(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104243145 A
(43)申请公布日 2014.12.24

(21)申请号 201410439953.8

(22)申请日 2003.06.20

(30)优先权数据
10/177,017 2002.06.20 US

(62)分案原申请数据
03819297.7 2003.06.20

(71)申请人 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 上海专利商标事务所有限公司 31100
代理人 陈炜

(51)Int.Cl.
H04L 9/08(2006.01)
H04W 12/04(2009.01)
H04W 12/06(2009.01)

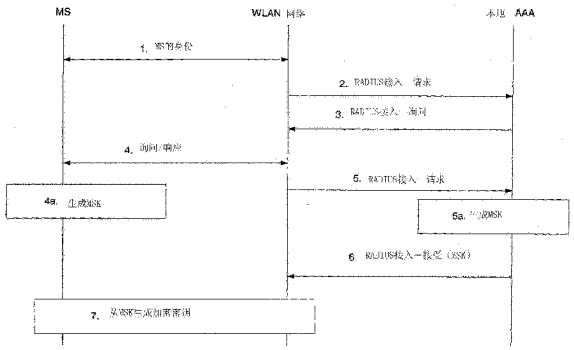
权利要求书2页 说明书9页 附图4页

(54)发明名称

通信系统中的密钥生成

(57)摘要

本发明涉及通信系统中的密钥生成。通信系统生成主阶段密钥(MSK),用于到不提供对话务加密的系统实体的接入。本地服务器和用户都生成相同的MSK。所述MSK被用于为话务生成加密密钥。在一个实施例中,使用哈希函数和对于所述请求者的特定信息来生成MSK。所述本地服务器根据接入请求消息所包含的信息来确定生成MSK的需要。一旦生成MSK,它被提供给系统实体,使得该实体能够加密通信。



CN 104243145 A

1. 一种用于在包括第一网络和第二网络的通信系统中验证的方法，所述方法包括：

由移动站 MS 使用网络接入标识符与所述第一网络协商 MS 的身份；

从所述第一网络的认证授权计费 AAA 服务器向所述第二网络的 AAA 服务器发送远程身份验证拨入用户服务 RADIUS 接入请求；

从所述第二网络的 AAA 服务器经由所述第一网络向 MS 发送询问握手认证协议 CHAP 询问；

由 MS 向所述第一网络提供对所述 CHAP 询问的响应；

从所述第一网络向所述第二网络的 AAA 服务器发送包括所述响应的 RADIUS 接入请求；

在所述 MS 和所述第二网络的 AAA 服务器从共享的根密钥和用户标识值产生主阶段密钥 MSK；以及

由所述第二网络的 AAA 服务器向所述第一网络发送包括所述 MSK 的 RADIUS 接入接受消息，

其中所述第一网络为无线局域网 WLAN，而所述第二网络为蜂窝网络系统中的高数据速率 HDR 类型网络。

2. 如权利要求 1 所述的方法，其特征在于，使用所述 MSK 导出用于保护所述第一网络的接入点和所述 MS 之间话务的加密密钥。

3. 如权利要求 1 所述的方法，其特征在于，所述 HDR 类型网络是第三代 3G 电信网络。

4. 如权利要求 1 所述的方法，其特征在于，所述用户标识值是网络接入标识符 NAI。

5. 如权利要求 1 所述的方法，其特征在于，所述 MSK 进一步基于询问响应值产生。

6. 如权利要求 5 所述的方法，其特征在于，所述询问响应值是 CHAP 询问值。

7. 如权利要求 1 所述的方法，其特征在于，所述 MSK 作为询问响应值和随机值中的至少一者、所述共享的根密钥以及所述用户标识值的哈希函数来产生。

8. 一种用于无线局域网 WLAN 中的设备，包括：

用于使用网络接入标识符与移动站 MS 协商 MS 身份的装置；

用于在 WLAN 的认证授权计费 AAA 服务器向蜂窝网络系统中的高数据速率 HDR 类型网络的 AAA 服务器发送远程身份验证拨入用户服务 RADIUS 接入请求的装置；

用于将由所述 HDR 类型网络的 AAA 服务器提供的询问握手认证协议 CHAP 询问发送到 MS 的装置；

用于将包括 MS 对所述 CHAP 询问的响应的 RADIUS 接入请求发送到所述 HDR 类型网络的 AAA 服务器的装置；

用于从所述 HDR 类型网络的 AAA 服务器接收包括主阶段密钥 MSK 的 RADIUS 接入接受消息的装置，其中所述 MSK 基于共享的根密钥和用户标识值；以及

用于从所述 MSK 导出对所述 WLAN 的接入点和 MS 之间话务进行保护的加密密钥的装置。

9. 如权利要求 8 所述的设备，其特征在于，所述 HDR 类型网络是第三代 3G 电信网络。

10. 如权利要求 8 所述的设备，其特征在于，所述用户标识值是网络接入标识符 NAI。

11. 如权利要求 8 所述的设备，其特征在于，所述 MSK 进一步基于询问响应值产生。

12. 如权利要求 11 所述的设备，其特征在于，所述询问响应值是 CHAP 询问值。

13. 如权利要求 8 所述的设备，其特征在于，所述 MSK 作为询问响应值和随机值中的至少一者、所述共享的根密钥以及所述用户标识值的哈希函数来产生。

14. 一种用于蜂窝网络系统中高数据速率 HDR 类型网络中的设备，包括：

用于在所述 HDR 类型网络的认证授权计费 AAA 服务器从无线局域网 WLAN 的 AAA 服务器接收远程身份验证拨入用户服务 RADIUS 接入请求的装置；

用于在所述 HDR 类型网络的 AAA 服务器经由所述 WLAN 向移动站 MS 发送询问握手认证协议 CHAP 询问的装置；

用于在所述 HDR 类型网络的 AAA 服务器从所述 WLAN 接收包括 MS 对所述 CHAP 询问的响应的 RADIUS 接入请求的装置；

用于在所述 HDR 类型网络的 AAA 服务器从共享的根密钥和用户标识值产生主阶段密钥 MSK 的装置；以及

用于在所述 HDR 类型网络的 AAA 服务器将包括所述 MSK 的 RADIUS 接入接受消息发送到所述 WLAN 的装置。

15. 如权利要求 14 所述的设备，其特征在于，所述用户标识值是网络接入标识符 NAI。

16. 如权利要求 14 所述的设备，其特征在于，所述 MSK 进一步基于询问响应值产生。

17. 如权利要求 16 所述的设备，其特征在于，所述询问响应值是 CHAP 询问值。

18. 如权利要求 14 所述的设备，其特征在于，所述 MSK 作为询问响应值和随机值中的至少一者、所述共享的根密钥以及所述用户标识值的哈希函数来产生。

19. 如权利要求 14 所述的设备，其特征在于，所述接入请求消息具有第一字段，其中所述接入请求消息的格式包括标识用于对所述通信系统进行接入的属性信息类型的类型字段和用于所述属性信息的值字段，所述值字段包括标识用于所述接入的子属性信息类型的第二类型字段和用于所述子属性信息的第二值字段。

