[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04Q 7/38
H04L 9/32

[12] 发明专利说明书

[21] ZL 专利号 00818525.5

[45] 授权公告日 2005 年 4 月 27 日

[11] 授权公告号 CN 1199510C

[22] 申请日 2000.11.21 [21] 申请号 00818525.5
[30] 优先权
[32] 1999.11.23 [33] US [31] 09/447,761
[86] 国际申请 PCT/IB2000/001713 2000.11.21
[87] 国际公布 WO2001/039538 英 2001.5.31
[85] 进入国家阶段日期 2002.7.19
[71] 专利权人 诺基亚有限公司
地址 芬兰埃斯波
[72] 发明人 J·阿拉-劳里拉 H·汉森
J·萨尔维拉
审查员 赵 颖

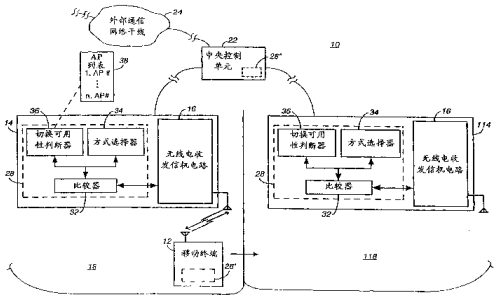
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 杨 凯 王忠忠

权利要求书 4 页 说明书 17 页 附图 11 页

[54] 发明名称 移动终端切换过程中的安全性关联的传送

[57] 摘要

当无线电通信系统、如 IEEE 082.11 或 HIPERLAN 中发生通信切换事件时重建已有的安全性关联，其中在网络内发生通信切换时保持移动终端和无线通信网络之间已有的安全性关联。 切换事件期间的验证通过查询/响应程序来实现。 根据查询/响应程序，由新接入点和正在切换到该新接入点的移动终端构成的通信对的各个成员向该通信对的其它成员发送查询。 然后通信对的各个成员计算对其接收的查询的响应，并将这些响应发回通信对的另一成员。 然后通信对的各成员将其接收的响应与正确响应比较。 当这些比较都正确时，在第二接入点和移动终端之间开始净荷通信。



ISSN1008-4274

1. 一种当与给定的移动终端的通信从第一接入点切换到第二接入点时提供信息安全性的方法，它包括以下步骤:

设置具有多个接入点的通信系统，各个接入点服务于所述通信系统所服务的整个地理区域内的不同地理区域;

在所述整个地理区域内设置多个移动终端;

检测与所述给定的移动终端的通信何时从所述第一接入点切换到所述第二接入点;

通过在所述第一接入点检索安全性关联参数，通过根据所述检索的安全性关联参数在所述第二接入点创建安全性关联，并且通过根据所述检索的安全性关联参数在所述给定的移动终端中创建安全性关联，对所述检测步骤作出响应；以及

根据所述响应步骤在所述给定的移动终端与所述第二接入点之间发起通信。

2. 如权利要求 1 所述的方法，其特征在于,所述响应步骤还包括:

从所述给定的移动终端向所述第二接入点发出验证接入点查询消息，并从所述第二接入点向所述给定的移动终端发出验证移动终端查询消息；及

还包括以下步骤:

响应从所述给定的移动终端接收的所述验证接入点查询消息，在所述第二接入点中生成验证接入点响应消息;

将所述验证接入点响应消息发送到所述给定的移动终端;

响应从所述第二接入点接收的所述验证移动终端查询消息，在所述给定的移动终端中生成验证移动终端响应消息;

将所述验证移动终端响应消息发送到所述第二接入点;

在所述给定的移动终端中把所述验证接入点响应消息与正确响应消息进行第一比较;

在所述第二接入点中把所述验证移动终端响应消息与正确响应消息进行第二比较；以及

根据所述第一比较步骤和所述第二比较步骤，在所述给定的移动终端与所述第二接入点之间发起通信。

3. 如权利要求 2 所述的方法，其特征在于：所述多个移动终端具有媒体接入控制层和兼容物理层而且每个所述消息是媒体接入控制层消息。

4. 如权利要求 3 所述的方法，其特征在于：每个所述消息在无线局域网内发送。

5. 如权利要求 2 所述的方法，其特征在于：所述通信系统是无线局域网通信系统，其中采用安全性协议来为数据分组提供端到端安全性。

6. 如权利要求 5 所述的方法，其特征在于：所述端到端安全性是通过对所述数据分组进行验证和/或加密来提供的，所述安全性协议提供需要在通信链路两端使用相同的加密和/或验证密钥的对称密码术。

7. 如权利要求 6 所述的方法，其特征在于：所述安全性协议包括用来生成用于所述安全性协议的对称密钥的可缩放密钥管理协议。

8. 如权利要求 6 所述的方法，其特征在于包括以下步骤：

在所述给定的移动终端与所述第二接入点之间设置会话相关的动态加密密钥；以及

当所述给定的移动终端在所述通信系统提供的通信覆盖范围内移动时，将有效的安全性关联从第一接入点转移到所述第二接入点。

9. 如权利要求 4 所述的方法，其特征在于包括以下步骤：

将所述通信系统设置为局域网；

在所述局域网内设置服务器；

在通信切换期间，在所述局域网内提供密钥管理和安全性关联的重建，而不需要修改端到端安全性关联，由于在所述通信切换期间通

信持续进行，使得所述通信切换只影响所述移动终端与所述第一和第二接入点之间的安全性功能。

10. 如权利要求 9 所述的方法，其特征在于：所述局域网包括在所述多个接入点与所述多个移动终端之间的基于因特网协议安全性的安全性关联。

11. 如权利要求 1 所述的方法，其特征在于：为由所述给定的移动终端与所述第一和第二接入点构成的通信对的两端提供验证密钥，所述验证密钥是由可缩放密钥管理协议生成的。

12. 如权利要求 1 所述的方法，其特征在于：根据可缩放密钥管理协议，在所述给定的移动终端与所述第一接入点之间存在验证密钥或安全性关联；以及在通信切换期间，安全性关联在所述多个接入点之间转移，以便避免对新密钥交换的需要。

13. 如权利要求 12 所述的方法，其特征在于：所述可缩放密钥管理协议是因特网密钥交换，且其中安全性关联在所述第一接入点和所述第二接入点之间转移。

14. 如权利要求 13 所述的方法，其特征在于包括对携带所述密钥的消息加密的步骤。

15. 一种保持装置，用于当随着移动终端从第一通信接入点所服务的第一地理区域物理移动到第二通信接入点所服务的第二地理区域而发生通信切换时、保持无线电通信系统中给定的安全性关联，所述移动终端最初与所述第一通信接入点构成第一通信对，在所述通信切换之后，所述移动终端与所述第二通信接入点构成第二通信对，所述第一通信对的各成员具有与之相关的所述给定的安全性关联，所述装置包括：

