协商建立加密无线网络连接；解决了用户使用现有的接入方法使得用户终端接入假冒的公众Wi-Fi时，导致用户终端向假冒的公众Wi-Fi所传输的数据以及用户终端内部的数据均会受到安全威胁的问题；达到了通过认证服务器对无线接入点进行身份认证，只有可信任无线接入点才能获取与用户名对应的主密钥，从而与用户终端根据各自持有的主密钥建立加密无线网络连接，提高了用户终端传输的数据以及用户终端内部的数据安全性的效果。

[0226] 同时，认证服务器与无线接入点之间通过加密通道进行数据传输，提高了传输过程中数据的安全性。

[0227] 需要说明的一点是，本实施例中对步骤501至步骤506和步骤507的先后顺序不作具体限制。也即，无线接入点在认证服务器中的认证过程和用户终端向认证服务器注册用户名和密钥信息的过程之间没有必然的先后顺序；但是与用户终端建立加密无线网络连接的无线接入点必须是存储于认证服务器的可信任无线接入点。

[0228] 需要说明的另一点是，本发明实施例中，无线接入点与认证服务器在通过加密通道进行数据传输时，在传输的数据中还可以携带的信息有各自生成的随机数、发送数据的时间戳等。比如：无线接入点向认证服务器发送数据时，在数据中还携带有无线接入点生成的随机数、发送该数据的时间戳等信息。本发明实施例无线接入点与认证服务器进行数据传输过程中，除上述实施例中数据携带的信息外，对数据中还可以携带的信息不作具体限定。同理，用户终端与认证服务器通过独立通道进行数据传输时，在传输的数据中还可以携带的信息有各自生成的随机数、发送数据的时间戳等，此处不再赘述。针对数据还可以携带的信息的变换实施例都是本发明实施例的等同替换实施例，包含在本发明的保护范围之内。

[0229] 在一个具体的实施例中，假如黑客设置假冒的无线接入点，该假冒的无线接入点与真实的无线接入点具有完全相同的硬件信息。

[0230] 第一，用户终端在获取到假冒的无线接入点时，向该假冒的无线接入点发送第一接入请求，该接入请求中携带有用户终端对应的用户名。

[0231] 第二、假冒的无线接入点向认证服务器发送第二接入请求，第二接入请求携带有用户名。

[0232] 假冒的无线接入点获取与认证服务器对应的第一公钥，并使用与认证服务器对应的第一公钥对第二接入请求进行加密，并将加密后的第二接入请求发送给认证服务器。

[0233] 第三、认证服务器通过与认证服务器对应的第一私钥对第二接入请求进行解密，得到与假冒的无线接入点对应的第二公钥和用户名。

[0234] 第四、认证服务器验证与假冒的无线接入点对应的第二公钥是否存在于可信任公钥集合中。

[0235] 虽然假冒的无线接入点与真实的无线接入点具有完全相同的硬件信息，但与假冒的无线接入点对应的第二公钥和与真实的无线接入点对应的第二公钥是不相同的，因此，认证服务器在验证与假冒的无线接入点对应的第二公钥是否存在于可信任公钥集合中时，会将假冒的无线接入点确定为不可信任无线接入点。认证服务器在确定该无线接入点为假冒的无线接入点后，不会将与用户名对应的主密钥发送给假冒的无线接入点。

[0236] 综上所述，假如黑客设置假冒的无线接入点，该假冒的无线接入点与真实的无线接入点具有完全相同的硬件信息时，在图5A所示的实施例提供的无线网络接入方法中，假冒的无线接入点也无法与用户终端建立加密无线网络连接。在步骤511中，与假冒的无线接入点对应的第二公钥并不存在于认证服务器存储的可信任公钥集合中，因此被认证服务器确定为不可信任无线接入点。因此，图5A实施例提供的无线网络接入方法，提高了用户终端传输的数据以及用户终端内部数据的安全性。

[0237] 请参考图6，其示出了本发明一个实施例提供的无线网络连接装置的结构方框图。该无线网络连接装置可以通过软件、硬件或者两者的结合实现成为图1中无线接入点的全部或一部分。该无线网络连接装置包括：

[0238] 第一接收模块610，用于接收用户终端发送的第一接入请求，第一接入请求携带有用户终端的用户名；

[0239] 第二接收模块620，用于向认证服务器发送第二接入请求，第二接入请求携带有用户名；

[0240] 密钥接收模块630，用于接收认证服务器发送的与用户名对应的主密钥，主密钥是认证服务器在接收到第二接入请求后，验证无线接入点属于可信任无线接入点时，与用户终端进行第一身份认证成功后协商生成的密钥；

[0241] 网络连接模块640，用于与用户终端根据各自持有的主密钥协商建立加密无线网络连接。

[0242] 综上所述，本实施例提供的无线网络接入装置，通过接收用户终端发送的第一接入请求；向认证服务器发送第二接入请求；接收认证服务器发送的与用户名对应的主密钥；与用户终端根据各自持有的主密钥协商建立加密无线网络连接；解决了用户使用现有的接入方法使得用户终端接入假冒的公众Wi-Fi时，导致用户终端向假冒的公众Wi-Fi所传输的数据以及用户终端内部的数据均会受到安全威胁的问题；达到了通过认证服务器对无线接入点进行身份认证，只有可信任无线接入点才能获取与用户名对应的主密钥，从而与用户终端根据各自持有的主密钥建立加密无线网络连接，提高了用户终端传输的数据以及用户终端内部的数据安全性的效果。

[0243] 请参考图7，其示出了本发明另一个实施例提供的无线网络连接装置的结构方框图。该无线网络连接装置可以通过软件、硬件或者两者的结合实现成为图1中无线接入点的全部或一部分。该无线网络连接装置包括：

[0244] 密钥生成模块710，用于生成与无线接入点对应的第二公钥和第二私钥；

[0245] 公钥获取模块720，用于获取与认证服务器对应的第一公钥；

[0246] 信息发送模块730，用于向认证服务器发送身份认证请求，身份认证请求携带有认证信息和与无线接入点对应的第二公钥，认证信息和与无线接入点对应的第二公钥均使用与认证服务器对应的第一公钥进行加密，认证信息至少包括硬件信息和/或拥有者信息。

