(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
2011 年 7 月 14 日 (14.07.2011)

PCT

(10) 国际公布号
WO 2011/082529 A1

(51) 国际专利分类号:
H04L 12/28 (2006.01)

(21) 国际申请号: PCT/CN2010/070062

(22) 国际申请日: 2010 年 1 月 8 日 (08.01.2010)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人 (对除美国外的所有指定国): 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。

(72) 发明人及
(75) 发明人/申请人 (仅对美国): 胡建如 (HU, Jianru) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。 刘国平 (LIU, Guoping) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。 颜林志 (YAN, Linzhi) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。 唐建文 (TANG, Jianwen) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (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 100140 (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, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 喊亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: METHOD, APPARATUS AND SYSTEM FOR UPDATING GROUP TRANSIENT KEY

(54) 发明名称: 一种组临时密钥更新方法、装置和系统

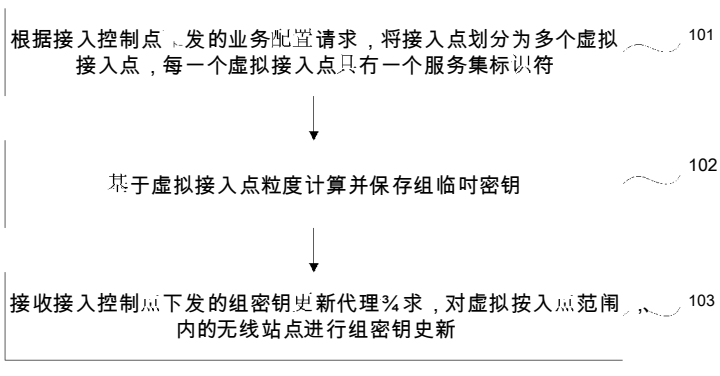

图 1 | Fig. 1

101 SEPARATING AN AP INTO SEVERAL VAPS ACCORDING TO THE SERVICE CONFIGURATION REQUEST SENT FROM AC, WHEREIN EACH VAP HAS A SSID
102 CALCULATING THE GTK BASED ON THE GRANULARITY OF THE VAP AND SAVING THE GTK
103 RECEIVING A GTK UPDATE DEPUTIZING REQUEST SENT FROM THE AC AND UPDATING GTK FOR STAS WITHIN THE RANGE OF THE VAP

(57) Abstract: A method, apparatus and system for updating Group Transient Key (GTK) are provided. Said method includes the following steps: separating an Access Point (AP) into several Virtual Access Points (VAP) according to the service configuration request sent from Access Control point (AC), wherein each VAP has a Service Set IDentifier (SSID); calculating the GTK based on granularity of the VAP and saving the GTK; receiving a GTK update deputizing request sent from the AC and updating the GTK for Stations (STA) within the range of the VAP. The method, apparatus and system provided by the embodiments of the present invention not only change the position of the GTK management from AC to AP, which highly releases the burden of AC under the network mode of thin AC centralized management, but also change the range of GTK update from the level of Extended Service Set (ESS) to that of VAP, which reduces the range of update and the network flow of the whole system, and lessens the shake of the system.

[见续页]

WO 2011/082529

本国际公布：

- 包括国际检索报告(条约第21条(3))。

(57) 摘要：

一种组临时密钥更新方法、装置和系统，所述方法包括以下步骤：根据接入控制点下发的业务配置请求将接入点划分为多个虚拟接入点，每个虚拟接入点具有一个服务组标识符；基丁虚拟接入点粒度计算并保存组临时密钥；接收接入控制点下发的组临时密钥更新代i甲请求，对虚拟接入点范围内的无线站点STA进行组临时密钥更新。通过本发明实施例提供的方法、装置和系统，不仅改变了组临时密钥的管理的位置，由AC转移到AP，在瘦AC集中式管i甲的网络模型下，极大的减轻了AC的负扣.，还改变了组临时密钥更新的范闱，由ESS级降到VAP级，缩小了更新的范围，减少了整个系统网络的流量，减轻了系统的震荡。

一种组临时密钥更新方法、装置和系统

技术领域

本发明涉及无线局域网,尤其涉及一种组临时密钥更新方法、装置和系统。

背景技术

WLAN (Wireless Local Area Network, 无线局域网)是20世纪90年代计算机与无线通信技术相结合的产物,它使用无线信道来接入网络,为通信的移动化,个人化和多媒体应用提供了潜在的手段,并成为宽带接入的有效手段之一。

802.11 是 IEEE 制定的一个无线局域网标准,其体系结构的组成包括:无线站点 STA(station),无线接入点 AP(access point),独立基本服务组 IBSS (independent basic service set),基本服务组 BSS (basic service set),分布式系统 DS (distribution system) 和扩展服务组 ESS (extended service set)。其中,无线站点 STA 通常由一台 PC 机或笔记本计算机加上一块无线网卡构成,也可以是非计算机终端上的能提供无线连接的嵌入式设备,例如支持 802.11 的手机。无线接入点 AP 可以看成是一个无线的 Hub, 它的作用是提供 STA 和现有骨干网络 (有线或无线的)之间的桥接,为无线用户提供对有线或无线网络的访问。

在802.11 网络中,出于对空间信息传播技术的安全性考虑,会采用组临时密钥 (Group Transient Key, GTK) 加密和解密广播和组播报文,同样出于安全性考虑,还需要定期和不定期的更新组临时密钥,在现有的瘦 AP 方案中,组临时密钥是在接入控制点AC (Access Control) 上基于ESS粒度进行更新,目前触发组临时密钥的更新有以下几点:

1、AC定期更新其管理的ESS 内用户 (无线站点STA) 的组临时密钥;

2、AC响应ESS 内用户触发的更新组临时密钥的请求,为该ESS 内所有用户更新组播密钥。

以上的更新操作，均需要在接入控制点 AC 上完成，由于 WLAN 网络的特点，在 AC 上管理的每一个 ESS 包括很多用户，用户的上线、下线是很频繁的现象，因此会经常触发组临时密钥的更新操作，由此触发 AC 系统频繁处理这些报文，导致系统的效率低下，性能下降，甚至瘫痪。

发明内容

本发明实施例提供一种组临时密钥更新方法、装置和系统，以避免由 AC 进行集中式频繁处理组临时密钥的更新操作带来的系统性能瓶颈问题。

本发明实施例的上述目的是通过如下技术方案实现的：

一种组临时密钥更新方法，所述方法包括：根据接入控制点下发的业务配置请求将接入点划分为多个虚拟接入点，每一个虚拟接入点具有一个服务组标识符；基于虚拟接入点粒度计算并保存组临时密钥；接收接入控制点下发的组密钥更新代理请求，对虚拟接入点范围内的无线站点进行组密钥更新。

一种接入装置，所述装置上划分有多个虚拟接入点，所述装置包括：检测单元，用于检测特定虚拟接入点是否需要更新组临时密钥；确定单元，用于在所述检测单元检测到所述特定虚拟接入点需要更新组临时密钥时，确定该特定虚拟接入点待更新的新组临时密钥；更新单元，用于将所述新组临时密钥发送给所述特定虚拟接入点范围内的所有在线无线站点以进行组临时密钥更新。

一种通信系统，所述系统包括接入点和无线站点，所述接入点连接所述无线站点，所述接入点上划分有多个虚拟接入点，所述接入点用于检测到特定虚拟接入点需要更新组临时密钥时，确定该特定虚拟接入点待更新的新组临时密钥；将确定的新组临时密钥发送给该特定虚拟接入点范围内的所有在线无线站点以进行组临时密钥更新。

通过本发明实施例提供的方法、装置和系统，不仅改变了组密钥的管理的位置，由 AC 转移到 AP，在瘦 AP 集中式管理的网络模型下，极大的减轻

了AC 的负担，还改变了组密钥更新的范围，由ESS 级降到VAP 级，缩小了更新的范围，减少了整个系统网络的流量，减轻了系统的震荡。

附图说明

此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，并不构成对本发明的限定。在附图中：

图1为本发明实施例的方法流程图；

图2为瘦AC 网络结构示意图；

图3为本发明一实施例的STA 通过AP 接入AC 的流程图；

图4为本发明一实施例的链路建立流程图；

图5为本发明一实施例的信息认证流程图；

图6为本发明实施例的一种GTK 更新方法流程图；

图7为本发明实施例的另外一种GTK 更新方法流程图；

图8为本发明实施例的另外一种GTK 更新方法流程图；

图9为本发明实施例的另外一种GTK 更新方法流程图；

图10 为本发明实施例的另外一种GTK 更新方法流程图；

图11 为本发明实施例的装置组成框图；

图12 为本发明实施例的系统组成框图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚明白，下面结合实施例和附图，对本发明实施例做进一步详细说明。在此，本发明的示意性实施例及其说明用于解释本发明，但并不作为对本发明的限定。

