(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2016 年 11 月 24 日 (24.11.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/184351 A1

(51) 国际专利分类号:
H04L 9/30 (2006.01) *H04L 9/32* (2006.01)

(21) 国际申请号: PCT/CN2016/081952

(22) 国际申请日: 2016 年 5 月 13 日 (13.05.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510262722.9 2015 年 5 月 21 日 (21.05.2015) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: 朴云 (PIAO, Yun); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (CN)。

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

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

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) Title: IP ADDRESS ALLOCATION METHOD AND SYSTEM FOR WIRELESS NETWORK

(54) 发明名称 : 无线网络的 IP 地址分配方法和系统

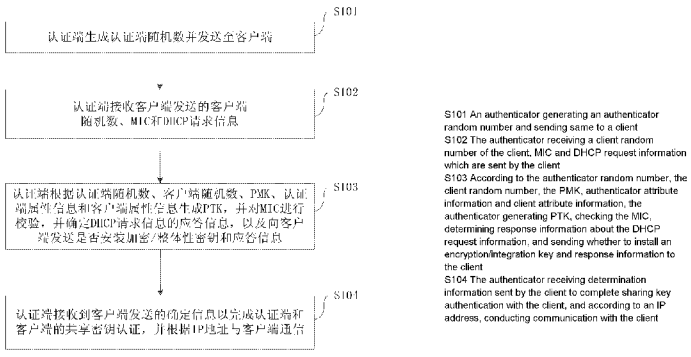

图 1

(57) Abstract: Proposed are an IP address allocation method and system for a wireless network. The method comprises: generating an authenticator random number and sending same to a client; receiving a client random number of the client, MIC and DHCP request information which are sent by the client; checking the MIC, determining response information about the DHCP request information, and sending whether to install an encryption/integration key and response information to the client; and receiving determination information sent by the client, so as to complete sharing key authentication with the client, and according to an IP address, conducting communication with the client. By means of the IP address allocation method for a wireless network in the embodiments of the present invention, the time needed for the client to access or switch a wireless network is reduced, further, the time for the client to affect an application layer when the client accesses or switches the wireless networks is reduced.

(57) 摘要:

[见续页]

WO 2016/184351 A1

本发明提出一种无线网络的 IP 地址分配方法和系统。该方法包括：生成认证端随机数并发送至客户端；接收客户端发送的客户端随机数、MIC 和 DHCP 请求信息；对 MIC 进行校验，并确定 DHCP 请求信息的应答信息，以及向客户端发送是否安装加密/整体性密钥和应答信息；接收到客户端发送的确定信息以完成和客户端的共享密钥认证，并根据 IP 地址与客户端通信。本发明实施例的无线网络的 IP 地址分配方法，减少了客户端接入或切换无线网络时所需的时间，进一步地，减少了客户端接入或切换无线网络时对应用层的影响时间。

无线网络的 IP 地址分配方法和系统

本申请要求 2015 年 05 月 21 日递交的申请号为 201510262722.9、发明名称为“无线网络的 IP 地址分配方法和系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及无线通信技术领域，尤其涉及一种无线网络的 IP 地址分配方法、系统、认证端和客户端。

背景技术

在无线网络如 Wi-Fi（Wireless-Fidelity）中，出于安全和便捷性的考虑，通常使用基于 PSK(Pre-shared key，预共享密钥)的 WPA（Wi-Fi Protected Access，保护无线网络安全系统）。

然而，在接入这样的无线网络时，认证端，如无线访问接入点 AP（Wireless Access Point）和客户端，如站 station 通过 EAPOL-key（EAP （Extensible Authentication Protocol，可扩展身份验证协议） over LAN （Local Area Network，局域网） key）包的四次握手进行认证和密钥的协商，并且，在密钥协商好之后，如果客户端设置的是动态 IP 获取方式，则需要通过 DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）获取或续约上次使用过的 IP 地址。相关技术存在的问题是，客户端接入无线网络或者切换无线网络时，只有在无线链路层的连接后才开始 IP 地址获取或续约，建立有效网络的耗时长。

发明内容

本发明旨在至少在一定程度上解决相关技术中的技术问题之一。

为此，本发明的第一个目的在于提出一种无线网络的 IP 地址分配方法。该方法减少了客户端接入或切换无线网络时所需的时间。

本发明的第二个目的在于提出一种无线网络的 IP 地址分配系统。

本发明的第三个目的在于提出一种认证端。

本发明的第四个目的在于提出一种客户端。

为了实现上述目的，本发明第一方面实施例的无线网络的 IP 地址分配方法，包括：

生成认证端随机数并发送至客户端；接收所述客户端发送的客户端随机数、消息完整性校验码 MIC 和动态主机配置协议 DHCP 请求信息，其中，所述客户端生成所述客户端随机数，并根据所述认证端随机数、所述客户端随机数、成对主密钥 PMK、认证端属性信息和客户端属性信息生成临时成对密钥 PTK；根据所述认证端随机数、所述客户端随机数、所述成对主密钥 PMK、所述认证端属性信息和所述客户端属性信息生成所述临时成对密钥 PTK，并对所述 MIC 进行校验，并确定所述 DHCP 请求信息的应答信息，以及向所述客户端发送是否安装加密/整体性密钥和所述应答信息，以使所述客户端安装加密/整体性密钥并根据所述应答信息确定 IP 地址；接收到所述客户端发送的确定信息以完成和所述客户端的共享密钥认证，并根据所述 IP 地址与所述客户端通信。

本发明实施例的无线网络的 IP 地址分配方法，和客户端进行四次握手的同时完成客户端 IP 地址的申请或续约，这样只要建立了无线链路连接的共享密钥认证之后即可申请或续约 IP 地址，也就是说，只要建立了无线链路连接的共享密钥认证之后上层应用即可开始通信发送和接收数据，无需再进行申请或续约 IP 地址，从而减少了客户端接入或切换无线网络时所需的时间，进一步地，减少了客户端接入或切换无线网络时对应用层的影响时间。

为了实现上述目的，本发明第二方面实施例的无线网络的 IP 地址分配系统，包括：认证端和客户端，其中，所述认证端，用于生成认证端随机数并发送至所述客户端；所述客户端，用于生成客户端随机数，并根据所述认证端随机数、所述客户端随机数、成对主密钥 PMK、认证端属性信息和客户端属性信息生成临时成对密钥 PTK，并发送所述客户端随机数、消息完整性校验码 MIC 和动态主机配置协议 DHCP 请求信息至所述认证端；所述认证端，还用于根据所述认证端随机数、所述客户端随机数、所述成对主密钥 PMK、所述认证端属性信息和所述客户端属性信息生成所述临时成对密钥 PTK，并对所述 MIC 进行校验，并确定所述 DHCP 请求信息的应答信息，以及向所述客户端发送是否安装加密/整体性密钥和所述应答信息；所述客户端，还用于安装加密/整体性密钥并根据所述应答信息确定 IP 地址，并发送确定信息至所述认证端以完成所述认证端和所述客户端的共享密钥认证，并根据所述 IP 地址与所述认证端进行通信。

