[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)
H04L 12/28 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200610092552.5

[43] 公开日 2006 年 12 月 6 日

[11] 公开号 CN 1874222A

[22] 申请日 2004.3.11
[21] 申请号 200610092552.5
分案原申请号 200480006315.1
[30] 优先权
[32] 2003.3.14 [33] US [31] 60/454,542
[71] 申请人 汤姆森特许公司
地址 法国布洛涅
[72] 发明人 张俊彪 索拉布·马瑟 萨钦·莫迪

[74] 专利代理机构 北京市柳沈律师事务所
代理人 黄小临 王志森

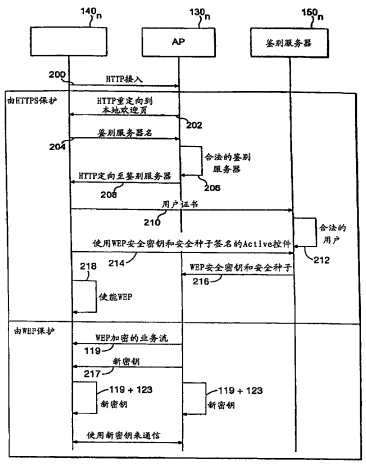
权利要求书 4 页 说明书 7 页 附图 3 页

[54] 发明名称

提供安全通信会话的方法、终端设备和接入点

[57] 摘要

本发明提供一种通过在用户鉴别阶段在无线用户机和 WLAN 接入点二者上都安装两个共享秘密而不是初始会话密钥这一个共享秘密来改进 WLAN 环境中移动终端的安全的方法。一个共享秘密用作初始会话密钥，而另一个用作安全种子。由于初始鉴别是安全的，因此这两个密钥对于潜在的黑客是未知的。尽管初始会话密钥最终可能会被潜在的黑客破解，但由于安全种子没有在任何不安全的通信中使用，因此它仍然是安全的。



1. 一种在通信网络中给用户终端提供安全通信会话的方法，所述方法包括:

由所述用户终端使用安全通信方法接收安全密钥和安全种子，该安全密钥和安全种子适于存储在用户终端中以便在安全通信会话期间使用;

由该用户终端使用当前会话密钥加密并发送数据，并且使用当前会话密钥解密由用户终端接收的数据，该安全密钥被初始用作当前会话密钥；以及

由所述用户终端周期性接收随后会话密钥，并且在随后的通信期间，使用随后会话密钥作为当前会话密钥。

2. 如权利要求 1 所述的方法，其中，所述用户终端是移动终端。

3. 如权利要求 1 所述的方法，其中，所述通信网络是无线网络。

4. 如权利要求 3 所述的方法，其中，所述无线网络是无线局域网。

5. 如权利要求 1 所述的方法，进一步包括：由所述用户终端发送下网消息以结束所述安全通信会话，所述下网消息是加密形式的并且包括安全密钥。

6. 一种在通信网络中给移动终端提供安全通信会话的方法，所述方法包括:

由所述移动终端使用安全通信方法接收安全密钥，该安全密钥被存储在该移动终端中以便在安全通信会话期间使用;

由该移动终端使用当前会话密钥加密并发送数据，并且使用当前会话密钥解密由所述移动终端接收的数据；以及

由所述用户终端发送下网消息以结束安全通信会话，所述下网消息是加密形式的并且包括安全密钥。

7. 如权利要求 6 所述的方法，进一步包括：由所述移动终端接收安全种子，该安全种子被存储在所述移动终端中以便在所述安全通信会话期间使用。

8. 如权利要求 7 所述的方法，进一步包括：使用所述安全种子来周期性生成随后会话密钥。

9. 如权利要求 7 所述的方法，进一步包括：使用新密钥和安全种子的组合周期性生成随后会话密钥，该新密钥是使用安全密钥生成的。

10. 如权利要求 9 所述的方法，其中，所述周期性生成步骤包括：通过将新密钥与安全种子级联并且运行用于产生随后会话密钥的散列算法，产生

随后会话密钥。

11. 一种在通信网络中给移动终端提供安全通信会话的方法，所述方法包括:

由所述通信网络使用安全通信方法接收安全密钥，该安全密钥被存储在该通信网络中以便在安全通信会话期间使用;

由所述通信网络使用当前会话密钥加密并发送数据，并且使用当前会话密钥解密由所述通信网络接收的数据，该安全密钥被初始用作当前会话密钥;以及

由所述通信网络周期性接收随后会话密钥，并且在随后的通信期间，使用随后会话密钥作为当前会话密钥。

12. 如权利要求 11 所述的方法，进一步包括：由所述通信网络接收下网消息，所述下网消息是加密形式的并且包括所述安全密钥。

13. 一种在通信网络中给移动终端提供安全通信会话的方法，所述方法包括:

在用户鉴别阶段期间，在移动终端上安装至少两个共享秘密，由此第一秘密是初始会话密钥，而第二秘密用作产生随后会话密钥的安全种子。

14. 如权利要求 13 所述的方法，还包括步骤：生成新密钥，并且使用当前会话密钥对该新密钥进行加密。

15. 如权利要求 14 所述的方法，其中，所述生成新密钥包括将所述当前会话密钥与安全种子级联的步骤。

16. 如权利要求 15 所述的方法，还包括步骤：通过对所述级联的结果应用散列算法来生成新会话密钥。

17. 如权利要求 16 所述的方法，还包括步骤：在随后的通信中使用所述新会话密钥。

18. 一种在通信网络中给移动终端提供安全通信会话的方法，所述方法包括:

在用户鉴别阶段期间，在接入点中安装至少两个共享秘密，由此第一秘密是初始会话密钥，而第二秘密用作产生随后会话密钥的安全种子。

19. 如权利要求 18 所述的方法，还包括步骤：生成新密钥，并且使用当前会话密钥对该新密钥进行加密。

20. 如权利要求 19 所述的方法，其中，所述生成新密钥包括将所述当前

会话密钥与安全种子级联的步骤。

21. 如权利要求 20 所述的方法，还包括步骤：通过对所述级联的结果应用散列算法来生成新会话密钥。

22. 如权利要求 21 所述的方法，还包括步骤：在随后的通信中使用所述新会话密钥。

23. 一种在移动终端与通信网络之间提供安全通信会话的方法，所述方法包括：

在会话下网期间，由所述移动终端将经加密的下网请求随同安全种子一起发送，使得安全种子出现在下网请求中。

24. 一种在移动终端与通信网络之间提供安全通信会话的接入点，包括：

用于使用安全通信方法接收安全密钥和安全种子的装置；

用于使用该安全密钥来加密数据的装置；以及

用于使用该安全种子来周期性生成随后会话密钥的装置。

25. 如权利要求 24 所述的接入点，其中，用于周期性生成随后会话密钥的装置包括：用于使用新密钥和安全种子的组合生成随后会话密钥的装置，该新密钥是使用安全密钥生成的。

26. 如权利要求 24 所述的接入点，其中，用于周期性生成随后会话密钥的装置包括：用于通过级联新密钥和安全种子来生成随后会话密钥的装置，和用于运行产生随后会话密钥的散列算法的装置。

27. 一种给通信网络提供安全通信会话的终端设备，包括：

用于接收安全密钥和安全种子的装置，以及用于存储安全密钥和安全种子以便在安全通信会话期间使用的装置；

用于接收数据的装置，以及用于在安全通信会话期间使用当前会话密钥解密数据的装置，该安全密钥初始用作当前会话密钥；

用于使用所述当前会话密钥来解密和发送数据的装置；以及

用于使用当前会话密钥和安全种子生成随后会话密钥的装置，其后使用随后会话密钥作为用于随后的通信的当前会话密钥。

28. 如权利要求 25 所述的终端设备，其中，该终端设备包括移动终端，而该通信网络包括无线局域网。

29. 一种在移动终端与通信网络之间提供安全通信会话的接入点，包括：

用于发送安全密钥和安全种子的装置，以及用于存储安全密钥和安全种

子以便在安全通信会话期间使用的装置；

用于加密数据的装置，用于将数据发送给所述移动终端的装置，以及用于接收数据的装置，用于在安全通信会话期间使用当前会话密钥解密来自该移动终端的数据的装置，该安全密钥初始用作当前会话密钥；和

用于使用当前会话密钥和安全种子生成随后会话密钥的装置，其后使用随后会话密钥作为用于随后的通信的当前会话密钥。

提供安全通信会话的方法、终端设备和接入点

本申请是申请人为 2004 年 3 月 11 日、申请号为 200480006315.1、发明名称为“使用重新生成安全密钥和下网的 WLAN 会话管理技术”的发明专利申请的分案申请。

相关申请的交叉引用

本申请要求于 2003 年 3 月 14 日提交的美国临时申请第 60/454,542 号的权益，其援引于此以供参考。

技术领域

本发明涉及一种用于在局域网中提供安全通信会话的装置和方法，并且具体涉及一种使用周期性密钥更新和安全下网(logoff)给 WLAN 中的移动终端提供安全通信会话的装置和方法。

背景技术

本发明的背景是采用 IEEE 802.1x 架构的无线局域网（或 WLAN）家族，其具有接入点（AP）来为移动设备提供到其他网络（例如有线局域网和诸如因特网之类的全球网络）的接入。WLAN 技术的发展产生了在暂停区、咖啡馆、图书馆和类似公共设施处（“热点”，hotspot）的公共接入无线通信。目前，公共 WLAN 为移动通信设备用户提供到专用数据网络（例如公司内联网）或公共数据网络（例如因特网、对等对对等通信和实况无线 TV 广播）的接入。用于实施和操作公共 WLAN 的相对低的成本以及可用的高带宽（通常超过 10Mb/秒）使得公共 WLAN 成为理想的接入机制，移动无线通信设备用户可以通过它与外部实体交换分组。然而如下面将要讨论的，除非存在足够的识别和鉴别手段，否则这种开放使用可能会损害安全。