图1为本发明实施例提供的一种组临时密钥更新方法的流程图，该方法可以应用于无线局域网络WLAN 中接入点AP，请参照图1，该方法包括：

步骤101：将接入点AP 划分为多个虚拟接入点。

本实施例的方法可以应用于瘦AP 网络架构，图2为瘦AP 网络结构示

意图，请参照图2，该网络架构包括接入控制点AC、由AC集中控制的AC下连接的各个接入点AP、以及各个接入点下连接的无线站点设备STA。

在本实施例中，划分VAP处理可以是AP接收到接入控制点AC向AP下发业务配置请求后触发。接入点AP根据该业务配置请求中携带的业务类型、业务配置参数等，在AP上划分多个虚拟AP，即VAP，每一个VAP对应一个服务组标识符SSID，即用一个SSID标识。AP根据业务配置请求确定需要配置的业务类型，将该业务类型添加到已有的一个或多个VAP中。AP上划分VAP的处理也可以是业务支撑系统根据需要通过管理接口远程配置，当然也可以是操作维护人员通过配置命令行或人机交互界面配置等。其中，AP上划分的多个VAP中，每一个VAP可以包含一个或多个业务，比如AP上划分成3个VAPs，即VAP 1、VAP2和VAP3，其中，VAP 1只提供上网服务，VAP 2只提供视频服务，VAP 3既提供上网又提供视频服务等，本实施例并不以此作为限制。由于每个VAP逻辑上独立，多个VAP间互不影响，便于业务运营、维护和管理。

在本实施例中，VAP的SSID用于标识VAP，以便无线站点通过无线网卡扫描到SSID后，可以便利地接入到AP上多个VAP中与该SSID对应的VAP，以便与AC进行关联，以使STA接入到网络。

步骤102：在AP上基于VAP粒度计算组临时密钥；

在本实施例中，AP上多个VAP计算各自对应的组临时密钥，一个组临时密钥对应一个VAP，该VAP下的所有STA公用该组临时密钥，AC上可以不再保存基于ESS的GMK (Group Master Key，组主密钥)、GTK信息，而是在AP上基于VAP粒度进行计算并保存，也即AP为每个VAP计算并保存一份GMK、GTK信息。若该VAP下有用户(无线站点)下线或者其它原因需要更新组临时密钥时，只需要更新该VAP的组临时密钥(GTK)，同时通告该VAP下的所有在线用户。这样整个更新过程就不需要AC参与，同时每次更新也只涉及最多100左右的用户。

步骤 103：AP 将计算得到的组临时密钥发送相应 VAP 下的所有在线用户以更新该 VAP 的组临时密钥。

例如，AP 接收 AC 下发的组密钥更新代理请求，响应该组密钥更新代理请求，确定多个 VAP 中需要更新组临时密钥的 VAP, 对确定的 VAP 范围内的所有在线 STA 进行组密钥更新。

在本实施例中，在 AP 上检测是否需要为该 AP 上特定 VAP 更新组临时密钥，以便触发更新该特定 VAP 的处理。

在本发明的一实施例中，检测是否需要为该 AP 上特定 VAP 更新组临时密钥是通过 AP 检测 AC 发送的组密钥更新代理请求实现的。AP 检测到 AC 发送的组密钥更新代理请求，确定需要更新组临时密钥的 VAP, 在确定的 VAP 范围内进行组临时密钥的更新。

在本发明的另一实施例中，检测是否需要为该 AP 上特定 VAP 更新组临时密钥是通过 AP 检测其覆盖区域内的 STA 的连接状态实现的。AP 检测到其覆盖区域内特定 STA 从在线状态变成下线状态，如果确定需要为该 STA 所属 VAP 更新组临时密钥，在该 STA 所属 VAP 范围内进行组临时密钥的更新。

由于整个更新过程就不需要 AC 参与，减轻了 AC 的处理负担；另外，原 AC 管理的 ESS 包括其下连接的所有 AP，本发明实施例中将更新的范围由 AC 管理的 ESS 级降到 AP 的 VAP 级，缩小了更新的范围，因此减少了整个系统网络的流量，减轻了系统的震荡。

图 3 为 STA 通过 AP 接入网络时，AP 根据本发明实施例提供的方法的处理流程图，请参照图 3，该接入流程包括：

步骤 301：STA 通过其上的无线网卡扫描附近的无线信号，得到一组无线接入列表，也即本实施例的 AP 在划分 VAP 后提供的一组服务组标识符 SSID, 该无线站点 STA 选择其中一个进行连接；

在本实施例中，根据认证方式的不同，需要输入密码、提供证书等方式证明是合法接入，这些可以通过现有技术的方式实现，在此不再赘述。

在本实施例中，STA 选择一个 SSID 进行无线连接可以通过图 4 所示的步骤完成，但本实施例并不以此作为限制，请参照图 4，该方法包括：

步骤 401：STA 向 AP 发送链路验证请求（Authentication request-open system）；

其中，该链路验证请求中也可以携带选择的 VAP 的 SSID 和 STA 的用户标识。

步骤 402: AP 接收所述链路验证请求，进行链路验证并向 STA 返回链路认证响应；

步骤 403：接收到 AP 返回的链路认证响应后，STA 经由 AP 向 AC 发送关联请求（Association request）；

其中，该关联请求中可以携带 STA 选择的 VAP 的 SSID 和 STA 的用户标识。

步骤 404: AC 决策该 STA 可以接入时，在 AC 上建立 VAP 和所述 STA 的关联关系，向所述 STA 返回关联响应（Association response），允许该 STA 接入无线网络，同时 AC 记录 STA 的关联信息，如 STA 的 MAC 地址、VAP、SSID 等。

其中，关联响应中可以携带 STA 和 VAP 的关联关系，如 SSID 和 STA 的对应关系信息。由于 STA 和 AC 间交互的消息都经由 AP 转发，AP 可以截取关联响应，如果确定 AC 对 STA 认证成功，根据关联响应中的 VAP 和 STA 的关联关系在 AP 上建立 STA 和 VAP 的关联。至此，AP 上也保存了 STA 的 MAC 和 VAP、SSID 等对应关系信息，此时无线链路已经接通。

步骤 302: 无线链路接通后，STA 经由 AP 与 AC 进行信息认证；

在本实施例中，该信息认证过程可以通过四次握手过程实现，在这四次握手过程中，AC 不将 GTK 信息发送到 STA, 请参照图 5，该过程包括如下步骤：

步骤 501：AC 向 STA 发送消息 1;

其中，该消息 1 包含一个随机值 A-nonce ，是四次握手消息中的第一个消息，与现有的四次握手消息 (4-Way Handshake Message) 相同，在此不再赘述。

在本实施例中，STA 根据该 A-nonce, 向 AC 返回一些认证信息，这是现有技术的内容，在此不再赘述。

其中，nonce 是为了防范重放攻击的随机值，A-nonce 表示 AC 发送给 STA 的随机数。

步骤 502: STA 经由 AP 向 AC 发送消息 2;

其中，该消息 2 包含 STA 的 MAC 地址、消息验证码 MIC 以及 S-nonce ，其中，MIC 是一个保护该消息 2 不被篡改的消息验证码，S-nonce 表示 STA 发送给 AC 的随机数。同样的，该消息 2 是四次握手消息中的第二个消息，与现有的四次握手消息 (4-Way Handshake Message) 相同，在此不再赘述。

在本实施例中，AC 根据该消息 2 中的 STA 的 MAC 地址和 S-nonce 以及 AC 的 MAC 地址和 A-nonce 计算出 PTK (Pairwise Transient Key, 成对临时密钥)，根据该 PTK 计算出 MIC, 将计算出的 MIC 与消息 2 中的 MIC 进行比较，以验证该 STA 是否合法，这里可以通过现有技术的手段实现，在此不再赘述。

在本实施例中，如果验证的结果为计算出的 MIC 与消息 2 中的 MIC 相同，则该 STA 合法。

步骤 503: AC 经由 AP 向 STA 发送消息 3;

其中，该消息 3 包含 AC 的 MIC 校验值以及 AC 的加密状态，同样的，该消息 3 是四次握手消息中的第三个消息，第三个消息表明 AC 核实 STA 是否知道 PMK, 以及通知 STAAC 准备安装和使用数据加密密钥，与现有的四次握手消息 (4-Way Handshake Message) 相同，在此不再赘述。

在本实施例中，STA 根据该消息 3 中的 MIC 校验值，与自己的 MIC 进行比较，以确定 AC 是否为可信任一方，并根据该消息 3 中的 AC 的加密状

态，确定该AC是否已经准备安装和使用数据加密密钥。

步骤504: STA经由AP向AC发送消息4;

其中，该消息4包含了密钥核实信息，同样的，该消息4是四次握手消息中的第四个消息，与现有的四次握手消息（4-Way Handshake Message）相同，在此不再赘述。