[0247] 在一种可能的实现方式中，认证信息是通过与无线接入点对应的第二私钥进行加密的信息。

[0248] 第一接收模块740，用于接收用户终端发送的第一接入请求，第一接入请求携带有用户终端的用户名。

[0249] 第二接收模块750，用于向认证服务器发送第二接入请求，第二接入请求携带有用户名。

[0250] 密钥接收模块760，用于接收认证服务器发送的与用户名对应的主密钥，主密钥是认证服务器在接收到第二接入请求后，验证无线接入点属于可信任无线接入点时，与用户终端进行第一身份认证成功后协商生成的密钥。

[0251] 在一种可能的实现方式中，密钥接收模块760，还用于接收认证服务器发送的第一加密后的主密钥，第一加密后的主密钥是认证服务器在无线接入点属于可信任无线接入点时，使用与无线接入点对应的第二公钥对主密钥进行加密后的主密钥。

[0252] 在另一种可能的实现方式中，密钥接收模块760，还用于接收认证服务器发送的第二加密后的主密钥，第二加密后的主密钥是认证服务器在无线接入点属于可信任无线接入点时，使用与无线接入点对应的第二公钥对主密钥进行第一加密，再使用与认证服务器对应的第一私钥对第一加密后的主密钥进行第二加密后的主密钥。

[0253] 网络连接模块770，用于根据主密钥与用户终端协商建立加密无线网络连接。

[0254] 在第一种可能的实现方式中，网络连接模块770，可以包括：第一解密单元771和第一连接单元772；

[0255] 第一解密单元771，用于使用与无线接入点对应的第二私钥对第一加密后的主密钥进行解密，得到主密钥。

[0256] 第一连接单元772，用于与用户终端根据各自持有的主密钥协商建立加密无线网络连接。

[0257] 在第二种可能的实现方式中，网络连接模块770，可以包括：第二解密单元773、第三解密单元774和第二连接单元775。

[0258] 第二解密单元773，用于使用与认证服务器对应的第一公钥对第二加密后的主密钥进行解密，得到第二密文。

[0259] 第三解密单元774，用于使用与无线接入点对应的第二私钥对第二密文进行解密，得到主密钥。

[0260] 第二连接单元775，用于与用户终端根据各自持有的主密钥协商建立加密无线网络连接。

[0261] 其中，第二密文是认证服务器通过与无线接入点对应的第二公钥对主密钥进行加密的密文。

[0262] 在第三种可能的实现方式中，网络连接模块770，还用于与用户终端使用各自持有的主密钥，协商生成本次连接所使用的临时密钥，使用临时密钥与用户终端建立加密无线网络连接。

[0263] 综上所述，本实施例提供的无线网络接入装置，通过接收用户终端发送的第一接入请求；向认证服务器发送第二接入请求；接收认证服务器发送的与用户名对应的主密钥；与用户终端根据各自持有的主密钥协商建立加密无线网络连接；解决了用户使用现有的接

入方法使得用户终端接入假冒的公众Wi-Fi时，导致用户终端向假冒的公众Wi-Fi所传输的数据以及用户终端内部的数据均会受到安全威胁的问题；达到了通过认证服务器对无线接入点进行身份认证，只有可信任无线接入点才能获取与用户名对应的主密钥，从而与用户终端根据各自持有的主密钥建立加密无线网络连接，提高了用户终端传输的数据以及用户终端内部的数据安全性的效果。

[0264] 请参考图8，其示出了本发明一个实施例提供的无线网络连接装置的结构方框图。该无线网络连接装置可以通过软件、硬件或者两者的结合实现成为图1中认证服务器的全部或一部分。该无线网络连接装置包括：

[0265] 请求接收模块810，用于接收无线接入点发送的第二接入请求，第二接入请求携带有用户名；

[0266] 信任验证模块820，用于在接收到第二接入请求后，验证无线接入点是否属于可信任无线接入点；

[0267] 用户认证模块830，用于在无线接入点属于可信任无线接入点时与用户终端进行第一身份认证；

[0268] 密钥生成模块840，用于在第一身份认证成功时，与用户终端协商生成主密钥，并向用户终端发送主密钥。

[0269] 密钥发送模块850，用于在无线接入点属于可信任无线接入点时向无线接入点发送与用户名对应的密钥信息，以便无线接入点与用户终端根据各自持有的主密钥协商建立加密无线网络连接。

[0270] 综上所述，本实施例提供的无线网络接入装置，通过接收无线接入点发送的第二接入请求；在接收到第二接入请求后，验证无线接入点是否属于可信任无线接入点；在无线接入点属于可信任无线接入点时与用户终端进行第一身份认证，在第一身份认证成功时与用户终端协商生成主密钥，并向用户终端发送主密钥；向无线接入点发送与用户名对应的主密钥；解决了用户使用现有的接入方法使得用户终端接入假冒的公众Wi-Fi时，导致用户终端向假冒的公众Wi-Fi所传输的数据以及用户终端内部的数据均会受到安全威胁的问题；达到了通过认证服务器对无线接入点进行身份认证，只有可信任无线接入点才能获取与用户名对应的主密钥，从而与用户终端根据各自持有的主密钥建立加密无线网络连接，提高了用户终端传输的数据以及用户终端内部的数据安全性的效果。

[0271] 请参考图9，其示出了本发明另一个实施例提供的无线网络连接装置的结构方框图。该无线网络连接装置可以通过软件、硬件或者两者的结合实现成为图1中认证服务器的全部或一部分。该无线网络连接装置包括：

[0272] 认证接收模块910，用于接收无线接入点发送的身份认证请求，身份认证请求携带有认证信息和与无线接入点对应的第二公钥，认证信息和与无线接入点对应的第二公钥均使用与认证服务器对应的第一公钥进行加密，认证信息至少包括硬件信息和/或拥有者信息。

