

(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
2013 年 12 月 5 日 (05.12.2013)



(10) 国际公布号
WO 2013/178017 A1

- (51) 国际专利分类号:
H04W 12/06 (2009.01)
- (21) 国际申请号: PCT/CN2013/075553
- (22) 国际申请日: 2013 年 5 月 13 日 (13.05.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210170228.6 2012 年 5 月 28 日 (28.05.2012) CN
- (71) 申请人: 中国移动通信集团公司 (CHINA MOBILE COMMUNICATIONS CORPORATION) [CN/CN]; 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。
- (72) 发明人: 邓辉 (DENG, Hui); 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。罗海云 (LUO, Haiyun); 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。曹振 (CAO, Zhen); 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。陈一帆 (CHEN, Yifan); 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。邵春菊 (SHAO, Chunju); 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。

(CN)。刘鸿 (LIU, Hong); 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。

(74) 代理人: 北京银龙知识产权代理有限公司 (DRAGON INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区西直门北大街 32 号院枫蓝国际中心 2 号楼 10 层, Beijing 100082 (CN)。

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

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,

[见续页]

(54) Title: METHOD, RELATED DEVICE, COMPUTER PROGRAM AND STORAGE MEDIUM FOR PROCESSING AUTHENTICATION INFORMATION IN WIRELESS LOCAL AREA NETWORK

(54) 发明名称: 无线局域网中认证信息处理方法及相关设备、计算机程序及存储介质

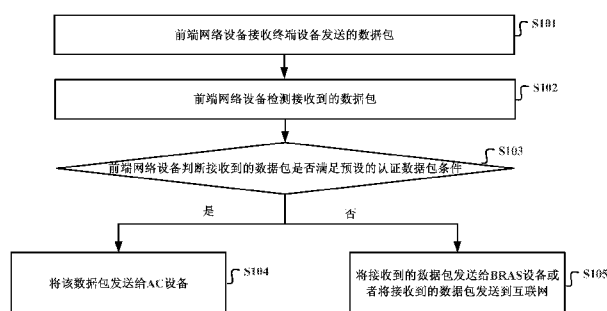


图 1 /Fig.1

S101 A FRONT END NETWORK DEVICE RECEIVES PACKETS FROM A TERMINAL DEVICE

S102 THE FRONT END NETWORK DEVICE DETECTS THE RECEIVED PACKETS

S103 THE FRONT END NETWORK DEVICE DETERMINES WHETHER THE RECEIVED PACKETS SATISFY A PRESET AUTHENTICATION PACKET CONDITION

S104 THE FRONT END NETWORK DEVICE SENDS THE PACKETS TO AN AC DEVICE

S105 THE FRONT END NETWORK DEVICE SENDS THE RECEIVED PACKETS TO A BRAS DEVICE OR INTERNET

(57) Abstract: A method, related network device, computer program and storage medium for processing authentication information in a wireless local area network (WLAN) are disclosed to reduce the data flow pass through an AC device, wherein, the method for processing the authentication information in the WLAN comprises the following steps: a front end network device receives packets from a terminal device, detects the packets, and sends the packets to the AC device when the packets are determined to satisfy a preset authentication packet condition, wherein the front end network is located before the AC device in the WLAN system.

(57) 摘要: 本发明公开了一种无线局域网中认证信息处理方法及相关网络设备、计算机程序及存储介质, 用以减少流经 AC 设备的数据流量, 其中, 无线局域网中认证信息处理方法, 包括: 前端网络设备接收终端设备发送的数据包, 所述前端网络设备位于 WLAN 系统中的 AC 设备之前; 并检测所述数据包; 以及确定所述数据包满足预设的认证数据包条件时, 将所述数据包发送给 AC 设备。

WO 2013/178017 A1



RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, **本国际公布:**

CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

— 包括国际检索报告(条约第 21 条(3))。

无线局域网中认证信息处理方法及相关设备、计算机程序及存储介质

技术领域

本发明涉及无线通信技术领域，尤其涉及一种无线局域网中认证信息处理方法及相关设备、计算机程序及存储介质。

背景技术

无线局域网 (WLAN, Wireless Local Area Network) 是一种能够在一定区域范围内支持移动特性的无线宽带接入方式，WLAN 为用户访问互联网提供了一种宽带接入方式。通过 WLAN 接入系统，用户能够使用万维网 (WWW, World Wide Web)，文件传输协议 (FTP, File Transfer Protocol)，E-mail 等各种互联网业务。WLAN 接入系统完成用户的接入，接入控制，计费信息采集以及业务管理和控制等。WLAN 接入系统主要由接入点 (AP, Access Point) 设备和业务控制 (AC, Access Controller) 设备以及其它相关网络设备组成。AP 设备是 WLAN 的小型无线基站设备，完成 802.11 系列标准的无线接入；AP 设备也是一种网络桥接器，是连接有线网络与无线网络的桥梁，任何 WLAN 终端设备均可通过相应的 AP 设备接入到有线网络资源。在安全控制方面，AP 设备可以通过网络标志和介质访问控制 (MAC 设备, Media Access Control) 地址来控制用户接入；同时 AP 设备支持有线等效保密 (WEP, Wired Equivalent Privacy) 空中加密，保护用户信息安全；在数据通讯方面，AP 设备负责完成它与 WLAN 终端设备之间所传输的数据包的加密和解密。