在本实施例中，AC根据该消息4，确定密钥正准备安装和开始加密，同时根据该消息4确定握手过程结束。

步骤303：信息认证成功后，接入控制点AC下发PTK到VAP后，由VAP保存PKT信息，用来对单播报文进行加密和解密，同时启动GTK的更新。

在本实施例中，经过STA和AC的四次握手过程，AC将计算获得的成对临时密钥PTK发送给VAP，由VAP收到PTK后，启动组临时密钥更新过程。

在本实施例中，VAP启动GTK的更新，可以通过两次握手过程实现，请继续参照图5，该过程包括：

步骤505: AP向STA发送消息5;

其中，该消息5包含了组临时密钥，其为组密钥握手消息1（Group Key Handshake Message 1）。

在本实施例中，AP是以VAP的粒度下发组临时密钥，也即在VAP的范围内，向VAP范围的所有在线STA下发组临时密钥。

步骤506: STA向AP发送消息6;

其中，消息6为消息5的响应消息，其为组密钥握手消息2（Group Key Handshake Message 2）。

在本实施例中，STA接收到组临时密钥后，进行组临时密钥的更新，并通过消息6向AP返回更新完毕的信息。

在本实施例中，握手过程的消息可以为EAPOL-Key（Extensible Authentication Protocol over LAN-Key，基于局域网的扩展认证协议密钥）报文，格式和现有的EAPOL-Key报文的报文格式一样，包括：描述类型、密

钥信息、密钥长度、重复计时器、Key Nonce、EAPOL-Key IV、密钥起始序列、密钥标志符、密钥 MIC (16)、密钥数据长度 (2)、密钥数据 (0…1) 等字段，其中，描述类型字段为 254，标志这个报文是 WPA1 的报文，描述类型字段为 2，标志这个报文是 WPA2 的报文；密钥信息字段包含了几个字段，提供密钥类型和怎样使用的信息，也包含各种与握手过程相关的控制位；密钥长度字段用字节表示的密钥长度，主要对于成对密钥，尽管实际的 PTK 没有在这个密钥帧中发送，这是 PTK 的长度，它是目标密钥；重复计时器字段的值随着每个消息而增长来探测任何以重复旧消息的攻击企图，当这个消息是一个 ACK 请求的回应时例外，在这个情况下，那个被"回复"的重复值插入到此字段；Key Nonce 字段的当前值用于派生出临时成对密钥和组密钥；EAPOL-Key IV 字段时用于对于组密钥的传输，GTK 使用 EAPOL-Key 加密字连同这个 IV 值进行加密，这个加密过的 GTK 放在密钥数据区；密钥起始序列字段在密钥安装后，希望收到的第一个帧的序列号这个序列号用于防止重复攻击；密钥标志符字段没有于 WPA, 在将来它可能用于使能事先建立多个密钥；密钥 MIC 字段是一个完整性校验值，计算的范围是从 EAPOL 协议版本字段到密钥材料结束 (在计算过程中，这个字段置 0)；密钥数据长度字段以字节为单位定义了密钥数据字段的长度，密钥数据字段可以不同于实际密钥本身；密钥数据字段为需要秘密传送的数据，例如，在组密钥情况下，这是加密的 GTK; 在一些成对密钥信息情况下，这个字段携带了一个信息要素。

其中，密钥信息字段说明如表一所示：

0-3 比特	目前未用置0
4-9 比特	握手不同阶段的控制位
10-1 1 比特	密钥指数，在组密钥的情况下指明密钥的索引。这允许通过安装新的组密钥稍侯进行更新。新的组密钥的索引位置不同于现在的组密钥的索引位置
12 比特	密钥类型：区分成对密钥和组密钥消息
13~15 比特	标志版本并且允许在将来使用不同的方案和密钥加密方法。

表一

其中，4~9 比特说明如表二所示：

请求（4）	这个标志位用于申请者请求认证方初始化一个新的四次握手过程来更新密钥
错误（5）	在TKIP中，如果移动设备检测到一个MIC校验失败，一个包含着错误的标志位位置位的消息将发往接入点。请求标志比特也置位，请求一个更新密钥操作
安全（6）	当四次握手的时候密钥交互完成，标志着连接现在是安全时，这个标志位置位
MIC （7）	当MIC已经计算并已插入到MIC字段，这个标志置位
ACK（8）	在从认证方发送的消息中这个标志比特标示认证方期待申请者的回应
安装（9）	对于成对密钥，这个标志比特表示新的密钥应该被安装生效。对于组密钥，这个该置0

表二

图6为根据本发明实施例提供的方法AP根据STA的主动请求对该STA接入的VAP范围内的所有STA进行组密钥更新的流程图，请参照图6，该方法包括：

步骤601：AP接收STA的组临时密钥更新请求，表一中的密钥信息字段中第十二个比特用来表明是否是组密钥更新报文；

步骤602: AP更新所述STA接入的VAP的组临时密钥；

AP可以根据组临时密钥更新请求报文中的MAC地址信息,找到该STA关联的VAP, 根据VAP再查找对应的组临时密钥;该存储在本地的与该VAP标识对应的组临时密钥是AP在接收到组临时密钥更新请求之前，自身计算并保存的，组临时的计算方法是现有技术的内容，不再赘述。

步骤603:AP向所述STA接入的VAP范围内的所有在线STA发送更新后的组临时密钥的报文。

图7为根据本发明实施例提供的方法，AP在STA正常下线时对该STA原来接入的VAP范围内的所有STA进行组密钥更新的流程图，请参照图7，该方法包括：

步骤701：AP接收STA的去关联请求：STA离开VAP后，会向AP发送去关联报文，AP收到报文后先删除AP上该STA的信息，再通知AC删除之前保存的STA信息，如STA的MAC、VAP、SSID等，

步骤702: AP更新所述STA原来接入的VAP的组临时密钥；

AP 可以根据去关联请求报文中的 MAC 地址信息，找到该 STA 关联的 VAP, 根据 VAP 再查找对应的组临时密钥；该存储在本地的与该 VAP 标识对应的组临时密钥是 AP 在接收到组临时密钥更新请求之前，自身计算并保存的，组临时的计算方法是现有技术的内容，不再赘述。

步骤 703：AP 向所述 STA 原来接入的 VAP 范围内的 STA 发送更新后的组临时密钥的报文。

由此，AP 触发了 VAP 范围内的 STA 的组临时密钥的更新。

图 8 为根据本发明实施例提供的方法，AP 在 STA 异常下线时对该 STA 原来接入的 VAP 范围内的所有 STA 进行组密钥更新的流程图，请参照图 8，该方法包括：

步骤 801：AP 检测 STA 是否下线；

在本实施例中，AP 可以根据报文流量检测 STA 是否下线。

步骤 802: AP 定期的检测 AP 芯片上对应的 STA 是否有流量统计，芯片上根据 STA 的 MAC 统计，通过如果检测到 STA 没有流量，则认为 STA 下线，则 AP 更新该 STA 原来接入的 VAP 的组临时密钥；

步骤 803：AP 向所述 STA 原来接入的 VAP 范围内的所有在线 STA 发送更新后的组临时密钥的报文。

由此，AP 触发了 VAP 范围内的 STA 的组临时密钥的更新。

图 9 为根据本发明实施例提供的方法，AP 在 STA 漫游时对该 STA 原来接入的 VAP 范围内的所有 STA 进行组密钥更新的流程图，请参照图 9，该方法包括：

步骤 901：AP 接收 STA 的去关联或去认证请求；

在本实施例中，STA 离开了老的 VAP, 去新的 VAP 认证，会向老的 VAP 发出去关联或者去认证请求。

步骤 902: AP 更新所述 STA 原来接入的 VAP 的组临时密钥；

在本实施例中，老的 VAP 收到该去关联或去认证请求后，触发这个 VAP

范围内的 STA 进行组密钥更新。

AP 可以根据去关联请求或去认证请求报文中的 MAC 地址信息，找到该 STA 关联的 VAP, 根据 VAP 再查找对应的组临时密钥；该存储在本地的与该 VAP 标识对应的组临时密钥是 AP 在接收到组临时密钥更新请求之前，自身计算并保存的，组临时的计算方法是现有技术的内容，不再赘述。

步骤 903：AP 向所述 STA 原来接入的 VAP 范围内的 STA 发送更新后的组临时密钥的报文。

由此，AP 代理 AC 触发了 VAP 范围内的 STA 的组临时密钥的更新。

图 10 为根据本发明实施例提供的方法，AP 定时更新 VAP 范围内的所有 STA 的组密钥更新的流程图，请参照图 10，该方法包括：

步骤 1001： 定时更新组临时密钥；

步骤 1002: 向 VAP 范围内的 STA 发送更新后的组临时密钥的报文。

通过本实施例的方法，AP 根据 AC 的组密钥更新代理请求，在需要更新组临时密钥时，代替 AC 在 VAP 范围内进行组临时密钥的更新，由于整个更新过程就不需要 AC 参与，减轻了 AC 的处理负担，又由于更新的范围由 ESS 级降到 VAP 级，缩小了更新的范围，因此减少了整个系统网络的流量，减轻了系统的震荡。