测定器，用于检测是否需要启动所述通信切换；

在所述无线电通信系统内的第一控制元件，用于对所述测定器检测启动所述通信切换的所述需要作出响应，并在所述第二通信接入点建立所述给定的安全性关联；

在所述移动终端中的第二控制元件，用于生成作为所述给定的安全性关联函数的接入点查询，并将所述接入点查询发送到所述第二通信接入点；

在所述第二通信接入点中的第三控制元件，用于在所述第二通信接入点生成移动终端查询，并将所述移动终端查询发送到所述移动终端；

其中所述第二控制元件响应所述移动终端查询，生成发送到所述第二通信接入点的移动终端响应；且

其中所述第三控制元件响应所述接入点查询，生成发送到所述移动终端的接入点响应；且

其中所述第二控制元件响应所述接入点响应，判断所述接入点响应是否正确；以及

响应所述移动终端响应，判断所述移动终端响应是否正确；以及

其中所述第一控制元件在所述移动终端响应和所述接入点响应都正确时建立所述通信切换。

16. 如权利要求 15 所述的装置，其特征在于：所述无线电通信系统是无线局域网。

移动终端切换过程中的安全性关联的传送

技术领域

本发明涉及无线电通信系统，其中无线局域网(WLAN)是非限定性的实例。更具体地说，本发明涉及在移动终端从第一基站或接入点(AP)切换到第二基站或接入点(AP)时提供信息安全性。

背景技术

在一种最小配置中，通信系统由通过通信信道互联的发射站和接收站构成。发射站生成的通信信号通过通信信道发送，并被接收站接收。

在无线电通信系统中，至少一部分通信信道是由一部分电磁谱构成的。在无线电通信系统中，可以增加通信的移动性，因为在发射站和接收站之间不需要固定或硬连线的连接。

蜂窝通信系统(其中蜂窝电话系统是一个实例)是无线电通信系统的一个实例。当蜂窝通信系统的用户的移动终端在物理位置上处于该蜂窝通信系统的网络基础设施所覆盖的整个区域中几乎任何位置时，该移动终端能够通过蜂窝通信系统与另一个移动终端进行通信。

典型的无线通信系统的网络基础设施包括物理上间隔开的、均含有收发信机的基站或接入点(AP)。在这种典型的系统中，各基站或AP 定义通信系统的地理区域或小区。在第一移动终端用于与第二移动终端通信，而且第一移动终端在系统的各小区之间穿行或移动时，通过将通信从一个基站切换到另一个基站，不间断通信是可能的。这种通信切换由切换处理来提供。

高性能无线局域网、如 HIPERLAN 类型-2 支持三种类型的切换。HIPERLAN/2 提供便携式装置与宽带 IP、ATM 和 UMTS 网络之间的

高速(通常为 25Mb/s 的数据速率)通信，能够支持多媒体应用，其中典型应用是室内应用。HIPERLAN/2 通过移动和固定终端提供到不同基础设施网络(例如 IP、ATM 和 UMTS)的本地无线接入，所述移动终端和固定终端与接入点交互作用，而接入点常常连接到 IP、ATM 或 UMTS 主干。需要许多接入点来服务于网络。作为一个整体的无线网络支持接入点之间连接的切换，从而提供移动性。典型的工作环境包括商用网和家居住宅网。HIPERLAN/2 接入网的概述由欧洲电信标准协会(ETSI)文档 DTR/BRAN-00230002，1998 年提出，现通过引用结合于此。

根据移动终端的切换判决，按照 HIPERLAN/2 可能进行扇区切换(扇区间)、无线电切换(接入点收发信机间/接入点间的切换)、网络切换(接入点间/网络间的切换)或者强制切换。

在执行切换之前，移动终端必须收集当前接入点所采用的频率的相关测量值以及供切换的候选接入点所采用的频率的相关测量值。有关正服务的频率的测量可由移动终端在与当前接入点同步时进行。但是，为了测量相邻接入点的频率，移动终端必须临时性地离开当前接入点。

在移动终端离开过程中，移动终端临时与当前接入点断开连接，以便该移动终端可以对相邻接入点执行测量。在此期间，移动终端与当前接入点之间无法通信。作为此离开过程的一部分，移动终端告知当前接入点：它将离开 n 个帧。在此离开过程中，移动终端无法被当前接入点达到。在离开时段之后，当前接入点可以触发移动终端有效序列，以便检查移动终端是否可用。

在扇区切换期间，接入点的天线扇区改变，同一个接入点控制整个切换处理。在扇区切换成功之后，移动终端通过新扇区进行通信。无线电切换涉及每个接入点具有不止一个收发信机的接入点，例如，两个接入点收发信机和一个接入点控制器。无线电切换在移动终端从一个接入点的覆盖区移动到同一个接入点所服务的另一个

覆盖区时执行。因为无线电切换可以在数据链路控制(DLC)层内执行，所以不涉及较高层协议(HL)。当移动终端检测到需要切换到另一个接入点控制器时，该移动终端可能仍与当前接入点同步。在此情况中，移动终端可通知它的接入点控制器，该移动终端将执行到另一个接入点控制器的切换。在无线电切换的情况中，在该接入点中可以使用有关正在进行的连接、安全性参数等的所有相关信息，所以不重新协商该信息。

在移动终端从一个接入点移动到另一个接入点时执行网络切换。因为移动终端离开无线链路控制(RLC)实例的服务区，所以网络切换涉及到汇聚层(CL)和 HL(视需要而定)以及 DLCI(数据链路连接识别)。为了保持 HL 关联和连接，可能需要经由干线的特定信令。当移动终端检测出需要切换到另一个(目标)接入点时，该移动终端仍可能会与当前接入点同步。在此情况中，移动终端可通知它的接入点，它将执行到另一个接入点的切换。被通知的接入点则会停止向该移动终端发送，但会在被指示时，在指定时间内保持关联。

强制切换为当前接入点提供命令某个移动终端离开当前接入点的小区的机会。强制切换由接入点向移动终端发送“强制切换”信号来启动。在一种程序中，移动终端执行常规切换并离开它的旧小区，而不管它是否找到新小区。在另一种程序中，如果切换失败，移动终端有机会回到该旧小区。

有关 HIPLERLAN/2 特征的进一步讨论，参见 ETSI 标准化组织提供的“宽带无线电接入网(BRAN)”、“HIPERLAN 类型 2 的功能说明”、“无线链路控制(RLC)”，将其通过引用合并于此。

已经实现了几种无线通信系统，而另一些已经被提议，以便覆盖有限的地理区域，例如建筑物或建筑物内办公场所包围的有限区域。诸如微小区网、专用网和 WLAN 等无线通信系统就是这种系统的实例。

无线通信系统通常是按照标准构建的，这些标准是由管理机构

或者准管理机构公布的。例如，IEEE(电气及电子工程师学会)公布的IEEE 802.11 标准是通常与商用 2.4GHz 无线局域网有关的无线局域网(LAN)标准。802.11 标准指定无线终端与基站或接入点之间的接口以及无线终端之间的接口。有关物理层和媒体接入控制(MAC)层的标准也在这种标准中提出。本标准允许包括兼容物理层的不同装置之间的自动媒体共享。在该标准中提供了异步数据传输，一般通过 MAC 层，利用载波检测多址/防碰撞(CSMA/CA)通信方案来实现。

虽然 IEEE 802.11 标准规定了利用被配置成按照此标准可互相操作的移动终端的无线通信，但是本标准不足以提供实时无线业务。例如，在该标准的实施中，从一个 AP 到另一个 AP 的通信切换期间，有时会遇到明显的质量损失。过多的数据帧容易丢失或发生延迟，导致通信质量的损失，或者甚至通信中断。因此，尤其是对于实时无线业务，需要与 IEEE 802.11 标准中提出的方式不同的操作方式。已经提出一些专用功能，与按照现有 IEEE 802.11 标准的操作相比，可以改善通信质量。可用来完成这种专用功能的 AP 和移动终端被称为有专用方式功能。

