



(12) 发明专利

(10) 授权公告号 CN 101018178 B

(45) 授权公告日 2013. 05. 08

(21) 申请号 200710088377. 7

(22) 申请日 2003. 06. 20

(30) 优先权数据

10/176, 562 2002. 06. 20 US

(62) 分案原申请数据

03818430. 3 2003. 06. 20

(73) 专利权人 高通股份有限公司

地址 美国加利福尼亚州

(72) 发明人 R·T·苏

(74) 专利代理机构 北京市柳沈律师事务所

11105

代理人 邵亚丽

(51) Int. Cl.

H04L 12/28 (2006. 01)

H04L 29/06 (2006. 01)

H04L 9/32 (2006. 01)

(56) 对比文件

CN 1259811 A, 2000. 07. 12, 全文.

WO 01/37497 A1, 2001. 05. 25, 全文.

CN 1150511 A, 1997. 05. 21, 全文.

Juha Ala-Laurila, Jouni Mikkonen,
Jyri Rinnemaa. Wireless LAN Access
Network Architecture for Mobile Operators.
IEEE Communications Magazine 39
11. 2001, 39(11), 82-83, 86.

审查员 汤广强

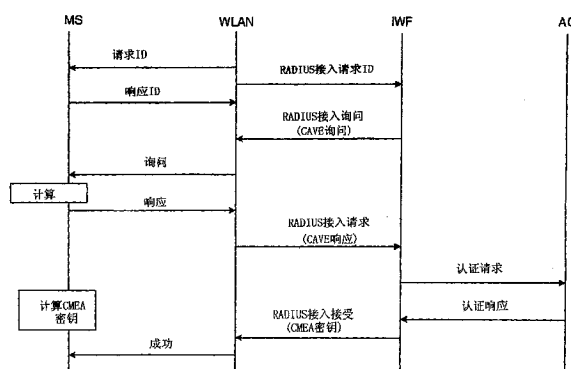
权利要求书1页 说明书8页 附图7页

(54) 发明名称

通信系统的互通功能

(57) 摘要

用于在无线局域网 (WLAN) 和通信系统间接口的互通功能 (IWF)。IWF 可包含足够的信息来认证用户到 WLAN 的接入, 或者 IWF 可需要向通信系统请求认证。在一实施例中, IWF 向 WLAN 发送对于用户的接入询问。然后, IWF 会把对该询问的响应传送到通信系统以供认证。IWF 允许 WLAN 使用通信系统的认证能力来进行本地认证。



1. 一种把无线局域网 WLAN 与一通信系统相接的方法,包括:
为通信系统的用户从 WLAN 接收一接入请求,所述接入请求包含移动台的身份;
通过用移动台的身份索引数据库来确定移动台的认证能力,所述数据库存储与所述移动台相关联的认证能力,所述认证能力包括 AKA 和 CAVE;
确定所述用户的认证状态;以及
把表明所述认证状态的响应提供给 WLAN
其中,确定所述用户的认证状态还包括:
向 WLAN 发送一接入询问消息;以及
从 WLAN 接收一接入响应
其中,确定所述认证状态还包括:
向通信系统发送一认证请求;以及
从通信系统接收所述用户的认证状态。
2. 如权利要求 1 所述的方法,其特征在于,所述认证请求包括来自 WLAN 的接入请求。
3. 如权利要求 1 所述的方法,其特征在于还包括:
从通信系统接收用户的安全信息;以及
响应于所述安全信息为所述用户产生加密密钥。
4. 如权利要求 1 所述的方法,其特征在于还包括:
为所述用户产生一加密密钥。

通信系统的互通功能

[0001] 背景

技术领域

[0002] 本发明涉及通信系统的互通功能,尤其涉及通过互通功能进行公共认证和密钥交换供无线局域网(WLAN)中使用的机制。

背景技术

[0003] 无线局域网(WLAN)允许用户对互联网协议(IP)服务和数据网络的实质上不受限制的接入。WLAN的使用不限于膝上电脑及其它计算设备,而是快速地扩展以包括蜂窝电话、个人数字助理(PDA)以及外部网络或载体所支持的其它小型无线设备。例如,经由蜂窝载波通信的无线设备会漫游到网络咖啡店或工作室内的WLAN。在该情况下,无线设备接入蜂窝系统,但希望接入WLAN。WLAN的接入要求认证。因为无线设备已经获准接入蜂窝系统,因此对进一步认证的需求便成为冗余。因此,需要一种互通功能,它允许一种对蜂窝系统和对WLAN的公共认证。

附图说明

[0004] 图1是包括无线局域网(WLAN)的通信系统。

[0005] 图2是具有互通功能(IWF)单元的通信系统。

[0006] 图3是通信系统中认证过程的定时图。

[0007] 图4是认证过程的流程图。

[0008] 图5是通信系统中认证过程的定时图。

[0009] 图6是通信系统中IWF处的认证过程的流程图。

[0010] 图7是移动站处的认证处理的流程图。

具体实施方式

[0011] 这里使用单词“示例性”意指“充当示例、实例或说明”。这里描述为“示例性”的任何实施例都不必被视为比其它实施例更为优选或有利。

[0012] HDR订户站(在此称为接入终端(AT))可以是移动的或固定的,并且与一个或多个HDR基站(在此称为调制解调器库收发机(MPT))通信。接入终端通过一个或多个调制解调器库收发机向HDR基站控制器发送数据分组或从其接收数据分组,HDR基站控制器在此称为调制解调器库控制器(MPC)。调制解调器库收发机和调制解调器库控制器是称为接入网络的网络的一部分。接入网络在多个接入终端之间传输数据分组。接入网络还能连到接入网络外的其它网络,比如公司内联网或互联网,并且可以在每个接入终端和这种外部网络间传输数据分组。已经与一个或多个调制解调器库收发机建立活动话务信道连接的接入终端称为活动接入终端,并且被称为处于话务状态。正在与一个或多个调制解调器库收发机建立活动话务信道连接过程中的接入终端被称为处于连接设立状态。接入终端可以是

通过无线信道或通过有线信道进行通信的任何数据设备,例如通过使用光纤或同轴电缆进行通信。接入终端还可以是多类设备的任一种,包括但不限于 PC 卡、微型闪存、外置或内置调制解调器或者无线或有线电话。接入终端向调制解调器库收发机发送信号所通过的通信链路称为反向链路。调制解调器库收发机向接入终端发送信号所通过的通信链路称为前向链路。

[0013] 图 1 中示出无线局域网 (WLAN) 100 有多个接入点 (AP) 106、108、110。AP 是为 WLAN 100 的无线端提供星型拓扑控制以及到有线网络接入的集线器或网桥。