图 11 为本发明实施例提供的接入装置组成框图，请参照图 11，该装置上划分有多个虚拟接入点，所述装置包括：

检测单元 111，用于检测特定虚拟接入点是否需要更新组临时密匙。

确定单元 112，用于在检测单元 111 检测到特定虚拟接入点需要更新组临时密匙时，确定该特定虚拟接入点待更新的新组临时密匙。

更新单元 113，用于将所述新组临时密匙发送给所述特定虚拟接入点范围内在线无线站点以进行组临时密匙更新。

所述接入装置还包括划分单元 114，用于根据接入控制点的业务配置请求将在所述接入装置上划分多个虚拟接入点。

其中，所述检测单元 111 具体可以包括第一检测模块 1111 和第二检测模块 1112，其中：

所述第一检测模块 1111 用于根据报文流量检测到无线站点下线时，判定所述无线站点所属的虚拟接入点需要更新组临时密匙。

所述第二检测模块 1112 用于检测到无线站点发送的去关联请求或去认证请求时，确定所述无线站点所属的虚拟接入点需要更新组临时密钥。

所述更新单元 113 还可以定时将新组临时密匙向虚拟接入点下的无线站点发送。

本实施例的装置的各组成部分分别用于实现前述方法实施例的各方法的步骤，由于在方法实施例中，已经对各步骤进行了详细说明，在此不再赘述。

本实施例的装置可以应用于接入点 AP，在此不再赘述。

通过本实施例的装置，AP 根据 AC 的组密钥更新代理请求，在需要更新组临时密钥时，代替 AC 在 VAP 范围内进行组临时密钥的更新，由于整个更新过程就不需要 AC 参与，减轻了 AC 的处理负担，又由于更新的范围由 ESS 级降到 VAP 级，缩小了更新的范围，因此减少了整个系统网络的流量，减轻了系统的震荡。

图 12 为本发明实施例提供的一种通信系统组成框图，请参照图 12，该系统包括接入点（AP）122 以及无线站点 (STA) 123，AP 122 上划分有多个虚拟接入点，其中：

AP 122 用于检测到特定虚拟接入点需要更新组临时密钥时，确定该特定虚拟接入点待更新的新组临时密钥；将确定的新组临时密钥发送给该特定虚拟接入点范围内的所有在线无线站点以进行组临时密钥更新。

所提供的系统还可以包括接入控制点（AC) 121，所述 AC 121 用于向 AP 122 下发业务配置请求，AP 122 可以根据该业务配置请求将 AP 122 划分成多个虚拟接入点。

具体的，AC 121 用于向 AP 122 下发业务配置请求和组密钥更新代理请求。

接入点 122 用于根据 AC 121 下发的业务配置请求将 AP 122 划分为多个 VAPs, 例如 VAPl ~VAPn ,n 为正整数 ,其中 ,每一个 VAPi (Ki<n) 具下发的组密钥更新代理请求 ,对 VAPi 范围内的无线站点进行组密钥更新。

在本实施例中 ,物理上 ,无线站点 STA 是与接入点 122 相连 ,但由于接入点 122 被划分为了多个虚拟接入点 122i ,因此 ,连接到接入点 122 下的无线站点 STA 也分别隶属于该多个虚拟接入点 VAPi, 也即每一个虚拟接入点 VPAi 对应多个无线站点。

在本实施例中 ,接入点 122 可以包含图 11 所示的接入装置 ,由于在图 11 的说明中 ,已经对该通信装置进行了详细说明 ,在此不再赘述。

无线站点 123 用于接收所述接入点 122 下发的更新后的组临时密钥。

在本实施例中 ,该无线站点 123 是与接入点 122 相连的属于某一虚拟接入点 VAPi 的范围的无线站点 ,可以是多个 ,具体取决于接入点 122 对虚拟接入点的划分及更新请求。例如 ,如果接入点 122 被划分为 n 个虚拟接入点 VAP, 即 VAPl~VAPn ,根据接入控制点 121 的组密钥更新代理请求 ,需要对 VAP1 范围内的 STA 进行组密钥更新 ,则该接入点 122 将 VAP1 的组临时密钥更新后下发到 VAP1 范围内的 STA。

通过本实施例的系统 ,AP 根据 AC 的组密钥更新代理请求 ,在需要更新组临时密钥时 ,代替 AC 在 VAP 范围内进行组临时密钥的更新 ,由于整个更新过程就不需要 AC 参与 ,减轻了 AC 的处理负担 ,又由于更新的范围由 ESS 级降到 VAP 级 ,缩小了更新的范围 ,因此减少了整个系统网络的流量 ,减轻了系统的震荡。

本发明实施例提供的方法、装置和系统 ,与现有的组临时密钥更新方法相比 ,具有如下优势 :

1、改变了组密钥的管理的位置 ,由 AC 转移到 AP ,在瘦 AC 集中式管理的网络模型下 ,极大的减轻了 AC 的负担 ;

2、改变了组密钥更新的范围 ,由 ESS 级降到 VAP 级 ,缩小了更新的范

围，减少了整个系统网络的流量，减轻了系统的震荡；

3、WPA 分为 WPA1 和 WAP2 两种标准，本发明实施例的技术方案，还对 WPA2 的组密钥更新流程做了优化。

结合本文中所公开的实施例描述的方法或算法的步骤可以直接用硬件、处理器执行的软件模块，或者二者的结合来实施。软件模块可以置于随机存储器（RAM）、内存、只读存储器（ROM）、电可编程 ROM、电可擦除可编程 ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的存储介质中。

以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限定本发明的保护范围，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权利要求书

1. 一种无线局域网络组临时密钥更新方法，其特征在于，所述方法包括：

将接入点划分为多个虚拟接入点；

接入点检测到特定虚拟接入点需要更新组临时密钥，确定该特定虚拟接入点待更新的新组临时密钥；

接入点将确定的新组临时密钥发送给该特定虚拟接入点范围内的所有在线无线站点以进行组临时密钥更新。

2. 根据权利要求 1 所述的方法，其特征在于，确定该特定虚拟接入点待更新的新组临时密钥的步骤包括：

接入点根据本地配置的密钥更新策略计算所述特定虚拟接入点待更新的新组临时密钥。

3. 根据权利要求 1所述的方法，其特征在于，所述方法还包括：

接入点接收接入控制点定期下发的虚拟接入点的组临时密钥，利用该组临时密钥更新本地数据库中虚拟接入点的服务组标识符和组临时密钥对应关系表；

所述确定该特定虚拟接入点待更新的新组临时密钥的步骤包括：

接入点获得特定虚拟接入点的服务组标识符，从组临时密钥对应关系表中查询与该特定虚拟接入点的服务组标识符匹配的最近更新的组临时密钥作为新组临时密钥。

4. 根据权利要求 1至 3任一项所述的方法，其特征在于，

接入点根据报文流量检测到特定无线站点下线，确定所述无线站点所属的虚拟接入点需要更新组临时密钥。

5. 根据权利要求 1至 3任一项所述的方法，其特征在于，

接入点检测到特定无线站点发送的去关联请求或去认证请求，确定所述特定无线站点所属的虚拟接入点需要更新组临时密钥。

6. 一种接入装置，其特征在于，所述装置上划分有多个虚拟接入点，所述装置包括：

检测单元，用于检测特定虚拟接入点是否需要更新组临时密钥；

确定单元，用于在所述检测单元检测到所述特定虚拟接入点需要更新组临时密钥时，确定该特定虚拟接入点待更新的新组临时密钥；

更新单元，用于将所述新组临时密钥发送给所述特定虚拟接入点范围内的所有在线无线站点以进行组临时密钥更新。

7. 根据权利要求 6 所述的装置，其特征在于，所述检测单元具体包括：

第一检测模块，用于根据报文流量检测到无线站点下线时，判定所述无线站点所属的虚拟接入点需要更新组临时密匙。

8. 根据权利要求 7 所述的装置，其特征在于，所述检测单元还包括：

第二检测模块，用于检测到无线站点发送的去关联请求或去认证请求，确定所述无线站点所属的虚拟接入点需要更新组临时密钥。

9. 根据权利要求 7 所述的装置，其特征在于，所述装置还包括划分单元，所述划分单元用于根据接入控制点的业务配置请求将所述接入装置划分为多个虚拟接入点。

10. 一种通信系统，所述系统包括接入点和无线站点，所述接入点连接所述无线站点，所述接入点上划分有多个虚拟接入点，其特征在于：

所述接入点，用于检测到特定虚拟接入点需要更新组临时密钥时，确定该特定虚拟接入点待更新的新组临时密钥；将确定的新组临时密钥发送给该特定虚拟接入点范围内的所有在线无线站点以进行组临时密钥更新。