但是，由移动终端和该移动终端通过其来通信的 AP 构成的通信对的两端必须能够以专用方式工作。如果通信对的两端不一起按照专用方式工作，则需要按照 IEEE 802.11 标准的常规操作。因此，在允许通信对的两端以专用方式工作之前，必须判断该通信对的两端是否能够一起按照专用方式工作。

上述共同未决的专利申请提出了这类装置，它可用来识别通信对的两端是否可一起以专用方式工作，当判断存在对兼容性时，则该装置进行操作以激活通信对的两端，使之以专用方式工作，此后在移动终端在物理上从第一 AP 所服务的小区移动到第二 AP 所服务的小区的切换过程期间，该装置进行操作以保持专用方式工作。除了该共同未决的申请的装置所提出的有价值特征以外，最好在发生 AP 到 AP 切换时重新构建安全性关联。

许多客户、尤其是商业环境需要高度的数据安全性，这种数据安全性不能因 WLAN 设置的使用而被折衷。因为对 WLAN 的访问权无法以物理方式进行限制，所以通常采用密码法来保护发送的数据和网元。当前 IEEE 802.11 和 ITEF 因特网标准提供了两种互补机制，用于通过无线链路提供保密数据通信、即因特网协议安全性(IPSEC)。IPSEC 是基于 IP 的安全性协议，它提供两个 IP 主机之间的 FOR 保密通信。IPSEC 协议通常用于“虚拟专用网(VPN)”的建筑物中。

在 WLAN 系统中，IPsec 协议可以用于提供数据分组的端到端安全性，这种安全性是通过对所发送的数据分组验证和/或加密来提供的。IPsec 采用对称密码术，它需要在通信链路的两端使用相同的加密和/或验证密钥。密封密钥管理协议、如 IKE 可用于生成 IPsec 栈的对称密钥。

虽然因特网密钥交换(IKE)密钥管理协议对于在初始移动终端/接入点关联期间建立 IP 级安全性关联有用，但是当产生通信切换的需要时，使用 IKE 或其他类似的协议对实现切换造成相当大的时间延迟，因为这类协议需要进行多个消息交换，它们使用公钥加密需要非常繁重的计算。由于仅在新 AP 与移动终端之间已经建立有效的安全性关联之后才能恢复净荷业务的切换，所以使用 IKE 密钥管理协议或其它此类协议在切换期间存在问题。

当在移动终端与 AP 之间应用任何利用动态加密密钥、即与会话相关的动态密钥的安全性协议时，最好找一种机制，用于在移动终端在无线无线电网络或系统提供的覆盖范围内移动时，将有效安全性关联从一个 AP 转移到另一个 AP。

根据此背景信息，本发明提供一种低或短延迟的方法/装置，用于 WLAN 通信切换期间的密钥管理和安全性关联的重建，其中不需要在切换期间修改端到端安全性关联(例如，移动终端与服务器之间的 IPsec 净荷连接)，而且其中切换仅影响移动终端与新 AP 和旧 AP

之间的安全性功能。

发明内容

本发明涉及无线电通信、IEEE 802.11 2.4GHz WLAN 标准、高性能无线电局域网(HIPERLAN)、ETSI HIPERLAN 类型 2 标准以及无线终端与网元之间的 IPSEC 级安全性关联。本发明在任何基于 IP 的无线网络中得到应用，其实例包括 ETSI BRAN 和 IEEE 802.11。此外，本发明还可用于移动终端在两个 IPSEC 路由器实体之间移动时的情况，其中无线终端与不是无线接入点的端点进行通信。

本发明提供一种用于在无线电通信系统、如 IEEE 802.11 或 HIPERLAN 中发生切换事件时、重建现有的安全性关联的有效方法/装置。本发明的操作提高了切换性能，将与重新协商新 AP 与移动终端之间的安全性关联相关的延迟减至最小。

本发明提供一种在网络内发生切换时、保持移动终端与无线通信网络之间已建立的安全性关联的有效方式。本发明应用的一个实例是 WLAN，在 WLAN 内的 AP 与移动终端之间具有基于“因特网协议安全性(IPsec)”的安全性关联。但是，本发明还可用于维持任何类型的动态安全性关联，如 HIPERLAN/2 无线电层安全性功能。

根据本发明的一种当与给定的移动终端的通信从第一接入点切换到第二接入点时提供信息安全性的方法，它包括以下步骤：设置具有多个接入点的通信系统，各个接入点服务于所述通信系统所服务的整个地理区域内的不同地理区域；在所述整个地理区域内设置多个移动终端；检测与所述给定的移动终端的通信何时从所述第一接入点切换到所述第二接入点；通过在所述第一接入点检索安全性关联参数，通过根据所述检索的安全性关联参数在所述第二接入点创建安全性关联，并且通过根据所述检索的安全性关联参数在所述给定的移动终端中创建安全性关联，对所述检测步骤作出响应；以及根据所述响应步骤在所述给定的移动终端与所述第二接入点之间

发起通信。

根据本发明所述方法的一个方面，其特征在于,所述响应步骤还包括：从所述给定的移动终端向所述第二接入点发出验证接入点查询，并从所述第二接入点向所述给定的移动终端发出验证移动终端查询消息；及还包括以下步骤:响应从所述给定的移动终端接收的所述验证接入点查询消息，在所述第二接入点中生成验证接入点响应消息；将所述验证接入点响应消息发送到所述给定的移动终端；响应从所述第二接入点接收的所述验证移动终端查询消息，在所述给定的移动终端中生成验证移动终端响应消息；将所述验证移动终端响应消息发送到所述第二接入点；在所述给定的移动终端中把所述验证接入点响应消息与正确响应消息进行第一比较；在所述第二接入点中把所述验证移动终端响应消息与正确响应消息进行第二比较；以及根据所述第一比较步骤和所述第二比较步骤，在所述给定的移动终端与所述第二接入点之间发起通信。

按照本发明的一种保持装置，用于当随着移动终端从第一通信接入点所服务的第一地理区域物理移动到第二通信接入点所服务的第二地理区域而发生通信切换时、保持无线电通信系统中给定的安全性关联，所述移动终端最初与所述第一通信接入点构成第一通信对，在所述通信切换之后，所述移动终端与所述第二通信接入点构成第二通信对，所述第一通信对的各成员具有与之相关的所述给定的安全性关联，所述装置包括：检测器，用于检测是否需要启动所述通信切换；在所述无线电通信系统内的第一控制元件，用于对所述检测器检测启动所述通信切换的所述需要作出响应，并在所述第二通信接入点建立所述给定的安全性关联；在所述移动终端中的第二控制元件，用于生成作为所述给定的安全性关联函数的接入点查询，并将所述接入点查询发送到所述第二通信接入点；在所述第二通信接入点中的第三控制元件，用于在所述第二通信接入点生成移动终端查询，并将所述移动终端查询发送到所述移动终端；其中所

述第二控制元件响应所述移动终端查询，生成发送到所述第二通信接入点的移动终端响应；且其中所述第三控制元件响应所述接入点查询，生成发送到所述移动终端的接入点响应；且其中所述第二控制元件响应所述接入点响应，判断所述接入点响应是否正确；并响应所述移动终端响应，判断所述移动终端响应是否正确；以及其中所述第一控制元件在所述移动终端响应和所述接入点响应都正确时建立所述通信切换。