本发明实施例的无线网络的 IP 地址分配系统，在认证端和客户端进行四次握手的同时完成客户端 IP 地址的申请或续约，这样只要建立了无线链路连接的共享密钥认证之后即可申请或续约 IP 地址，也就是说，只要建立了无线链路连接的共享密钥认证之后上层应用即可开始通信发送和接收数据，无需再进行申请或续约 IP 地址，从而减少了客户端

接入或切换无线网络时所需的时间，进一步地，减少了客户端接入或切换无线网络时对应用层的影响时间。

为了实现上述目的，本发明第三方面实施例的认证端，包括：第一生成模块，用于生成认证端随机数；第一发送模块，用于将所述认证端随机数发送至客户端；第一接收模块，用于接收所述客户端发送的客户端随机数、消息完整性校验码 MIC 和动态主机配置协议 DHCP 请求信息，其中，所述客户端生成所述客户端随机数，并根据所述认证端随机数、所述客户端随机数、成对主密钥 PMK、认证端属性信息和客户端属性消息生成临时成对密钥 PTK；第二生成模块，用于根据所述认证端随机数、所述客户端随机数、所述成对主密钥 PMK、所述认证端属性信息和所述客户端属性信息生成所述临时成对密钥 PTK；校验模块，用于对所述 MIC 进行校验；确认模块，用于确定所述 DHCP 请求信息的应答信息；第二发送模块，用于向所述客户端发送是否安装加密/整体性密钥和所述应答信息，以使所述客户端安装加密/整体性密钥并根据所述应答信息确定 IP 地址；第二接收模块，用于接收所述客户端发送的确定信息以完成和所述客户端的共享密钥认证，并根据所述 IP 地址与所述客户端通信。

本发明实施例的认证端，在接收客户端发送的客户端随机数和 MIC 的同时接收 DHCP 请求信息，并在发送是否安装加密/整体性密钥的同时发送 DHCP 请求信息的应答信息，使得在认证端和客户端进行四次握手的同时完成客户端 IP 地址的申请或续约，从而减少了客户端接入或切换无线网络时所需的时间，进一步地，减少了客户端接入或切换无线网络时对应用层的影响时间。

为了实现上述目的，本发明第四方面实施例的客户端，包括：第一接收模块，用于接收认证端发送的认证端随机数；第一生成模块，用于生成客户端随机数；第二生成模块，用于根据所述认证端随机数、所述客户端随机数、成对主密钥 PMK、认证端属性信息和客户端属性信息生成临时成对密钥 PTK；第一发送模块，用于将所述客户端随机数、消息完整性校验码 MIC 和动态主机配置协议 DHCP 请求信息发送至所述认证端；第二接收模块，用于接收所述认证端发送的是否安装加密/整体性密钥和所述 DHCP 请求信息的应答信息，以安装加密/整体性密钥并根据所述应答信息确定 IP 地址；第二发送模块，用于向所述认证端发送确定信息以完成所述认证端和所述客户端的共享密钥认证，并根据所述 IP 地址与所述认证端通信。

本发明实施例的客户端，在发送客户端随机数和 MIC 的同时发送 DHCP 请求信息，并在接收是否安装加密/整体性密钥的同时接收到 DHCP 请求信息的应答信息，使得在认

证端和客户端进行四次握手的同时完成客户端 IP 地址的申请或续约，从而减少了客户端接入或切换无线网络时所需的时间，进一步地，减少了客户端接入或切换无线网络时对应用层的影响时间。

本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中，

图 1 是根据本发明一个实施例的无线网络的 IP 地址分配方法的流程图；

图 2 是根据本发明一个实施例的四次握手的流程图；

图 3 是根据本发明一个实施例的无线网络的 IP 地址分配系统的结构框图；

图 4 是根据本发明一个实施例的认证端的结构框图；

图 5 是根据本发明一个实施例的客户端的结构框图。

具体实施方式

下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能理解为对本发明的限制。相反，本发明的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

在本发明的描述中，需要说明的是，除非另有明确的规定和限定，术语 “相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连。对于本领域的普通技术人员而言，可以具体情况理解上述术语在本发明中的具体含义。此外，在本发明的描述中，除非另有说明，“多个”的含义是两个或两个以上。

流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被

本发明的实施例所属技术领域的技术人员所理解。

相关技术中，为了保证无线通信的安全，认证端和客户端之间建立无线链路连接时，首先进行认证端和客户端之间的共享密钥认证，在共享密钥认证之后客户端再申请或续约 IP 地址，根据申请或续约的 IP 地址才能在认证端和客户端之间进行数据的转发和接收，然而，此过程在客户端接入或切换无线网络时导致无线链路连接的耗时较长。其中，认证端和客户端之间进行共享密钥认证时通过四次握手实现，如果能在四次握手的同时实现 IP 地址的申请或续约，则可以节约申请或续约 IP 地址所需的时间，从而使得客户端接入或切换无线网络时无线链路连接的耗时减小，基于这样的构想，本发明提供了一种无线网络的 IP 地址分配方法、系统、认证端和客户端，下面参考附图进行详细描述。

图 1 是根据本发明一个实施例的无线网络的 IP 地址分配方法的流程图，图 2 是根据本发明一个实施例的四次握手的流程图。下面结合图 1 和图 2 说明本发明实施例的无线网络的 IP 地址分配方法。

如图 1 所示，该无线网络的 IP 地址分配方法包括：

S101，认证端生成认证端随机数 ANonce（Authenticator Nonce）并发送至客户端。其中，认证端可以是无线访问接入点（AP，Wireless Access Point），无线路由器等；客户端可以是站（Station），移动设备，无线设备等。也就是说，认证端和客户端是布置在无线网络中的设备，认证端负责客户端的身份认证并与客户端进行通信，对于认证端和客户端的具体设备本发明的实施例不进行限定。

具体地，认证端随机数为认证端只使用一次的数值，类型可以包括时间戳、大随机数和序列号等中的至少一种。认证端为认证方，客户端为申请方，认证端首先在无线网络范围内广播认证端随机数以使得无线网络范围内的客户端能够接收到该认证端随机数。