[0273] 信息解密模块920，用于通过与认证服务器对应的第一私钥对身份认证请求进行解密，得到认证信息和与无线接入点对应的第二公钥。

[0274] 信息认证模块930，用于对认证信息进行第二身份认证，在第二身份认证成功时，将与无线接入点对应的第二公钥添加至可信任公钥集合中。

[0275] 可选的，认证信息是无线接入点通过与无线接入点对应的第二私钥进行加密的信息。

[0276] 作为一种可能的实现方式，信息认证模块930，可以包括：第一解密单元931和第一认证单元932。

[0277] 第一解密单元931，用于通过与无线接入点对应的第二公钥对认证信息进行解密，得到硬件信息和/或拥有者信息；

[0278] 第一认证单元932，用于对硬件信息和/或拥有者信息进行第二身份认证，在第二身份认证成功时，将与无线接入点对应的第二公钥添加至可信任公钥集合中。

[0279] 请求接收模块940，用于接收无线接入点发送的第二接入请求，第二接入请求携带有用户名。

[0280] 信任验证模块950，用于在接收到第二接入请求后，验证无线接入点是否属于可信任无线接入点。

[0281] 作为一种可能的实现方式，本实施例中，信任验证模块950，可以包括：公钥获取单元951和第一验证单元952。

[0282] 公钥获取单元951，用于获取第二接入请求中携带的第一密文和与无线接入点对应的第二公钥。

[0283] 可选的，公钥获取单元951，还用于通过与认证服务器对应的第一私钥对第二接入请求进行解密，得到第一密文和与无线接入点对应的第二公钥；

[0284] 其中，第二接入请求是无线接入点通过与认证服务器对应的第一公钥对第一密文和与无线接入点对应的第二公钥进行加密的请求。

[0285] 第一验证单元952，用于验证与无线接入点对应的第二公钥是否存在于可信任公钥集合中；若与无线接入点对应的第二公钥存在于可信任公钥集合中，则将无线接入点验证为可信任无线接入点；

[0286] 其中，可信任公钥集合存储有成功通过第二身份认证的无线接入点对应的第二公钥。

[0287] 用户认证模块960，用于在无线接入点属于可信任无线接入点时与用户终端进行第一身份认证。

[0288] 作为一种可能的实现方式，本实施例中，用户认证模块960，可以包括：密文解密单元961、密钥查询单元962和密钥认证单元963。

[0289] 密文解密单元961，用于在无线接入点属于可信任无线接入点时，使用与无线接入点对应的第二公钥对第二接入请求中携带的第一密文进行解密，得到用户名。

[0290] 密钥查询单元962，用于查询与用户名对应的密钥信息；

[0291] 密钥认证单元963，用于根据密钥信息与用户终端进行第一身份认证。

[0292] 其中，第一密文是无线接入点通过与无线接入点对应的第二私钥对用户名进行加密的密文。

[0293] 密钥生成模块970，用于在第一身份认证成功时，与用户终端协商生成主密钥，并向用户终端发送主密钥。

[0294] 密钥发送模块980，用于向无线接入点发送与用户名对应的主密钥，以便无线接入点与用户终端根据各自持有的主密钥协商建立加密无线网络连接。

[0295] 可选的，密钥发送模块980，还用于使用与无线接入点对应的第二公钥对协商生成的主密钥进行第一加密，向无线接入点发送第一加密后的主密钥。

[0296] 可选的，密钥发送模块980，还用于使用与认证服务器对应的第一私钥对第一加密后的主密钥进行第二加密，向无线接入点发送第二加密后的主密钥。

[0297] 综上所述，本实施例提供的无线网络接入装置，通过接收无线接入点发送的第二接入请求；在接收到第二接入请求后，验证无线接入点是否属于可信任无线接入点；在无线接入点属于可信任无线接入点时与用户终端进行第一身份认证，在第一身份认证成功时与用户终端协商生成主密钥，并向用户终端发送主密钥；向无线接入点发送与用户名对应的主密钥；解决了用户使用现有的接入方法使得用户终端接入假冒的公众Wi-Fi时，导致用户终端向假冒的公众Wi-Fi所传输的数据以及用户终端内部的数据均会受到安全威胁的问题；达到了通过认证服务器对无线接入点进行身份认证，只有可信任无线接入点才能获取与用户名对应的主密钥，从而与用户终端根据各自持有的主密钥建立加密无线网络连接，提高了用户终端传输的数据以及用户终端内部的数据安全性的效果。

[0298] 请参考图10，其示出了本发明实施例提供的一种无线网络连接系统的结构方框图，该系统包括：用户终端1020、无线接入点1040和认证服务器1060；

[0299] 用户终端1020，用于向无线接入点发送第一接入请求，以及与认证服务器进行第一身份认证；

[0300] 无线接入点1040，包括如图6所示实施例或图7所示实施例任一所述的无线网络连接装置；

[0301] 认证服务器1060，包括如图8所示实施例或图9所示实施例任一所述的无线网络连接装置。

[0302] 需要说明的是：上述实施例提供的无线网络连接的装置在连接无线网络时，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，即将设备的内部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，上述实施例提供的无线网络连接与无线网络连接的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。