[0014] 每个 AP 106、108、110 以及其它未示出的接入点都支持到数据服务的连接,比如互联网。工作站 102,比如膝上电脑或其它数字计算设备经由空中接口与 AP 通信,从而称为无线 LAN。然后,AP 与认证服务器 (AS) 或认证中心 (AC) 通信。AC 是为请求到网络的许可的设备执行认证服务的组件。实施方式包括远程认证拨入用户服务 (RADIUS),它是在 RFC 2138 中描述的互联网用户认证, C. Rigney 等人所著的“Remote Authentication Dial In User Service (RADIUS)”,于 1997 年 4 月出版,还包括其它认证、授权和核算 (AAA) 服务器。

[0015] 无线联网成为网际互通的一个重要方面。它表示基于无线网络的唯一边界是无线信号强度这一事实的一组唯一问题。没有线路能定义网络中的成员组成。没有物理方法能把无线范围内的系统限制为无线网络的成员。无线联网比任何其它连网技术都需要认证和接入控制机制。现在各个组织正在开发一种标准的认证机制。目前所接受的标准是 IEEE 802. 11。

[0016] 基于 RF 的网络的性质使其对于发射机范围内的任何无线电的分组拦截都是开放式的。通过使用高增益天线,拦截会出现在远离用户的“工作”范围外的地方。根据容易可用的工具,窃听者不限于仅仅采集分组以供后来分析,而能实际看到交互的会话,就像有效的无线用户所能查看的 Web 网页。窃听者会捕获弱的认证交换,比如一些网站登录。盗取者会稍后复制所述登录并获得接入。

[0017] 一旦攻击者获得了 WLAN 控制许可的知识,他就可能或者自己获得到网络的许可、或者偷取有效用户的接入。如果攻击者能模仿有效用户的 MAC 地址并且使用其分配到的 IP 地址,那么盗取用户的接入就很简单。攻击者等待直到有效的系统停止使用网络为止,然后接管它在网络中的位置。这会允许攻击者指引到网络内所有设备的接入,或者使用网络来获取对较宽范围的互联网的接入,同时看上去是被攻击网络的有效用户。因此,认证和加密成为实现 WLAN 的关键问题。

[0018] 认证是确认通信中的个人或应用的身份的过程。这种认证使服务提供商能把实体确认为有效的用户,还能对于所请求的特定服务而认证该用户。认证和授权实际上有很具体的意义,然而这两个名称通常可交换使用,实践中不会清晰分别。

[0019] 认证是用户对身份建立权利的过程,所述权利实质上是使用名称的权利。有大量技术可用来认证用户——密码、生物测定技术、智能卡、证书。

[0020] 名称或身份具有与其相关联的属性。属性可以紧密绑定于一名称(例如在证书有效负载内),或它们可能在与该名称对应的密钥下被存储在目录或其它数据库内。属性可随时间而改变。

[0021] 授权是确定是否允许一身份(假设一组与该身份相关联的属性)来执行某些行为的过程,所述行为比如接入一资源。注意到执行行为的许可不能确保可以执行该行为。注

意到认证和授权决定可由不同的实体在不同的点上作出。

[0022] 在蜂窝网络中,认证特性是一网络能力,其允许蜂窝网络确认无线设备的身份,从而减少蜂窝网络未经授权的使用。该过程对于订户是透明的。不要求用户在他们进行呼叫时做任何事以认证其电话的身份。

[0023] 认证一般包括加密方案,其中服务提供商和用户有一些共享的信息和一些专用的信息。共享信息一般称为“共享秘密”。

[0024] A—密钥

[0025] 认证密钥(A—密钥)是对于每个单独的蜂窝电话唯一的秘密值。它向蜂窝服务提供商注册并且被保存在电话和认证中心(AC)中。A—密钥被制造商编程到电话中。它也可由用户从无线设备菜单手动输入,或在售出点用特殊终端由用户手动输入。

[0026] 无线设备和AC必须有相同的A—密钥来产生相同的计算。A—密钥的主要功能是被用作计算共享秘密数据(SSD)的参数。

[0027] 共享秘密数据(SSD)

[0028] SSD被用作无线设备和AC中认证计算的输入,并且被保存在以上两个位置中。不像A—密钥那样,SSD可以经过网络而修改。AC和无线设备共享计算SSD的三个元件:1)电子序列号(ESN);2)认证密钥(A—密钥);以及3)共享秘密数据的随机数(RANDSSD)计算。

[0029] ESN和RANDSSD通过网络和空中接口被发送。SSD在设备作出其第一次系统接入时被更新,此后被周期性更新。在计算SSD时,结果是两个分开的值SSD-A和SSD-B。SSD-A用于认证。SSD-B用于加密和话音保密。

[0030] 根据提供服务的系统的能力,SSD可以在AC和服务移动交换中心(MSC)之间共享或不共享。如果秘密数据是共享的,则意味着AC会将其发送到服务MSC,服务MSC必须能执行CAVE。如果它不是共享的,则AC会保留数据并执行认证。

[0031] 共享类型影响到怎样实施认证询问。认证询问是为了询问无线设备的身份而发送的消息。基本上,认证询问发送一些信息供用户处理,所述信息一般是随机数数据。然后,用户处理信息并发送一响应。该响应为了确认用户而被分析。如果有共享的秘密数据,则在服务MSC处处理询问。如果有非共享数据,则由AC处理询问。通过共享秘密数据,系统可使所发送的话务量最小。并能使询问在服务交换机处发生得更快。

[0032] 认证过程

[0033] 在给定的系统中,本地位置寄存器(HLR)通过充当MSC和AC间的中介物来控制认证过程。设立服务MSC以支持与移动站的HLR的认证,反之亦然。

[0034] 通过通知服务MSC它是否能进行认证、通过在开销消息序列中设置一授权字段,设备开始该过程。响应于此,服务MSC开始用认证请求进行注册/认证过程。

[0035] 通过发送认证请求,服务MSC告知HLR/AC它是否能进行CAVE计算。AC控制在那些可用的服务MSC和设备能力中使用哪些服务MSC以及哪些设备能力。当服务MSC不具有CAVE能力时,SSD不能在AC和MSC之间共享,因此所有认证过程都在AC中执行。

[0036] 认证请求(AUTHREQ)的目的是认证电话并请求SSD。AUTHREQ包含两个用于认证的参数,AUTHR和RAND参数。当AC获取AUTHREQ时,它使用RAND和最后知道的SSD来计算AUTHR。如果它与AUTHREQ中发送的AUTHR匹配,则认证成功。如果SSD能被共享,AUTHREQ的返回结果会包含SSD。