11. 根据权利要求 10 所述的系统，其特征在于，所述系统还包括接入控制点，用于向所述接入点下发业务配置请求和组密匙更新代理请求。

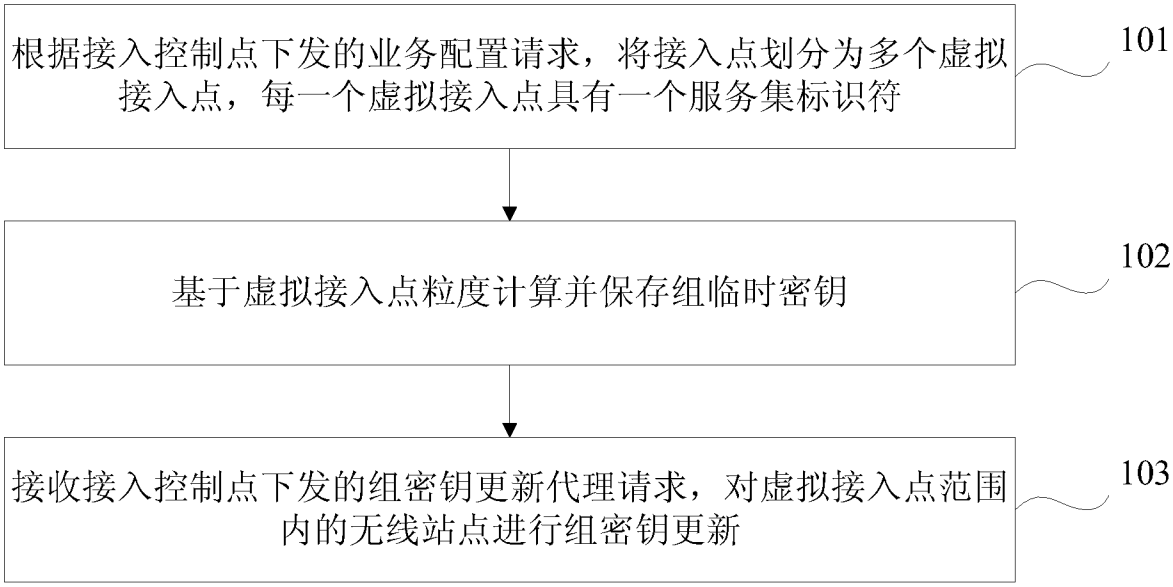
根据接入控制点下发的业务配置请求，将接入点划分为多个虚拟接入点，每一个虚拟接入点具有一个服务集标识符
101
基于虚拟接入点粒度计算并保存组临时密钥
102
接收接入控制点下发的组密钥更新代理请求，对虚拟接入点范围内的无线站点进行组密钥更新
103

图 1

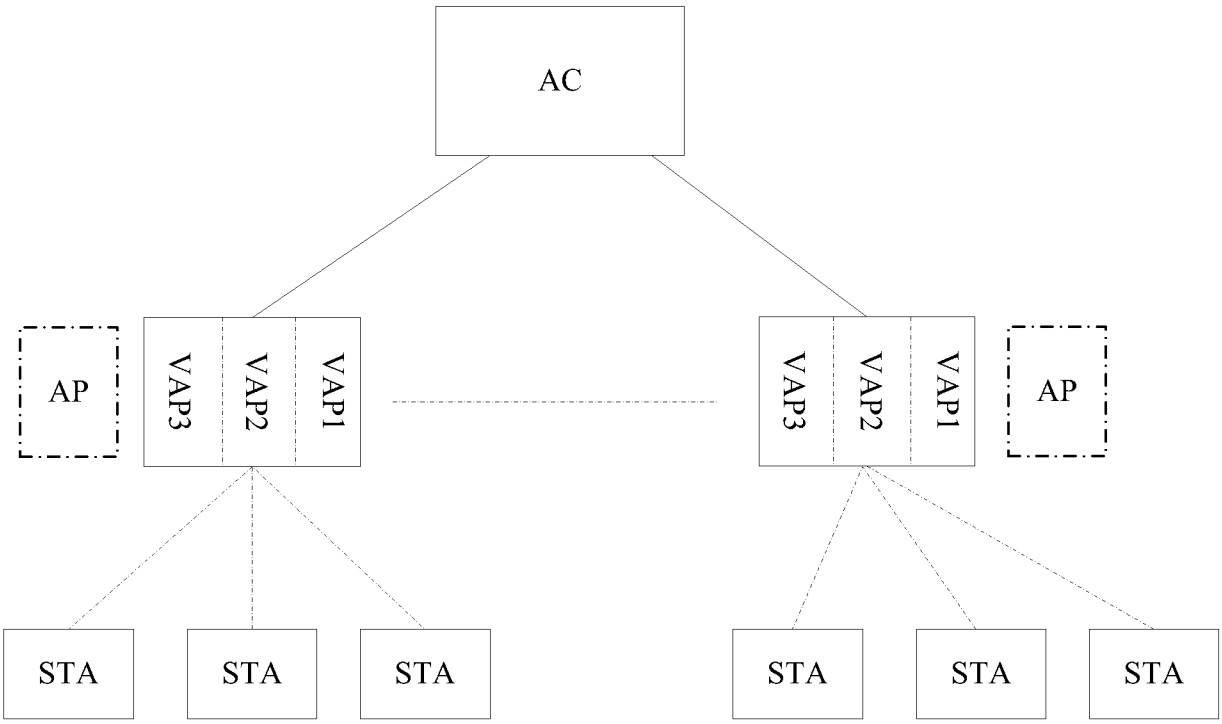
AC
AP
VAP3
VAP2
VAP1
VAP3
VAP2
VAP1
AP
STA
STA
STA
STA
STA
STA

图 2

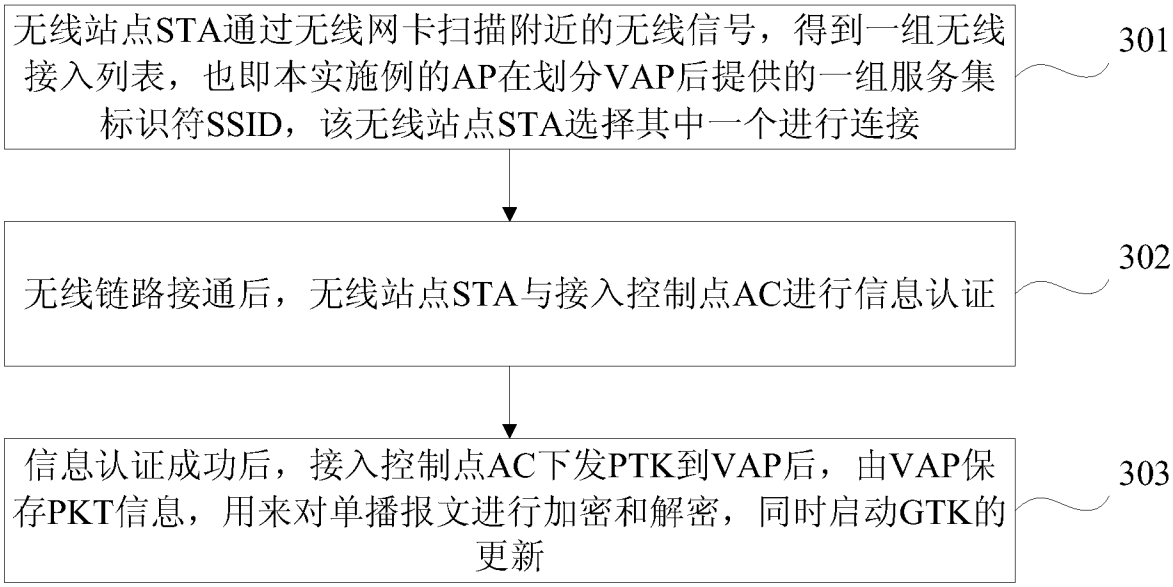
无线站点STA通过无线网卡扫描附近的无线信号，得到一组无线接入列表，也即本实施例的AP在划分VAP后提供的一组服务集标识符SSID，该无线站点STA选择其中一个进行连接
301
无线链路接通后，无线站点STA与接入控制点AC进行信息认证
302
信息认证成功后，接入控制点AC下发PTK到VAP后，由VAP保存PKT信息，用来对单播报文进行加密和解密，同时启动GTK的更新
303