目前，运营商部署的 WLAN 网络，AP 设备负责提供无线信号，AC 设备作为接入控制器，负责属下多个 AP 设备的无线管理配置。通常，AC 设备有两种形态，一种是合一模式，即 AC 设备既负责 AP 设备的无线管理配置，也负责业务/认证控制。另一种是分离模式，即 AC 设备只负责 AP 设备的无线管理配置，业务/认证控制这部分功能放在另外一台设备上完成，通常是宽带远程接入服务器 (BRAS, Broadband Remote Access Server)。

由于在分离模式下，网络发展和融合面临了很多问题，首先基于分离模式下的性能管理需要网管系统分别从 BRAS 和 AC 设备进行数据采集，并同

时完成数据合并，需要网管进行较大改造；其次，分离模式下，由于认证功能在 BRAS 上执行，为了实现 EAP-PEAP/EAP-SIM 等无感知认证（从已有用户信息中获取认证信息，用户对于认证过程无感知）技术，需要增加 AC 设备和 BRAS 设备接口，用于下发认证成功后的密钥等信息，耗费周期较长，难以满足无感知认证的时间要求。因此，现有技术中通常采用合一模式部署 AC 设备。

目前流经 AP 设备的数据包可以包括以下两类：包含认证信息的认证数据包和包含非认证信息的普通数据包，目前，WLAN 接入系统中，各设备对数据包处理流程如下：AP 设备接收到终端设备发送的数据包后，不进行任何处理即发送给 AC 设备，AC 设备解析接收到的数据包，若 AC 设备确认接收到的数据包为认证数据包，将对认证数据包进行处理，否则，若为普通数据包将发送到互联网。由上述流程可知，现有技术中，AP 设备接收到的所有数据包均需要发送给 AC 设备，但是 AC 设备只需要处理其中的认证数据包，这样，一方面造成了 AC 设备成为数据流量的处理瓶颈，降低了 AC 设备的处理速度，另一方面也浪费了 AC 设备的处理资源。

发明内容

本发明实施例提供一种无线局域网中认证信息处理方法及相关设备、计算机程序及存储介质，用以减少流经 AC 设备的数据流量。

本发明实施例提供一种无线局域网认证信息处理方法，包括：

前端网络设备接收终端设备发送的数据包，所述前端网络设备位于无线局域网 WLAN 系统中的接入控制 AC 设备之前；并

检测所述数据包；以及

确定所述数据包满足预设的认证数据包条件时，将所述数据包发送给 AC 设备。

本发明实施例提供一种网络设备，所述网络设备位于无线局域网 WLAN 系统中的接入控制 AC 设备之前，以及

所述网络设备，包括：

接收单元，用于接收终端设备发送的数据包；

检测单元，用于检测所述数据包，并确定所述数据包满足预设的认证数

据包条件；

发送单元，用于检测单元确定所述数据包满足预设的认证数据包条件时，将所述数据包发送给 AC 设备。

本发明的实施例还提供一种用于执行上述方法的计算机程序及存储该计算机程序的存储介质。

本发明实施例提供的无线局域网中认证信息处理方法及相关设备，位于 WLAN 系统中的 AC 设备之前的网络设备检测接收到的数据包，以确定该数据包是否满足预设的认证数据包条件，当接收到的数据包满足预设的认证数据包条件时，将该数据包发送给 AC 设备处理，当接收到的数据包不满足预设的认证数据包条件时，将该数据包发送给 BRAS 或者互联网，从而使得非认证数据包不会发送给 AC 设备，从而，减少了 AC 设备处理的数据流量，节约了 AC 设备的处理资源，同时，由于减少了 AC 设备需要处理的数据流量，相应地，提高了 AC 设备的处理速度。

本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

图 1 为本发明实施例中，无线局域网中认证信息处理方法的实施流程示意图；

图 2 为本发明实施例中，AP 设备对接收到的数据包进行处理的处理流程示意图；

图 3 为本发明实施例中，网络设备的结构示意图。

具体实施方式

为了减少流经 AC 设备的数据流量，节约 AC 设备的处理资源，提高 AC 设备的处理速度，本发明实施例提供了一种无线局域网中认证信息处理方法及相关设备。

以下结合说明书附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明，并且

在不冲突的情况下，本发明中的实施例及实施例中的特征可以相互组合。

如图 1 所示，为本发明实施例中，无线局域网中认证信息处理方法的实施流程示意图，包括以下步骤：

S101、前端网络设备接收终端设备发送的数据包；

其中，前端网络设备可以为位于无线局域网（WLAN）系统中的 AC 设备之前的网络设备；终端设备发送的数据包可以为认证数据包，也可以为普通数据包。

S102、前端网络设备检测接收到的数据包；

S103、前端网络设备判断接收到的数据包是否满足预设的认证数据包条件，如果是，执行步骤 S104，否则执行步骤 S105；

S104、将该数据包发送给 AC 设备；

S105、将接收到的数据包发送给 BRAS 设备或者将接收到的数据包发送到互联网。

具体实施时，本发明实施例提供了两种实现方式，一种是在 AP 设备上对数据包进行检测，一种是在与 AP 设备连接的上一层网络设备上对数据包进行检测，其中，与 AP 设备连接的上一层网络设备可以但不限于为路由器设备或者交换机设备，以下分别介绍之。