20. 如权利要求 19 所述的设备，还包括：

用于确定所述第一字段的状态的装置；并且

其中用于产生 MSK 的装置在所述状态是第一值的情况下产生 MSK。

通信系统中的密钥生成

[0001] 本申请是申请日为2003年6月20日申请号为第03819297.7号发明名称为“通信系统中的密钥生成”的中国专利申请的分案申请。

[0002] 背景

[0003] 领域

[0004] 本发明涉及用于通信系统的交互工作功能，尤其涉及在无线局域网(WLAN)中使用的经由交互工作功能的通用认证和密钥交换的机制。

[0005] 背景

[0006] 无线局域网(WLAN)允许用户可以实际上不受限制地使用Internet协议(IP)服务和数据网络。对WLAN的使用不仅限于膝上型计算机和其它计算设备，而是迅速地扩展到蜂窝电话、个人数字助理(PDA)和其它由外部网络或载体支持的小型无线设备。例如，在网吧或工作区中，经由蜂窝载体通信的无线设备会漫游到WLAN中。在这种情况下，无线设备有权接入蜂窝系统，但期望访问WLAN。WLAN访问要求认证。由于无线设备已经获取了接入蜂窝系统的权力，进一步认证的要求是多余的。因此，需要一种允许对蜂窝系统和WLAN的接入通用认证的机制。而且，需要一种生成通信过程中使用的加密密钥的通用机制。

附图说明

[0007] 图1是包含高数据速率(HDR)或HDR类型网络和无线局域网(WLAN)的通信系统。

[0008] 图2是通信系统中认证程序的时序图。

[0009] 图3是通信系统中认证程序的时序图。

[0010] 图4和5是接入请求消息格式。

[0011] 图6是包含生成主阶段密钥(MSK)功能的无线装置。

具体实施方式

[0012] 本发明使用“示例性”一词意指“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理解为比其它实施例更为优选或有利。

[0013] HDR订户站，这里被称为接入终端(AT)，可以是移动的或固定的，并且可以与一个或多个HDR基站通信，这里被称为调制解调器池收发机(MPT)。接入终端通过一个或多个调制解调器池收发机发送和接收数据分组至HDR基站控制器，这里被称为调制解调器池控制器(MPC)。调制解调器池收发机和调制解调器池控制器是网络的部分，被称为接入网络。接入网络在多个接入终端之间传输数据分组。接入网络可以进一步连接到该接入网络之外的另外的网络，诸如公司内部互联网或因特网，并且可以在每个接入终端和这样的外部网络之间传输数据分组。与一个或多个调制解调器池收发机建立起活动话务信道连接的接入终端被称为活动接入终端，并且被称为处于话务状态。在与一个或多个调制解调器池收发机建立活动话务信道连接的过程中的接入终端被称为处于连接建立状态。接入终端可以是任何通过无线信道或通过诸如使用光纤或同轴电缆等有线信道通信的数据设备。此外，接入终端可以是多种类型的设备中的任何一种，所述多种类型的设备包括但不限于PC卡、紧

凑式闪存、外置或内置调制解调器，或无线或有线电话。接入终端将信号发送至调制解调器池收发机所通过的通信链路被称为反向链路。调制解调器池收发机将信号发送至接入终端所通过的通信链路被称为前向链路。

[0014] 图 1 示出了含有带有多个接入点 (AP) 的无线局域网 (WLAN)104 的通信系统。AP 是集线器或桥，提供对 WLAN104 的无线方面的星型拓扑控制和对有线网络的接入。

[0015] 每个AP110，同其它未示出的一样，支持到数据服务的连接，诸如因特网。MS102，诸如膝上型计算机或其它数字计算设备，经由无线电接口与 AP 通信，由此得出术语无线 LAN。AP 接着与认证服务器 (AS) 或认证中心 (AC) 通信。AC 是为请求准入网络的设备执行认证服务的组件。实施包括远程身份验证拨入用户服务 (RADIUS) 和其它认证授权计费 (AAA) 服务器，所述 RADIUS 是 RFC2138 中，C. Rigney et al. 的“Remote Authentication Dial In User Service(RADIUS)”（于 1997 年 4 月出版）中所描述的因特网用户认证。

[0016] 无线连网成为了网络互连的重要方面。基于无线网络的唯一界限就是无线电信号强度的事实，它呈现出一组独特的问题。没有线路来定义网络中的成员资格。没有物理方法来限制无线电范围内的系统成为无限网络的成员。无线连网，更甚于任何其它的网络技术，需要一种认证和接入控制机制。当前，各个团体正致力于开发一种标准的认证机制。当前，公认的标准是 IEEE802.11。

[0017] 基于 RF 的网络的性质使得它对于收发机范围内任何无线电的分组侦听是开放的。通过使用高增益天线，侦听可以在远远超过用户“工作”范围外发生。使用容易的可用工具，偷听者不限于仅仅收集分组用于以后的分析，而是可以实际上看到交互式会话，如同网页被合法的无线用户看到一样。偷听者也可以抓住不牢靠的认证交换，如同一些网站登陆。之后，该偷听者可以复制该登陆并获取接入。

[0018] 一旦攻击者获取了 WLAN 如何控制准入的消息，他可以能够靠自己获取准入该网络或窃取合法用户的接入。如果攻击者可以模拟合法用户的 MAC 地址并使用分配给它的 IP 地址，窃取用户的接入是简单的。攻击者等待直至合法系统停止使用网络，接着接任网络中所述合法系统的位置。这将允许攻击者直接接入网络中所有的设备，或使用该网络来获取到更广阔的 Internet 的接入，在所有的这些时候看上去是被攻击网络的合法用户。因此，在 WLAN 的实施中，认证和加密成为了主要关心的问题。