图 3

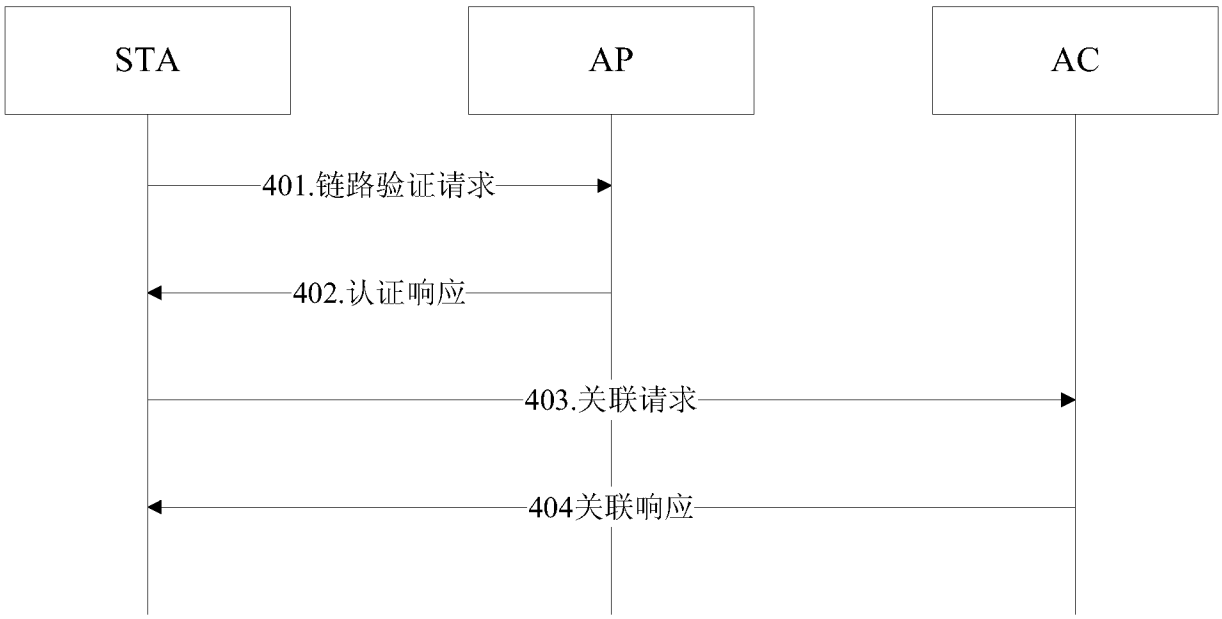
STA
AP
AC
401.链路验证请求
402.认证响应
403.关联请求
404关联响应

图 4

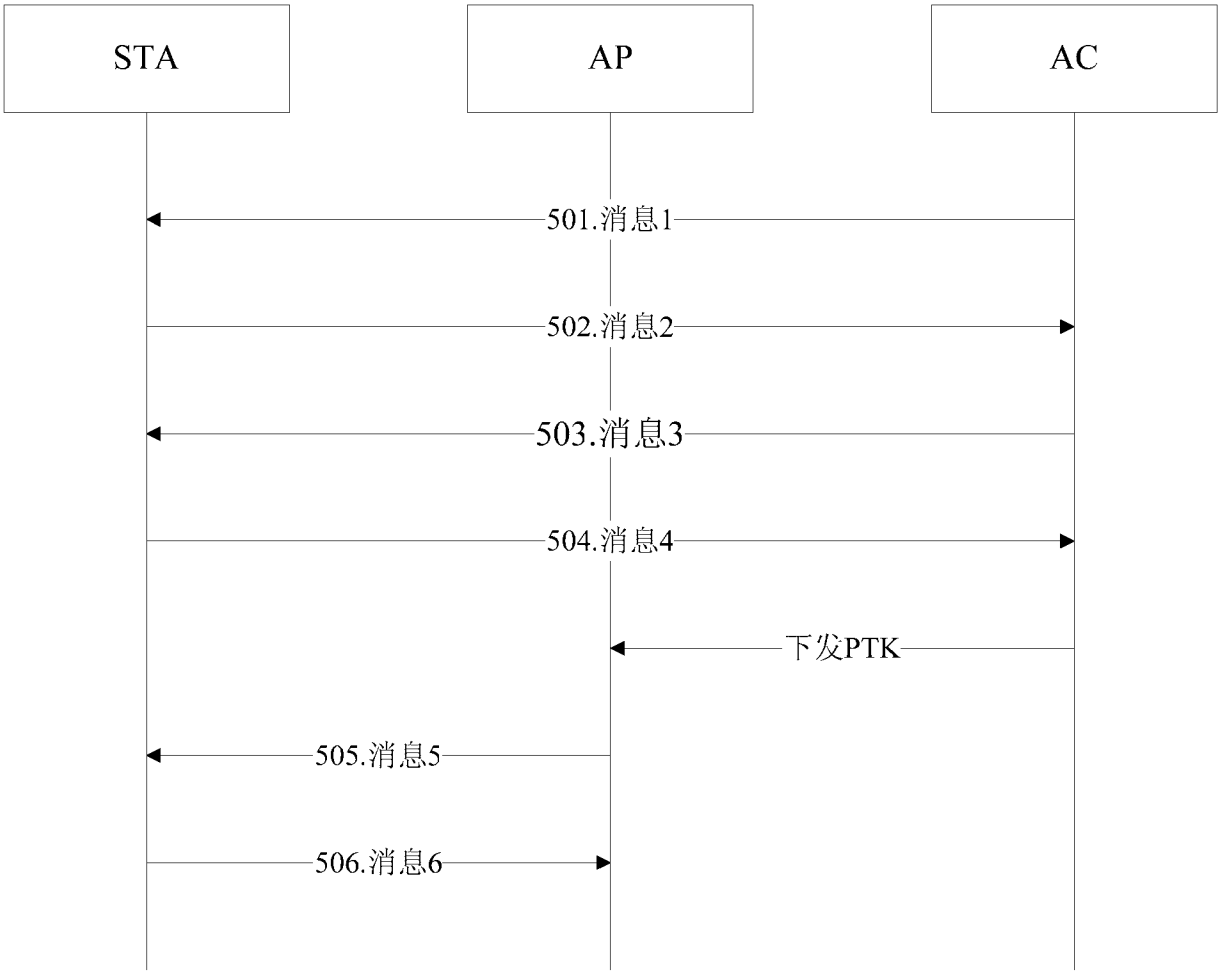

图 5

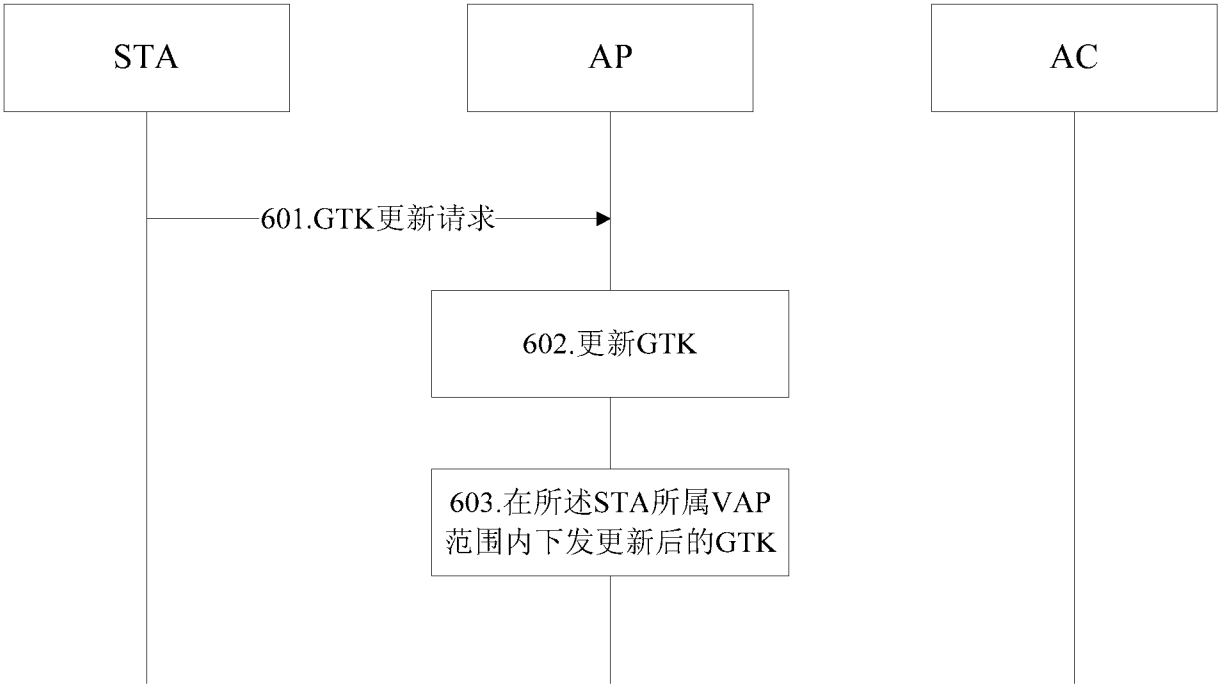
STA
AP
AC
601.GTK更新请求
602.更新GTK
603.在所述STA所属VAP
范围内下发更新后的GTK