实现方式一 AP 设备对数据包进行检测

当 AP 设备接收到终端设备发送的数据包之后，首先要判断该数据包是否为认证数据包，然后，将认证数据包的数据包发送给 AC 设备进行处理；对于非认证数据包的数据包，AP 设备将直接通过 AP 设备与 BRAS 设备之间的隧道进行转发，或者直接进行 MAC 层转换后发送到互联网中。

具体实施时，终端设备在接入 WLAN 时，需要完成网络认证，特别是在无感知网络认证中，通常采用不同的可扩展认证协议（EAP，Extensible Authentication Protocol）认证方法，当终端与网络之间采用 EAP 认证方法时，所传输的认证数据包称为 EAP 认证数据包，为了便于描述，本发明实施例中以认证数据包为 EAP 认证数据包为例进行说明。

EAP 认证数据包通过 EAPOL（EAP over LAN）协议进行封装，其数据包格式如表 1 所示：

表 1

意义	字节数
802.1x Ethernet type	2
Protocol version	1
Packet type	1
Packet body length	2
Packet body	根据长度可变

其中，802.1x Ethernet type 表示以太网类型，Protocol version 表示采用的协议版本号；Packet type 表示数据包类型；Packet body length 表示数据包包体长度；Packet body 表示包体，其占用的字节数由 Packet body length 确定。其中，Packet Type 包含以下几种数据包：a) EAP-PACKET：EAP 认证数据包，Packet Type=0；b) EAPOL-START：EAP 认证开始，Packet Type =1；c) EAPOL-LOGOFF：EAP 认证终止，Packet Type =2；d) EAPOL-KEY：EAP 认证成功后的密钥传递，Packet Type =3；e) EAPOL-ENCAPSULATED-ASF-ALERT：供通过非授权端口传递紧急信息，Packet Type =4。

目前，表 1 中的 802.1x Ethernet Type 已经由 IEEE 分配了一个值为 0x888E（16 进制数，对应十进制 34958），所有的 EAP 认证数据包都具有这个特征值，从而，AP 设备可以通过检查该字节的取值来判断出此数据包是 EAP 认证数据包。当 AP 设备识别出 EAP 认证数据包时，需要使用某种隧道协议对该 EAP 数据包进行封装，以便将该 EAP 认证数据包发送给 AC 设备。具体实施时，AP 设备对 EAP 认证数据包进行封装所采用的隧道协议可以但不限于包括无线接入点的控制和配置（CAPWAP，Control and Provision of Wireless Access Points）协议、GRE（通用路由封装）协议、UDP（用户数据包）协议、IP-in-IP（IP 里面封装 IP）协议或者 IPSEC（IP 安全协议）等，相应地，AP 设备使用该隧道协议建立与 AC 设备之间的隧道，并通过建立的隧道将封装

后的 EAP 认证数据包发送给 AC 设备。特别地，若 AP 设备和 AC 设备之间采用 CAPWAP 协议封装 EAP 认证数据包时，CAPWAP 协议中包含两种封装方式，CAPWAP-DATA 封装和 CAPWAP-CONTROL 封装，其中 CAPWAP-DATA（CAPWAP 数据）用于封装数据消息，CAPWAP-CONTROL（CAPWAP 控制）用于封装控制消息。本发明实施例中，既可以使用 CAPWAP-DATA 信道封装 EAP 认证消息，也可以使用 CAPWAP-CONTROL 信道封装 EAP 认证消息。以下以使用 CAPWAP-CONTROL 信道封装 EAP 认证消息为例进行说明。

具体实施时，使用 CAPWAP-CONTROL 信道封装 EAP 认证消息可以包括以下两种方式：

方式一

1) 扩展 CAPWAP 协议中的控制消息类型(Control Message Type)，目前控制消息类型共有 1-256 个可选值，其中仅有 1-26 被明确定义，但是不包含封装 EAP 认证的类型，因此本发明实施例中可以新增 MESSAGE TYPE——“AUTHENTICATION CONTROL”，定义其值为 27-255 中的正整数；

2) 扩展 CAPWAP 协议中消息元素（MESSAGE ELEMENT）——AUTHENTICATION PAYLOAD ELEMENT，定义所有 AUTHENTICATION CONTROL 消息中需要携带该 ELEMENT，现有技术定义了消息元素的通用 TLV 格式，其中 TYPE（类型）占 16 位，LENGTH（长度）占 16 位，VALUE（值）为可变长度（由 LENGTH 字段定义），且定义了 TYPE 字段从 1-49 的语义，本发明实施例中，如果使用 CAPWAP-CONTROL 消息传递 EAP 认证数据包，则需要定义新的消息元素类型，定义其值为 50-255 之间的正整数；

定义了上述的 MESSAGE TYPE 和 MESSAGE ELEMENT TYPE 之后，AP 设备就可以把 EAP 认证数据包封装在 CAPWAP-CONTROL 隧道中。AP 设备和 AC 设备在处理 AUTHENTICATION CONTROL 类型的消息时，由于该消息只是借用 CAPWAP-CONTROL 隧道，因此，不需要对 CAPWAP 中定义的序列号等元素做严格检查。