[0303] 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。

[0304] 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。

[0305] 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。

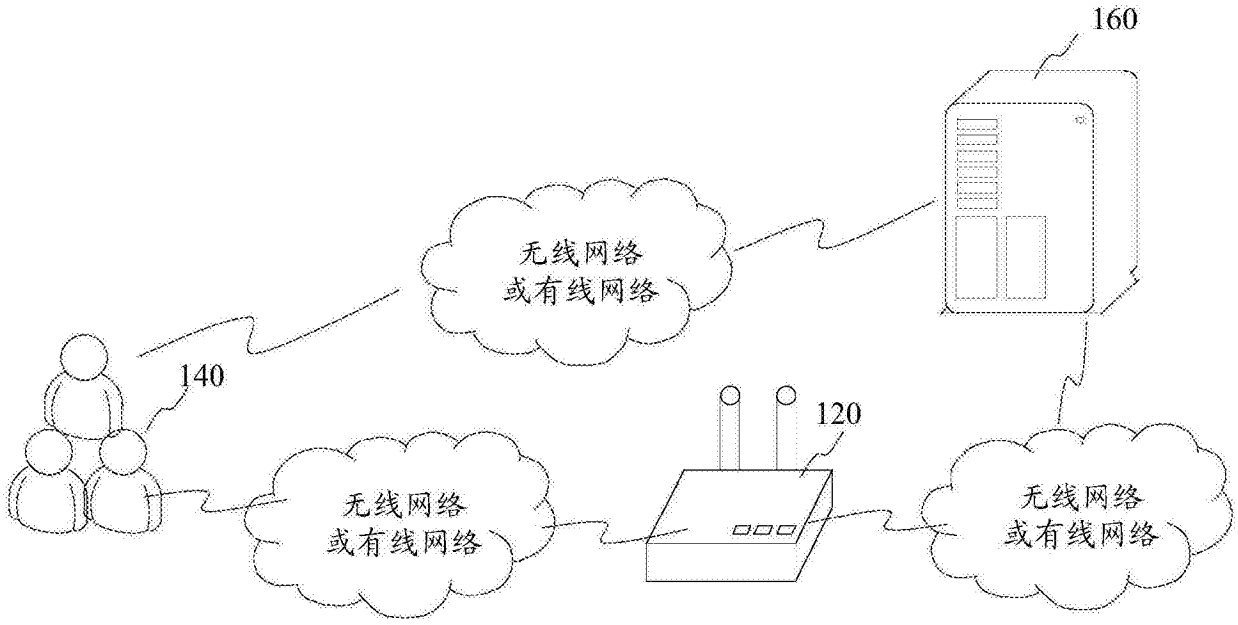

160
无线网络
或有线网络
140
120
无线网络
或有线网络
无线网络
或有线网络

图1

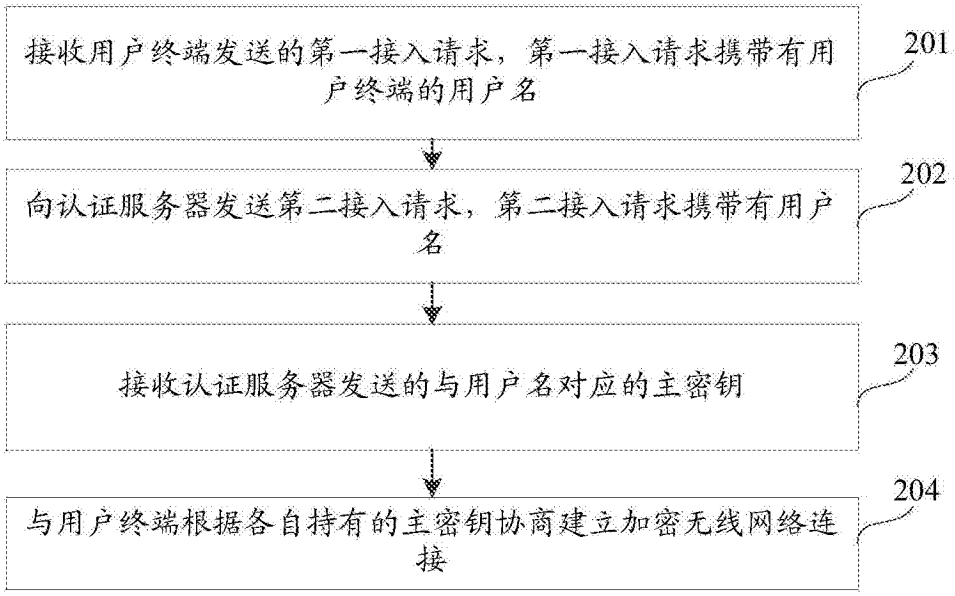

接收用户终端发送的第一接入请求，第一接入请求携带有用户终端的用户名
201
向认证服务器发送第二接入请求，第二接入请求携带有用户名
202
接收认证服务器发送的与用户名对应的主密钥
203
与用户终端根据各自持有的主密钥协商建立加密无线网络连接
204