当用户在公共 WLAN 覆盖区域内尝试接入服务时，WLAN 在准许网络接入之前首先鉴别并授权用户接入。在鉴别之后，公共 WLAN 向无线通信设备开放安全数据信道，以保护在 WLAN 和设备之间传输的数据的保密性。目

前，许多 WLAN 设备的制造商对所使用的设备采用了 IEEE 802.1x 协议。因此，主流的 WLAN 鉴别机制使用这个标准。不幸的是，IEEE 802.1x 协议被设计成以专用 LAN 接入作为其用途模型。因此，IEEE 802.1x 协议不提供改善公共 WLAN 环境中的安全性的某些特征。

在基于网络浏览器的鉴别方法中，移动终端使用以超文本传送协议安全套接字（HTTPS）协议工作的网络浏览器与鉴别服务器通信，确保在移动终端和鉴别服务器之间的路径上的任何人无法侵入或窃取机密的用户信息。然而，鉴别服务器涉及移动终端的唯一信息就是其 IP 地址。

用户一旦经 WLAN 鉴别，就建立由用户和 WLAN 共享的安全会话密钥。所有随后的通信都使用该会话密钥加密。为了防止安全攻击，例如搜索(exploring)IEEE 802.11 WEP 加密协议中的安全漏洞的攻击，并且为了保证强的安全性，需要周期性更新会话密钥。实际上，如果使用初始会话密钥作为有线对等加密（WEP）密钥，则在无线用户和 WLAN 接入点之间使用 WEP 进行一定次数的通信交换之后，潜在的黑客可以破解该密钥。在 IEEE 802.1x 中，用于 WLAN 中的安全接入控制的、其中更新会话密钥的协议依赖于鉴别服务器。本质上，每次更新密钥时，用户需要经过类似于初始鉴别的鉴别步骤。这个过程可能是低效率的，且在某些应用中是不可能。WLAN 技术可以从这样一种方法中获益：一旦用户经过鉴别并且建立了会话密钥，将来的密钥更新就不再需要鉴别服务器的参与。

此外，处理管理信息，特别是下网请求的应用典型地要求防止攻击的安全性。然而，在 IEEE 802.1x 中，这些信息是以明文发送的，从而使得移动终端易于受到攻击，其中，潜在的黑客即使没有会话密钥也可以下网经过鉴别的用户。同样地，WLAN 技术可以获益于一种提供使用会话密钥额外加密的、经加密的密钥更新或下网请求的方法。

发明内容

所期望的是一种通过使用会话密钥加密终端和通信网络之间的通信而在终端和通信网络之间提供安全通信会话的方法，其中会话密钥可以从一组密钥得到，该组密钥包括存储在终端和通信网络的接入点中的安全密钥。该安全密钥也可以用于提供安全的下网机制。

本发明这里还提供一种改进 WLAN 环境中移动终端的安全的方法，该方

法在用户鉴别阶段在无线用户机和 WLAN AP 上都安装两个共享密钥而不是安装被称为初始会话密钥的一个共享秘密。一个共享密钥用作初始会话密钥，而另一个共享密钥用作安全种子（secure seed）。由于初始鉴别的通信是安全的，因此一旦建立了这两个安全密钥，潜在的黑客事实上不可能破解这种形式的保护。并且尽管初始会话密钥最终可能会被潜在的黑客破解，但由于安全种子没有在任何不安全的通信中使用，因此它总是安全的。

本发明的一个实施例包括在密钥更新期间生成新密钥并将其在 WLAN 接入点和移动终端之间交换的过程。接入点和移动终端将该新密钥与安全种子一起使用以生成新会话密钥，而不是直接使用该新密钥。例如，可以通过将安全种子与该新密钥级联、然后计算诸如报文摘译 5（MD5）散列算法（hash algorithm）之类的单向散列函数来产生固定的串来产生新会话密钥。由于潜在的黑客没有安全种子，即使其可以破解旧会话密钥，也无法成功获取新会话密钥。

本发明的一个实施例还包括在会话下网期间移动终端保持安全以防止潜在的黑客下网经鉴别的移动终端的过程。由于下网请求在未加密的帧中承载，因此基于 IEEE 802.1x 的方案不提供安全的下网。然而，在本发明的一个实施例中，移动终端发送伴随有安全种子的经加密的主销请求。这样即使潜在的黑客破解会话密钥，也不可能下网经鉴别的用户，这是由于安全种子出现在下网请求中并且不再有效（每次用户登录时需要协商新安全种子），这样即使潜在的黑客破解了旧安全种子，也不会导致进一步的危害。