图 6

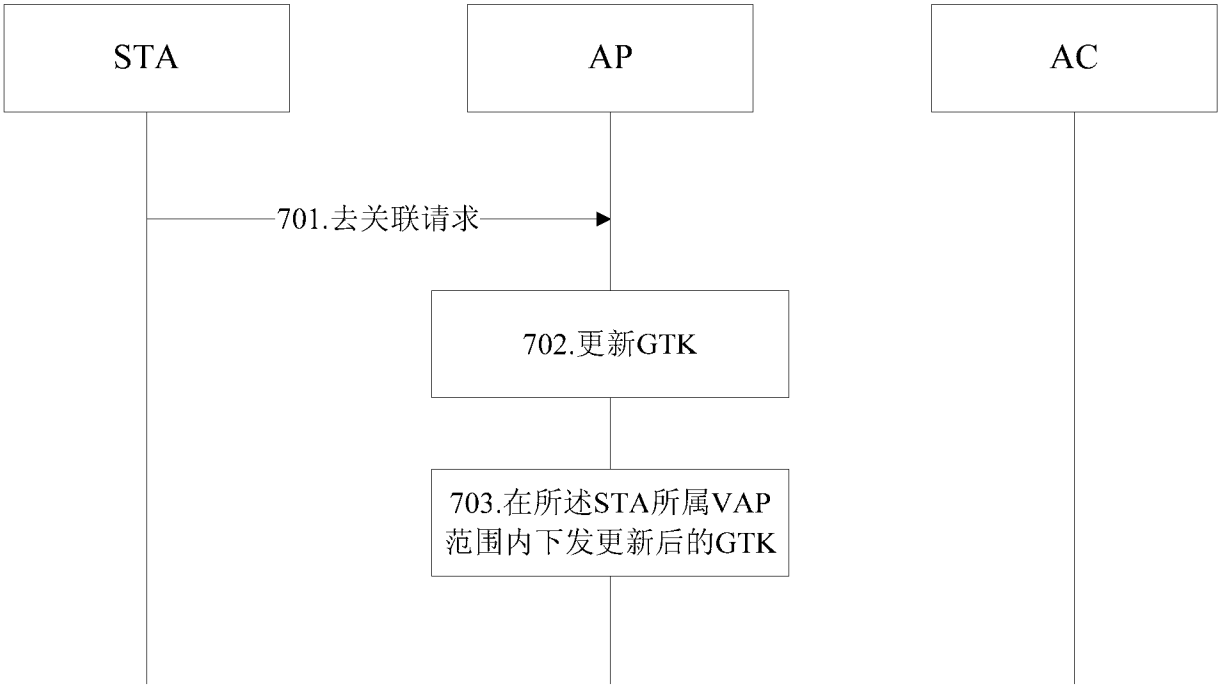
STA
AP
AC
701.去关联请求
702.更新GTK
703.在所述STA所属VAP
范围内下发更新后的GTK

图 7

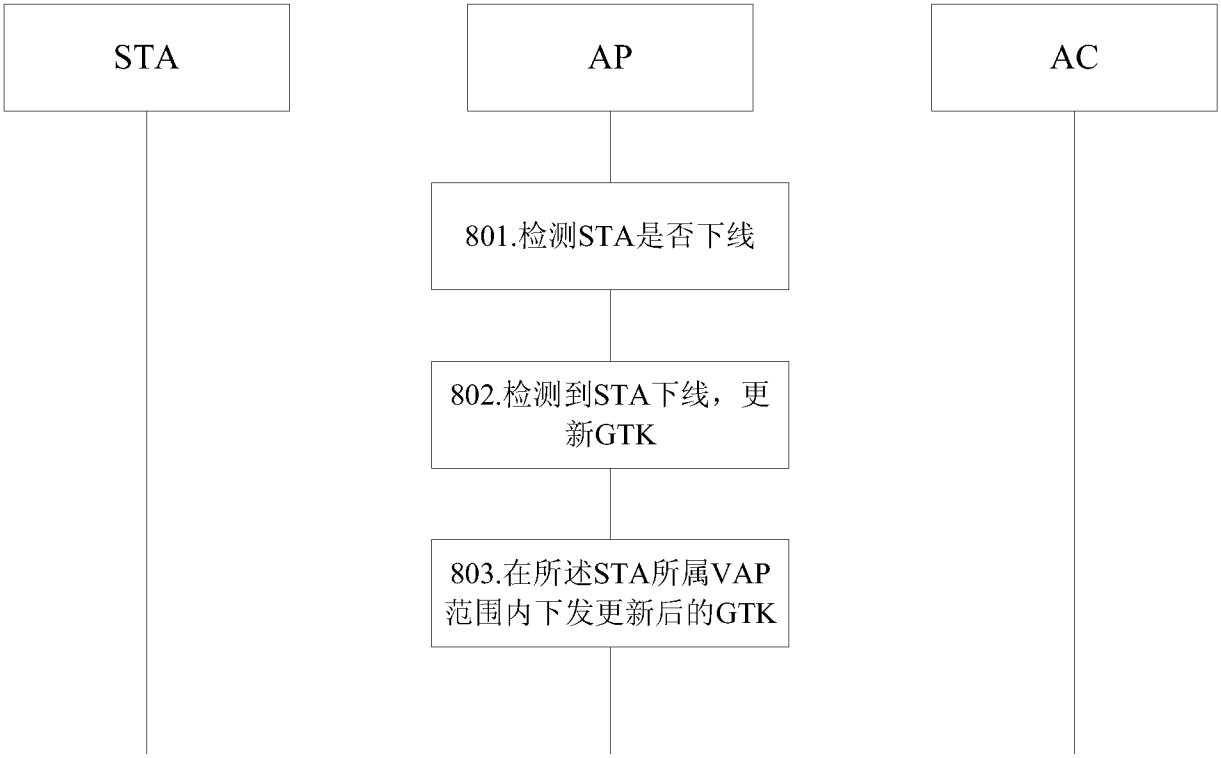
STA
AP
AC
801.检测STA是否下线
802.检测到STA下线，更新GTK
803.在所述STA所属VAP范围内下发更新后的GTK

图 8

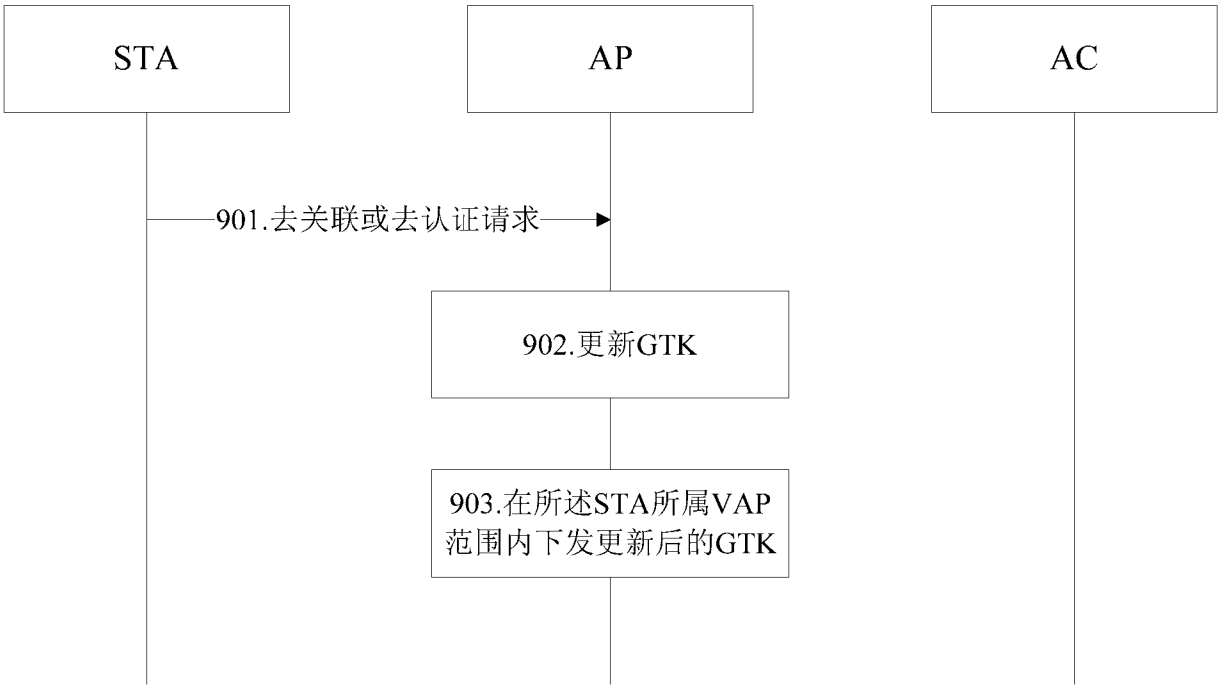
STA
AP
AC
901.去关联或去认证请求
902.更新GTK
903.在所述STA所属VAP范围内下发更新后的GTK