如图 2 所示，认证端发送认证端随机数至客户端，即认证端和客户端进行第一次握手，也就是说，认证端向客户端发送消息 1，该消息 1 中包含认证端生成的认证端随机数。

在本发明的一个实施例中，认证端和客户端通过 EAPOL-KEY（EAP （Extensible Authentication Protocol，可扩展身份验证协议） over LAN （Local Area Network，局域网）包进行数据发送。也就是说，在第一握手时，认证端向客户端发送携带认证端随机数的 EAPOL-KEY 包。

S102，认证端接收客户端发送的客户端随机数、MIC（Message Integrity Code，消息

完整性校验码）和 DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）请求信息，其中，客户端生成客户端随机数，并根据认证端随机数、客户端随机数、PMK（Pairwise Master Key，成对主密钥）、认证端属性信息和客户端属性信息生成 PTK（Pairwise Transient Key，临时成对密钥）。另外，认证端属性信息和客户端属性信息可以是唯一表示对应的设备的信息，例如，设备唯一标识符、MAC（Media Access Control，介质访问控制）地址等。

具体地，客户端获得认证端发送的认证端随机数后，生成客户端随机数 SNonce（Supplicant Nonce），客户端随机数为客户端只使用一次的数值，类型可以包括时间戳、大随机数和序列号等中的至少一种。然后，客户端根据认证端随机数、客户端随机数、PMK、认证端属性信息和客户端属性信息生成 PTK，从而实现客户端的 PTK 更新。再然后，如图 2 所示，客户端发送客户端随机数、MIC 和 DHCP 请求信息至认证端，即客户端和认证端进行第二次握手，也就是说，客户端向认证端发送消息 2，该消息 2 中包含客户端生成的客户端随机数、MIC 和 DHCP 请求信息，认证端接收到消息 2。

同样地，在本发明的一个实施例中，客户端将客户端随机数、MIC 和 DHCP 请求信息添加至 EAPOL-KEY 包并发送至认证端。

S103，认证端根据认证端随机数、客户端随机数、PMK、认证端属性信息和客户端属性信息生成 PTK，并对 MIC 进行校验，并确定 DHCP 请求信息的应答信息，以及向客户端发送是否安装加密/整体性密钥和应答信息，以使客户端安装加密/整体性密钥并根据应答信息确定 IP 地址。

具体地，认证端在接收到消息 2 之后，获得客户端生成的客户端随机数，并根据认证端随机数、客户端随机数、PMK、认证端属性信息和客户端属性信息生成 PTK，从而认证端完成 PTK 的更新。

在本发明的一个实施例中，认证端完成 PTK 的更新后，该无线网络的 IP 地址分配方法还包括：认证端向 DHCP 服务器转发 DHCP 请求信息；认证端接收 DHCP 服务器反馈的应答信息。具体地，如图 2 所示，客户端将 DHCP 请求信息添加至第二次握手的消息 2 中，认证端将接收到的 DHCP 请求信息转交给 DHCP 服务器进行处理，并获得 DHCP 服务器的处理结果。通常，如果认证端为家用路由器，这个 DHCP 服务器即是认证端本身。

认证端在获得应答信息之后，将应答信息和组临时密钥 GTK（Group Transient Key）发送至客户端。如图 2 所示，认证端和客户端进行第三次握手，即发送消息 3 至客户端，

该消息 3 中包括应答信息和 GTK，以使得客户端确定是否安装加密/整体性密钥。同样地，在本发明的一个实施例中，认证端将应答信息和 GTK 添加至 EAPOL-KEY 包并发送至客户端。

S104，认证端接收到客户端发送的确定信息以完成无线访问接入点和客户端的共享密钥认证，并根据 IP 地址与客户端通信。

具体地，客户端和无认证端进行第四次握手，客户端将确定信息发送给认证端之后，确定认证端和客户端的共享密钥认证完成，以确认本次四次握手结果，同时，也根据应答信息确定客户端的 IP 地址。

本发明实施例的无线网络的 IP 地址分配方法，在认证端和客户端进行四次握手的同时完成客户端 IP 地址的申请或续约，这样只要建立了无线链路连接的共享密钥认证之后即可申请或续约 IP 地址，也就是说，只要建立了无线链路连接的共享密钥认证之后上层应用即可开始通信发送和接收数据，无需再进行申请或续约 IP 地址，从而减少了客户端接入或切换无线网络时所需的时间，进一步地，减少了客户端接入或切换无线网络时对应用层的影响时间。

在本发明的一个实施例中，请求信息和应答消息分别以供应商特定信息元素 VSIE 格式作为密钥数据 KEY data 的扩展加入到 EAPOL-KEY 包中。具体地，四次握手和 EAPOL-KEY 包可以参考 802.11 等相关协议，VSIE 格式也可以参考 802.11 等相关协议，在此不再赘述。

在本发明的一个实施例中，请求信息和应答消息分别省去 sname 和 file 字段。由此，减少了 DHCP 请求信息以及 DHCP 应答信息构成的 VSIE 的长度，在传输过程中省去 DHCP 请求信息的 sname 和 file 字段，接收方（即认证端）处理时默认将这两个字段当做 0 处理。

在本发明的一个实施例中，将请求信息和应答消息分别以 EAPOL-KEY 加密密钥 KEK (EAPOL-Key Encryption Key)进行加密。由此，保证了安全性。

为了实现上述实施例，本发明的实施例还提出一种无线网络的 IP 地址分配系统。

图 3 是根据本发明一个实施例的无线网络的 IP 地址分配系统的结构框图。如图 3 所示，无线网络的 IP 地址分配系统包括：认证端 10 和客户端 20。

具体地，认证端 10 用于生成认证端随机数并发送至客户端 20。其中，认证端随机数为认证端 10 只使用一次的数值，类型可以包括时间戳、大随机数和序列号等中的至少一种。认证端 10 为认证方，客户端 20 为申请方，认证端 10 首先在无线网络范围内广播

认证端随机数以使得无线网络范围内的客户端 20 能够接收到该认证端随机数

如图 2 所示，认证端 10 发送认证端随机数至客户端 20，即认证端 10 和客户端 20 进行第一次握手，也就是说，认证端 10 向客户端 20 发送消息 1，该消息 1 中包含认证端 10 生成的认证端随机数。

在本发明的一个实施例中，认证端 10 和客户端 20 通过 EAPOL-KEY 包进行数据发送。也就是说，在第一握手时，认证端 10 向客户端 20 发送携带认证端随机数的 EAPOL-KEY 包。