[0037] 询问

[0038] 认证过程由询问和响应对话组成。如果 SSD 是共享的,则该对话在 MSC 和设备间运行。如果 SSD 不是共享的,则该对话在 HLR/AC 和设备间运行。根据交换机类型, MSC 能进行或是唯一询问 (Unique Challenge) 或全局询问 (Global Challenge) 或两者。一些 MSC 目前不能进行全局询问。唯一询问是仅出现在呼叫尝试期间的询问,因为它使用语音信道。唯一询问在呼叫始发和呼叫传送期间向单个设备作出认证。全局询问是出现在注册、呼叫始发和呼叫传送期间的询问。全局询问向正在使用特定无线电控制信道的所有 MS 作出认证询问。因为它在无线电控制信道上被广播,因此它被称为全局询问,该询问由接入该控制信道的所有电话使用。

[0039] 在询问期间,设备对由 MSC 或 AC 所提供的随机数进行应答。设备使用该随机数和设备中保存的共享秘密数据来计算对 MSC 的响应。MSC 还使用随机数和共享秘密数据来计算来自设备的应是什么响应。这些计算通过 CAVE 算法完成。如果响应不同,则服务被拒绝。询问过程不增加它连到呼叫所花费的时间量。实际上,呼叫可在某些情况下继续,仅仅在认证失败时被拆卸。

[0040] 无线局域网 (WLAN) 获得了极大的流行作为一种手段来向用户提供对 IP 数据网的不受限制的接入。第三代 (3G) 无线网络也被设计成提供高速数据接入;然而它们所支持的数据速率一般比 WLAN 的数据速率要低,3G 网络在更广泛的区域上提供数据覆盖。尽管它们可被视为竞争者,然而 WLAN 和 3G 网络可以是互补的:WLAN 在诸如候机室或酒店大堂等公共区域提供高容量的“热点 (hot-spot)”覆盖,而 3G 网络会向用户提供运动时几乎到处存在的数据服务。因此,同一通信公司能在单个用户订购下提供 3G 和 WLAN 接入服务。这意味着 MS 对于这两类接入认证都使用相同的认证方法和秘密。

[0041] 在 3G 接入认证中,认证中心 (AC) 认证 MS。AC 和 MS 具有共享密钥。在网络端,共享密钥被安全地存储在 AC 中,并且不被分发给任何其它网络实体。在 MS 端,共享密钥被安全地存储在安全存储器中,并且不对其向外分发。AC 和 MS 使用蜂窝认证语音加密 (CAVE) 或认证密钥协议 (AKA) 作为认证算法。认证参数在 MS 和 AC 间经由 3G 空中信令消息和网络信令消息传送 (IS-41)。

[0042] 在 WLAN 接入认证中,希望 MS 由同一 AC 使用相同的共享密钥和认证算法 (AKA 或 CAVE) 来认证。然而,使用了不同的机制在 WLAN 中传送认证参数。特别是,认证参数经由可扩展认证协议 (EAP) 和 AAA 协议 (RADIUS 或 Diameter) 传送。难题是在 3G 和 WLAN 间互通传送机制,使得对于 WLAN 接入认证能在 MS 和 AC 间传送认证参数。

[0043] 如上所述,CAVE 算法通常用于蜂窝通信,因此被经常使用和分发。也可以使用其它用于认证的算法。特别是在数据通信中,存在复杂度和应用不同的许多算法。为了协调这些机制,已经开发了可扩展认证协议 (EAP) 作为支持多种认证和密钥分发机制的一种通用协议框架。EAP 在 L. Blunk 等人所著的“PPP Extensible Authentication Protocol (EAP)”中描述, RFC 2284, 1998 年 3 月出版。

[0044] EAP 所支持的一种这样的机制是 AKA 算法,在 J. Arkko 等人所著的“EAP AKA Authentication”中定义, 2002 年 2 月作为互联网草案出版。因此,需要扩展 EAP 以包括蜂窝算法 CAVE。希望为新的系统和网络提供后向兼容。

[0045] EAP

[0046] 可扩展认证协议 (EAP) 是支持多种认证机制的一种通用认证协议。EAP 在链路设立和控制期间不选择特定的认证机制,而是将其推迟到认证过程开始后。这使认证者能在确定特定的认证机制前请求更多的信息。认证者被定义为要求认证的链路的结尾。认证者指定要在链路建立期间使用的认证协议。

[0047] 互通功能 (IWF)

[0048] 按照一实施例,实现一新的网络实体并称为互通功能 (IWF),更具体地是称为 AAA/IS-41 互通功能 (IWF)。IWF 在诸如 3G 这样的无线网络和 WLAN 网络间互通认证参数的传送机制 (例如 CAVE、AKA)。图 2 所示的 IWF 204 是通信系统 200 的一部分。系统 200 包括 WLAN 202、IWF 204 和 AC 206。如图所示,工作站 208 目前处在 WLAN202 的通信范围内。IWF 204 在 AC 206 和 WLAN 202 之间提供一接口,允许使用公共认证使 MS 208 能获准接入网络。注意到 MS 208 会是无线工作站、远程用户或者能经由除 WLAN 202 以外的网络通信的其它无线设备,该情况下所述网络是 AC 206 为其一部分的网络。

[0049] IWF 204 是单向互通功能,即认证请求始发自 WLAN 202。注意到在当前的实施例和说明中,AAA 是用于在 WLAN 202 和 IWF 204 之间传输认证参数的传送机制。而且,IS-41 是用于在 IWF 204 和 AC 206 之间传输认证参数的传送机制。特别对于该例,会使用 RADIUS 作为 AAA 协议。

[0050] 图 3 说明了认证处理。首先,IWF 204 接收一 RADIUS 接入请求消息,该消息包含希望执行认证以接入 WLAN 202 的 MS 208 (或无线工作站) 的身份。IWF 204 配置有一数据库 210,其存储与 MS 208、以及目前经由 AC 206 注册的其它 MS 208 相关联的认证能力。数据库 210 由每个 MS 208 的身份来索引。这样,IWF 204 可以确定 MS 208 的认证能力 (例如 AKA 和 / 或 CAVE)。

[0051] 如果 MS 208 仅支持 CAVE, IWF 204 就执行与图 3 一致的以下过程。IWF 发送一 RADIUS 接入询问消息,该消息包含 EAP 请求消息, EAP 请求消息包含一 CAVE 询问。如上所述,询问包含要由 MS 208 用来计算认证响应的随机数。IWF 204 接收包含 EAP 响应消息 (包含 CAVE 询问响应) 的 RADIUS 接入请求消息。CAVE 响应包含 MS 209 的认证响应,即使用随机数计算的结果、以及其它对于 MS 208 特定的参数。