图 9

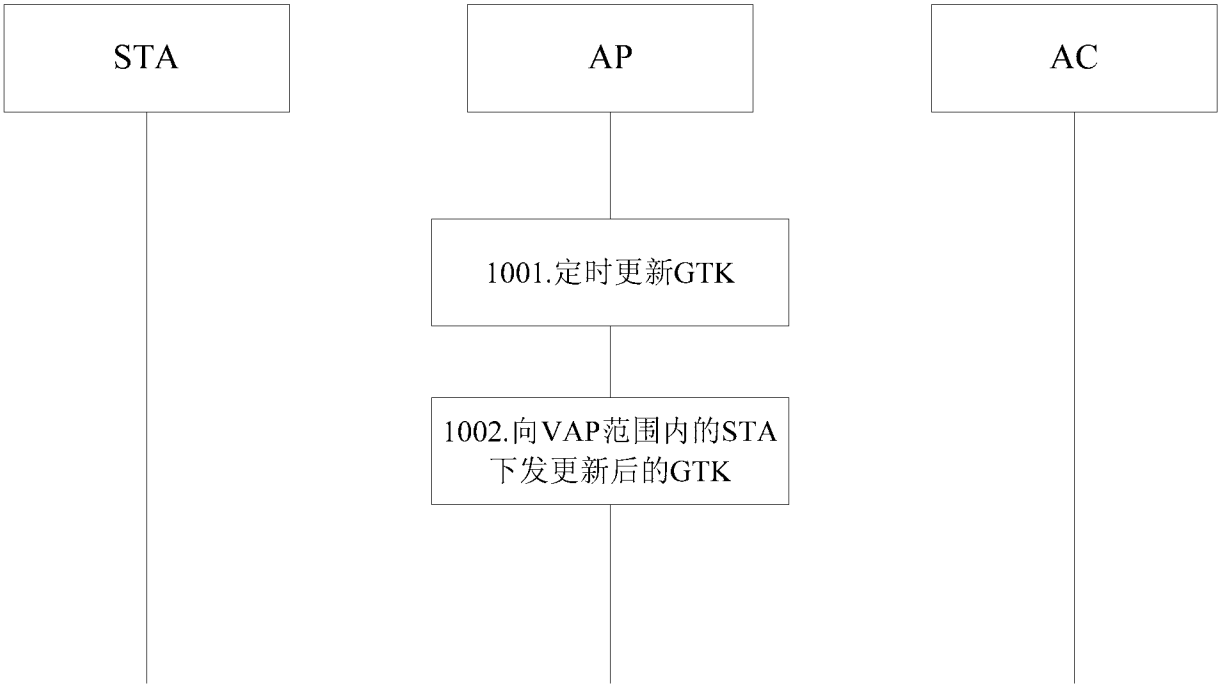

图 10

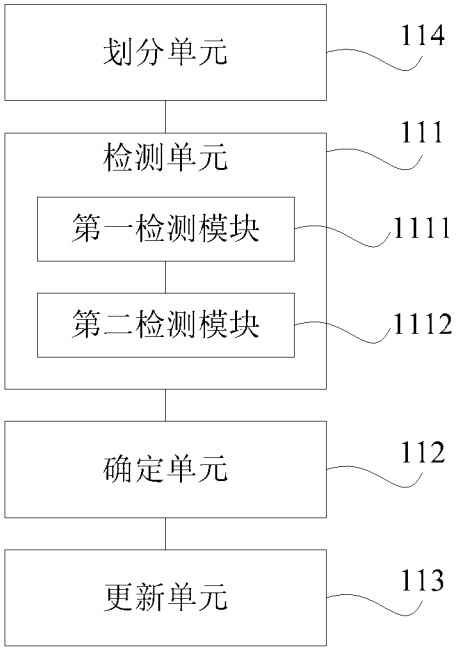
划分单元
114
检测单元
111
第一检测模块
1111
第二检测模块
1112
确定单元
112
更新单元
113

图 11

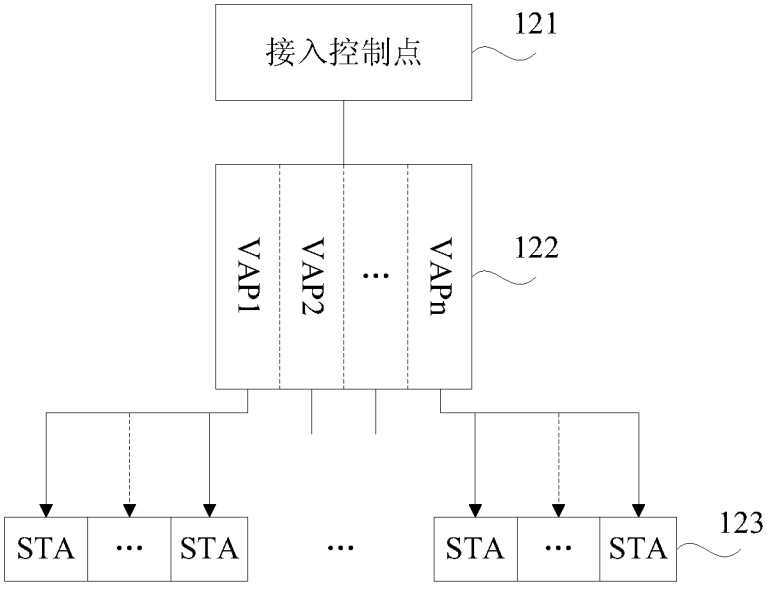
接入控制点
121
VAP1
VAP2
…
VAPn
122
STA
…
STA
…
STA
…
STA
123

图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN20 10/070062

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/28 (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)

IPC: H04L H04Q H04W

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)

WPI; EPODOC; CNPAT; CNKI; IEEE: virtual, access w point, VAP, group, transient, temporal, key, GTK, distribut+, update, refresh, multicast, broadcast

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	P. CALHOUN RFC5416 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11, Mar. 2009 (03.2009) the whole document	1-11
A	US2004/0141617A1 (VOLPANO) 22 Jul. 2004 (22.07.2004) the whole document	1-11
A	CN101222388A (HUAWEI TECHNOLOGIES CO., LTD) 16 Jul. 2008 (16.07.2008) the whole document	1-11
A	CN101453409A (CHINA MOBILE COMM. CORP.) 10 Jun. 2009(10.06.2009)the whole document	1-11
A	CN1455556A (SOUTHEAST UNIVERSITY) 12 Nov. 2003 (12.11 .2003) the whole document	1-11

☐ 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
08 Sep. 2010 (08.09.2010)	28 Oct. 2010 (28.10.2010)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 [Facsimile No. 86-10-62019451	Authorized officer WANG, Ming Telephone No. (86-10)62413333

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN20 10/070062

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US2004/0141617A1	22.07.2004	WO2005069784A2	04.08.2005
		EP1702434A2	20.09.2006
		KR20060 129005 A	14.12.2006
		CN1910861A	07.02.2007
		INKOLNP20060 1692E	11.05.2007
		JP2007518356T	05.07.2007
		KR20090081006A	27.07.2009
		KR20 10000228 3A	06.01.2010
		CN101707596A	12.05.2010
CN101222388A	16.07.2008	NONE	
CN101453409A	10.06.2009	NONE	
CN1455556A	12.11 .2003	NONE	

国 际 检 索 报 告

国际申请号
PCT/CN2010/070062

A. 主题的分类

H04L 12/28 (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)

IPC: H04L H04Q H04W

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))

WPI; EPODOC; CNPAT; CNKI; IEEE: 虚拟，接入点，组，临时，暂时，密钥，分配，更新，刷新，组播，广播，virtual, access w point, VAP, group, transient, temporal, key, GTK, distribut+, update, refresh, multicast, broadcast

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	P. CALHOUN ET AL. RFC5416 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11 3月 2009 (03.2009) 全文	1-11
A	US2004/0141617A1 (VOLPANO) 22.7月 2004 (22.07.2004) 全文	1-11
A	CN101222388A (华为技术有限公司) 16.7月 2008 (16.07.2008) 全文	1-11
A	CN101453409A (中国移动通信集团公司) 10.6月 2009 (10.06.2009) 全文	1-11
A	CN1455556A (东南大学) 12.11月 2003 (12.11.2003) 全文	1-11

□ 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J¾¾¾

"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
08.9月 2010 (08.09.2010)	28.10月 2010 (28.10.2010)

ISA/CN的名称和邮寄地址：	受权官员
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	王 明
传真号： (86-10)62019451	电话号码：(86-10) 62413333

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2010/070062

检索报告中引用的专利文件	公布日期	同族专利	公布日期
US2004/0141617A1	22.07.2004	WO2005069784A2	04.08.2005
		EP1702434A2	20.09.2006
		KR20060129005A	14. 12.2006
		CN1910861A	07.02.2007
		INKOLNP200601692E	11.05.2007
		JP20075 18356T	05.07.2007
		KR2009008 1006A	27.07.2009
		KR20100002283A	06.01 .2010
		CN101707596A	12.05.2010
CN101222388A	16.07.2008	无	
CN101453409A	10.06.2009	无	
CN1455556A	12. 11.2003	无	