方式二

与方式一不同，方式二无需扩展 CAPWAP 的控制消息类型，而是使用现

有的 CAPWAP 控制消息封装认证数据包, 例如, 使用 Data Transfer Request/Response 封装 EAP 认证数据包, 该控制消息类型的取值分别为 21/22, 在该控制消息中, 具体的消息元素可以采用消息元素 Vendor Specific Payload (Type: 37) 来承载 EAP 认证数据包, 在使用时可以自行定义 Element ID 以识别 EAP 认证数据包。

特别地, 在现有技术中, 由 AC 设备记录终端设备使用的数据流量, 但是, 由于本发明实施例中, 在 AC 设备根据接收到的数据包对终端设备完成认证之后, 终端设备使用的数据流量 (即非认证数据包) 由 AP 设备直接转发至 BRAS 或者互联网, 因此, 流量计费和用户下线功能无法在 AC 设备上执行, 需要其他的功能实体才能实现流量计费。

较佳地, 本发明实施中, 可以由 AP 设备记录终端设备使用的数据流量信息, 并按照预设周期、通过 AP 设备和 AC 设备之间建立的隧道将终端设备使用的数据流量信息上报给 AC 设备, 当终端设备使用的数据流量达到该终端设备预设流量的一定比例时, 可以提供定期的提醒功能。例如, 当使用流量达到预设流量的 20%, 50%, 80% 时分别发送提醒消息给终端设备, 便于用户更好的管理自己的流量。具体的, AP 设备确定 AC 设备在根据接收到的数据包完成对终端设备的认证之后, 开始记录终端设备使用的数据流量信息, 具体实施时, AC 设备在完成对终端设备的认证之后, 会向 AP 设备发送认证成功消息, 例如 AC 设备在认证成功之后, 会向 AP 设备下发密钥, AP 设备以接收到密钥之后确定 AC 设备对终端设备认证成功。

基于上述分析, 本发明实施例中, AP 设备可以按照以下方法对数据包进行处理, 如图 2 所示, 包括以下步骤:

S201、AP 设备接收终端设备发送的数据包;

具体的, 终端设备需要与 WLAN 建立连接时, 将向 AP 设备发送认证数据包; 当终端设备与 WLAN 建立连接之后, 通过 WLAN 访问互联网时, 将向 AP 设备发送普通数据包。

S202、AP 设备检查接收到的数据包指定字段的取值;

S203、AP 设备判断该指定字段的取值是否为预设值, 如果是, 执行步骤 S204, 否则, 执行步骤 S205;

例如，若认证数据包为 EAP 认证数据包时，指定字段为 802.1x Ethernet Type，而其对应的取值为 0x888E。

S204、AP 设备确定接收到的数据包满足预设的认证数据包条件，并执行步骤 S206；

若接收到的数据包满足预设的认证数据包条件，AP 设备可以确定接收到的数据包为认证数据包。

S205、AP 设备确定接收到的数据包不满足预设的认证数据包条件，并执行步骤 S215；

S206、AP 设备采用 CAPWAP 协议对该数据包进行封装；

S207、将封装后的数据包通过与 AC 之间的 CAPWAP 隧道发送给 AC 设备；

S208、AC 设备根据接收到的数据包对终端设备执行认证操作；

S209、AC 设备完成对该终端设备的认证之后，通过 CAPWAP 隧道将密钥发送给 AP 设备；

S210、AP 设备将接收到的密钥转发给终端设备；

S211、终端设备通过接入的 WLAN 访问互联网；

具体的，终端设备访问互联网时，将向 AP 设备发送普通数据包，产生普通数据流量；

S212、AP 设备记录终端设备使用的数据流量信息；

S213、AP 设备按照预设周期、通过 CAPWAP 隧道将终端设备使用的数据流量信息上报给 AC 设备；

S214、AC 设备在终端使用的数据流量信息达到预设流量的一定比例时，通过短信方式通知终端设备；

S215、AP 设备将接收到的数据包转发给 BRAS 设备或者互联网。

具体的，AP 设备在确定接收到的数据包为普通数据包时，将该数据包通过与 BRAS 之间的隧道转发给 BRAS 设备处理，或者直接进行 MAC 层转换发送到互联网。

实现方式一中，在 AP 设备上通过认证数据包的特征值检测 AP 设备接收到的数据包是否为认证数据包，如果是，将该数据包进行封装后，通过 AP

设备和 AC 设备之间的隧道发送给 AC 设备进行处理，如果否，将该数据包发送通过 AP 设备与 BRAS 设备之间的隧道发送给 BRAS 设备处理或者发送给互联网，这样，只有部分流经 AP 设备的数据流量被转发至 AC 设备处理，从而，减少了 AC 设备上处理的数据流量，节约了 AC 设备的处理资源，相应地，能够提高 AC 设备的处理速度。