[0052] 如果 IWF 204 不能确认 EAP 响应消息,或特别是不能确认对 CAVE 询问的 CAVE 响应, IWF 204 就向 AC 206 发送一 AUTHREQ 消息,该消息是一 IS-41 消息。在该情况下, IWF 204 没有确认询问响应所必要的信息。AUTHREQ 消息包含分配给 MS 208 的 IMSI、随机数 (即询问) 以及 MS 208 所产生的认证响应。AC 206 具有对于 MS 208 特定的共享秘密的知识,于是它确认 MS 208 的询问响应。AC 206 向 IWF 返回 AUTHREQ 消息,该消息是一 IS-41 消息。AUTHREQ 消息包含认证结果。如果成功,AUTHREQ 消息还包含称为蜂窝消息加密算法 (CMEA) 密钥的一个密钥,该密钥用于保护 WLAN202 中的 MS 208 话务。如果 IWF 在预定次数的重试后不能从 AC 206 接收 AUTHREQ 消息,则 IWF 204 向 WLAN 202 发送包含 EAP 失败的 RADIUS 接入拒绝消息。不能接收 AUTHREQ 消息会表明 IWF 204 和 AC 206 之间的网络问题。

[0053] 如果 IWF 204 能认证来自 MS 208 的询问响应,并且这种确认是成功的, IWF 204 就产生 CMEA 密钥。如果 MS 208 被成功认证, IWF 204 就向 WLAN 202 发送一 RADIUS 接入接受消息。这种消息包含 EAP 成功消息以及 CMEA 密钥。如果 MS 208 未能进行认证, IWF 204

就向 WLAN 202 发送包含 EAP 失败消息的 RADIUS 接入拒绝消息。

[0054] 图 4 说明了按照一实施例的认证过程 400, 其中 MS 208 支持 CAVE 协议。当 MS 208 和 WLAN 202 在步骤 402 开始标识协商时, 该过程开始。同样在该步骤, WLAN202 发送一 RADIUS 接入请求消息, 该消息包含 MS 208 的身份。如上所述, 身份可由 IMSI 或其它对于 MS 202 的唯一标识符来提供。该过程包括 MS 208 设法接入 WLAN202, 以及响应于此, WLAN 202 从 MS 208 请求标识, 步骤 402。在这一点, 在步骤 404, IWF 204 向 WLAN 202 发送一 RADIUS 接入询问消息, 其包含 CAVE 询问。响应于该询问, MS 208 计算一响应并把该响应提供给 WLAN 208 (未示出)。然后在步骤 406, 该响应在 RADIUS 接入响应消息内被发送到 IWF 204。如果 IWF 204 在判决菱形 408 处不知道 MS 208 的共享秘密, 处理就继续到步骤 410, 其中 IWF 204 向 AC 206 发送一 AUTHREQ 消息。AUTHREQ 消息请求认证 MS 208。如果在判决领先 412 处返回 AUTHREQ 消息, 处理就继续到判决菱形 414 以确定 AUTHREQ 消息是否表明成功的认证, 即确认用于接入 WLAN 的认证结果。如果在判决菱形 412 未接收到 AUTHREQ 消息, 处理就继续到步骤 416, 其中 IWF 发送一 RADIUS 接入拒绝消息。

[0055] 从判决菱形 408 继续, 如果 IWF 204 知道 MS 208 共享秘密信息, IWF 204 就能在判决菱形 418 处确定认证是否成功。成功认证继续到步骤 420 以计算 CMEA 密钥。RADIUS 接入接受消息然后在步骤 424 被发送。注意到步骤 414 的成功认证 (用于由 AC 206 的认证) 还继续到步骤 420。从判决菱形 418, 如果认证不成功, IWF 就在步骤 422 发送一 RADIUS 接入拒绝消息。

[0056] 在一可替代实施例中, IWF 204 使用 AKA 协议来发送询问。如图 5 所示, 如果 MS 208 支持 AKA, IWF 204 就实现 AKA 询问, 并且改变认证处理的顺序。在该情况下, 在认证向量 (AV) 中提供足以认证用户的信息, 所述用户比如 MS 208。注意到 AC 206 可能在 AV 中向 IWF 204 发送共享秘密 (SS) 信息。按照本实施例, AV 包括 SS、询问和密码密钥 (CK)。CK 用于对 MS 话务进行加密。

[0057] 如果 IWF 204 没有认证向量 (AV) 来认证 MS 208, IWF 204 就发送一 AUTHREQ 消息以便向 AC 206 请求 AV。AUTHREQ 消息包含 MS 208 的身份, 比如 IMSI、以及对于 AV 的请求。AC 206 用包含 AV 的 AUTHREQ 消息应答。AC 由随机数 (RAND)、期望的响应 (XRES)、密码密钥 (CK) 和认证标记 (AUTN) 组成。AC 可以在 AUTHREQ 消息中提供多个 AV, 因此 IWF 无须向 AC 206 请求后续的认证。

[0058] 如果 IWF 204 不能从 AC 206 接收 AUTHREQ 消息 (可能在预定次数的重试后), IWF 204 就向 WLAN 202 发送一 RADIUS 接入拒绝消息, 该消息包含 EAP 失败消息, 比如在 IWF 204 和 AC 206 之间存在网络问题时。

[0059] 如果接收到的 AUTHREQ 不包含 AV, IWF 204 就向 WLAN 202 发送包含 EAP 失败消息的 RADIUS 接入拒绝消息。例如, 这一情况会在 MS 202 具有一到期的预订的情况下出现。

[0060] 如果 IWF 204 具有 AV, IWF 204 就向 WLAN 202 发送一 RADIUS 接入询问消息, 该消息包含 EAP 请求消息, EAP 请求消息有一 AKA 询问。AKA 询问包含 AUTN 和 RAND。AUTN 传送 AC 206 证书, 并且将由 MS 208 确认。RAND 是对 MS 208 的询问, 该询问用于计算认证响应 (RES)。MS 208 向 WLAN 202 提供 RES。

[0061] IWF 204 从 WLAN 202 接收包含 EAP 响应的 RADIUS 接入请求消息, 所述 EAP 消息包括 CAVE 询问。CAVE 询问包含经由 WLAN 202 接收的 MS 208 认证响应 (RES)。IWF 204

把 RES 与 XRES 相比较。对于匹配情况, MS 208 被成功认证, IWF 204 向 WLAN 202 发送一 RADIUS 接入接受消息。这种消息包含 EAP 成功消息和 CK。CK 将用于保护 WLAN 202 中的 MS 208 话务。如果 MS 208 未能成功进行认证, IWF 204 就向 WLAN 202 发送包含 EAP 失败消息的 RADIUS 接入拒绝消息。

[0062] 图 5 说明了使用 AV 的认证过程 500。如果 IWF 204 具有足以在判决菱形 502 处确认 MS 208 的 AV, 过程就继续到步骤 506, 否则就继续到步骤 504。在步骤 506, IWF 204 向 WLAN 204 发送对于 MS 208 的 RADIUS 接入询问消息。询问于是就被转发到 MS 208 进行处理, 然后把一响应提供回 WLAN 202(未示出)。IWF 204 在步骤 510 接收 RADIUS 接入请求消息, 并在判决菱形 512 确定 MS 认证是否成功。如果认证成功, IWF 204 就在步骤 514 发送一 RADIUS 接入接受消息, 否则 IWF 204 在步骤 516 发送一 RADIUS 接入拒绝消息。