图2

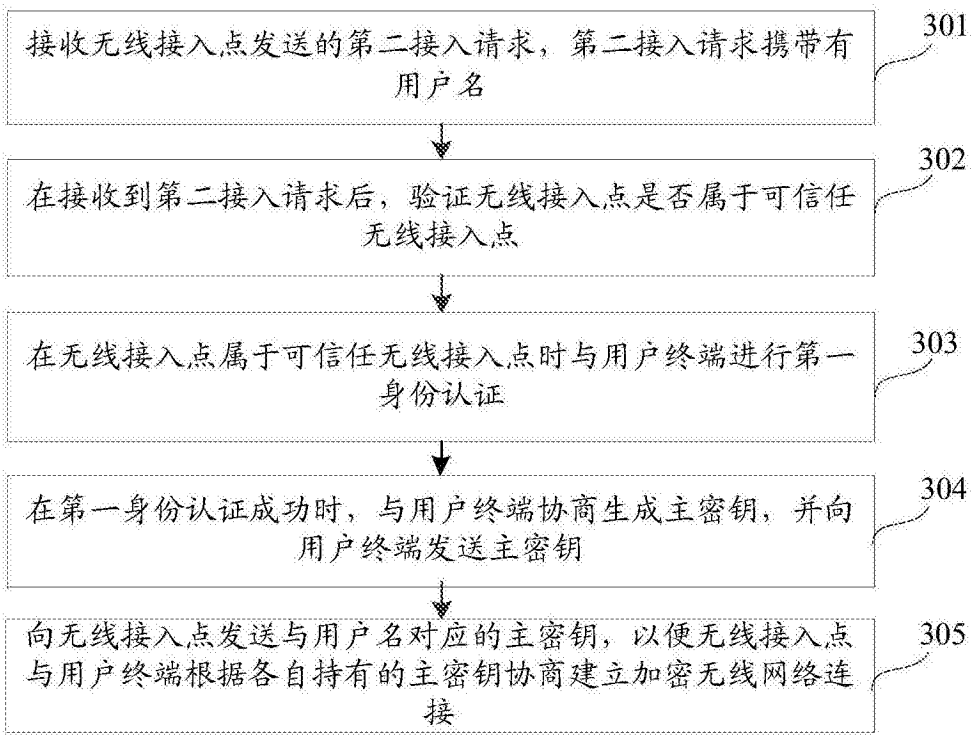

接收无线接入点发送的第二接入请求，第二接入请求携带有用户名
301
在接收到第二接入请求后，验证无线接入点是否属于可信任无线接入点
302
在无线接入点属于可信任无线接入点时与用户终端进行第一身份认证
303
在第一身份认证成功时，与用户终端协商生成主密钥，并向用户终端发送主密钥
304
向无线接入点发送与用户名对应的主密钥，以便无线接入点与用户终端根据各自持有的主密钥协商建立加密无线网络连接
305

图3

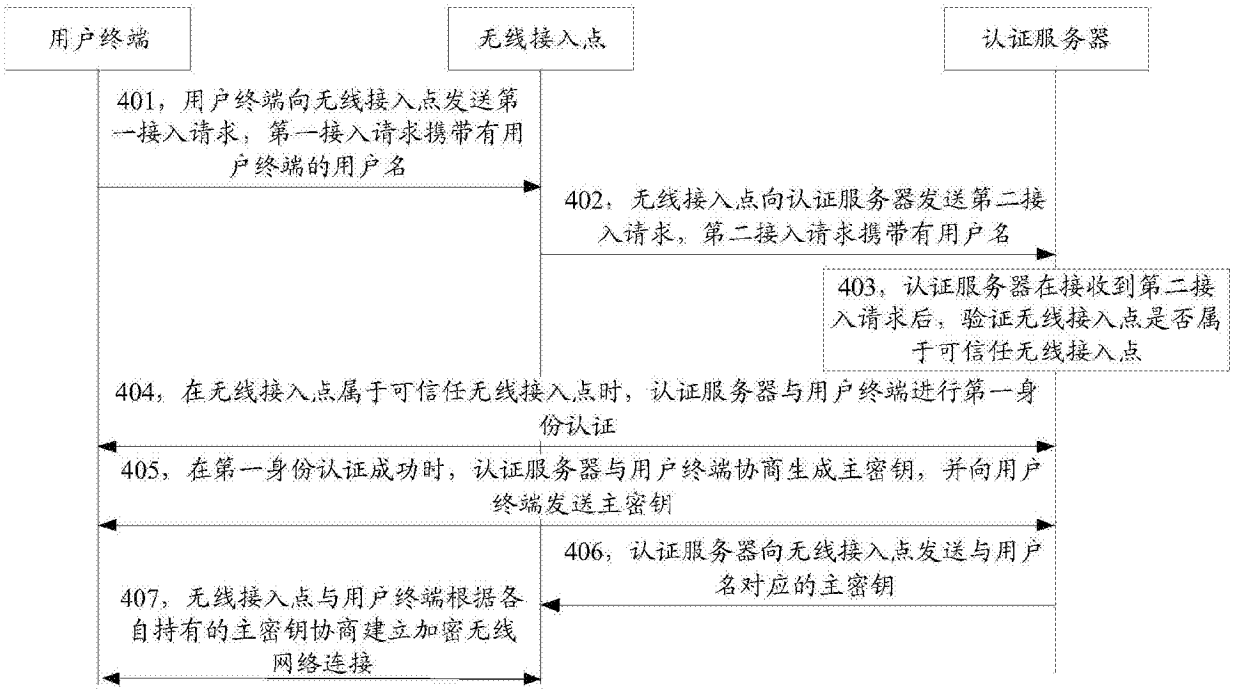

用户终端
无线接入点
认证服务器
401，用户终端向无线接入点发送第一接入请求，第一接入请求携带有用户终端的用户名
402，无线接入点向认证服务器发送第二接入请求，第二接入请求携带有用户名
403，认证服务器在接收到第二接入请求后，验证无线接入点是否属于可信任无线接入点
404，在无线接入点属于可信任无线接入点时，认证服务器与用户终端进行第一身份认证
405，在第一身份认证成功时，认证服务器与用户终端协商生成主密钥，并向用户终端发送主密钥
406，认证服务器向无线接入点发送与用户名对应的主密钥
407，无线接入点与用户终端根据各自持有的主密钥协商建立加密无线网络连接