按照本发明所述装置的一个方面，其特征在于：所述无线电通信系统是无线局域网。

根据本发明，切换事件期间的移动终端的验证是通过查询/响应程序来实现的。根据该查询/响应程序，新的 AP 向移动终端发出查询，因此移动终端(MT)通过向新 AP 发送响应来作出响应。

由移动终端和 AP 构成的通信对的两端的验证密钥最初由可缩放密钥管理协议、例如因特网密钥交换(IKE)生成。安全性关联在无线通信系统内的各种 AP 之间转移，以便免除每次切换期间对新的和不同的密钥交换的需要。

切换处理过程中，新 AP 请求密钥及其相关信息，密钥和其他信息在传递于旧 AP 和新 AP 之间的一个或多个切换消息中、从旧 AP 转移到新 AP。验证查询和响应的交换都集成到切换中涉及的新 AP 和移动终端之间产生的切换信令中。

根据本发明的特征，所述消息是媒体接入控制(MAC)层消息。

应当指出，本发明的提供接入点验证的特征是值得要的，但是它是任选特征。

虽然接入点之间最好有安全连接，但是这种特征并非本发明的精神和范围所要求的。

本领域的技术人员通过参考本发明的下列详细描述，将会理解本发明的这些及其他特征和优点，所述描述引用了附图。

附图说明

图 1 是本发明的实施例可用的通信系统的示意图。

图 2 是根据本发明的前向切换处理的示意图。

图 3 是根据本发明的后向切换处理的示意图。

图 4A-4C 提供图 2 的前向切换处理的另一个示意图。

图 5A-5C 提供图 3 的后向切换处理的另一个示意图。

图 6 是根据本发明的 HIPERLAN/2 强制切换的示意图。

图 7 是根据本发明的 HIPERLAN/2 前向切换的示意图。

具体实施方式

图 1 是提供与多个移动终端的无线电通信以及这些移动终端之间的无线电通信的通信系统的实例，其中移动终端 12 是一个实例。在另一个实例中，接入点包含无线电接口和固定网络的网桥，且所述接入点与所述固定网络连接，该实例不需要图 1 中所示的中央控制单元(CCU)。通信系统 10 构成 WLAN，它如 IEEE 802.11 标准所述、提供与多个移动终端 12 的通信，也可能按照如上述共同未决的专利申请中所描述的专用操作方式。其他通信系统是类似的，本发明的操作也可用于此类的其他通信系统中。

WLAN 10 包括多个以定距离间隔的 AP 14 和 114，它们各自位于两个以定距离间隔的地理位置上。虽然图中只表示出两个 AP 14 和 114，但在实际情况中，采用了大量的 AP。AP 14 和 114 有时称为基站或远程天线装置(RAD)。这里，术语“接入点”、“AP”或“ap”一般用来标识构成通往通信系统 10 的网络基础设施的点的装置。术语“移动终端”、“MT”或“mt”一般用来标识构成通往接入点的各点的装置。

各个 AP 14 和 114 包括无线电收发信机电路 16，该电路能够在移动终端 12 处于特定 AP 的通信范围内时、与该移动终端进行无线电通信信号的收发。一般，当移动终端 12 处于接近给定接入点且由

其定义的地理区域或小区 18 和 118 内时，该移动终端与 AP 14 和 114 通信。在图 1 中，小区 18 与接入点 14 相关联，移动终端 12 驻留在小区 18 内，而小区 118 与接入点 114 相关联。应当指出，仅在本发明的实施采用专用无线电链路级消息时，才包括方式选择器 34，这不是本发明的实施所必需的。

接入点 14 和 114 与中央控制单元(CCU) 22 耦合。CCU 22 通常是集线器和 IP 路由器。CCU 22 提供与外部通信网络干线 24 的连接。虽然未示出，但是其他通信装置、如其他通信站和其他通信网络通常与通信网络干线 24 连接。这样，可以构成通信路径，提供移动终端 12 与直接或间接连接到通信网络干线 24 的通信站之间的通信。而且，允许多个移动终端 12 之间的本地通信。在成对的移动终端 12 之间的通信中，其间形成的通信路径包括两个分离的无线电链路。

AP 14 和 114 包括控制单元 28，它们执行有关各个 AP 的操作的各种控制功能。在图 1 中，控制单元 28 各表示成包括比较器 32、方式选择器 34 和切换可用性判断器 36，所述控制单元是以任何期望的方式工作和实现的，例如可由处理电路执行的算法。在另一种实现中，此类单元所执行的功能设在其他位置，如设在方框 28' 所表示的移动终端 12 上，或设置在方框 28" 所表示的 CCU 22 中。因此，这些控制单元所执行的功能可以分布在几个不同的装置中。

应当指出，根据本发明，比较器 32 包括安全性功能，方框 28 包括媒体接入控制(MAC)功能。

在图 1 的结构和设置中，如上述共同未决的专利申请所述，当判断由 AP 14 和 114 以及移动终端 12 构成的通信对并非都兼容专用方式时，通信对按照 IEEE 802.11 标准方式工作，而当判断通信对的双方都具有专用方式功能时，按照专用方式工作。为了得到此结果，比较器 32 接收标识构成通信对的移动终端和接入点的运行方式的标识符。然后方式选择器 34 为该移动终端与接入点之间的通信选择工作的标准方式或工作的专用方式。

当给定的通信会话期间移动终端 12 的物理位置从小区 18 改变到小区 118 时，移动终端 12 离开 AP 14 服务的第一地理区域 18，并进入 AP 114 所服务的第二地理区域 118。这种小区至小区或区域至区域的移动需要从与第一区域 18 相关的旧 AP 14 到与第二区域 118 相关的新 AP 114 的通信切换，从而实现与移动终端 12 的持续通信。

切换可用性判断器 36 向移动终端 12 提供可向其作出通信切换的可用 AP 的指示。可用接入点列表 38 中包含这种可用性，该列表中包含可用于通信切换的 AP 的身份。

可用接入点列表 38 可以选定的时间间隔发给移动终端 12，或者接入点列表 38 可以在各个移动终端 12 最初激活时提供给该移动终端，或者可以利用网络前缀或网络前缀列表来达到同样的目的。

在本发明的说明中，假定移动终端 12 与当前或旧 AP 14 之间存在安全性关联(SA)。即，假定移动终端 12 和 AP 14 共享同一个公用密钥集和实现安全性功能所需的其他信息。根据本发明，当移动终端从小区 18 移动到小区 118 时，这个已建立和共享的安全性关联以保密的方式从旧 AP 14 转移到新 AP 114。此转移是以非常快的方式如下完成的：将实行转移所需的消息数目减至最小，而且免除使用公钥加密。因此，对往返于移动终端 12 的净荷业务的中断被减至最小，任何此类型的中断对于实时服务、如 IP 语音传输(VOIP)和视频发布都是至关重要的。

根据本发明，通信链路(即涉及移动终端 12 和 AP 14 的链路)两端的验证密钥或安全性关联是利用密封密钥管理协议、如 IKE 生成的，应当指出，也可以利用 Diffie-Hellman 密钥交换协议。

稍后，当移动终端 12 从小区 18 及其 AP 14 移动到小区 118 及其 AP 114 时，切换处理期间的验证通过本发明的简单查询/响应程序来实现。而且安全性关联在旧 AP 14 和新 AP 114 之间转移，从而在从旧 AP 14 到新 AP 114 切换期间不需要新的密钥交换。