[0063] 返回到判决菱形 502, 如果 IWF 204 没有 AV, IWF 就在步骤 504 向 AC 206 发送一 AUTHREQ 消息。在接收到 AV 时, IWF 204 把处理继续到步骤 506, 否则处理继续到步骤 516。

[0064] 图 7 说明了适用于在 WLAN(未示出)和 AC(未示出)间接口的 IWF600, 因此它能执行对于两者间的通信、认证、密钥交换及其它安全通信所必要的过程。IWF 600 包括一 WLAN 接口单元 602, 它准备、发送、接收和 / 或解释与 WLAN 间的通信。类似地, IWF 600 包括一接口单元 604, 其准备、发送、接收和 / 或解释与 AC 的通信。IWF 600 进一步包括一 CAVE 过程单元 608、EAP 过程单元 610 以及 RADIUS 过程单元 612。IWF 600 可包括给定系统中的互通功能所需的任何数量的这种过程单元(未示出)。诸如 CAVE 过程单元 608、EAP 过程 610 和 RADIUS 过程 612 等过程单元可以用软件、硬件、固件或它们的组合来实现。IWF 600 内的各个模块经由通信总线 614 通信。

[0065] 本领域的技术人员可以理解, 信息和信号可以用多种不同技术和工艺中的任一种来表示。例如, 上述说明中可能涉及的数据、指令、命令、信息、信号、比特、码元和码片可以用电压、电流、电磁波、磁场或其粒子、光场或其粒子或它们的任意组合来表示。

[0066] 本领域的技术人员能进一步理解, 结合这里所公开的实施例所描述的各种说明性的逻辑框、模块和算法步骤可以作为电子硬件、计算机软件或两者的组合来实现。为了清楚说明硬件和软件间的互换性, 各种说明性的组件、框图、模块、电路和步骤一般按照其功能性进行了阐述。这些功能性究竟作为硬件或软件来实现取决于整个系统所采用的特定的应用和设计约束。技术人员可能以对于每个特定应用不同的方式来实现所述功能, 但这种实现决定不应被解释为造成背离本发明的范围。

[0067] 结合这里所描述的实施例来描述的各种说明性的逻辑框、模块和算法步骤的实现或执行可以用: 通用处理器、数字信号处理器 (DSP)、应用专用集成电路 (ASIC)、现场可编程门阵列 (FPGA) 或其它可编程逻辑器件、离散门或晶体管逻辑、离散硬件组件或者为执行这里所述功能而设计的任意组合。通用处理器可能是微处理器, 然而或者, 处理器可以是任何常规的处理器、控制器、微控制器或状态机。处理器也可能用计算设备的组合来实现, 如, DSP 和微处理器的组合、多个微处理器、结合 DSP 内核的一个或多个微处理器或者任意其它这种配置。

[0068] 结合这里所公开实施例描述的方法或算法的步骤可能直接包含在硬件中、由处理器执行的软件模块中或在两者当中。软件模块可能驻留在 RAM 存储器、闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可移动盘、CD-ROM 或本领域中已知的任何其它

形式的存储媒质中。示例性存储媒质与处理器耦合,使得处理器可以从存储媒质读取信息,或把信息写入存储媒质。或者,存储媒质可以与处理器整合。处理器和存储媒质可能驻留在ASIC中。ASIC可能驻留在用户终端中。或者,处理器和存储媒质可能作为离散组件驻留在用户终端中。

[0069] 上述优选实施例的描述使本领域的技术人员能制造或使用本发明。这些实施例的各种修改对于本领域的技术人员来说是显而易见的,这里定义的一般原理可以被应用于其它实施例中而不使用创造能力。因此,本发明并不限于这里示出的实施例,而要符合与这里揭示的原理和新颖特征一致的最宽泛的范围。