图4

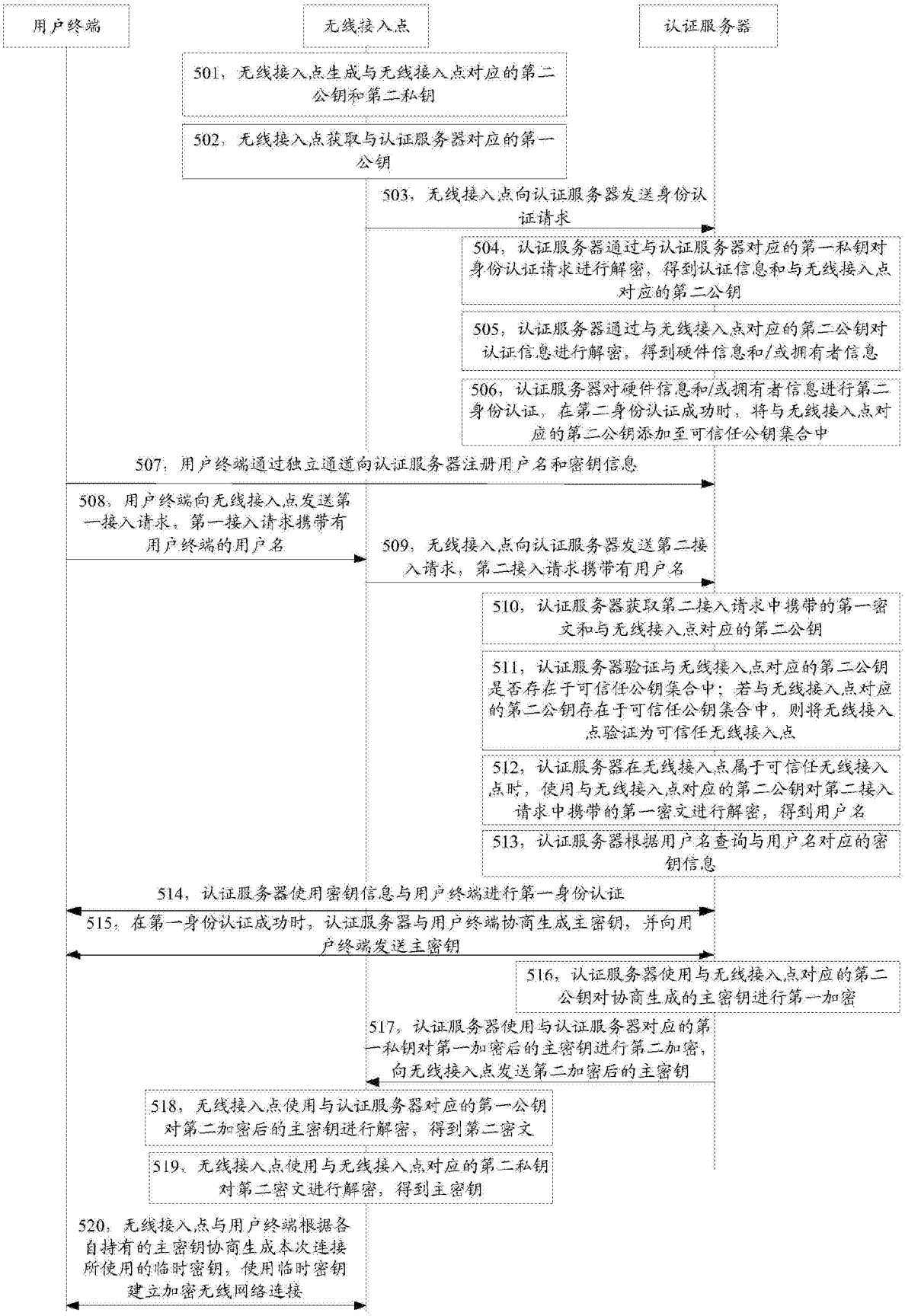

用户终端
无线接入点
认证服务器
501，无线接入点生成与无线接入点对应的第二公钥和第二私钥
502，无线接入点获取与认证服务器对应的第一公钥
503，无线接入点向认证服务器发送身份认证请求
504，认证服务器通过与认证服务器对应的第一私钥对身份认证请求进行解密，得到认证信息和与无线接入点对应的第二公钥
505，认证服务器通过与无线接入点对应的第二公钥对认证信息进行解密，得到硬件信息和/或拥有者信息
506，认证服务器对硬件信息和/或拥有者信息进行第二身份认证，在第二身份认证成功时，将与无线接入点对应的第二公钥添加至可信任公钥集合中
507，用户终端通过独立通道向认证服务器注册用户名和密钥信息
508，用户终端向无线接入点发送第一接入请求，第一接入请求携带有用户终端的用户名
509，无线接入点向认证服务器发送第二接入请求，第二接入请求携带有用户名
510，认证服务器获取第二接入请求中携带的第一密文和与无线接入点对应的第二公钥
511，认证服务器验证与无线接入点对应的第二公钥是否存在于可信任公钥集合中；若与无线接入点对应的第二公钥存在于可信任公钥集合中，则将无线接入点验证为可信任无线接入点
512，认证服务器在无线接入点属于可信任无线接入点时，使用与无线接入点对应的第二公钥对第二接入请求中携带的第一密文进行解密，得到用户名
513，认证服务器根据用户名查询与用户名对应的密钥信息
514，认证服务器使用密钥信息与用户终端进行第一身份认证
515，在第一身份认证成功时，认证服务器与用户终端协商生成主密钥，并向用户终端发送主密钥
516，认证服务器使用与无线接入点对应的第二公钥对协商生成的主密钥进行第一加密
517，认证服务器使用与认证服务器对应的第一私钥对第一加密后的主密钥进行第二加密，向无线接入点发送第二加密后的主密钥
518，无线接入点使用与认证服务器对应的第一公钥对第二加密后的主密钥进行解密，得到第二密文
519，无线接入点使用与无线接入点对应的第二私钥对第二密文进行解密，得到主密钥
520，无线接入点与用户终端根据各自持有的主密钥协商生成本次连接所使用的临时密钥，使用临时密钥建立加密无线网络连接