在查询/响应程序期间，新 AP 118 向移动终端 12 发送查询，随

后移动终端 12 向新 AP 118 发送响应。此外，在切换期间，移动终端 12 以类似的方式对新 AP 118 进行验证。

密钥和相关信息被新 AP 114 请求，因此它们在切换消息中从旧 AP 14 转移到新 AP 114。同样地，验证查询和相应的响应的交换集成到新 AP 114 和移动终端 12 之间所产生的切换信令中。

图 2 表示根据本发明的前向切换(HO)处理 20，它是本发明的最佳实施例。在前向切换处理 20 中，切换信令在移动终端(MT 或 mt)12 和新接入点(AP 或 ap)114 之间传送。这种类型的切换在无线电链路 21 丢失而无预先警告时尤其有用。

图 3 表示根据本发明的后向切换(HO)处理 30，在后向切换处理 30 中，由与旧 AP 14 通信的移动终端 12 请求切换，这产生与图 2 所示有所不同的消息序列。在后向切换期间，一种有利的选择是采用无线电接口消息 31，它将验证查询从旧 AP 14 载送到移动终端 12，从而也触发后向切换 33。即，验证查询 31 用于向移动终端 12 指示它应该断开与旧 AP 14 的连接而连接到新 AP 114，于是已经为移动终端 12 准备好安全性关联(SA) 35。

如此处所使用的术语“旧 AP”表示移动终端 12 最初或当前与之通信的接入点，如接入点 14。因此，术语“旧 AP”还表示在需要通信切换时移动终端 12 正在与之通信的“当前 AP”。

如此处所使用的术语“新 AP”表示由于移动终端 12 已经在地理位置上从旧小区 18 移动到新小区 118、所以必须开始与之通信的接入点，如接入点 114。因此，术语“新 AP”还表示在通信切换完成之后移动终端 12 将与之通信的“将来 AP”。

在图 2 和图 3 中，采用了 IEEE 802.11 消息名称，并表示了切换消息的附加参数。但是，消息的命名对于本发明的精神和范围来说并不是关键的，因为本发明可以在除 IEEE 802.11 以外的其它系统中实现。但是，在图 2 和图 3 中采用扩展 MAC(媒体接入控制)消息来通过无线电接口载送附加参数的有利之处是避免了发送附加消息的

需要。

为了确保安全性，最好消息载送已加密的密钥。因此，在 AP 14 和 114 之间转移安全性关联或 SA 以及其他控制业务，如图所示是通过 IPsec 加密和验证的。

判断移动终端 12 在物理位置上相对于小区 18 和 118 已经移动、使得需要切换的特定装置对于本发明来说并非关键。例如，该程序可以类似于在采用移动台协助切换程序的常规时分蜂窝系统中使用的。一般，移动终端 12 例如以计时间隔调谐到相邻小区、如小区 18 和 118 的基站或 AP 的控制信道上。然后，移动终端 12 测量或检测在这些控制信道上广播的信号的信号强度或某些其他信号特征，如误码率。然后移动终端 12 将基于其中测量的上行信号发送到网络 10，于是网络 10 判断是否应该实施通信切换。当判断需要切换时，向移动终端 12 发送指令，并开始图 2 或图 3 的通信切换处理。

图 4A-4C 提供另一种前向切换处理 20 的示意图，其中当移动终端从小区 18 移动到小区 118 时提供相对于旧 AP 14 和新 AP 114 的移动终端 12 的通信切换。此图中，移动终端或 MT 也用术语“mt”来称呼，接入点或 AP 也用术语“ap”来称呼。参考图 4A，根据事件 401 的指示需要切换的“是”输出 400，在移动终端 12 启动前向切换处理 20。现在移动终端 12 在功能 402 操作而激活它的无线电切换功能。

在功能 403，移动终端 12 向新 AP 114 生成查询，于是在功能 404，包含“mt_challenge”的 MAC_REASSOCIATE_REQ 消息被发送到新 AP 114。

在功能 405，新 AP 114 接受消息 404，于是新 AP 114 在功能 406 进行操作，以向旧 AP 14 发送切换请求。

旧 AP 14 则在功能 407 进行操作以从它的安全性关联数据库中检索安全性关联参数 SA,SA。然后旧 AP 14 在功能 408 操作，将包含参数 SA,SA 的切换请求发送到新 AP 114。

参考图 4B，新 AP 114 在功能 409 操作，创建安全性关联(SA)，在功能 410 操作，生成查询以对移动终端 12 验证，在功能 411 操作，计算对包含在附图 4A 的消息 404 中的“mt_challenge”的响应，以及在功能 412 操作，将 MAC_AUTHENTICATE_REQ 消息发送到移动终端 12。消息 412 包含由功能 411 的操作计算得到的“ap_response”，包含由功能 410 的操作生成的“ap_challenge”，包含“其他信息”。

现在移动终端 12 在功能 413 操作，更新它的安全性关联参数，在功能 414 操作，计算对通过消息 412 接收的“ap_challenge”的响应，并在功能 415 进行操作，将通过消息 412 接收的“ap_response”与正确的或期望的响应进行比较。

当功能 415 所执行的比较产生正确的比较结果时，功能 416 进行操作，对新 AP 114 验证，于是功能 417 进行操作，把 MAC_AUTHENTICATE_RESP 消息发送到新 AP 114，此消息包含功能 414 计算得到的“ mt_response”。

现在参考图 4C，在功能 418，新 AP 114 进行操作，将通过消息 417 接收的“mt_response”与适合的或正确的响应进行比较，当此比较得到正确的比较结果时，功能 419 进行操作，对移动终端 12 验证。然后，新 AP 114 在功能 420 操作，将 MAC_REASSOCIATE_RESP 消息发送到移动终端 12，至此切换完成，此后移动终端 12 在功能 421 进行操作，利用新 AP 114 恢复它的净荷业务。

图 5A-5C 提供另一种后向切换处理 30 的示意图，其中相对于旧 AP 14 和新 AP 114 为移动终端 12 提供通信切换。在此图中，移动终端或 MT 也使用术语“mt”，接入点或 AP 也使用术语“ap”。

参考图 5A，根据事件 501 的指示需要切换的“是”输出 500 在移动终端 12 启动后向切换处理 30。现在移动终端 12 在功能 502 操作，向旧 AP 14 发送切换请求。

当在旧 AP 14 接收到消息 502，功能 503 接受该消息，功能 504

进行操作，从它的安全性关联(SA)数据库中检索安全性关联参数SA,SA，然后功能 505 进行操作，将包含参数 SA,SA 的切换请求发送到新 AP 114。

利用在消息 505 中接收的参数 SA,SA，新 AP 114 在功能 506 进行操作，创建它自己的安全性关联(SA)。然后新 AP 114 在功能 507 进行操作，生成查询以对移动终端 12 验证，在功能 508 向旧 AP 14 发送切换请求，此请求 508 包含功能 507 中生成的“ap_challenge”和“其他信息”。

现在参考图 5B，响应消息 508，旧 AP 14 在功能 509 进行操作，向移动终端 12 发送 MAC_DISASSOCIATE 消息，此消息包含旧 AP 14 通过消息 508 从新 AP 114 接收的“ap_challenge”和“其他信息”。