客户端 20 用于生成客户端随机数，并根据认证端随机数、客户端随机数、PMK、认证端和客户端的属性信息生成 PTK，并发送客户端随机数、MIC 和 DHCP 请求信息至认证端 10。首先，客户端 20 获得认证端 10 发送的认证端随机数后，生成客户端随机数，客户端随机数为客户端 20 只使用一次的数值，类型可以包括时间戳、大随机数和序列号等中的至少一种。然后，客户端 20 根据认证端随机数、客户端随机数、PMK、认证端属性信息和客户端属性信息生成 PTK，从而实现客户端的 PTK 更新。再然后，如图 2 所示，客户端 20 发送客户端随机数、MIC 和 DHCP 请求信息至认证端 10，即客户端 20 和认证端 10 进行第二次握手，也就是说，客户端 20 向认证端 10 发送消息 2，该消息 2 中包含客户端 20 生成的客户端随机数、MIC 和 DHCP 请求信息，认证端 10 接收到消息 2。

同样地，在本发明的一个实施例中，客户端 20 将客户端随机数、MIC 和 DHCP 请求信息添加至 EAPOL-KEY 包并发送至认证端 10。

认证端 10 还用于根据认证端随机数、客户端随机数、PMK、认证端属性信息和客户端属性信息生成 PTK，并对 MIC 进行校验，并确定 DHCP 请求信息的应答信息，以及向客户端 20 发送是否安装加密/整体性密钥和应答信息。更具体地，认证端 10 在接收到消息 2 之后，获得客户端 20 生成的客户端随机数，并根据认证端随机数、客户端随机数、PMK、认证端属性信息和客户端属性信息生成 PTK，从而认证端 10 完成 PTK 的更新。认证端 10 在获得应答信息之后，将应答信息和 GTK 发送至客户端 20。如图 2 所示，认证端 10 和客户端 20 进行第三次握手，即发送消息 3 至客户端 20，该消息 3 中包括应答信息和 GTK，以使得客户端 20 确定是否安装加密/整体性密钥。同样地，在本发明的一个实施例中，认证端 10 将应答信息和 GTK 添加至 EAPOL-KEY 包并发送至客户端 20。

客户端 30 还用于安装加密/整体性密钥并根据应答信息确定 IP 地址，并发送确定信息至认证端 10 以完成认证端 10 和客户端 20 的共享密钥认证，并根据 IP 地址与认证端

10 进行通信。更具体地，客户端 20 和认证端 10 进行第四次握手，客户端 20 将确定信息发送给认证端 10 之后，确定认证端 10 和客户端 20 的共享密钥认证完成，以确认本次四次握手结果，同时，也根据应答信息确定客户端 20 的 IP 地址。

本发明实施例的无线网络的 IP 地址分配系统，在认证端和客户端进行四次握手的同时完成客户端 IP 地址的申请或续约，这样只要建立了无线链路连接的共享密钥认证之后即可申请或续约 IP 地址，也就是说，只要建立了无线链路连接的共享密钥认证之后上层应用即可开始通信发送和接收数据，无需再进行申请或续约 IP 地址，从而减少了客户端接入或切换无线网络时所需的时间，进一步地，减少了客户端接入或切换无线网络时对应用层的影响时间。

在本发明的一个实施例中，请求信息和应答消息分别以供应商特定信息元素 VSIE 格式作为密钥数据 KEY data 的扩展加入到 EAPOL-KEY 包中。具体地，四次握手和 EAPOL-KEY 包可以参考 802.11 等相关协议，VSIE 格式也可以参考 802.11 等相关协议，在此不再赘述。

在本发明的一个实施例中，请求信息和应答消息分别省去 sname 和 file 字段。由此，减少了 DHCP 请求信息以及 DHCP 应答信息构成的 VSIE 的长度，在传输过程中省去 DHCP 请求信息的 sname 和 file 字段，接收方（即认证端 10）处理时默认将这两个字段当做 0 处理。

在本发明的一个实施例中，将请求信息和应答消息分别以 EAPOL-KEY 加密密钥 KEK (EAPOL-Key Encryption Key)进行加密。由此，保证了安全性。

在本发明的一个实施例中，无线网络的 IP 地址分配系统还包括：DHCP 服务器（未示出），认证端 10 还用于向 DHCP 服务器转发 DHCP 请求信息；DHCP 服务器，用于向无线访问接入 10 点发送应答信息。更具体地，如图 2 所示，认证端 10 完成 PTK 的更新后，将接收到的 DHCP 请求信息转交给 DHCP 服务器进行处理，并获得 DHCP 服务器的处理结果。通常，如果认证端 10 为家用路由器，这个 DHCP 服务器即是认证端 10 本身。

为了实现上述实施例，本发明的实施例还提出一种认证端。

图 4 是根据本发明一个实施例的认证端的结构框图。如图 4 所示，认证端 10 包括：第一生成模块 110、第一发送模块 120、第一接收模块 130、第二生成模块 140、校验模块 150、确认模块 160、第二发送模块 170 和第二接收模块 180。

具体地，第一生成模块 110 用于生成认证端随机数。认证端随机数为认证端 10 只使

用一次的数值，类型可以包括时间戳、大随机数和序列号等中的至少一种。

第一发送模块 120 用于将认证端随机数发送至客户端 20。在本发明的一个实施例中，第一发送模块 120 通过 EAPOL-KEY 包将认证端随机数发送至客户端 20。

第一接收模块 130 用于接收客户端 20 发送的客户端随机数、MIC 和 DHCP 请求信息，其中，客户端 20 生成客户端随机数，客户端随机数为客户端只使用一次的数值，类型可以包括时间戳、大随机数和序列号等中的至少一种，并根据认证端随机数、客户端随机数、PMK、认证端和客户端的属性信息生成临时成对密钥 PTK，从而实现客户端 20 的 PTK 更新。客户端 20 发送客户端随机数、MIC 和 DHCP 请求信息至第一接收模块 130，同样地，在本发明的一个实施例中，客户端 20 将客户端随机数、MIC 和 DHCP 请求信息添加至 EAPOL-KEY 包并发送至第一接收模块 130。

第二生成模块 140 用于根据认证端随机数、客户端随机数、PMK、认证端属性信息和客户端属性信息生成临时成对密钥 PTK，从而认证端 10 完成 PTK 的更新。