图5A

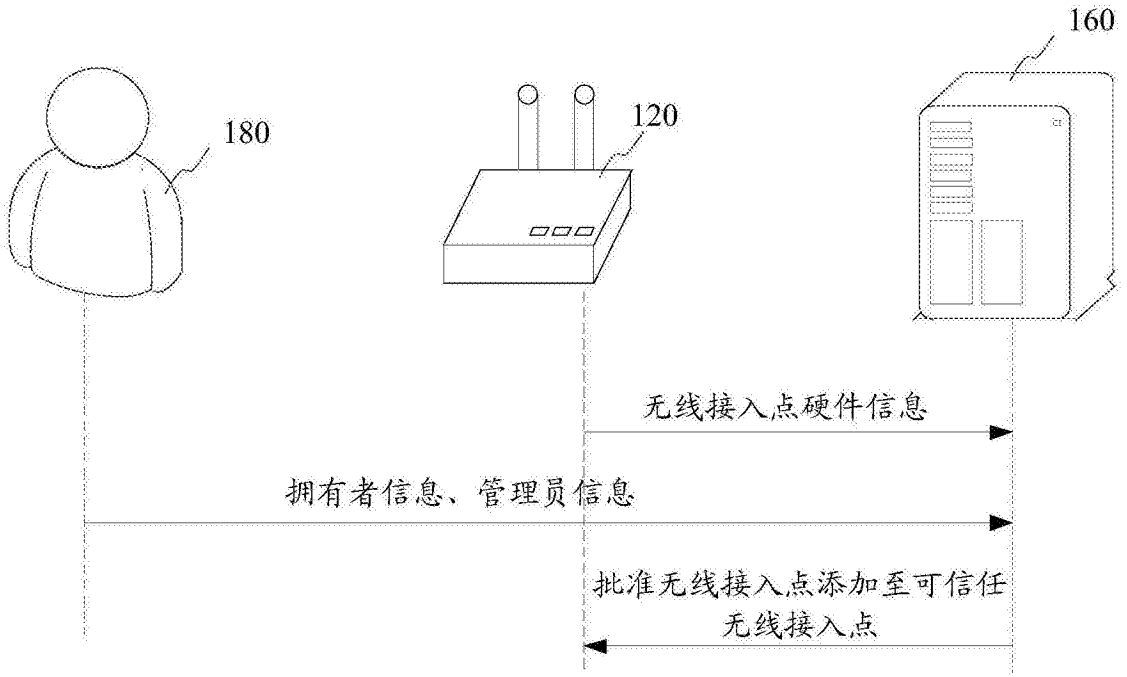

160
180
120
无线接入点硬件信息
拥有者信息、管理员信息
批准无线接入点添加至可信任
无线接入点

图5B


160
140
帐号申请请求
用户名和密钥信息

图5C

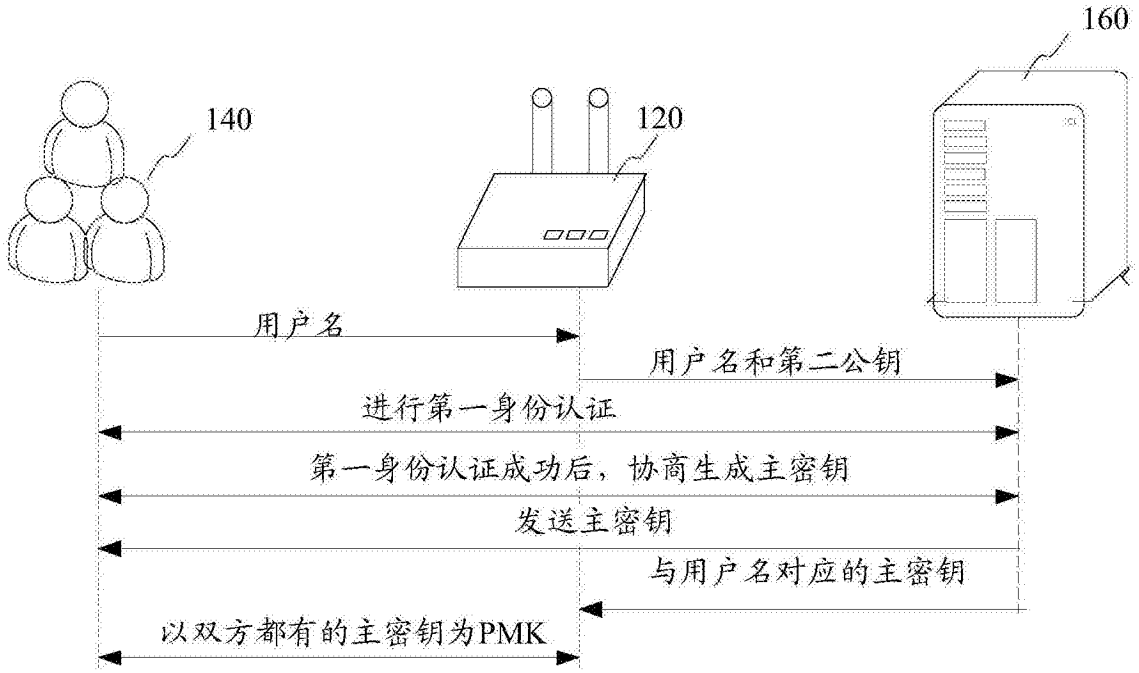

160
140
120
用户名
用户名和第二公钥
进行第一身份认证
第一身份认证成功后，协商生成主密钥
发送主密钥
与用户名对应的主密钥
以双方都有的主密钥为PMK