实现方式二

实现方式二中，在 WLAN 系统中、与 AP 设备连接且位于 AP 设备之后的网络设备上进行数据包检测，该网络设备可以为交换机设备或者路由器设备。需要说明的是，本发明实施例中，以终端发送的数据包在各网络设备间的传输顺序来描述各网络设备在网络中的位置，例如，数据包经由 AP 设备向交换机设备传输，则交换机设备为位于 AP 设备之后的网络设备。在这种实现方式下，该网络设备检测数据包是否为认证数据包的流程与 AP 设备检测数据包的流程相同，这里不再赘述。二者的区别在于：将确定为认证数据包的数据包发送给 AC 设备时的发送方式不同，具体的，当该网络设备确定接收到的数据包为认证数据包时，将对接收到的数据包进行处理，具体的，该网络设备使用隧道协议封装接收到的数据包；填充该数据包的源地址为与自身连接的 AP 设备的地址，以及填充该数据包的目标地址为 AC 设备地址；并根据填充的目标地址转发该数据包，使得 AC 设备能够接收到该数据包并进行处理。其中，该网络设备使用的隧道协议可以但不限于包括 CAPWAP 协议、GRE 协议、UDP 协议、IP-in-IP 协议或者 IP 安全协议 IPSEC 等。

AC 设备接收到数据包之后，根据接收到的数据包对终端设备进行认证，在完成对终端设备的认证之后，AC 设备将向 AP 设备发送认证成功消息，AP 设备接收到该认证成功消息之后，将开始记录该终端设备使用的数据流量信息，并按照预设周期上报给 AC 设备，使得 AC 设备能够根据终端设备使用的数据流量信息进行相应地处理，其处理方式与实现方式一中相同，这里不再赘述。

基于同一发明构思，本发明实施例中还提供了相关网络设备，这些，网络设备位于无线局域网 WLAN 系统中的接入控制 AC 设备之前，由于这些设备解决问题的原理与无线局域网中认证信息处理方法相似，因此这些设备的

实施可以参见方法的实施，重复之处不再赘述。

如图 3 所示，为本发明实施例提供的网络设备的结构示意图，包括：

接收单元 301，用于接收终端设备发送的数据包；

检测单元 302，用于检测接收单元 301 接收到的数据包，并确定该数据包满足预设的认证数据包条件；

发送单元 303，用于检测单元 302 确定该数据包满足预设的认证数据包条件时，将该数据包发送给 AC 设备。

具体实施时，发送单元 303，还可以用于确定该数据包不满足预设的认证数据包条件时，将该数据包发送给宽带远程接入服务器 BRAS 设备或者将该数据包发送到互联网。

较佳地，检测单元 302，可以包括：

检查子单元，用于检查所述数据包指定字段的取值；

确定子单元，用于若指定字段的取值为预设值时，确定所述数据包满足预设的认证数据包条件。

其中，该网络设备可以为 AP（接入点）设备，当该网络设备为接入点设备时，发送单元 303，可以用于使用隧道协议封装该数据包，以及封装后的数据包通过 AP 设备与 AC 设备之间的隧道发送给 AC 设备，该隧道使用该隧道协议建立。其中，使用的隧道协议可以但不限于包括 CAPWAP 协议、GRE 协议、UDP 协议、IP-in-IP 协议或者 IP 安全协议 IPSEC；具体实施时，若采用的隧道协议为 CAPWAP 协议时，发送单元 303，可以用于使用 CAPWAP-DATA 信道或者 CAPWAP-CONTROL 信道封装该数据包。

较佳地，若该网络设备为接入点设备时，接入点设备还可以包括：

记录单元，用于在接收到 AC 设备发送的认证成功消息之后，记录该终端设备使用的数据流量信息；

上报单元，用于按照预设周期向 AC 设备上报记录的数据流量信息。

具体实施时，该网络设备还可以为 WLAN 系统中，与 AP 设备连接且位于 AP 设备之后的网络设备，例如可以为路由器设备或者交换机设备，当该网络设备为与 AP 设备连接且位于 AP 设备之后的网络设备时，发送单元 303 可以用于使用隧道协议封装接收到的数据包；填充该数据包的源地址为 AP

设备的地址，以及填充该数据包的目标地址为 AC 设备地址；并根据填充的目标地址转发该数据包。

本发明实施例提供的无线局域网中认证信息处理方法及相关设备，在 WLAN 接入系统中，位于 AC 设备之前的网络设备，检测接收到的数据包，以确定该数据包是否满足预设的认证数据包条件，当接收到的数据包满足预设的认证数据包条件时，将该数据包发送给 AC 设备处理，当接收到的数据包不满足预设的认证数据包条件时，将该数据包发送给 BRAS 或者互联网，从而使得非认证数据包不会发送给 AC 设备，从而，减少了 AC 设备处理的数据流量，节约了 AC 设备的处理资源，同时，由于减少了 AC 设备需要处理的数据流量，相应地，提高了 AC 设备的处理速度。

本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本申请是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的