响应消息 509，移动终端 12 在 510 启动它的无线电切换功能。在功能 511，移动终端 12 更新它的安全性关联参数，在功能 511，移动终端 12 进行操作，计算对消息 508 和 509 的“ap_challenge”部分的响应，在功能 513，移动终端 12 进行操作，生成查询以对新 AP 114 验证，并在功能 514，移动终端 12 将 MAC_REASSOCIATE_REQ 消息发送到新 AP 114。消息 514 包含在功能 511 计算出的“mt_response”，在功能 512 生成的“mt_challenge”以及“其他信息”。

现在参考图 5C，功能 515 提供移动终端 12 的验证，功能 516 将通过消息 513 接收的“mt_response”与正确的或期望的响应进行比较，功能 517 计算对通过消息 513 接收的“mt_challenge”的响应，以及功能 518 进行操作，将 MAC_REASSOCIATE_RESP_ENH 消息发送到移动终端 12，消息 518 包含功能 517 计算的“ap_response”。

在功能 519，移动终端 12 进行操作，通过在功能 520 将消息 518 所包含的“ap_response”与正确的或期望的响应进行比较来对新 AP 114 验证，对于此正确的比较结果，功能 521 使移动终端 12 利用新 AP 114 恢复净荷业务。

根据上述内容可以看出，本发明提供了一种方法/装置，它在与给定的移动终端 12 的通信从第一接入点 14 切换到第二接入点 114 时提供信息安全性。通信系统 10 被设置成具有多个接入点，各个接入点服务于由通信系统 10 所服务的整个地理区域内的不同地理区域，多个移动终端 12 被设置成这样，其中移动终端各自可实际地在所述整个地理区域内和所述不同地理区域之间移动。

在本发明的切换处理/装置中，首先检测何时给定的移动终端 12 从第一接入点 14 的通信影响移动到第二接入点 114 的通信影响中(参见图 4A 的 401 和图 5A 的 501)。

当检测到这种移动时，从第一接入点 14 提取安全性关联参数(参见图 4A 的 407 和图 5A 的 504)，根据所检索的安全性关联参数在第二接入点 114 创建安全性关联(参见图 4B 的 409 和图 5A 的 506)，并根据所检索的安全性关联参数在给定的移动终端 12 创建安全性关联(参见图 4B 的 413 和图 5B 的 510)。

当检测到这种移动时，也会从给定的移动终端 12 向第二接入点 114 发送验证接入点查询(参见图 4A 的 404 和图 5B 的 513)，并从第二接入点 114 向给定的移动终端 12 发送验证移动终端查询(参见图 4B 的 412 和图 5A 的 508)。应当指出，上述接入点查询是本发明的任选特征。

响应从给定移动终端 12 接收的验证接入点查询，第二接入点 114 则生成验证接入点响应(参见图 4B 的 411 和图 5C 的 516),然后此验证接入点响应被发送到给定的移动终端 12(参见图 4B 的 412 和图 5C 的 517)。

响应从第二接入点 114 接收的验证移动终端查询，给定的移动终端 12 计算验证移动终端响应(参见图 4B 的 414 和图 5B 的 511)，然后此验证移动终端响应被发送到第二接入点 114(参见图 4B 的 417 和图 5B 的 513)。

在给定的移动终端 12 的第一比较现在进行操作，将从第二接入

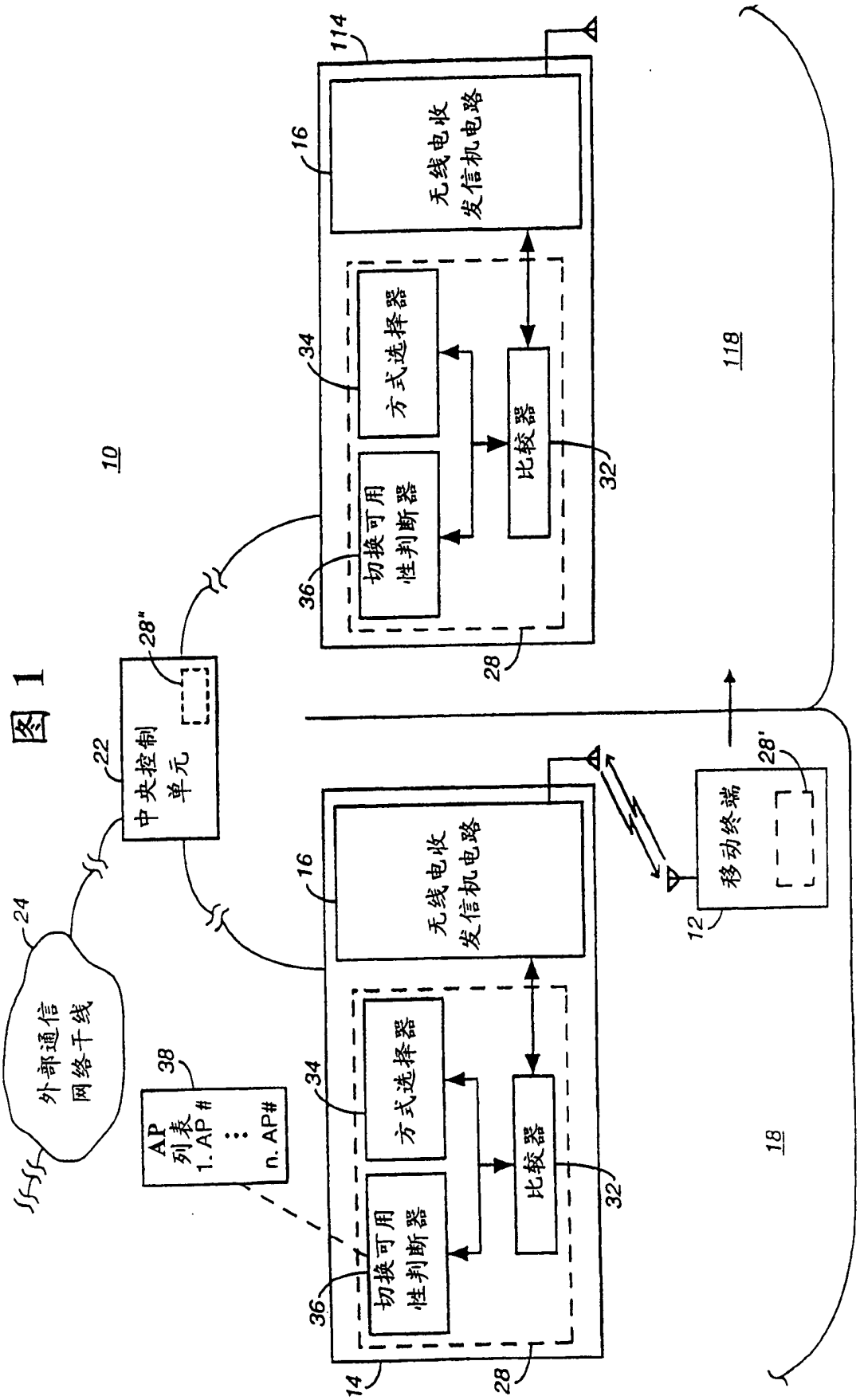
点 114 接收的验证接入点响应与正确的或期望的响应比较(参见图 4B 的 415 和图 5C 的 519)，在第二接入点 114 的第二比较现在进行操作，将从给定的移动终端 12 接收的验证移动终端响应与正确的或期望的响应进行比较(参见图 4C 的 418 和图 5C 的 515)。