[0019] 认证是校验通信中个体或应用程序身份的过程。这样的标识使得服务供应者可以验证实体为合法用户，并且也可以为特定服务的请求验证用户。认证和授权实际上具有非常特定的含义，虽然这两个名称经常可交换地使用，并且常常在实践中不被清楚地区分。

[0020] 认证是用户为某一身份建立权利，——实际上是使用某个名称的权力的过程。有许多技术可被用于认证用户——密码、生物遗传技术、智能卡、证书。

[0021] 名称或身份具有与它相关联的属性。属性会紧密地与名称相关联（例如，在认证净载中）或者它们会被存储在对应于该名称的密钥下的目录或其它数据库中。属性会随着时间变化。

[0022] 授权是确定身份（加上与该身份相关联的一组属性）是否被允许执行某些动作的过程，所述某些动作诸如接入资源。注意允许执行一动作并不保证该动作可以被执行。注意认证和授权的决定可以由不同的实体在不同的点作出。

[0023] 在蜂窝网络中，认证特性是允许蜂窝网络验证无线设备身份，由此减少对蜂窝网

络未经授权使用的网络性能。该过程对订户是透明的。用户在打电话时无需做任何事来认证他们电话的身份。

[0024] 认证一般涉及密码方案，其中服务供应商和用户由一些共享的信息和一些私有的信息。所述共享信息一般被称为“共享密钥 (shared secret)”。

[0025] A－密钥

[0026] 认证密钥 (A－密钥) 是一秘密的值，它对于每个个别的蜂窝电话是唯一的。它在蜂窝服务供应商处登记，并存储在电话和认证中心 (AC) 中。A－密钥由制造商编程到电话中。它也可以由用户从无线设备菜单或销售点的特定终端手动地输入。

[0027] 无线设备和 AC 必须具有相同的 A－密钥以作出相同的计算。A－密钥的主要功能是被用作计算共享密钥数据 (SSD) 的参数。

[0028] 共享密钥数据 (SSD)

[0029] SSD 被用作无线设备和 AC 中认证计算的输入，并被同时存储在这两个地方。不同于 A－密钥，SSD 可以通过网络来修改。AC 和无线设备共享三个参与 SSD 计算的元素 :1) 电子序列号 (ESN) ;2) 认证密钥 (A－密钥) ;以及 3) 用于共享密钥数据计算的随机数字 (RANDSSD)。

[0030] ESN 和 RANDSSN 通过网络和无线电接口发送。SSD 在设备第一次系统接入时被更新，并且在此后周期性地更新。当计算 SSD 时，结果是两个分开的值，SSD-A 和 SSD-B。SSD-A 被用于认证，SSD-B 被用于加密和语音保密。

[0031] 根据服务系统的性能，SSD 在 AC 和服务移动交换中心 (MSC) 之间可以是共享的或不共享的。如果密钥数据是共享的，它意味着 AC 将把它发送到服务 MSC，且该服务 MSC 必须能够执行 CAVE。如果它不是共享的，AC 将保存该数据并执行认证。

[0032] 共享的类型影响到如何处理认证询问。认证询问是被发送用于询问无线设备身份的消息。基本上，认证询问发送一些供用户执行的信息，一般为随机数字数据。接着，用户处理该信息并发送响应。分析所述响应以验证该用户。对于共享的密钥数据，询问在服务 MSC 处处理。对于非共享的密钥数据，询问由 AC 处理。系统可以通过共享密钥数据来最小化所发送话务的量，并允许询问在服务交换处更快地发生。

[0033] 认证程序

[0034] 在给定的系统中，归属位置寄存器 (HLR) 通过充当 MSC 和 AC 之间的中介来控制认证过程。服务 MSC 被配置成用移动的 HLR 支持认证，反之亦然。

[0035] 如果设备能够认证，它通过在管理消息列中设置授权字段来通知服务 MSC 以开始该过程。在响应中，服务 MSC 使用认证请求来开始注册 / 认证过程。

[0036] 通过发送认证请求，服务 MSC 告诉 HLR/AC 它是否能够做 CAVE 计算。AC 控制从那些可用的服务 MSC 中及设备性能中选择哪些将被使用。当服务 MSC 不具有 CAVE 性能时，SSD 不能在 AC 和 MSC 之间共享，由此所有的认证过程都在 AC 中执行。

[0037] 认证请求 (AUTHREQ) 的目的是认证电话和请求 SSD。AUTHREQ 包含两个用于认证的参数，AUTHR 和 RAND 参数。当 AC 得到 AUTHREQ 时，它使用 RAND 和上次已知的 SSD 来计算 AUTHR。如果它符合在 AUTHREQ 中发送的 AUTHR，那么认证是成功的。如果 SSD 可以被共享，返回到 AUTHREQ 的结果中将包含 SSD。

[0038] 询问

[0039] 认证过程由询问和响应会话组成。如果 SSD 被共享，会话在 MSC 和设备之间运行。如果 SSD 不被共享，会话在 HLR/AC 和设备之间运行。根据交换类型，MSC 会能够作唯一询问、总体询问或两者兼有。当前，一些 MSC 不能够作全体询问。唯一询问是只在呼叫尝试期间才发生的询问，因为它使用音频信道。唯一询问在呼叫开始和呼叫递送期间向单个设备出示认证。全体询问是在注册、呼叫开始和呼叫递送期间发生的询问。全体询问向所有使用特定无线电控制信道的 MS 出示认证询问。之所以称之为全体询问是因为它在无线电控制信道上广播，且该询问被所有接入那个控制信道的电话使用。

[0040] 在询问期间，设备响应由 MSC 或 AC 提供的随机数字。设备使用该随机数字和设备中存储的共享密钥数据来计算向 MSC 的响应。MSC 也使用随机数字和共享密钥数据来计算应该从设备获得什么响应。这些计算通过 CAVE 算法完成。如果响应不相同，服务被拒绝。询问程序不会增加连接到呼叫所需花费的时间量。实际上，在某些情况下，呼叫会进行，只在认证失败时被拆下。