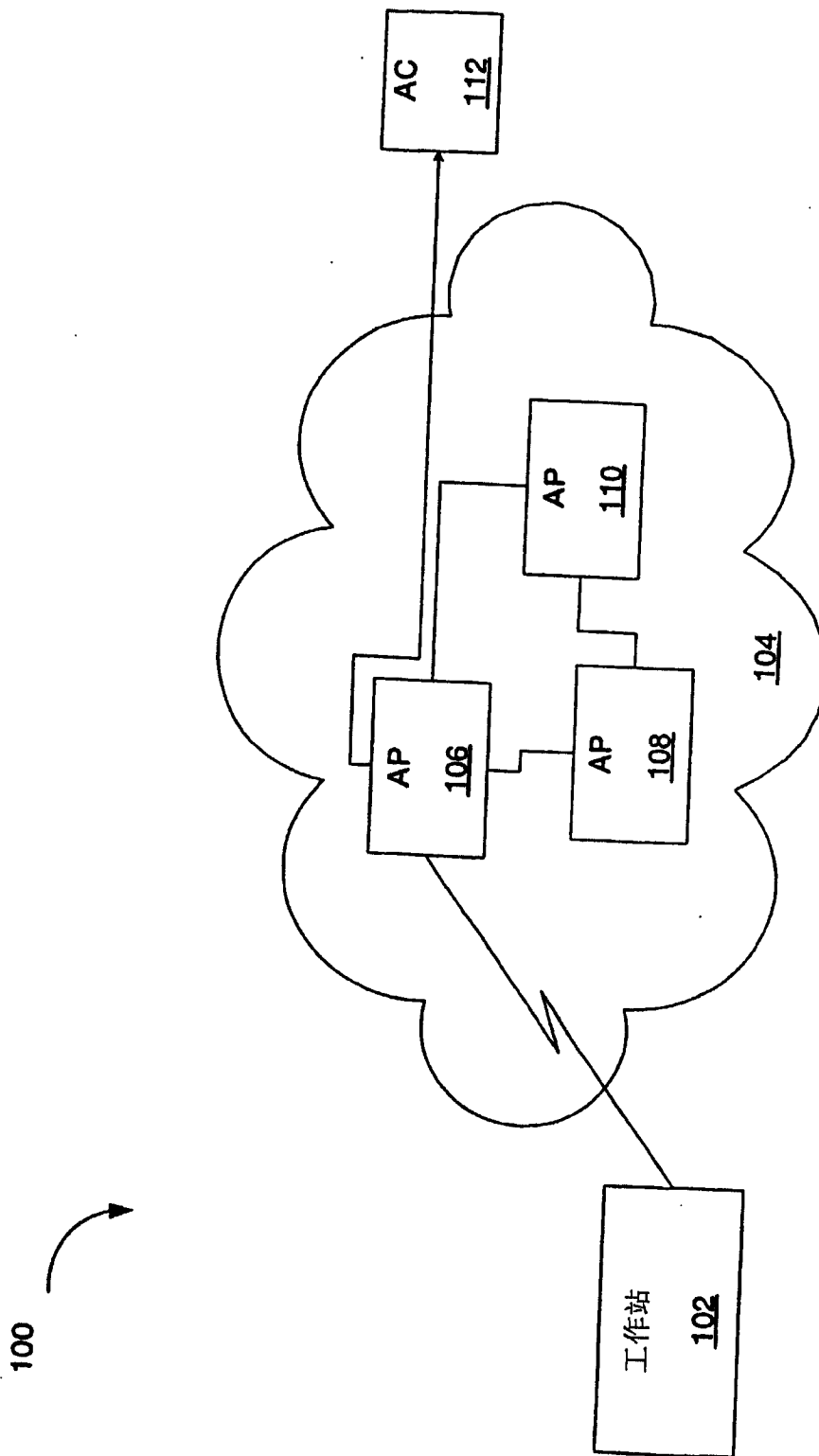


图 1

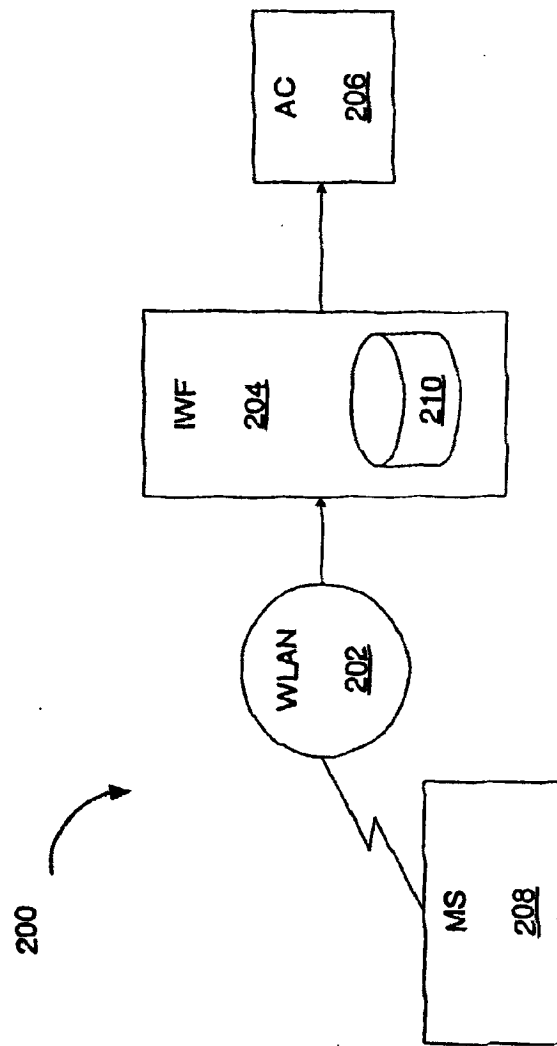


图 2