本发明的一个实施例还包括一种提供在移动终端和无线局域网（WLAN）之间的安全通信会话的方法，该方法包括步骤：生成第一和第二安全密钥；使用安全的通信方法发送第一和第二安全密钥给移动终端，第一和第二安全密钥存储在移动终端中以便在安全通信会话期间使用；使用当前会话密钥将数据加密并发送给移动终端，并且接收并使用当前会话密钥解密从移动终端接收的数据，第一安全密钥最初用作当前会话密钥；以及使用第二安全密钥周期性地生成随后会话密钥，并且在 WLAN 与移动终端之间随后的通信期间，使用随后会话密钥作为当前会话密钥。

本发明还包括一种提供移动终端与 WLAN 之间的安全通信会话的装置，包括用于生成第一和第二安全密钥的装置和用于将第一和第二安全密钥发送到移动终端的装置。移动终端存储用于解密随后接收到的数据的第一和第二

安全密钥。在 WLAN 中，一装置使用当前会话密钥加密并发送数据给移动终端。在 WLAN 中，用于周期性生成随后会话密钥的装置使用第二安全密钥，并且在 WLAN 和移动终端之间的通信期间使用随后会话密钥作为当前会话密钥。

附图说明

当结合附图阅读时，从下面详细描述中能最好地理解本发明。附图的各种特征不是穷举指出的。相反，为了清晰起见可以任意扩展或减少各种特征。下列特征包含在附图中：

图 1 是实践用于鉴别移动无线通信设备的本原理的方法的通信系统的方框图；

图 2 是本发明的建立两个安全密钥的方法的流程图；

图 3 是在本发明上建立安全的下网过程的方法的流程图；和

图 4 是实现本发明的装置的方框图。

具体实施方式

在要讨论的附图中，电路和相关的方框和箭头表示根据本发明的处理的功能，这些功能可以实现为电子电路和相关的传送电信号的线路或数据总线。或者，一个或多个相关的箭头可以表示软件例程之间的通信（如数据流），特别是当本发明的方法或装置实现为数字处理时。

根据图 1，由 140_1 到 140_n 表示的一个或多个移动终端通过接入点 130_n、本地计算机 120，与防火墙 122 和一个或多个虚拟操作员 150_{1-n}（例如鉴别服务器 150_n）进行相关通信。来自终端 140_{1-n} 的通信通常要求利用因特网 110 和相关联的通信路径 154 和 152 访问受保护的数据库或其他资源，因特网 110 和相关联的通信路径 154 和 152 要求高度安全，以免被诸如潜在的黑客之类的未授权的实体攻击。

如图 1 进一步所示，IEEE 802.1x 架构包括几个部件和服务，其交互来提供对于网络栈的高层是透明的站移动性。IEEE 802.1x 网络将诸如接入点 130_{1-n} 和移动终端 140_{1-n} 之类的站定义为以无线介质 124 进行通信的部件，并且包含 IEEE 802.1x 协议的功能性，即 MAC（媒体访问控制）138_{1-n} 和相应的 PHY（物理层）（未示出）以及到无线介质的级联 127。典型地，IEEE 802.1x

功能以无线调制解调器或者网络接入或接口卡的硬件和软件实现。本发明提出一种在通信流中实现识别手段的方法，从而与用于下行链路（即从鉴别服务器到诸如膝上电脑的移动终端）业务流的 IEEE 802.1x WLAN MAC 层兼容的接入点 130_{1-n} 可以参加一个或多个无线移动设备 140_{1-n}、本地或后端服务器 120 和鉴别服务器 150 的鉴别。

根据本原理，接入 160 使得每个移动终端 140_{1-n} 能通过鉴别移动终端自身及其根据 IEEE 802.1x 协议的通信流，安全地接入 WLAN 115。通过结合图 2 参照图 1 可以最佳地理解接入 160 使能这种安全接入的方式。

在移动无线通信设备（即移动终端 140_n）、公共 WLAN、局部网络服务器 120 和鉴别服务器 150 之间发生的交互的时间顺序是按照 IEEE 802.1x 协议的惯例描述的，其中图 1 的接入点 130_n 维持受控端口和未受控端口，接入点通过其与移动终端 140_{1-n} 交换信息。由接入点 130_n 维持的受控端口用作未鉴别信息（例如当在本地服务器 120 和移动终端 140_{1-n} 之间流动时通过接入点 130_n 的数据业务流）的入口。一般地，接入点 130_{1-n} 根据 IEEE 802.1x 协议保持各个受控端口关闭，直到相关移动终端 140_{1-n} 的鉴别通信为止。接入点 130_{1-n} 总是维持各个未受控端口打开，以允许移动终端 140_{1-n} 与鉴别服务器 150 交换鉴别数据。