校验模块 150 用于对 MIC 进行校验。

确认模块 160 用于确定 DHCP 请求信息的应答信息。更具体地，确认模块 160 向 DHCP 服务器转发 DHCP 请求信息；确认模块 160 接收 DHCP 服务器反馈的应答信息。如果认证端 10 为家用路由器，这个 DHCP 服务器即是认证端 10 本身。

第二发送模块 170 用于向客户端 20 发送是否安装加密/整体性密钥和应答信息，以使客户端 20 安装加密/整体性密钥并根据应答信息确定 IP 地址。在本发明的一个实施例中，第二发送模块 170 通过 EAPOL-KEY 包将发送是否安装加密/整体性密钥和应答信息发送至客户端 20。

第二接收模块 180 用于接收客户端 20 发送的确定信息以完成认证端 10 和客户端 20 的共享密钥认证，并根据 IP 地址与客户端 20 通信。在本发明的一个实施例中，客户端 20 通过 EAPOL-KEY 包将确定信息发送至第二接收模块 180。

在本发明的一个实施例中，请求信息和应答消息分别以供应商特定信息元素 VSIE 格式作为密钥数据 KEY data 的扩展加入到 EAPOL-KEY 包中。具体地，四次握手和 EAPOL-KEY 包可以参考 802.11 等相关协议，VSIE 格式也可以参考 802.11 等相关协议，在此不再赘述。

在本发明的一个实施例中，请求信息和应答消息分别省去 sname 和 file 字段。由此，减少了 DHCP 请求信息以及 DHCP 应答信息构成的 VSIE 的长度，在传输过程中省去 DHCP 请求信息的 sname 和 file 字段，接收方（即认证端 10）处理时默认将这两个字段

当做 0 处理。

在本发明的一个实施例中，将请求信息和应答消息分别以 KEK 进行加密。由此，保证了安全性。

本发明实施例的认证端，在接收客户端发送的客户端随机数和 MIC 的同时接收 DHCP 请求信息，并在发送是否安装加密/整体性密钥的同时发送 DHCP 请求信息的应答信息，使得在认证端和客户端进行四次握手的同时完成客户端 IP 地址的申请或续约，从而减少了客户端接入或切换无线网络时所需的时间，进一步地，减少了客户端接入或切换无线网络时对应用层的影响时间。

为了实现上述实施例，本发明的实施例还提出一种客户端。

图 5 是根据本发明一个实施例的客户端的结构框图。如图 5 所示，客户端 20 包括：第一接收模块 210、第一生成模块 220、第二生成模块 230、第一发送模块 240、第二接收模块 250 和第二发送模块 260。

第一接收模块 210 用于接收认证端 10 发送的认证端随机数。在本发明的一个实施例中，认证端 10 通过 EAPOL-KEY 包将认证端随机数发送至第一接收模块 210。

第一生成模块 220 用于生成客户端随机数。

其中，认证端随机数为认证端 10 只使用一次的数值，类型可以包括时间戳、大随机数和序列号等中的至少一种。客户端随机数为终 20 端只使用一次的数值，类型可以包括时间戳、大随机数和序列号等中的至少一种。

第二生成模块 230 用于根据认证端随机数、客户端随机数、PMK、认证端属性信息和客户端属性信息生成 PTK。从而实现客户端 20 的 PTK 更新。

第一发送模块 240 用于将客户端随机数、MIC 和 DHCP 请求信息发送至认证端 10。在本发明的一个实施例中，第一发送模块 240 将客户端随机数、MIC 和 DHCP 请求信息添加至 EAPOL-KEY 包并发送至认证端 10。

第二接收模块 250 用于接收认证端 10 发送的是否安装加密/整体性密钥和 DHCP 请求信息的应答信息，以安装加密/整体性密钥并根据应答信息确定 IP 地址。在本发明的一个实施例中，认证端 10 将是否安装加密/整体性密钥和 DHCP 请求信息的应答信息添加至 EAPOL-KEY 包并发送至客户端 20。

第二发送模块 260 用于向认证端 10 发送确定信息以完成认证端 10 和客户端 20 的共享密钥认证，并根据 IP 地址与认证端通信。在本发明的一个实施例中，第二发送模块 260 将确定信息添加至 EAPOL-KEY 包并发送至认证端 10。

在本发明的一个实施例中，请求信息和应答消息分别以供应商特定信息元素 VSIE 格式作为密钥数据 KEY data 的扩展加入到 EAPOL-KEY 包中。具体地，四次握手和 EAPOL-KEY 包可以参考 802.11 等相关协议，VSIE 格式也可以参考 802.11 等相关协议，在此不再赘述。

在本发明的一个实施例中，请求信息和应答消息分别省去 sname 和 file 字段。由此，减少了 DHCP 请求信息以及 DHCP 应答信息构成的 VSIE 的长度，在传输过程中省去 DHCP 请求信息的 sname 和 file 字段，接收方（即认证端）处理时默认将这两个字段当做 0 处理。

在本发明的一个实施例中，将请求信息和应答消息分别以 KEK 进行加密。由此，保证了安全性。

本发明实施例的客户端，在发送客户端随机数和 MIC 的同时发送 DHCP 请求信息，并在接收是否安装加密/整体性密钥的同时接收到 DHCP 请求信息的应答信息，使得在认证端和客户端进行四次握手的同时完成客户端 IP 地址的申请或续约，从而减少了客户端接入或切换无线网络时所需的时间，进一步地，减少了客户端接入或切换无线网络时对应用层的影响时间。

应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列（PGA），现场可编程门阵列（FPGA）等。

在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

尽管已经示出和描述了本发明的实施例，本领域的普通技术人员可以理解：在不脱离本发明的原理和宗旨的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由权利要求及其等同物限定。

权 利 要 求 书

1、一种无线网络的IP地址分配方法，其特征在于，包括：

生成认证端随机数并发送至客户端；

接收所述客户端发送的客户端随机数、消息完整性校验码 MIC 和动态主机配置协议DHCP请求信息，其中，所述客户端生成所述客户端随机数，并根据所述认证端随机数、所述客户端随机数、成对主密钥 PMK、认证端属性信息和客户端属性信息生成临时成对密钥PTK；

根据所述认证端随机数、所述客户端随机数、所述成对主密钥 PMK、所述认证端属性信息和所述客户端属性信息生成所述临时成对密钥PTK，并对所述MIC进行校验，并确定所述 DHCP 请求信息的应答信息，以及向所述客户端发送是否安装加密/整体性密钥和所述应答信息，以使所述客户端安装加密/整体性密钥并根据所述应答信息确定IP地址；