处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权利要求书

1、一种无线局域网中认证信息处理方法，其特征在于，包括：

前端网络设备接收终端设备发送的数据包，所述前端网络设备位于无线局域网 WLAN 系统中的接入控制 AC 设备之前；并

检测所述数据包；以及

确定所述数据包满足预设的认证数据包条件时，将所述数据包发送给 AC 设备。

2、如权利要求 1 所述的方法，其特征在于，还包括：

确定所述数据包不满足预设的认证数据包条件时，将所述数据包发送给宽带远程接入服务器 BRAS 设备或者将所述数据包发送到互联网。

3、如权利要求 1 所述的方法，其特征在于，按照以下方法确定所述数据包满足预设的认证数据包条件：

检查所述数据包指定字段的取值；以及

若指定字段的取值为预设值时，确定所述数据包满足预设的认证数据包条件。

4、如权利要求 3 所述的方法，其特征在于，所述前端网络设备为接入点 AP 设备；以及

将所述数据包发送给 AC 设备，具体包括：

使用隧道协议封装所述数据包；并

将封装后的数据包通过 AP 设备与 AC 设备之间的隧道发送给 AC 设备，所述隧道使用所述隧道协议建立。

5、如权利要求 4 所述的方法，其特征在于，若所述隧道协议为 CAPWAP 协议时，使用隧道协议封装所述数据包，具体包括：

使用 CAPWAP 数据 CAPWAP-DATA 信道或者 CAPWAP 控制 CAPWAP-CONTROL 信道封装所述数据包。

6、如权利要求 5 所述的方法，其特征在于，使用 CAPWAP-CONTROL 信道封装所述数据包时，还包括：

扩展 CAPWAP-CONTROL 消息类型,并定义扩展的 CAPWAP-CONTROL 消息类型值为 27~255 中任一整数值;或者

扩展 CAPWAP-CONTROL 消息元素,并定义扩展的 CAPWAP-CONTROL 消息元素类型值为 50~255 中任一整数值。

7、如权利要求 5 所述的方法,其特征在于,使用 CAPWAP-CONTROL 信道封装所述数据包,具体包括:

使用已定义的 CAPWAP-CONTROL 消息封装所述数据包,并定义 CAPWAP-CONTROL 消息的消息元素标识为指定值。

8、如权利要求 3 所述的方法,其特征在于,所述前端网络设备为与 AP 设备连接且位于 AP 设备之后的网络设备;以及

将所述数据包发送给 AC 设备,具体包括:

使用隧道协议封装所述数据包;并

填充所述数据包的源地址为所述 AP 设备的地址,以及填充所述数据包的目标地址为 AC 设备地址;并

根据所述目标地址转发所述数据包。

9、如权利要求 4~8 任一权利要求所述的方法,其特征在于,还包括:

所述 AP 设备在接收到所述 AC 设备发送的认证成功消息之后,记录所述终端设备使用的数据流量信息;并

按照预设周期向所述 AC 设备上报记录的数据流量信息。

10、一种网络设备,其特征在于,所述网络设备位于无线局域网 WLAN 系统中的接入控制 AC 设备之前,以及

所述网络设备,包括:

接收单元,用于接收终端设备发送的数据包;

检测单元,用于检测所述数据包,并确定所述数据包满足预设的认证数据包条件;

发送单元,用于检测单元确定所述数据包满足预设的认证数据包条件时,将所述数据包发送给 AC 设备。

11、如权利要求 10 所述的网络设备,其特征在于,

所述发送单元,还用于确定所述数据包不满足预设的认证数据包条件时,

将所述数据包发送给宽带远程接入服务器 BRAS 设备或者将所述数据包发送到互联网。

12、如权利要求 10 所述的网络设备，其特征在于，所述检测单元，包括：检查子单元，用于检查所述数据包指定字段的取值；

确定子单元，用于若指定字段的取值为预设值时，确定所述数据包满足预设的认证数据包条件。

13、如权利要求 10 所述的网络设备，其特征在于，所述网络设备为接入点 AP 设备，所述发送单元，具体用于使用隧道协议封装所述数据包，以及将封装后的数据包通过 AP 设备与 AC 设备之间的隧道发送给 AC 设备，所述隧道使用所述隧道协议建立。

14、如权利要求 13 所述的网络设备，其特征在于，

所述发送单元，具体用于使用 CAPWAP 数据 CAPWAP-DATA 信道或者 CAPWAP 控制 CAPWAP-CONTROL 信道封装所述数据包。

15、如权利要求 14 所述的网络设备，其特征在于，

所述发送单元，还用于使用 CAPWAP-CONTROL 信道封装所述数据包时，扩展 CAPWAP-CONTROL 消息类型，并定义扩展的 CAPWAP-CONTROL 消息类型值为 27~255 中任一整数；或者扩展 CAPWAP-CONTROL 消息元素，并定义扩展的 CAPWAP-CONTROL 消息元素类型值为 50~255 中任一整数。

16、如权利要求 14 所述的网络，其特征在于，

所述发送单元，具体用于使用已定义的 CAPWAP-CONTROL 消息封装所述数据包，并定义 CAPWAP-CONTROL 消息的消息元素标识为指定值。

17、如权利要求 13 所述的网络设备，其特征在于，还包括：

记录单元，用于在接收到 AC 设备发送的认证成功消息之后，记录所述终端设备使用的数据流量信息；

上报单元，用于按照预设周期向所述 AC 设备上报记录的数据流量信息。

18、如权利要求 10 所述的网络设备，其特征在于，所述网络设备为与接入点 AP 设备连接且位于 AP 设备之后的网络设备，所述发送单元，用于使用隧道协议封装所述数据包；填充所述数据包的源地址为所述 AP 设备的地址，