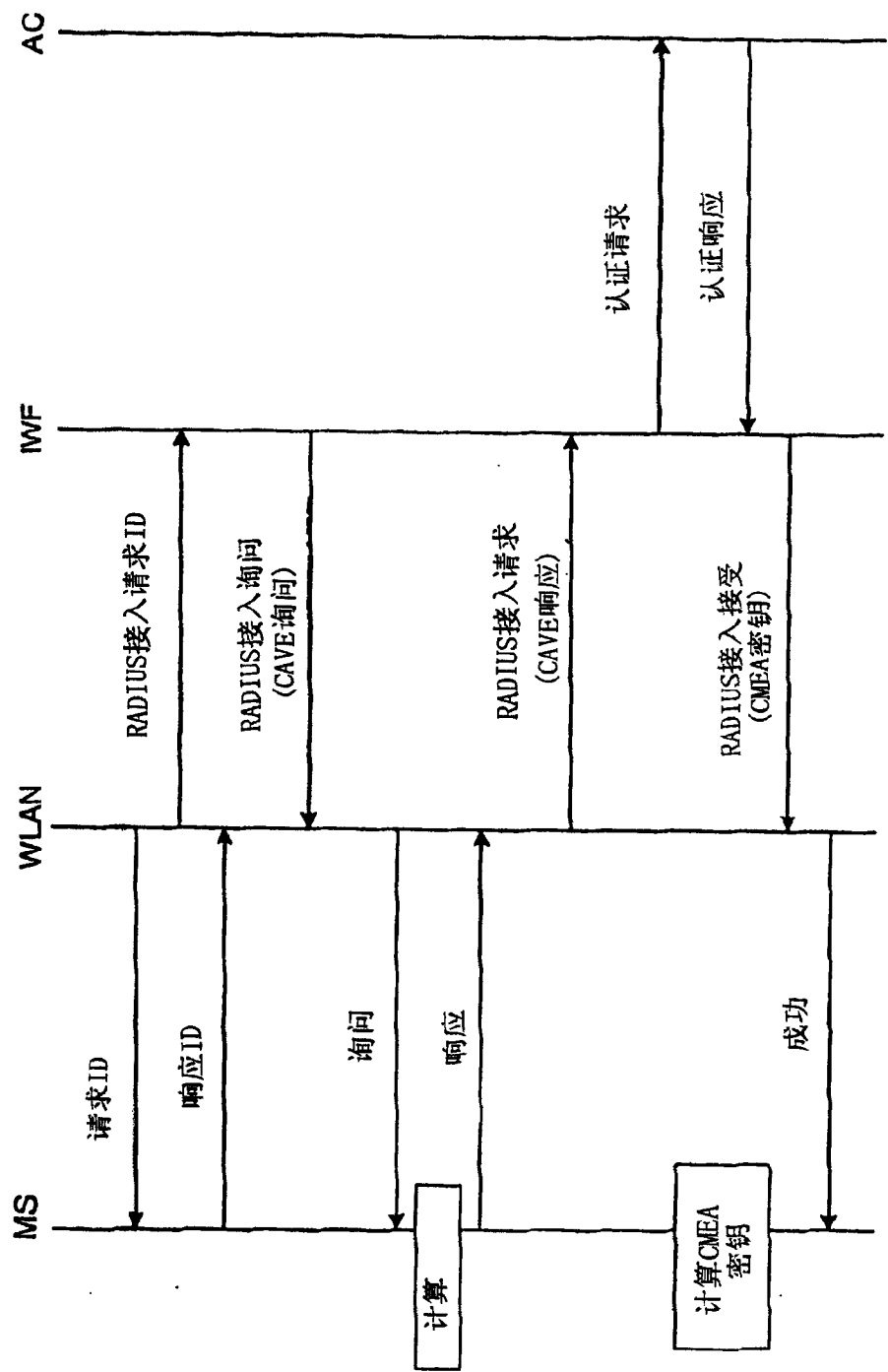


图 3

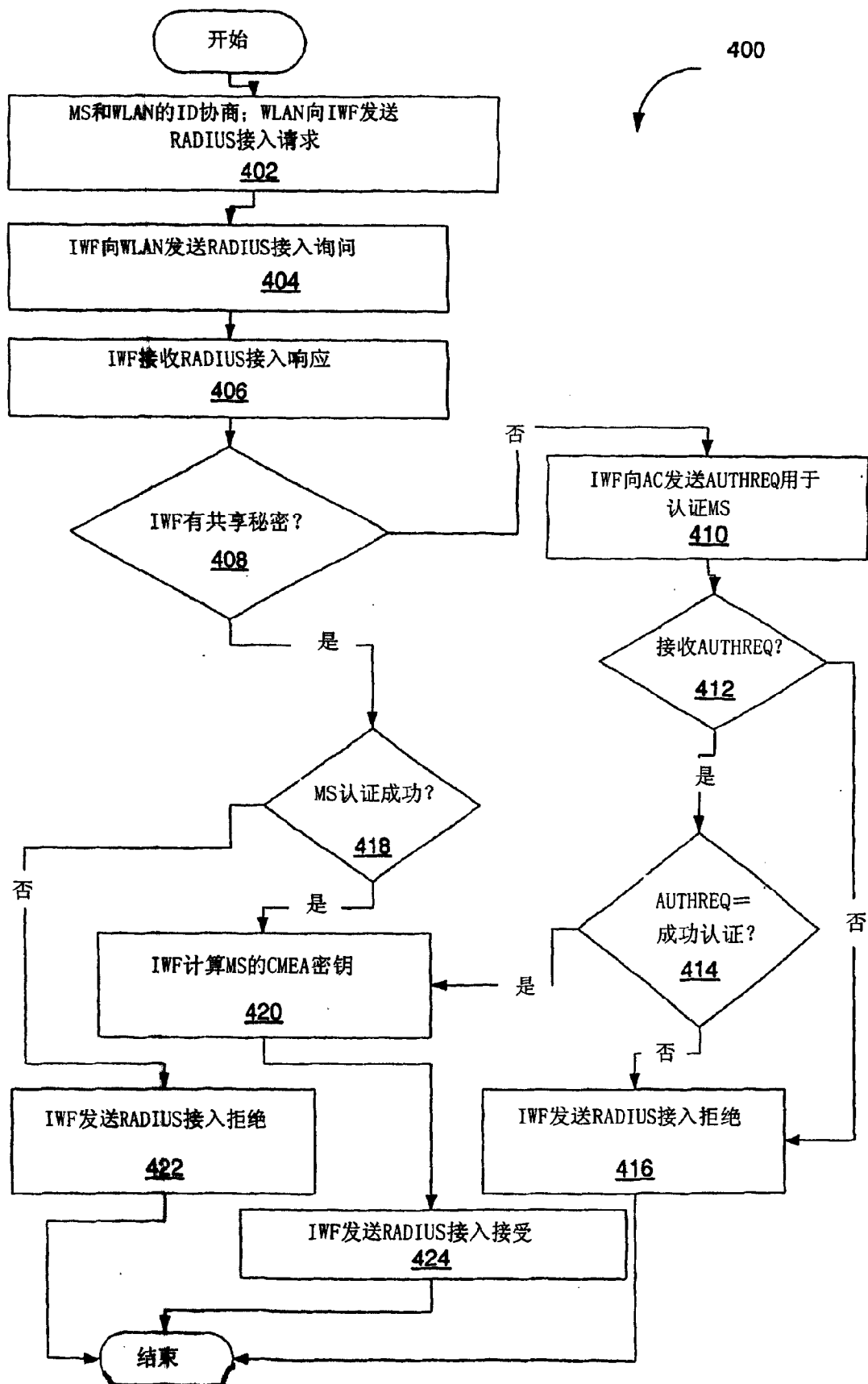


图 4

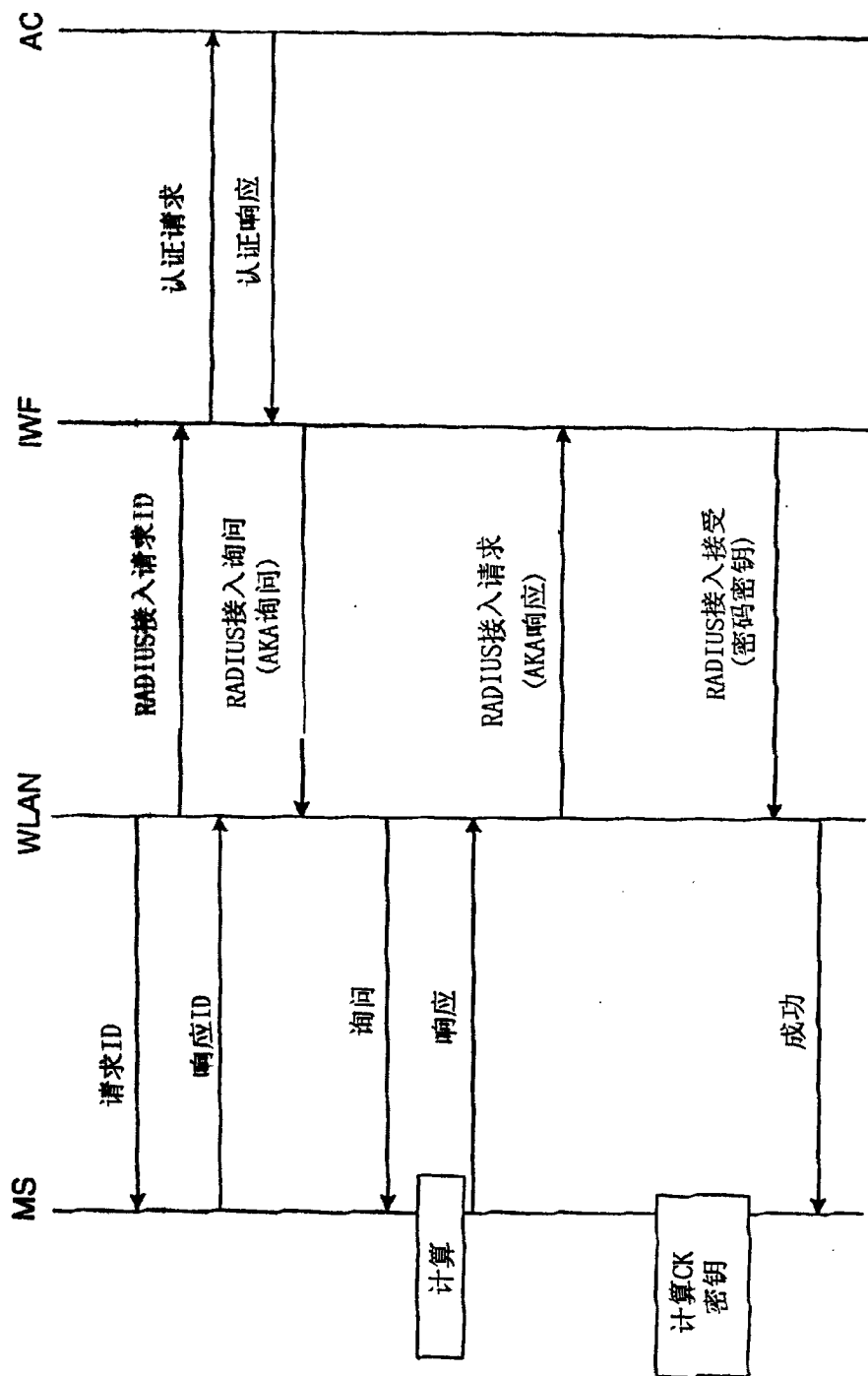