接收到所述客户端发送的确定信息以完成和所述客户端的共享密钥认证，并根据所述IP地址与所述客户端通信。

2、根据权利要求 1 所述的无线网络的 IP 地址分配方法，其特征在于，通过EAPOL-KEY包和所述客户端进行数据发送。

3、根据权利要求2所述的无线网络的IP地址分配方法，其特征在于，所述请求信息和所述应答消息分别以供应商特定信息元素VSIE格式作为密钥数据KEY data的扩展加入到所述EAPOL-KEY包中。

4、根据权利要求3所述的无线网络的IP地址分配方法，其特征在于，所述请求信息和所述应答消息分别省去 sname 和 file 字段，并以 EAPOL-KEY 加密密钥 KEK 进行加密。

5、根据权利要求1所述的无线网络的IP地址分配方法，其特征在于，还包括：

向DHCP服务器转发所述DHCP请求信息；

接收所述DHCP服务器反馈的所述应答信息。

6、一种无线网络的IP地址分配系统，其特征在于，包括：认证端和客户端，其中，

所述认证端，用于生成认证端随机数并发送至所述客户端；

所述客户端，用于生成客户端随机数，并根据所述认证端随机数、所述客户端随机数、成对主密钥 PMK、认证端属性信息和客户端属性信息生成临时成对密钥 PTK，并发送所述客户端随机数、消息完整性校验码MIC和动态主机配置协议DHCP请求信息

至所述认证端；

所述认证端，还用于根据所述认证端随机数、所述客户端随机数、所述成对主密钥PMK、所述认证端属性信息和所述客户端属性信息生成所述临时成对密钥 PTK，并对所述 MIC 进行校验，并确定所述 DHCP 请求信息的应答信息，以及向所述客户端发送是否安装加密/整体性密钥和所述应答信息；

所述客户端，还用于安装加密/整体性密钥并根据所述应答信息确定 IP 地址，并发送确定信息至所述认证端以完成所述认证端和所述客户端的共享密钥认证，并根据所述 IP 地址与所述认证端进行通信。

7、根据权利要求 6 所述的无线网络的 IP 地址分配系统，其特征在于，所述认证端和所述客户端通过 EAPOL-KEY 包进行数据发送。

8、根据权利要求 7 所述的无线网络的 IP 地址分配系统，其特征在于，所述请求信息和所述应答消息分别以供应商特定信息元素 VSIE 格式作为密钥数据 KEY data 的扩展加入到所述 EAPOL-KEY 包中。

9、根据权利要求 8 所述的无线网络的 IP 地址分配系统，其特征在于，所述请求信息和所述应答消息分别省去 sname 和 file 字段，并以 EAPOL-KEY 加密密钥 KEK 进行加密。

10、根据权利要求 6 所述的无线网络的 IP 地址分配系统，其特征在于，还包括：DHCP 服务器，其中

所述认证端，还用于向所述 DHCP 服务器转发所述 DHCP 请求信息；

所述 DHCP 服务器，用于向所述认证端发送所述应答信息。

11、一种认证端，其特征在于，包括：

第一生成模块，用于生成认证端随机数；

第一发送模块，用于将所述认证端随机数发送至客户端；

第一接收模块，用于接收所述客户端发送的客户端随机数、消息完整性校验码 MIC 和动态主机配置协议 DHCP 请求信息，其中，所述客户端生成所述客户端随机数，并根据所述认证端随机数、所述客户端随机数、成对主密钥 PMK、认证端属性信息和客户端属性消息生成临时成对密钥 PTK；