以及填充所述数据包的目标地址为 AC 设备地址；根据所述目标地址转发所述数据包。

19、一种包括指令的计算机程序，所述指令在由处理器执行时被设置成使所述处理器执行如权利要求1-9中任一项所述的方法。

20、一种存储了如权利要求19所述计算机程序的存储介质。

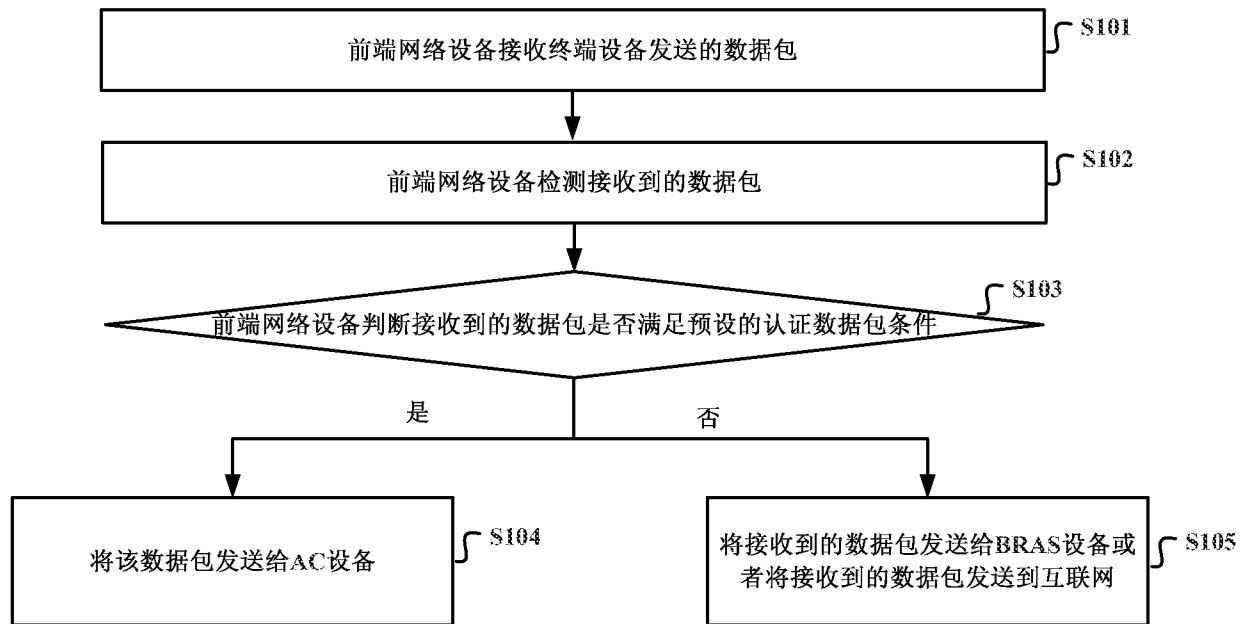


图 1

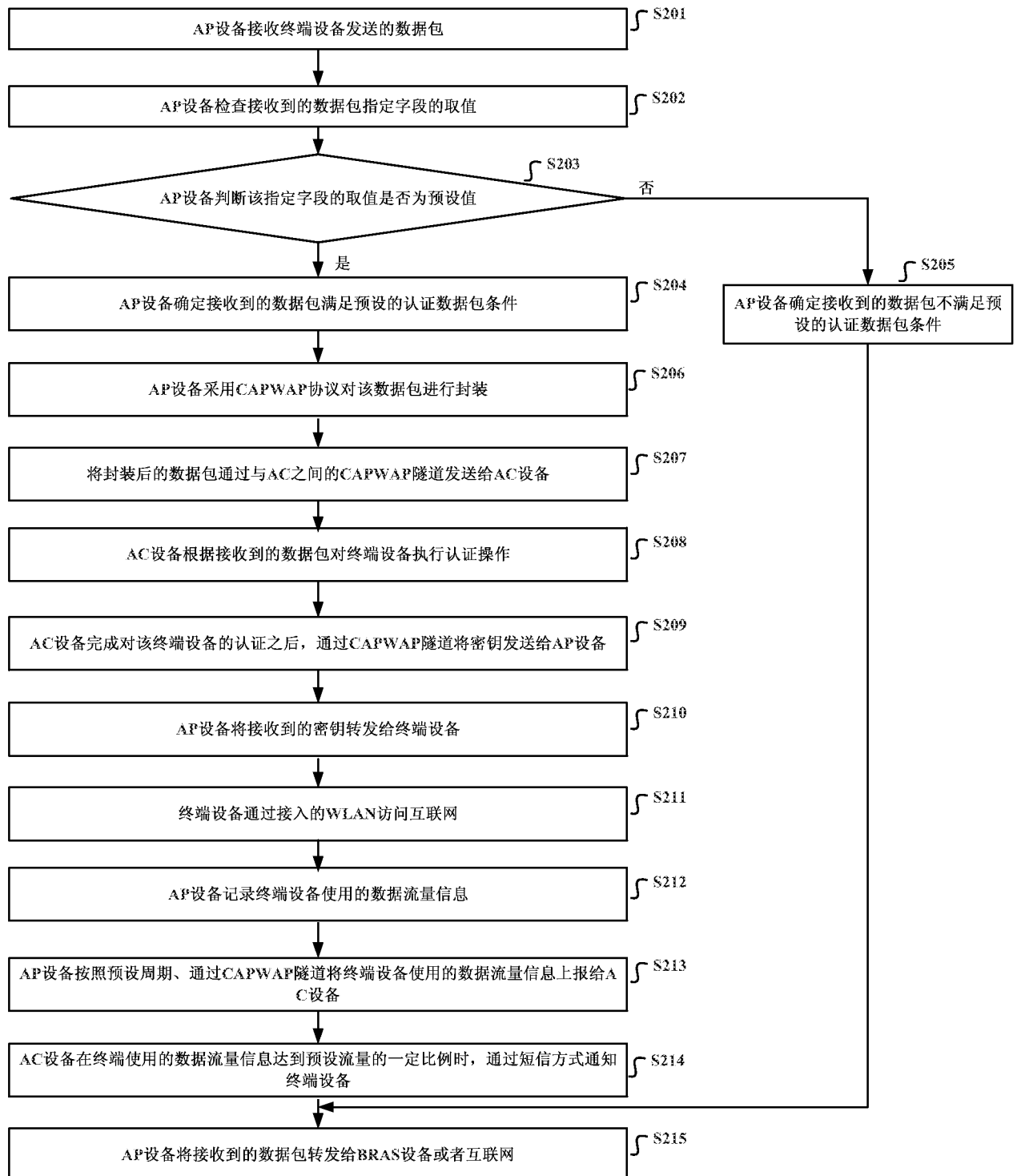


图 2

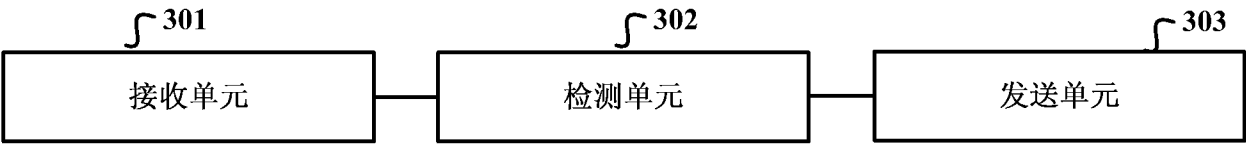


图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/075553

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06 (2009.01) 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)

IPC: H04W; H04L

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

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

CNABS, CNTXT, CNKI, VEN: wireless local area network, WLAN, authenticat+, access point, AP, access node, access control+, AC, detect+, check+, filter+, CAPWAP

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 1505329 A (ZTE CORPORATION) 16 June 2004 (16.06.2004) description, page 4, line 5 to page 5, line 19 and figures 1 to 3	1, 3, 10, 12, 19, 20
Y	the same as above	4-7, 13-16
Y	CN 101640621 A (ALCATEL SHANGHAI BELL CO., LTD.) 03 February 2010 (03.02.2010) description, page 2, lines 6-12, and page 12, line 19 to page 16, line 26 and figure 6	4-7, 13-16
A	US 7646713 B1 (ALCATEL LUCENT) 12 January 2010 (12.01.2010) the whole document	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 29 July 2013 (29.07.2013)	Date of mailing of the international search report 22 August 2013 (22.08.2013)
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 GONG, Silai Telephone No. (86-10) 62412152

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/075553