[0041] 作为向用户提供非限制地接入 IP 数据网络的方法，无线局域网 (WLAN) 获得了极大的普及。诸如 1xEV-DO 网络等高数据数率 (HDR) 网络和其它第三代 (3G) 网络也被设计成提供高速数据接入；虽然他们支持的数据率一般低于 WLAN 的数据率，但是 3G 网络提供了宽广得多的区域的数据覆盖。虽然 WLAN 和 HDR 网络会被当作竞争对手，但是它们会是互补的：WLAN 提供在诸如机场休息室和宾馆大厅等公共场所中提供高容量的“热点”覆盖，而 HDR 网络可以向用户提供移动时几乎随处存在的数据服务。因此，相同的载体在单一用户定购下会同时提供 HDR 和 WLAN 接入服务。这意味着 MS 对于两种接入认证类型都使用相同的认证方法和密钥。

[0042] 一个协议，诸如询问握手认证协议 (CHAP)，也被称为 MD5-Challenge，会既被用于 HDR 网络，又被用于 WLAN 接入认证。CHAP 特别地使用 RADIUS 协议来认证终端而不发送安全数据。MS 由它的本地 RADIUS 服务器认证，其中所述本地 RADIUS 服务器和 MS 共享根密钥。在 MS 经由 CHAP 询问被成功地认证之后，MS 和本地或 HDR 网络导出相同的用于保护 MS 和 WLAN 接入点 (AP) 之间交换话务的加密密钥。

[0043] 在经由 CHAP 询问成功的 WLAN 接入认证后，本地 RADIUS 服务器和 MS 从共享的根密钥生成相同的主阶段密钥 (MSK)。该 MSK 会被用于导出加密密钥，用于保护 MS 和 WLAN 的 AP 之间实际的话务。共享根密钥被配置到 MS，且是静态的。MSK 在每个分组数据会话时生成，且只在该会话期间保持不变。对于新的会话，会使用不同的随机数字从共享根密钥生成新的 MSK。

[0044] 因为在 MS 接入 HDR 网络时不需要 MSK，一个实施例提供了允许本地 RADIUS 服务器确定 MS 是接入 WLAN 还是 HDR 网络的机制。

[0045] 图 1 说明了包括 HDR 网络 106、WLAN104 和 MS102 的通信系统 100。MS102 能够接入 HDR 网络 106，并且漫游到 WLAN104 覆盖区域中。MS102 在 WLAN104 中寻找经由 AP110 到 WLAN104 的通道。注意 WLAN104 会包括任意数量的 AP（未示出）。WLAN104 也包括认证授权和计费实体或服务器 112。注意该 HDR 网络 106 也包括 AAA 服务器 108。

[0046] 图 2 说明了在通信系统 100 中使用 CHAP 或 MD5-Challenge 时，用于到 WLAN 的接入认证的消息流。MS102 使用网络接入标识符 (NAI) 用于标识。NAI 具有 username@realm 的格式，其中 realm 标识 MS 的本地网络，在此例中为 HDR 网络 106。WLAN 网络 104 中的 AAA

服务器 112 发起到 MS102 本地网络，即向 HDR 网络 106，的 AAA 服务器 108 的 RADIUS 接入－请求消息。诸如所述 HDR 网络 106 可以是任何支持高速数据数率传输的网络。接着，AAA108 经由 WLAN104 向 MS102 发出 CHAP 询问。MS102 基于该询问计算响应，所述询问诸如随机数字，并且该响应作为 RADIUS 接入－请求请求经由 WLAN104 向 AAA108 传送。如果认证成功，本地 AAA 服务器 108 使用 RADIUS 接入－接受消息来确认这个，所述 RADIUS 接入－接受消息准予 MS102 接入 WLAN 网络 104。如上文所述的，本地 AAA 服务器 108 和 MS102 都从共享根密钥生成相同的主阶段密钥 (MSK)。

[0047] 如上文所述的，CAVE 算法普遍用于蜂窝通信，因此被很好地使用和散布。也使用其它用于认证的算法。特别在数据通信中，多种算法存在不同的复杂性和应用。为了协调这些机制，开发出扩展认证协议 (EAP) 作为支持多种认证和密钥分配机制的一般协议框架。L.Blunk et al 在 RFC2284（发表于 1998 年三月）的“PPP Extensible Authentication Protocol(EAP)”中描述了 EAP。

[0048] EAP 支持的一个这样的机制，如由 J.Arkko et al. 在“EAP AKA 认证”中所定义的（于 2002 年 2 月作为因特网草案发表），是 AKA 算法。因此需要扩展 EAP 以包含蜂窝算法 CAVE。所期望的是为新的系统和网络提供向后兼容。

[0049] EAP

[0050] 扩展认证协议 (EAP) 是用于认证的一般协议，它支持多种认证机制。EAP 不在链接建立和控制期间选择特定的认证机制，而是将其延迟到直至认证程序开始。这允许认证者在确定特定的认证机制之前请求更多的信息。认证者被定义为需要认证的链路的结束。认证者规定链接建立期间所使用的认证协议。

[0051] 密钥生成

[0052] 密钥分级结构是用于从根密钥生成一组用于加密 / 解密消息或认证消息的加密密钥步骤的顺序。密钥分级结构应该包含一段时间变化的消息，这样每次使用该分级结构时，不会生成相同组的加密密钥。密钥分级结构也应该被配置成：如果导出的加密密钥变得已知，不能从加密密钥获得根密钥。

[0053] 在一个实施例中，总的密钥分级结构由三个较小的分层密钥分级结构组成：主密钥分级结构、密钥再生成密钥分级结构和每一分组密钥分级结构。主密钥分级结构根据分级结构和认证方法会包括 EAP 密钥生成 (keying)、预共享密钥或随机数字。如果 EAP 密钥生成被用于主密钥分级结构，主密钥分级结构将一般驻留在 RADIUS 服务器上。

[0054] 密钥再生成密钥分级结构有两种类型，被称为成对密钥分级结构和组密钥分级结构。这两种类型的密钥分级结构中的步骤是类似的；只有到这两种类型的输入是不同的。