第二生成模块，用于根据所述认证端随机数、所述客户端随机数、所述成对主密钥 PMK、所述认证端属性信息和所述客户端属性信息生成所述临时成对密钥 PTK；

校验模块，用于对所述 MIC 进行校验；

确认模块，用于确定所述 DHCP 请求信息的应答信息；

第二发送模块，用于向所述客户端发送是否安装加密/整体性密钥和所述应答信息，以使所述客户端安装加密/整体性密钥并根据所述应答信息确定 IP 地址；

第二接收模块，用于接收所述客户端发送的确定信息以完成和所述客户端的共享密钥认证，并根据所述 IP 地址与所述客户端通信。

12、一种客户端，其特征在于，包括：

第一接收模块，用于接收认证端发送的认证端随机数；

第一生成模块，用于生成客户端随机数；

第二生成模块，用于根据所述认证端随机数、所述客户端随机数、成对主密钥 PMK、认证端属性信息和客户端属性信息生成临时成对密钥 PTK；

第一发送模块，用于将所述客户端随机数、消息完整性校验码 MIC 和动态主机配置协议 DHCP 请求信息发送至所述认证端；

第二接收模块，用于接收所述认证端发送的是否安装加密/整体性密钥和所述 DHCP 请求信息的应答信息，以安装加密/整体性密钥并根据所述应答信息确定 IP 地址；

第二发送模块，用于向所述认证端发送确定信息以完成所述认证端和所述客户端的共享密钥认证，并根据所述 IP 地址与所述认证端通信。

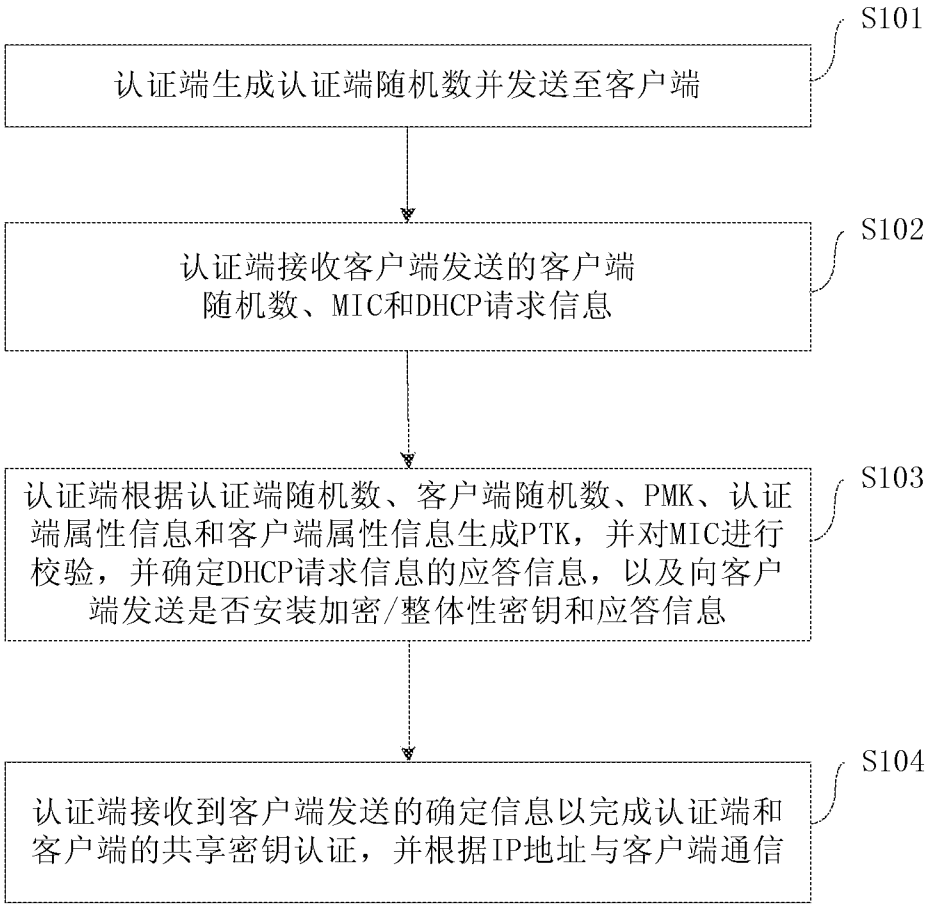
S101
认证端生成认证端随机数并发送至客户端
S102
认证端接收客户端发送的客户端随机数、MIC和DHCP请求信息
S103
认证端根据认证端随机数、客户端随机数、PMK、认证端属性信息和客户端属性信息生成PTK，并对MIC进行校验，并确定DHCP请求信息的应答信息，以及向客户端发送是否安装加密/整体性密钥和应答信息
S104
认证端接收到客户端发送的确定信息以完成认证端和客户端的共享密钥认证，并根据IP地址与客户端通信

图 1

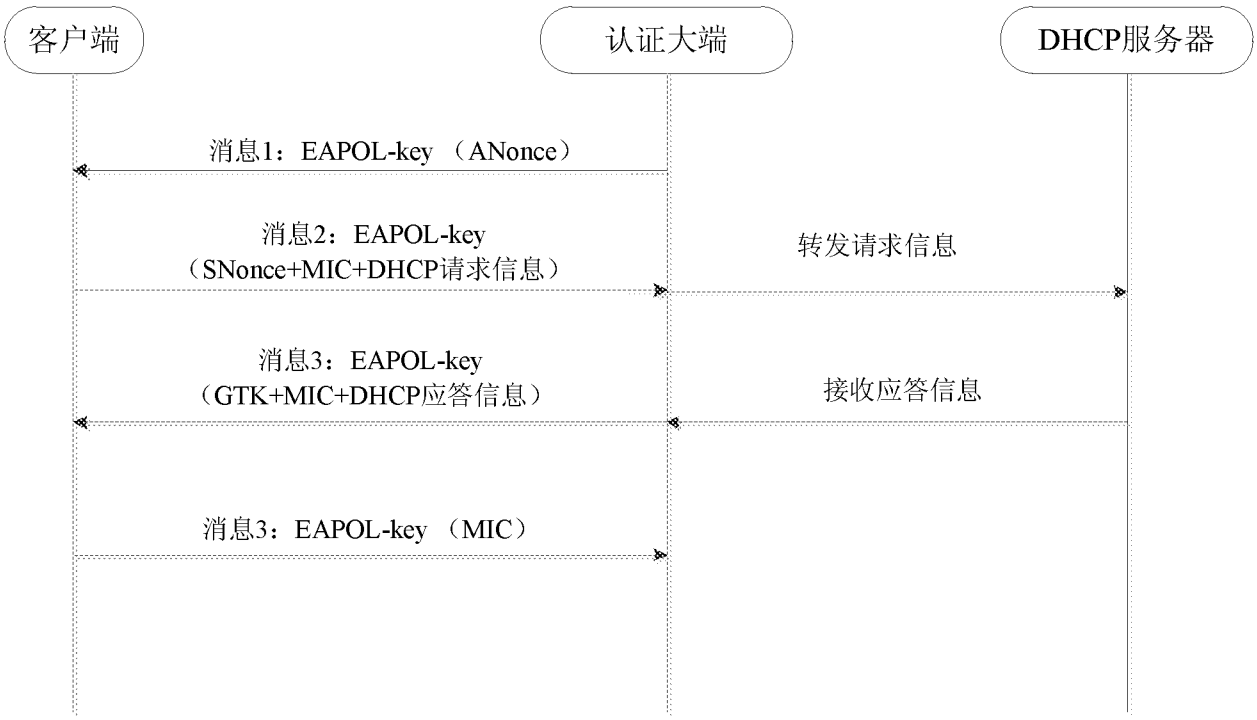
客户端
认证大端
DHCP服务器
消息1：EAPOL-key （ANonce）
消息2：EAPOL-key
（SNonce+MIC+DHCP请求信息）
转发请求信息
消息3：EAPOL-key
（GTK+MIC+DHCP应答信息）
接收应答信息
消息3：EAPOL-key （MIC）