更具体地说，参照图 2，根据本发明的用于改善 WLAN 环境中移动终端 140_n 的安全的方法在用户鉴别阶段在移动终端 140_n 和 WLAN 接入点 130_n 上都安装两个共享秘密而不是一个共享秘密。一个共享秘密用作初始会话密钥，而另一个用作安全种子。由于初始鉴别是安全的，因此这两个密钥对于潜在的黑客是未知的。可以使用公知的方法生成并分发这些密钥（例如使用鉴别服务器生成并分发这些密钥）给移动终端和 WLAN 接入点。尽管初始会话密钥最终可能会被潜在的黑客破解，但由于安全种子没有在任何不安全的通信中使用，因此它仍然是安全的。更具体地说，本发明的方法通过接入点 130_n 处理来自移动终端 140_n 的网络请求，以便嵌入会话 id 215。

参照图 2，根据本发明的方法通过包括在用户鉴别阶段在移动终端 140_n 和 WLAN 接入点 130_n 上都安装至少两个共享秘密的步骤，改善了 WLAN 环境中移动终端 140_n 的安全，其中第一秘密是初始会话密钥，而随后的密钥用作安全种子。

根据本发明的原理，提供一种技术，使得每个移动通信设备（例如设备

140_1-140_n中的每一个）能安全地接入 WLAN 115，来提供设备自身和从其发出的业务流的鉴别。图 2 中使用的鉴别技术描绘了在移动终端 140_n、接入点 130_n和鉴别服务器 150 之间发生的通信的时间顺序。为了启动安全接入，在图 2 的步骤 200 期间，移动终端 140_n向接入点 130_n发送接入请求。实际上，移动终端 140_n通过由移动终端 140_n执行的浏览器软件程序（未示出）所发起的 HTTPS 接入命令，启动接入请求。在步骤 202 期间，响应于该接入请求，接入点 130_n将移动终端 140_n中的浏览器软件重定向到接入点 130_n上的本地欢迎页上。

接着步骤 202，在步骤 204 期间，移动终端 140_n通过询问接入点 130_n适当的鉴别服务器的身份来启动鉴别顺序。作为响应，接入点 130_n在步骤 206 期间确定适当的鉴别服务器（例如服务器 150）的身份，然后在步骤 208 期间通过 HTTP 命令将移动终端 140_n中的浏览器软件定向到该服务器。现在已经在步骤 208 期间接收到鉴别服务器 150 的身份，移动终端 140_n然后在图 2 的步骤 210 期间将其用户证书发送给该服务器。

一旦从移动终端 140_n接收到用户证书，鉴别服务器 150 就在步骤 212 期间对移动终端 140_n是否构成合法用户进行确定。如果是合法用户，则鉴别服务器 150 在步骤 214 期间使用有线对等加密（WEP）加密密钥答复移动终端 140_n，该 WEP 加密密钥由设备通过设备浏览器软件经由 ActiveX 控件的 ActiveX 命令来调用。ActiveX 控件本质上是可以嵌入网页内的可执行程序。许多软件浏览器程序，例如 Microsoft Internet Explorer 具有显示这种网页并且调用可以从远程服务器（如鉴别服务器 150）下载的嵌入的 ActiveX 控件的能力。ActiveX 控件的执行受到内置于浏览器软件的安全机制限制。事实上，大多数浏览器程序具有几个不同的可选安全等级。在最低的等级中，可以不加限制地调用任何来自网络的 ActiveX 控件。在最高的等级中，不能从浏览器软件调用任何 ActiveX 控件。

根据本发明的方法包括在鉴别和授权之后、在步骤 217 中生成第一密钥并且将新密钥分发给接入点 130_n和移动终端 140_n的步骤。在步骤 121 中，被称为安全种子 123 的第二密钥被分发给移动终端 140_n和接入点 130_n。然后，移动终端和接入点使用第一密钥作为会话来加密数据来进行通信。然后，接入点 130_n和移动终端 140_n采用密钥 119 和安全种子 123 来周期性生成（225）新会话密钥 121，其中该新会话密钥用于移动终端和接入点之间随后的通信。

在通信会话期间，第二密钥总是作为秘密存储并保持在移动终端和接入点中，因此潜在的黑客无法确定第二密钥。可以采用几种技术来进一步帮助组合的密钥的管理，例如生成新会话密钥并且在为了安全而使用它之前将该新会话密钥与安全种子级联。一旦将组合的会话密钥和安全种子级联，处理就可以计算关于级联的新会话密钥和安全种子的散列算法，并且生成固定的串用于进一步传输。

用于改善 WLAN 环境中移动终端的安全的方法还包括步骤：移动终端 140_n 在会话下网期间发送伴随有安全种子的经加密的下网请求，使得安全种子出现在下网请求中。如图 3 所示，在会话下网期间，移动终端 140_n 保持安全以防止潜在的黑客下网经鉴别的移动终端 140_n。由于下网请求在未加密的帧内承载，因此基于 IEEE 802.1x 的方案不能提供安全的下网。然而在本发明的实施例中，移动终端 140_n 发送伴随有安全种子 123 的经加密的下网请求 228。这样，即使在潜在的黑客破解会话密钥的情况下，下网移动终端 140_n 上经鉴别的用户也是不可能的，原因在于安全种子 123 出现在下网请求 228 中，并且由于在每次用户登录时需要协商新安全种子而不会再使用。