[0055] 每一分组密钥分级结构。这会用于动态密钥完整性协议 (TKIP)（使用 RC4 加密引擎）或用于高级加密标准 (AES)。

[0056] 对偶密钥分级结构被用于导出用在无线网络两个实体之间的密钥 (AP 和相关联的站，或网络中一对站）。

[0057] 组密钥分级结构被用于导出和传递无线组中所有实体 (AP 和网络中与那个 AP 相关联的所有的站，或网络中所有的实体）使用的密钥。

[0058] 对偶密钥分级结构在两个使用成对密钥的实体上平行地实体化，每个实体使用共享信息计算相同组的加密密钥。两个实体中的一个驱动该成对密钥分级结构，那个实体称

为成对密钥所有者。对于给定的网络，成对密钥所有者是 AP ；对于其它网络，每个可能的站对将有成对的密钥分级结构，且该成对密钥所有者是具有较低媒体访问控制层地址的对的站。

[0059] 组密钥分级结构只在一个实体上实体化 (instantiaied)，并且所导出的加密密钥被传播给所有其它的实体 ；驱动组密钥分级结构的实体是组密钥的所有者。对于给定的网络，诸如被称作为基本服务组 (BSS)，组密钥的所有者是该 AP ；对于独立基本服务组 (IBSS) 网络，组密钥的所有者是当前信标的发送者。注意 BBS 网络是由 AP 和相关联的站组成，而 IBSS 网络是由一组站组成，所有所述的站互相成对。如这里所使用的站是工作站，且包括移动站或其它能够接入局域网的无线设备。

[0060] 每个站会至少有两个实体化的密钥分级结构，并且完全可能更多。在 BBS 网络中，AP 会有为每个相关联的站实体化的成对密钥分级结构，并且也至少有一个组密钥分级结构 ；AP 会是所有这些分级结构的密钥所有者。每个相关联的站会有一个实体化的成对密钥分级结构，且至少一个组密钥分级结构。对于 IBBS 网络，每个站会有为网络中的每个其它站实体化的成对密钥分级结构以及单个的组密钥分级结构。

[0061] 密钥所有者会有用于组密钥的单个组密钥再生成分级结构实例和用于每个关联的成对密钥再生成分级结构实例。密钥所有者对于组和成对临时密钥 (若有的话)，都会每个动态密钥完整性协议 (TKIP) 临时密钥有一每个分组密钥分级结构。非密钥所有者对组密钥和成对密钥，每个关联会有一密钥再生成分级结构实例，并且对于组和成对临时密钥 (若有的话)，都会每个 TKIP 临时密钥有一每个分组密钥分级结构。

[0062] MSK

[0063] 根据示例性实施例，MSK 包括蜂窝信息加密算法 (CMEA) 密钥和加密密钥 (CK)，所述的 CMEA 密钥用于保护诸如到 WLAN 的 MS 话务。

[0064] 图 3 说明了用于生成用于保护 MS102 和 WLAN 网络 104 之间话务的加密密钥。这个过程由 MS201 身份协商开始。接着，WLAN104 发送 RADIUS 接入请求消息到 AAA108，AAA108 以 RADIUS 接入询问消息响应。WLAN104 将该询问传递到 MS102，所述 MS102 从那里计算响应。接着，MS102 对该询问的响应被提供给 WLAN104。在步骤 4a 中，在 MS102 发送认证响应到 WLAN104 之后，MS102 使用根密钥来生成主阶段密钥 (MSK)。

[0065] WLAN104 发送 RADIUS 接入请求消息到 AAA108，包括询问响应。在步骤 5a 中，如果 MS102 成功地被认证，本地 AAA 服务器 108 使用 MS102 根密钥来生成与 MS102 在步骤 4a 所生成的相同的 MSK。在步骤 6 中，本地 AAA 服务器 108 使用属性将 MSK 包含在 RADIUS 接入一接受消息中，所述属性诸如 MS-MPPE-Recv-Key 属性。在步骤 7 中，MS102 和 WLAN 网络 104 使用程序来从 MSK 生成加密密钥，所述程序诸如于 2002 年 3 月发表的 IEEE Std802.11i/D2.0 中题为“Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part11:Wireless Medium Access Control(MAC)and physical layer(PHY)specifications:Specification for Enhanced Security”(这里称为“802.11i 标准”) 的文件中所指定的。

[0066] 以下提供了在 MS102 和本地 AAA 服务器 108 中用于生成 MSK 的算法和参数的两个例子。在第一实施例中，MSK 被定义为 ：

[0067] MSK ＝哈希函数 (密钥，询问，NAI，密钥) (1)

[0068] 其中所述 MSK 是使用以下参数应用哈希函数（例如，CHAP、HMAC）的结果：

[0069] ● MS102 根密钥；

[0070] ●用于在图 3 的步骤 4 － 5 中认证 MS102 的询问；

[0071] ● MS102NAI；以及

[0072] ●再一次 MS102 根密钥。

[0073] 根据这个实施例，MS102 和本地 AAA 服务器 108 具有需要独立生成相同 MSK 的所有密钥材料。换而言之，没有另外的密钥材料需要在 MS102 和本地 AAA 服务器 108 之间交换用于 MSK 生成。注意 MSK 和 MS102 接入认证响应是从相同的询问值生成的。可替换实施例从不同的随机值生成 MSK。

[0074] 第二个例子，根据另一实施例，将 MSK 定义为：

[0075] MSK ＝哈希函数（密钥，NAI，随机数字） (2)

[0076] 其中所述 MSK 是将哈希函数（例如，CHAP、HMAC）应用到以下参数上的结果：

[0077] ● MS102 根密钥；

[0078] ● MS102NAI；以及

[0079] ●由本地 AAA 服务器生成的随机数字，

[0080] 其中所述随机数字与询问值不同。根据这个实施例，MSK 由随机数字生成，所述随机数字不同于在 MS102 接入认证中使用的询问值。独立询问值的使用提供了 MSK 和 MS102 接入认证之间较少的联系，并且由此提供了改进的安全性。诸如所述随机数字被发送到 MS102 且 MSK 在那里生成。随机数字经由 RADIUS 接入－接受（图 3 的步骤 6）和在 802.11i 标准（图 3 的步骤 7）中定义的机制被发送到 MS102。