图 5

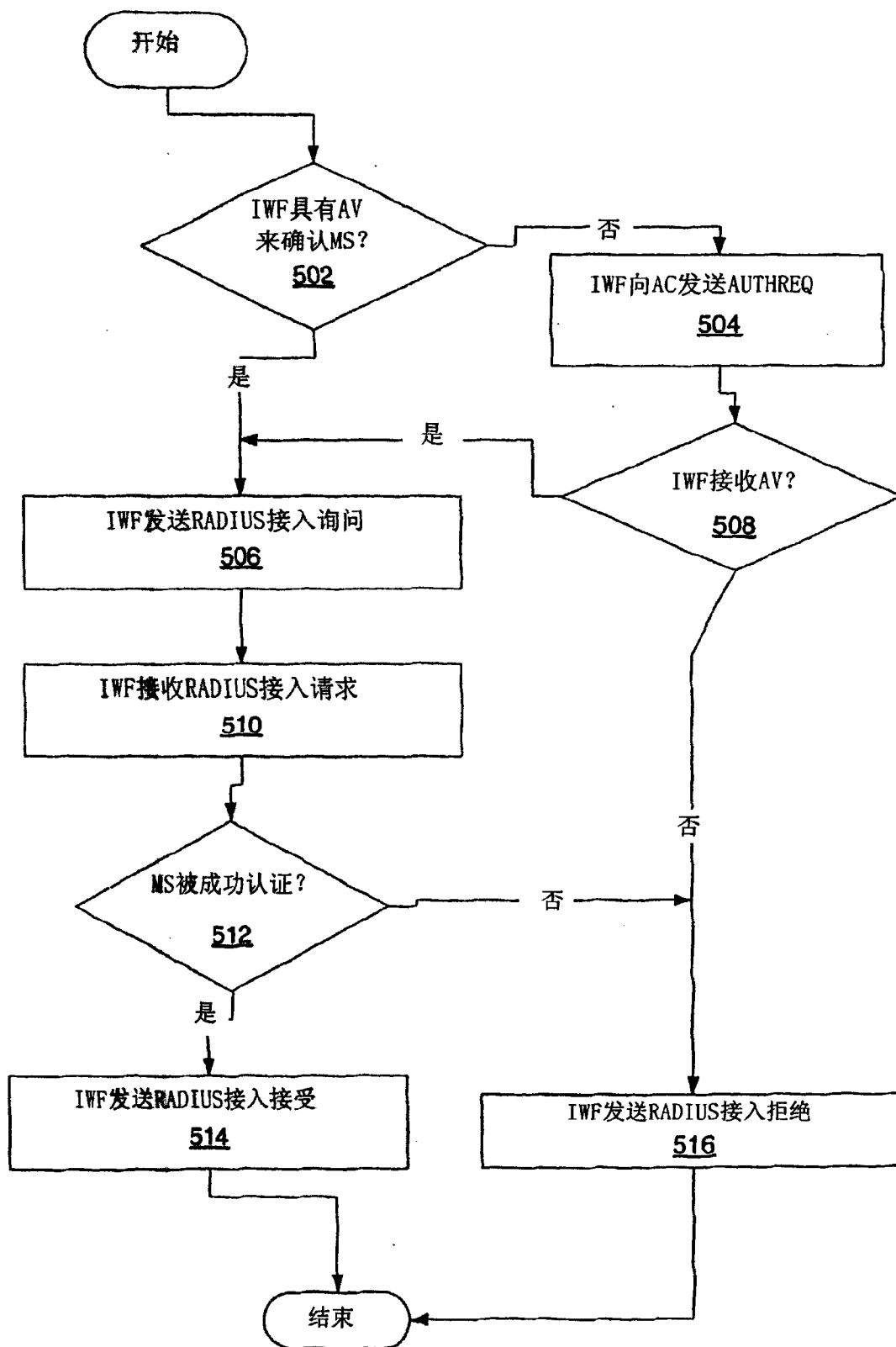


图 6

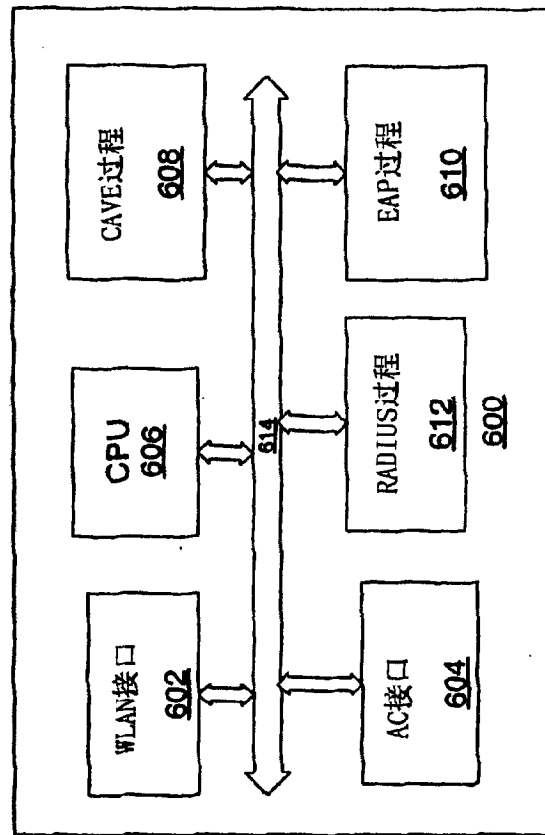


图 7