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1505329 A	16.06.2004	CN 1317859 C	23.05.2007
CN 101640621 A	03.02.2010	CN 101640621 B	19.09.2012
		WO 2010012152 A1	04.02.2010
US 7646713 B1	12.01.2010	None	

国际检索报告

国际申请号

PCT/CN2013/075553

A. 主题的分类

H04W 12/06 (2009.01) 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)

IPC: H04W, H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNABS, CNTXT, CNKI: 无线局域网, WLAN, 认证, 接入点, AP, 接入控制, AC, 检测, 检验, 过滤, CAPWAP

VEN: wireless local area network, WLAN, authenticat+, access point , AP, access node, access control+, AC, detect+,

check+, filter+, CAPWAP

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 1505329 A (深圳市中兴通讯股份有限公司) 16.6 月 2004 (16.06.2004) 说明书第 4 页第 5 行至第 5 页第 19 行, 附图 1-3	1, 3, 10, 12, 19, 20
Y	同上	4-7, 13-16
Y	CN 101640621 A (上海贝尔阿尔卡特股份有限公司) 03.2 月 2010 (03.02.2010) 说明书第 2 页第 6-12 行, 第 12 页第 19 行至第 16 页第 26 行, 附图 6	4-7, 13-16
A	US 7646713 B1 (ALCATEL LUCENT) 12.1 月 2010 (12.01.2010) 全文	1-20

☐ 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

29.7 月 2013 (29.07.2013)

国际检索报告邮寄日期

22.8 月 2013 (22.08.2013)

ISA/CN 的名称和邮寄地址:

中华人民共和国国家知识产权局

中国北京市海淀区蓟门桥西土城路 6 号 100088

传真号: (86-10)62019451

受权官员

龚思来

电话号码: (86-10) **62412152**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/075553

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN 1505329 A	16.06.2004	CN 1317859 C	23.05.2007
CN 101640621 A	03.02.2010	CN 101640621 B	19.09.2012
		WO 2010012152 A1	04.02.2010
US 7646713 B1	12.01.2010	无	