[0081] 生成 MSK 的程序在 MS102 接入 WLAN104 时使用，并且在 MS 接入 1xEV-DO 或其它 HDR 网络时不使用。这是由于由 HDR 系统提供的无线电加密。当 MS 开始到 WLAN 网络 104 或 HDR 网络 106 的接入时，MS102 能够确定是否需要 MSK 生成。然而，本地 AAA 服务器必须也确定何时生成 MSK。

[0082] 在一个实施例中，实施特定 RADIUS 属性来通知 AAA108 生成 MSK。在图 3 的步骤 2 和 5 中，WLAN 网络 104 发送包含指示 MS102 期望或请求 WLAN104 接入的特定或指定属性的 RADIUS 接入－请求消息。该属性状态会触发本地 AAA 服务器 108 来执行 MSK 生成（如果 MS102 认证是成功的）。当所指定的属性在 RADIUS 接入－请求消息中不存在时，本地 AAA 服务器 108 不会执行 MSK 生成。注意在符合 3GPP2 的系统中实施，指定属性是特定于 3GPP2 的，这样可被定义成使用 3GPP2 的卖方 ID 的卖方－特定属性。

[0083] 图 4 说明了发表于 2000 年 6 月，C. Rigney et al 的题为“Remote Authentication Dial In User Service(RADIUS)”的 RFC2865 中描述的 RADIUS 格式。数据格式 200 包括：编码字段 202 用于标识 RADIUS 分组的类型（例如，接入请求、接入拒绝等等）；ID 字段 204 用于调整匹配请求和响应；以及长度字段 206 用于指示相关联的分组的长度。也说明了属性 220，包含：类型字段 222 标识值字段 226 的内容；长度字段 224 给出属性的长度；以及值字段提供这个属性的特定信息。注意 RADIUS 支持卖方－特定属性，其中值字段 226 被用于提供卖方标识，后接属性信息。卖方－特定类型会如同在发表于 1999 年，由 G. Zorn 写的题为”Microsoft Vendor-specific RADIUS Attributes”的 RFC2548 中所描述的，用于应用到 CHAP 消息。

[0084] 可替换实施例在 RADIUS 接入－请求消息中实施名为网络接入服务器 (NAS) Internet 协议 (IP) 地址的标准属性。该标准属性标识发起 RADIUS 接入－请求消息的 RADIUS 客户端的 IP 地址。本地 AAA 服务器 108 被配置为带有包含 WLAN 网络 104 中所有 RADIUS 客户端 IP 地址的数据库。如果 NAS IP 地址属性中所指示的 IP 地址与数据库中的地址相匹配，那么该 RADIUS 接入－请求消息是从 WLAN 网络 104 发起的，并且本地 AAA 服务器 108 会执行 MSK 生成（如果 MS 认证是成功的）。否则，本地 AAA 服务器 108 将不会执行 MSK 生成。

[0085] 图 5 中说明了标准属性的格式以及加在值字段上的例子。属性格式 300 包含类型字段 302，用于指示值字段 306 的内容；长度字段 304，给出属性的长度；以及值字段 306，包含属性信息。注意对 RFC2865 中给出的描述不作修改，值字段 306 会被分成重要的字段：类型 322，用于指示子属性的类型，诸如 MSK 生成指令；长度字段 324，给出子属性的长度；以及值字段 326，包含子属性信息，诸如 MSK 生成指示符。作为例子，为了传达消息到 AAA108 来指示 AAA108MSK 生成，类型字段 322 会使用相应的预定义编码将该子属性标识为 MSK 生成指令。接着，值字段 326 会具有一个值：1 －指示 AAA108 生成 MSK；或 2 －指示 AAA108 不生成 MSK。

[0086] 图 6 说明了无线设备，诸如 MS102。设备 600 包含接收电路 602 和发送电路 604，分别用于接收传输和发送传输。接收电路 602 和发送电路 604 都被耦合到通信总线 612 上。设备 600 也包含中央处理器 (CPU)606，用于控制设备 600 内的操作。CPU606 对设备 600 内存储器存储设备 600 中存储的计算机可读指令响应。两个这样的存储设备被显示为存储认证程序 608 和 MSK 生成 610。注意可替换实施例会在硬件、软件、固件或其组合中实施该程序。接着，CPU606 响应来自认证程序 608 的认证处理指令。CPU606 将认证程序 608 消息置于传输格式，诸如 EAP 格式。当向 WLAN 认证时，CPU606 对 MSK 生成单元 610 作出响应以生成 MSK。CPU606 进一步处理接收到的传输格式消息，以从中提取认证消息。

[0087] 注意虽然这里所描述的实施例详述了 WLAN，这里所描述的方法和装置也可应用于其它系统实体。本发明提供了使系统实体能够向通信提供加密的方法。通过使用本地服务器来生成 MSK，并向系统实体提供该 MSK，向该实体提供了足够的消息来保护给用户的传输，所述用户诸如 MS。

[0088] 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，上述说明中可以涉及的数据、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。

[0089] 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块、模块、电路和算法步骤可以为电子硬件、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还是软件来实现取决于特定的应用和对总体系统设计上的约束。熟练的技术人员可能对于每个特定应用以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就此背离本发明的范围。

[0090] 结合这里所描述的实施例来描述的各种说明性的逻辑块、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)、专用集成电路 (ASIC)、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。处理器也可以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。

[0091] 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。软件模块可以驻留在 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 可能驻留在订户单元中。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。

[0092] 提供上述对所公开的具体实施方式的描述为了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，这里定义的总的原则可以被应用于其它实施例中而不背离本发明的精神和范围。因此，本发明并不要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。