最后，根据第一比较和第二比较的结果，在给定的移动终端 12 和第二接入点 114 之间发起通信(参见图 4C 的 421 和图 5C 的 520)。

图 6 和图 7 表示本发明的两个附加实施例。虽然图 6 和图 7 的实施例在特定细节上有所不同，但是通过比较本发明的上述图 2、3、4A-4B 和 5A-5B 的实施例，可以容易地理解图 6 和图 7 的实施例的内容。

虽然参考本发明最佳实施例对本发明进行了详细说明，但是该详细说明中的任何部分都不作为对本发明的精神和范围的限定，因为众所周知，一旦大体上理解了本发明，本领域的技术人员可容易地设想其它在本发明的精神和范围内的实施例。

图 1


外部通信网络干线
24
AP 列表 1. AP # ⋮ n. AP#
38
中央控制单元
22
28"
10
16
无线电收发信机电路
114
方式选择器
34
切换可用性判断器
36
比较器
32
28
14
118
移动终端
28'
12

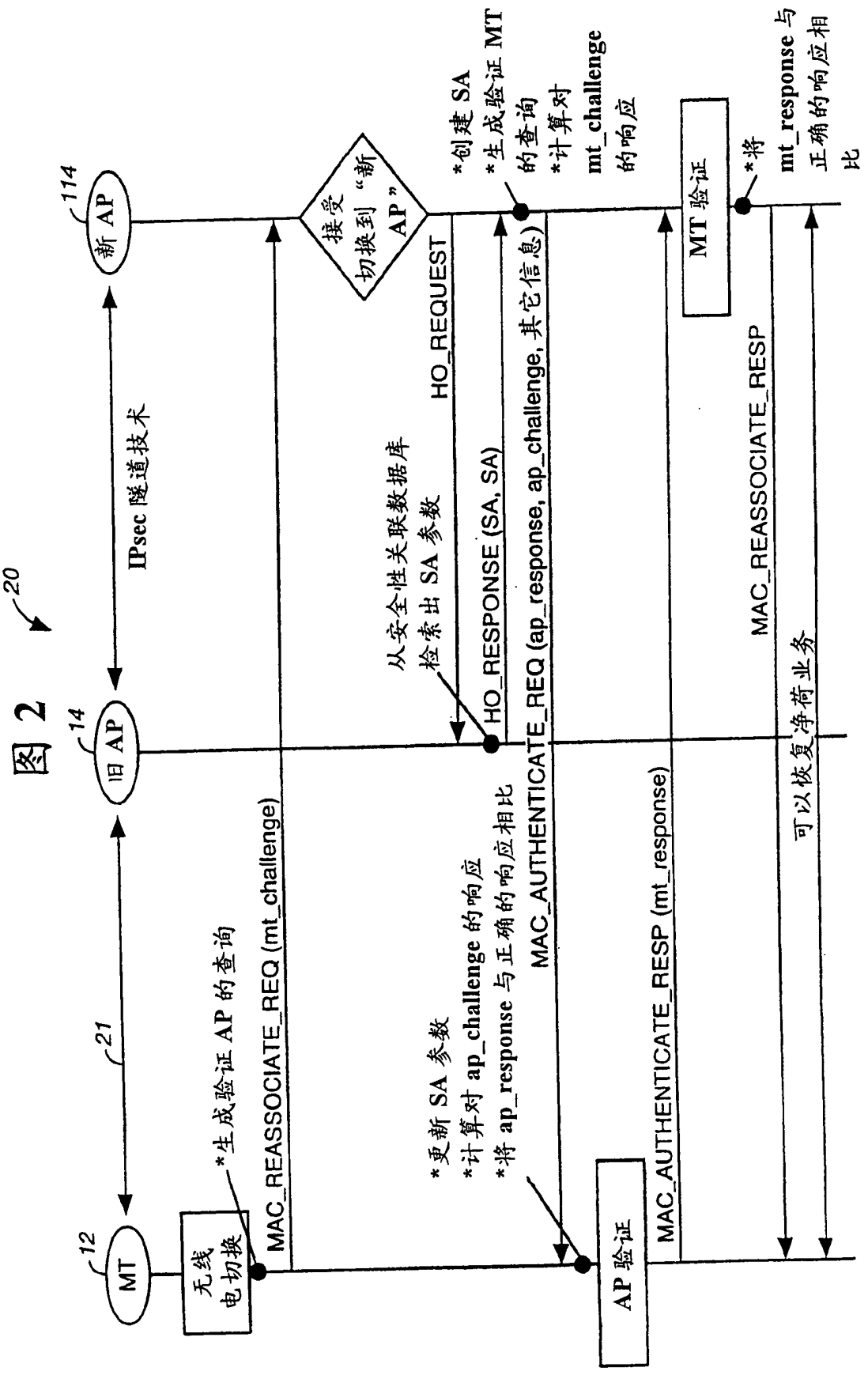
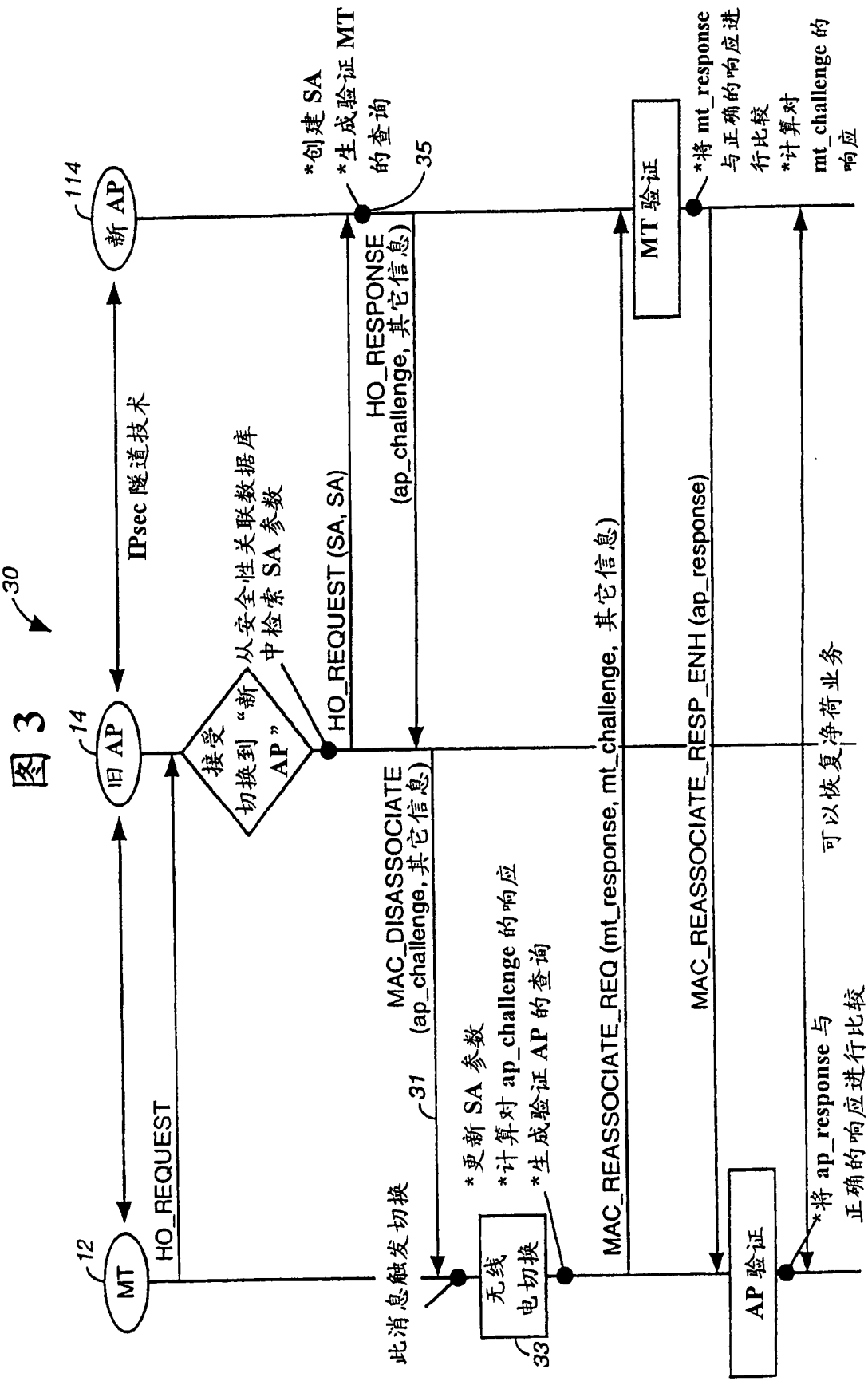