图 2

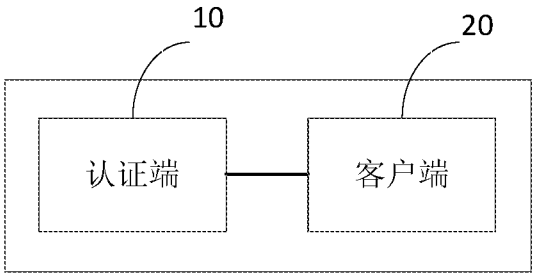
10
20
认证端
客户端

图 3

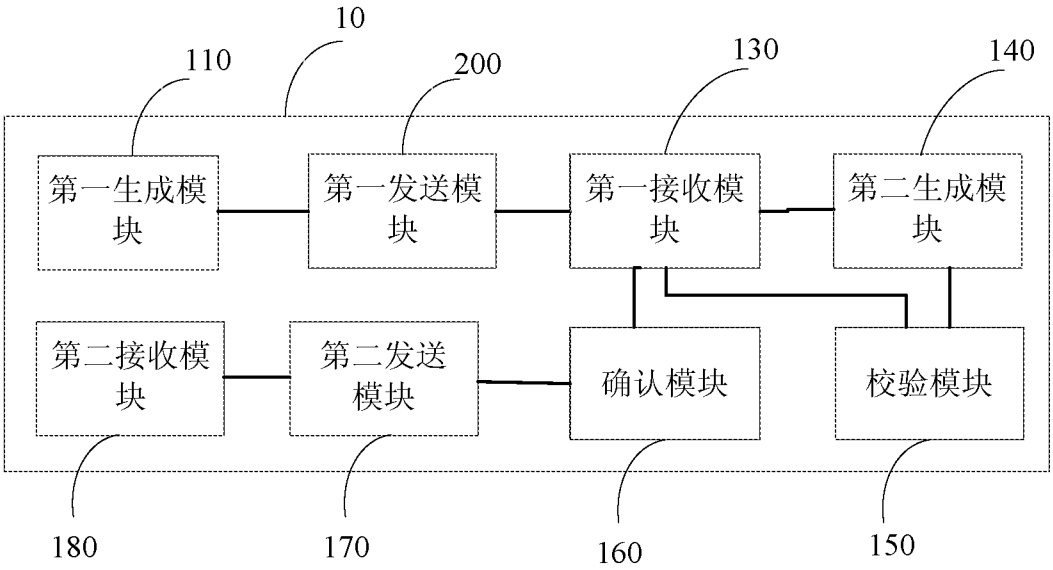
10
110
200
130
140
第一生成模块
第一发送模块
第一接收模块
第二生成模块
第二接收模块
第二发送模块
确认模块
校验模块
180
170
160
150

图 4

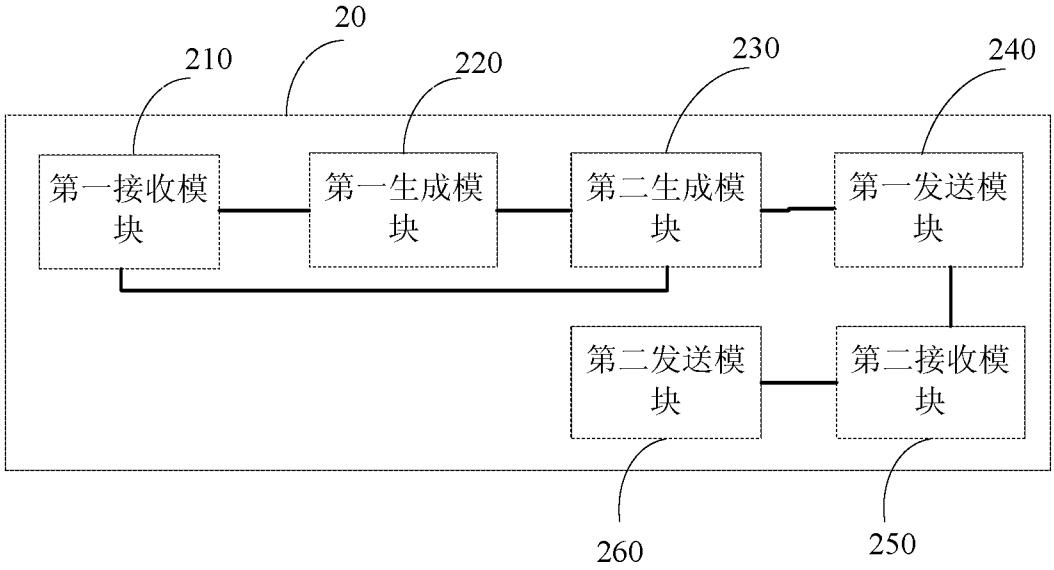
20
210
220
230
240
第一接收模块
第一生成模块
第二生成模块
第一发送模块
第二发送模块
第二接收模块
260
250

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/081952

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/30 (2006.01) i; H04L 9/32 (2006.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W; H04Q

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

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

CNTXT; VEN; CNABS; CNKI; BAIDU; Patentics: DHCP, access, establish+, random number, address, IP, IP address, client, time, distribut+, allocat+, authenticat+, reduc+, depress+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104219217 A (CHINA MOBILE COMMUNICATIONS CORPORATION) 17 December 2014 (17.12.2014) the abstract, claims 1 to 18	1-12
A	CN 101388770 A (HUAWEI TECHNOLOGIES CO., LTD.) 18 March 2009 (18.03.2009) the whole document	1-12
A	CN 105591748 A (HANGZHOU H3C TECHNOLOGIES CO., LTD.) 18 May 2016 (18.05.2016) the whole document	1-12
A	CN 101471767 A (HUAWEI TECHNOLOGIES CO., LTD.) 01 July 2009 (01.07.2009) the whole document	1-12
A	US 2006047835 A (GREAUX, JEFFREY EREC) 02 March 2006 (02.03.2006) the whole document	1-12

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

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 July 2016	03 August 2016
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer WU, Xinghua Telephone No. (86-10) 62089556

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/081952

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104219217 A	17 December 2014	None	
CN 101388770 A	18 March 2009	CN 101388770 B	22 August 2012
CN 105591748 A	18 May 2016	None	
CN101471767 A	01 July 2009	CN 101471767 B	14 September 2011
		WO 2009082950 A1	09 July 2009
US 2006047835 A1	02 March 2006	None	

国际检索报告

国际申请号 PCT/CN2016/081952

A. 主题的分类

H04L 9/30(2006.01)i; H04L 9/32(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L,H04W,H04Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNTXT;VEN;CNABS;CNKI;BAIDU,Patentics:接入，减少，随机数，分配，DHCP，IP地址，动态主机配置协议，客户端，认证，时间，access, establish+, random number, address, IP, client, time, distribut+, allocat+, authenticat+, reduc+,depress+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 104219217 A (中国移动通信集团公司) 2014年 12月 17日 (2014-12-17) 摘要，权利要求1-18	1-12
A	CN 101388770 A (华为技术有限公司) 2009年 3月 18日 (2009-03-18) 全文	1-12
A	CN 105591748 A (杭州华三通信技术有限公司) 2016年 5月 18日 (2016-05-18) 全文	1-12
A	CN 101471767 A (华为技术有限公司) 2009年 7月 1日 (2009-07-01) 全文	1-12
A	US 2006047835 A1 (GREAUX, JEFFREY EREC) 2006年 3月 2日 (2006-03-02) 全文	1-12

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

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

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

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

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

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

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 7月 29日	2016年 8月 3日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 吴兴华 电话号码 (86-10)62089556

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/081952

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	104219217	A	2014年 12月 17日		无		
CN	101388770	A	2009年 3月 18日	CN	101388770	B	2012年 8月 22日
CN	105591748	A	2016年 5月 18日		无		
CN	101471767	A	2009年 7月 1日	CN	101471767	B	2011年 9月 14日
				WO	2009082950	A1	2009年 7月 9日
US	2006047835	A1	2006年 3月 2日		无		