图5D

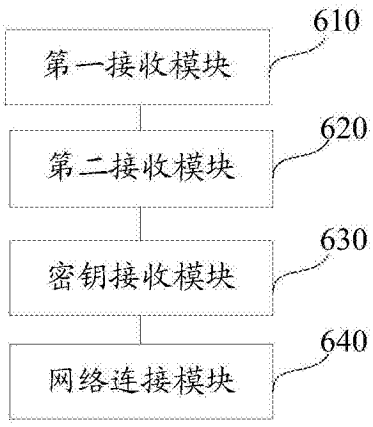

610
第一接收模块
620
第二接收模块
630
密钥接收模块
640
网络连接模块

图6

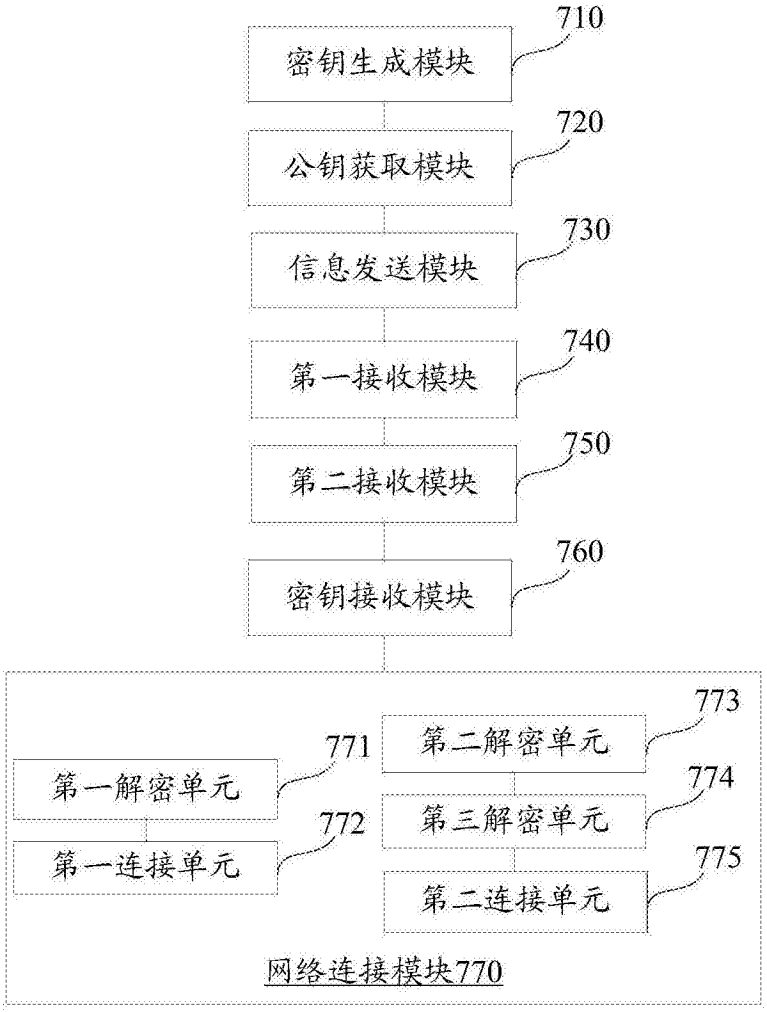

710
密钥生成模块
720
公钥获取模块
730
信息发送模块
740
第一接收模块
750
第二接收模块
760
密钥接收模块
773
第二解密单元
771
第一解密单元
774
第三解密单元
772
第一连接单元
775
第二连接单元
网络连接模块770

图7

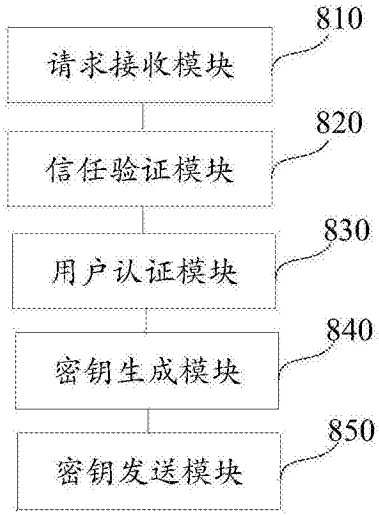

810
请求接收模块
820
信任验证模块
830
用户认证模块
840
密钥生成模块
850
密钥发送模块

图8

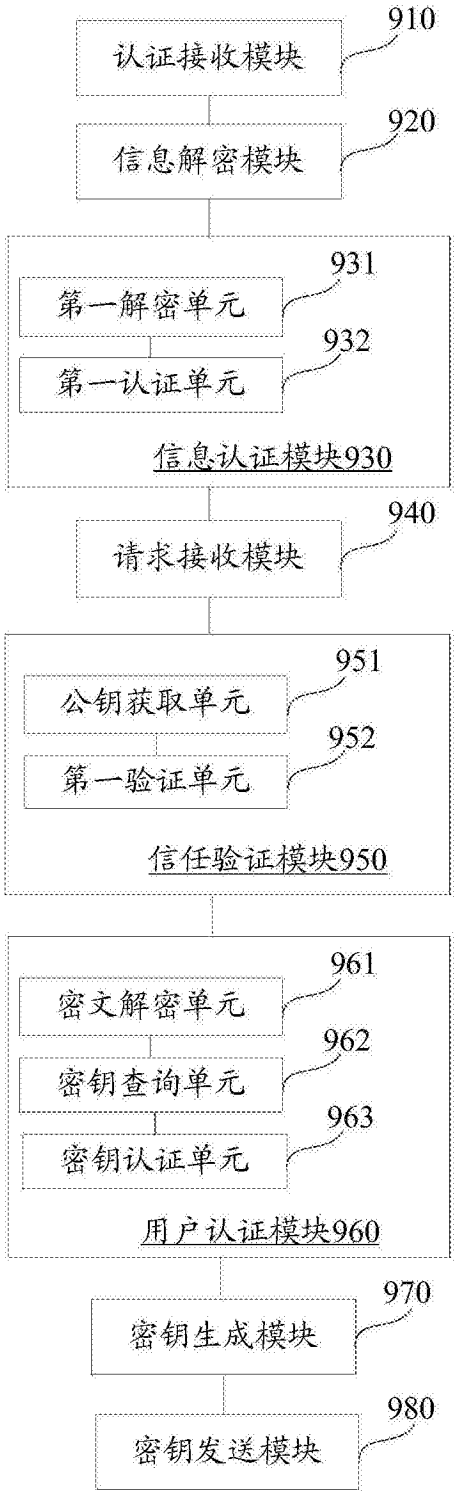

910
认证接收模块
920
信息解密模块
931
第一解密单元
932
第一认证单元
信息认证模块930
940
请求接收模块
951
公钥获取单元
952
第一验证单元
信任验证模块950
961
密文解密单元
962
密钥查询单元
963
密钥认证单元
用户认证模块960
970
密钥生成模块
980
密钥发送模块

图9

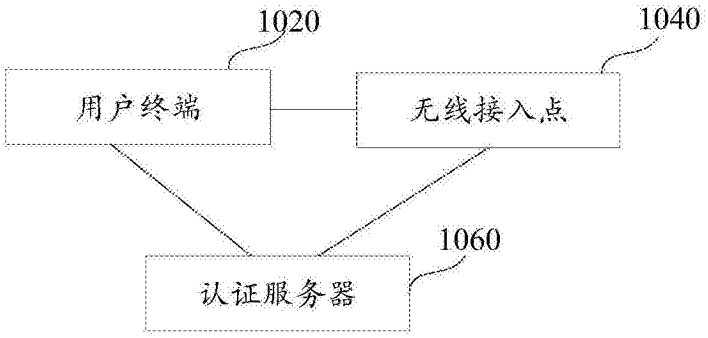


图10