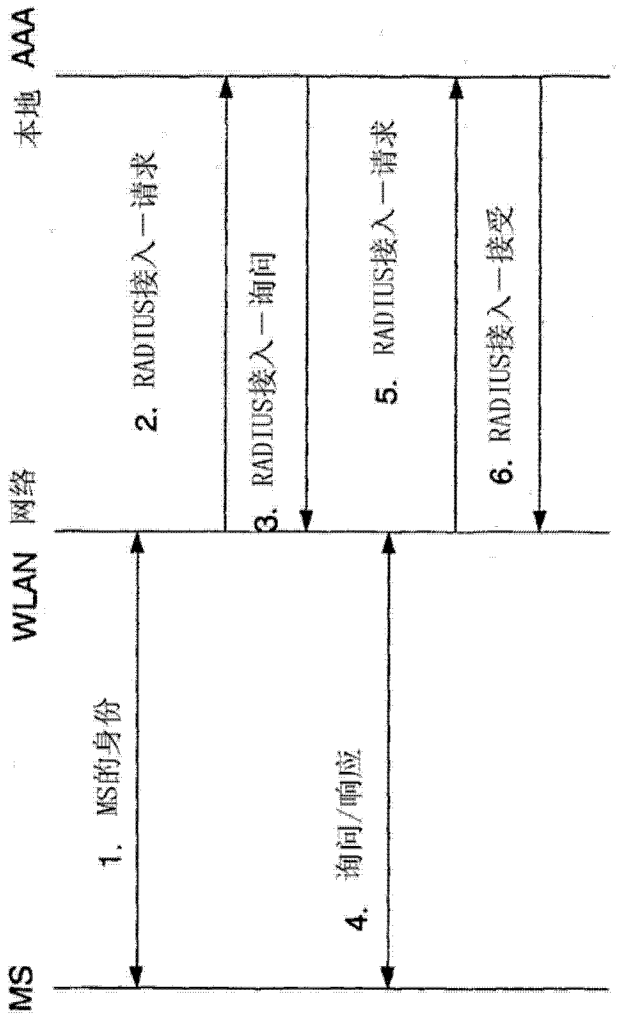

MS
WLAN 网络
本地 AAA
1. MS的身份
2. RADIUS接入－请求
3. RADIUS接入－询问
4. 询问/响应
5. RADIUS接入－请求
6. RADIUS接入－接受