在图 4 中示出用于移动终端 140_n 和 WLAN 之间安全通信会话的装置。接入点 130_n 包括用于生成第一和第二安全密钥的装置 410 和用于发送第一安全密钥 119 和第二安全密钥 123 给移动终端 140_n 的装置 420。移动终端 140_n 接收第一安全密钥 119 和第二安全密钥 123，并且将密钥存储在寄存器 430 中以便在安全通信会话期间使用。接入点 130_n 包括用于使用当前会话密钥加密数据的装置 415 和用于通过 WLAN 115 发送数据给移动终端 140_n 的装置 420。移动终端 140_n 包括用于接收的装置 450 和用于使用当前会话密钥 119 解密从接入点 130_n 接收的数据的装置 435，第一安全密钥最初被用作当前会话密钥 119。接入点 130_n 包括用于使用第二安全密钥周期性生成随后会话密钥的装置 425，并且在 WLAN 115 和移动终端 140_n 之间随后的通信期间使用随后会话密钥作为当前会话密钥。

应当理解的是，所示出的本发明的形式仅仅是优选实施例。可以对功能和部分的排列进行各种改变；可以用等效的装置替代所示出和描述的装置；并且可以在不背离权利要求书所限定的本发明的宗旨和范围的情况下相互独立地使用某些特征。

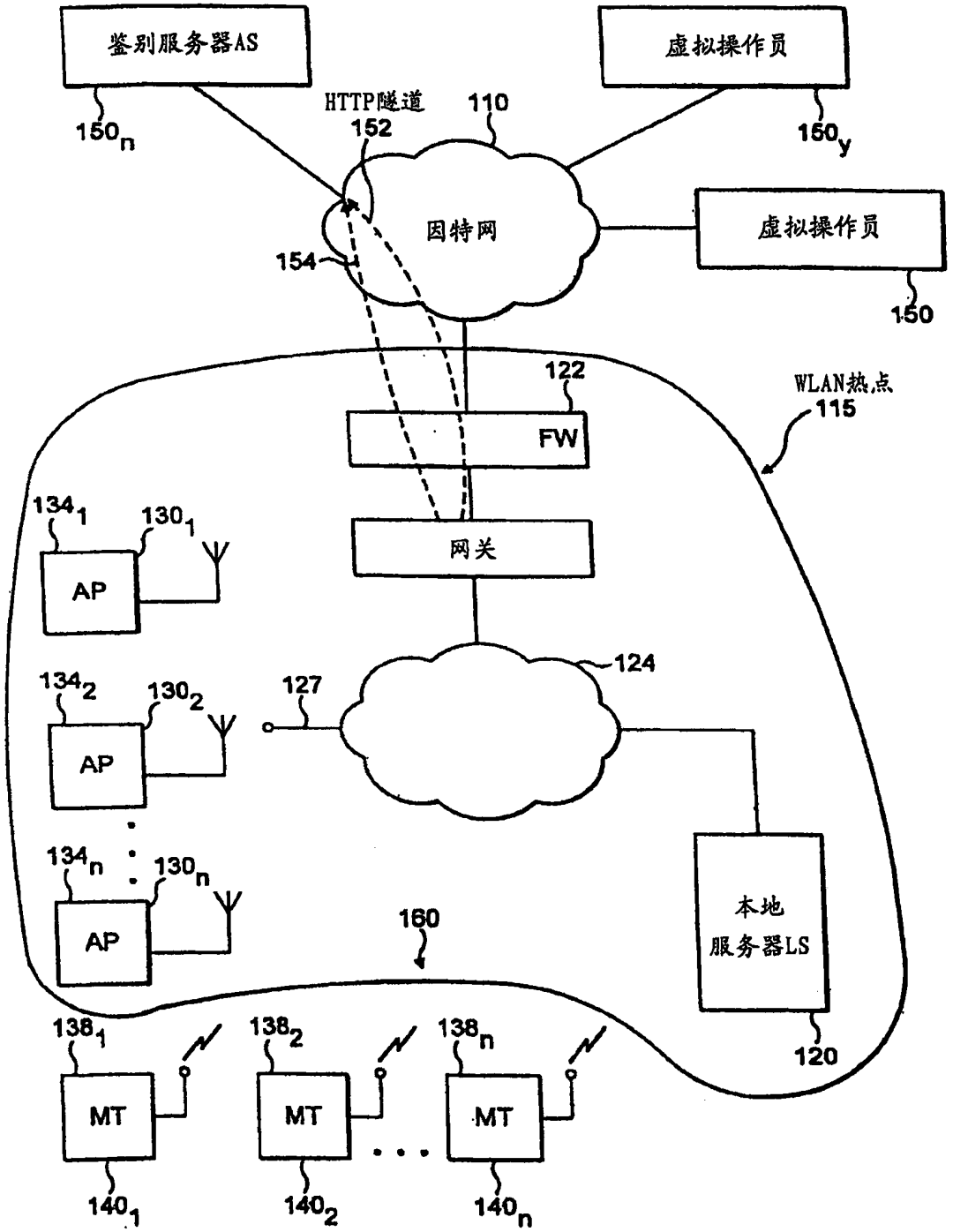

鉴别服务器AS
虚拟操作员
HTTP隧道
152
110
150n
150y
因特网
虚拟操作员
154
150
122
WLAN热点
115
FW
网关
134 1
130 1
AP
134 2
130 2
127
124
AP
134 n
130 n
AP
160
本地
服务器LS
120
138 1
138 2
138 n
MT
MT
MT
140 1
140 2
140 n

图 1

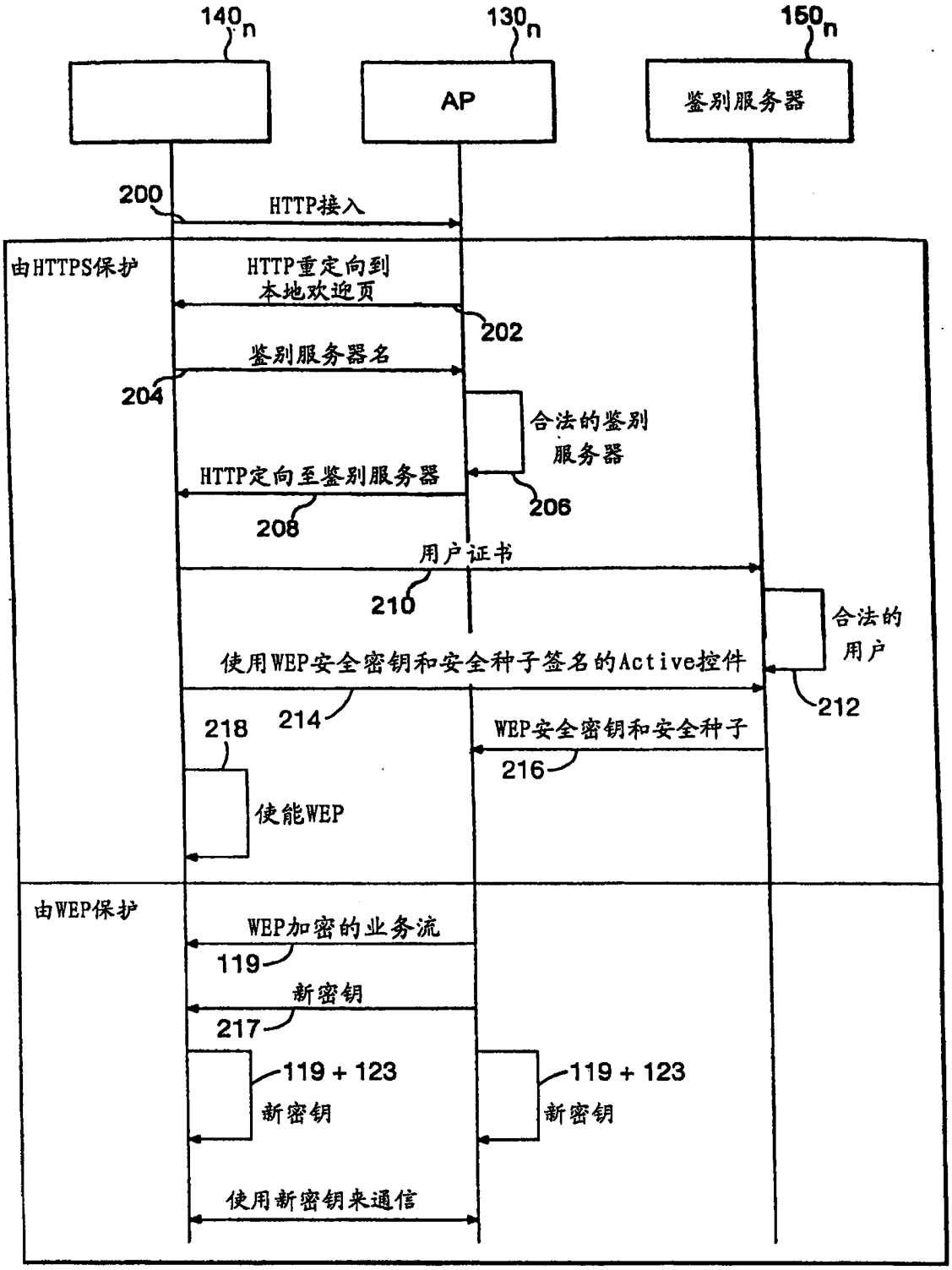

140n
130n
150n
AP
鉴别服务器
200
HTTP接入
由HTTPS保护
HTTP重定向到
本地欢迎页
202
鉴别服务器名
204
合法的鉴别
服务器
HTTP定向至鉴别服务器
206
208
用户证书
210
合法的
用户
使用WEP安全密钥和安全种子签名的Active控件
212
214
218
WEP安全密钥和安全种子
216
使能WEP
由WEP保护
WEP加密的业务流
119
新密钥
217
119 + 123
新密钥
119 + 123
新密钥
使用新密钥来通信