图 2

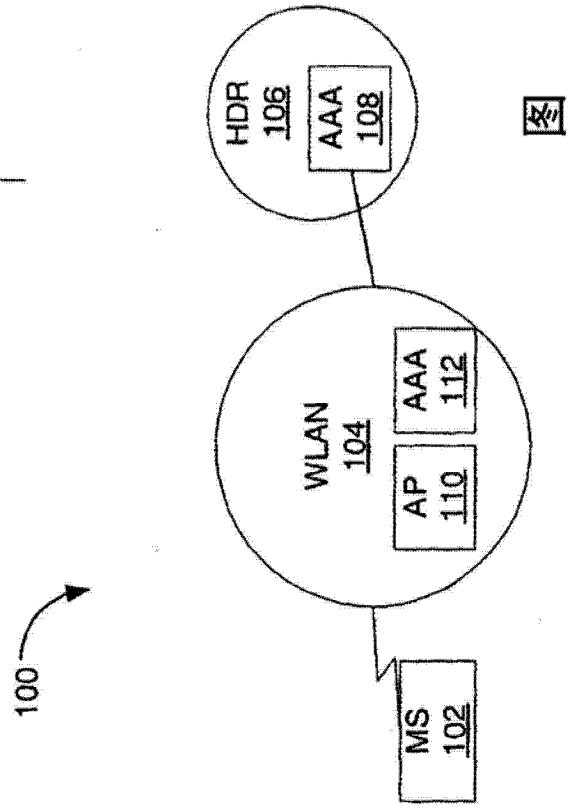

100
MS 102
WLAN 104
AP 110
AAA 112
HDR 106
AAA 108

图 1

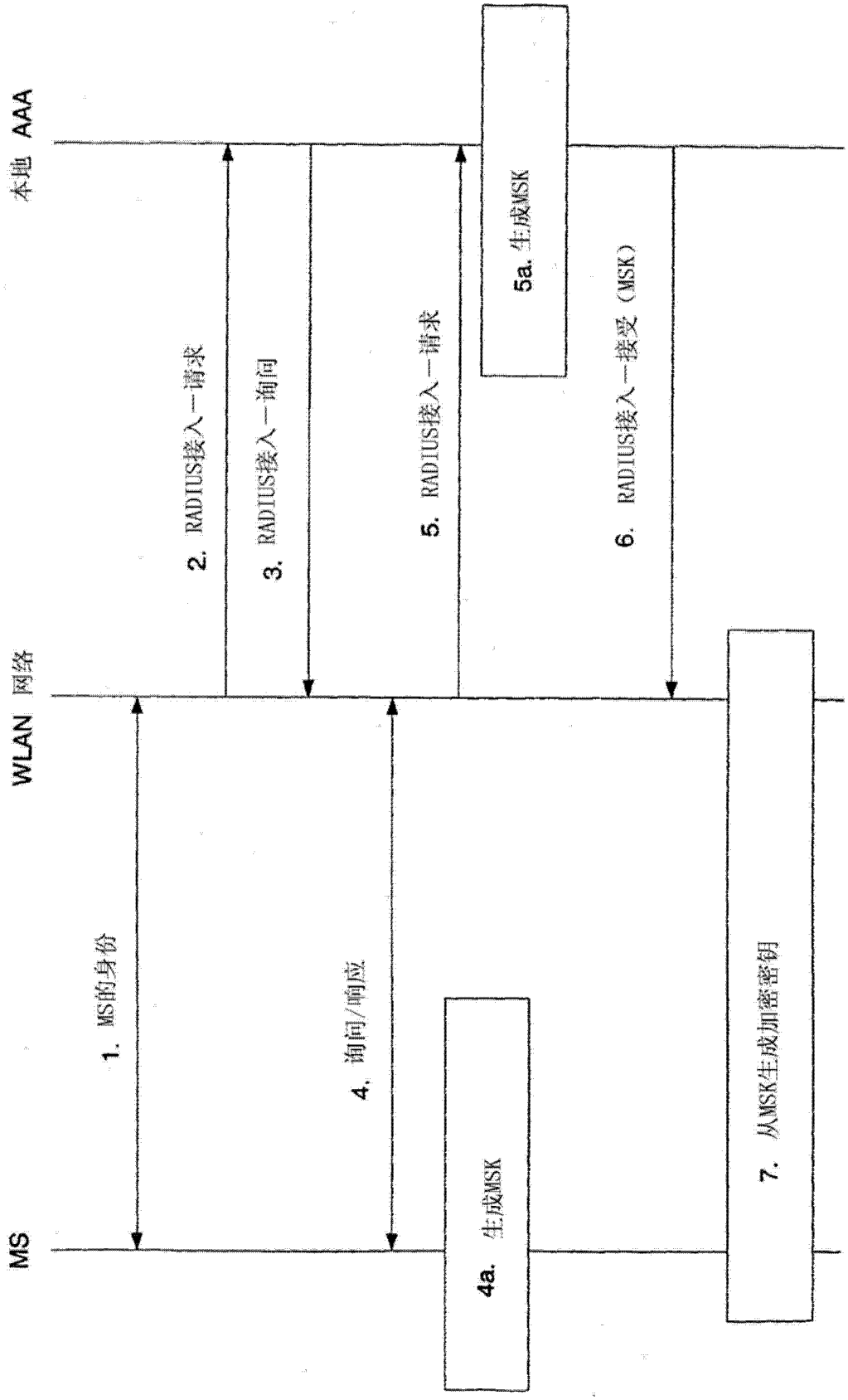

本地 AAA
WLAN 网络
MS
2. RADIUS接入—请求
3. RADIUS接入—询问
5. RADIUS接入—请求
5a. 生成MSK
6. RADIUS接入—接受（MSK）
1. MS的身份
4. 询问/响应
4a. 生成MSK
7. 从MSK生成加密密钥

图 3

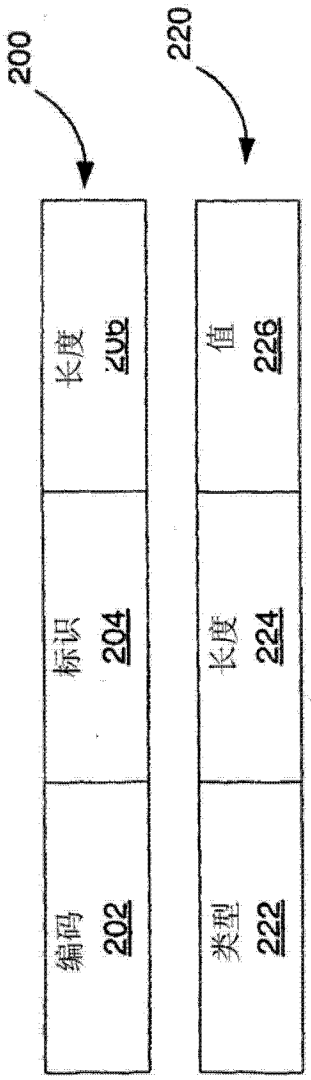

200
220
编码 202
标识 204
长度 206
类型 222
长度 224
值 226

图 4

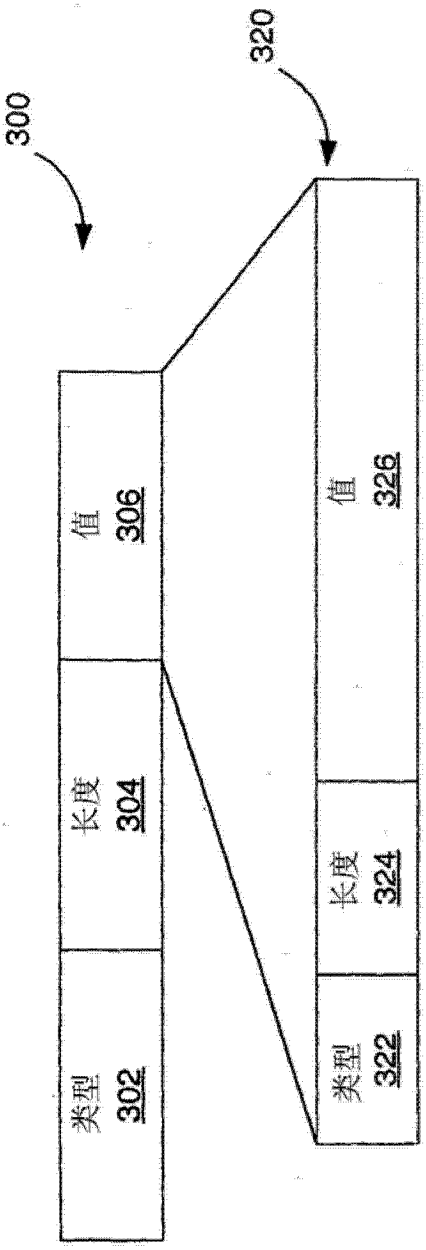

300
320
类型 302
长度 304
值 306
类型 322
长度 324
值 326

图 5

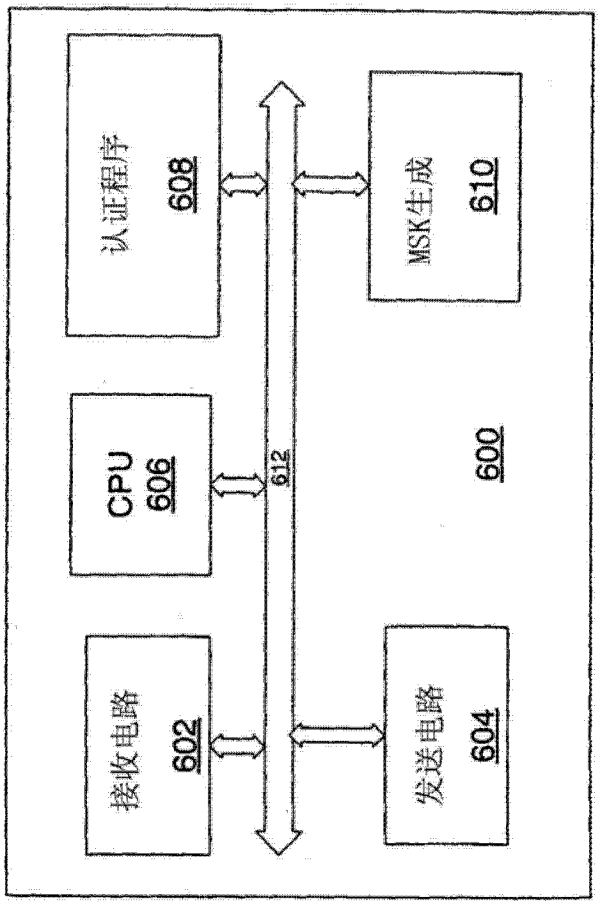


图 6