图 2

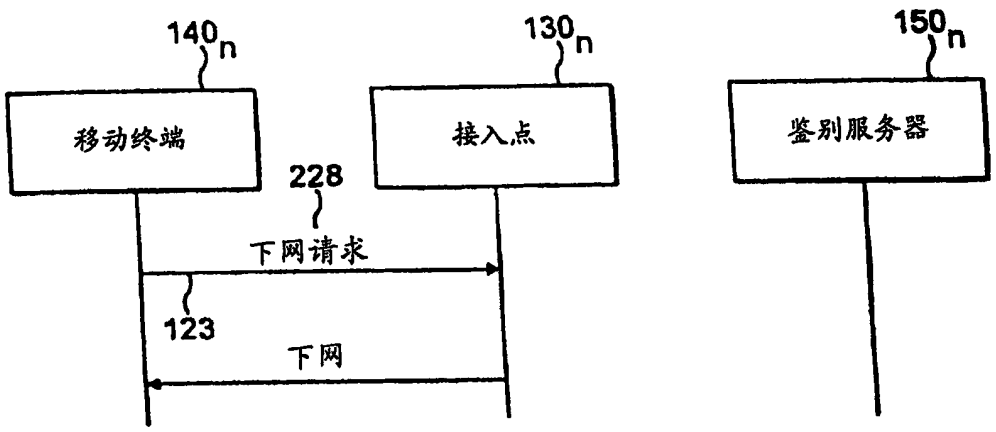

140n
130n
150n
移动终端
接入点
鉴别服务器
228
下网请求
123
下网

图 3

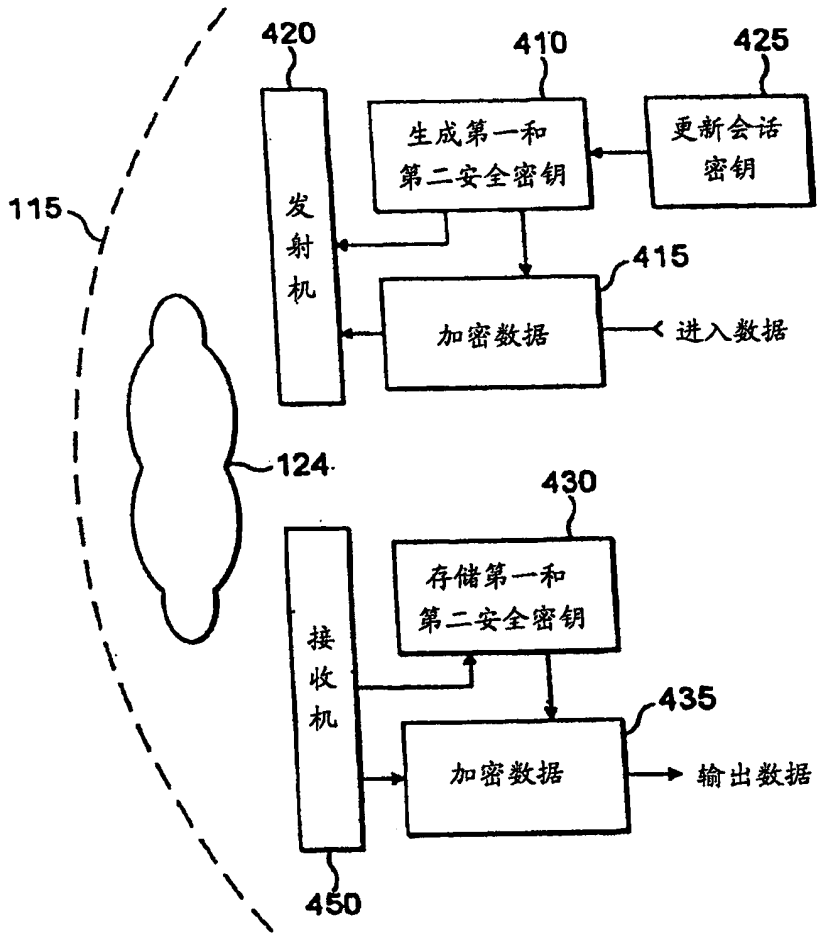

420
410
425
115
生成第一和
第二安全密钥
更新会话
密钥
发
射
机
415
加密数据
进入数据
124
430
存储第一和
第二安全密钥
接
收
机
435
加密数据
输出数据
450

图 4