20
图 2
MT
12
旧 AP
14
新 AP
114
21
IPsec 隧道技术
无线电切换
*生成验证 AP 的查询
MAC_REASSOCIATE_REQ (mt_challenge)
从安全性关联数据库检索出 SA 参数
接受切换到“新 AP”
HO_REQUEST
HO_RESPONSE (SA, SA)
*创建 SA
*生成验证 MT 的查询
*计算对 mt_challenge 的响应
MAC_AUTHENTICATE_REQ (ap_response, ap_challenge, 其它信息)
MT 验证
*将 mt_response 与正确的响应相比
MAC_REASSOCIATE_RESP
*更新 SA 参数
*计算对 ap_challenge 的响应
*将 ap_response 与正确的响应相比
AP 验证
MAC_AUTHENTICATE_RESP (mt_response)
可以恢复净荷业务

图 3


30
12
MT
14
旧 AP
114
新 AP
HO_REQUEST
IPsec 隧道技术
接受切换到“新 AP”
从安全性关联数据库中检索 SA 参数
HO_REQUEST (SA, SA)
*创建 SA
*生成验证 MT 的查询
35
HO_RESPONSE (ap_challenge, 其它信息)
MT 验证
*将 mt_response 与正确的响应进行比较
*计算对 mt_challenge 的响应
此消息触发切换
31
MAC_DISASSOCIATE (ap_challenge, 其它信息)
*更新 SA 参数
*计算对 ap_challenge 的响应
*生成验证 AP 的查询
无线电切换
33
MAC_REASSOCIATE_REQ (mt_response, mt_challenge, 其它信息)
MAC_REASSOCIATE_RESP_ENH (ap_response)
AP 验证
*将 ap_response 与正确的响应进行比较
可以恢复净荷业务

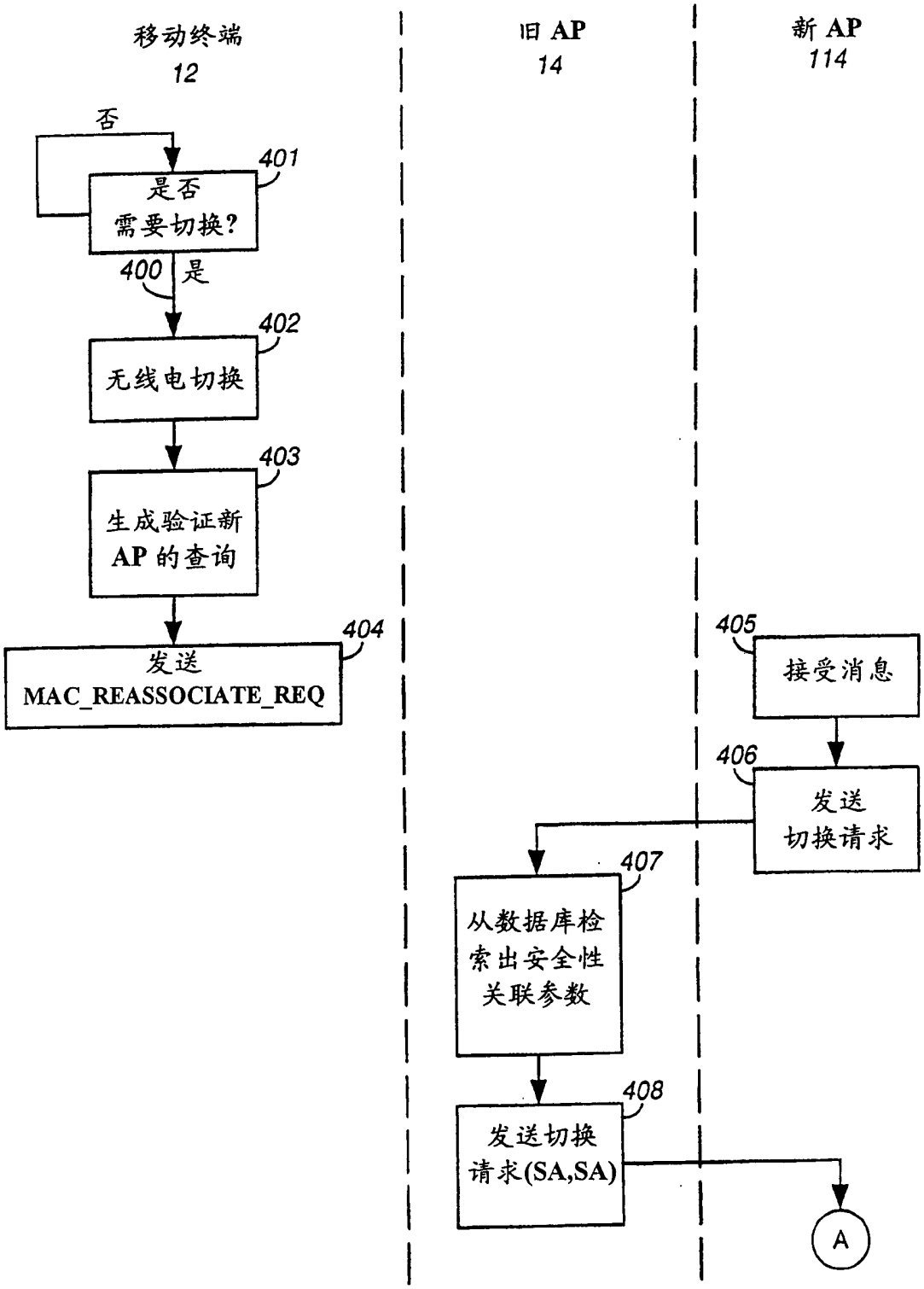

移动终端
12
旧 AP
14
新 AP
114
否
401
是否
需要切换?
400
是
402
无线电切换
403
生成验证新
AP 的查询
404
发送
MAC_REASSOCIATE_REQ
405
接受消息
406
发送
切换请求
407
从数据库检
索出安全性
关联参数
408
发送切换
请求(SA,SA)
A

图 4A

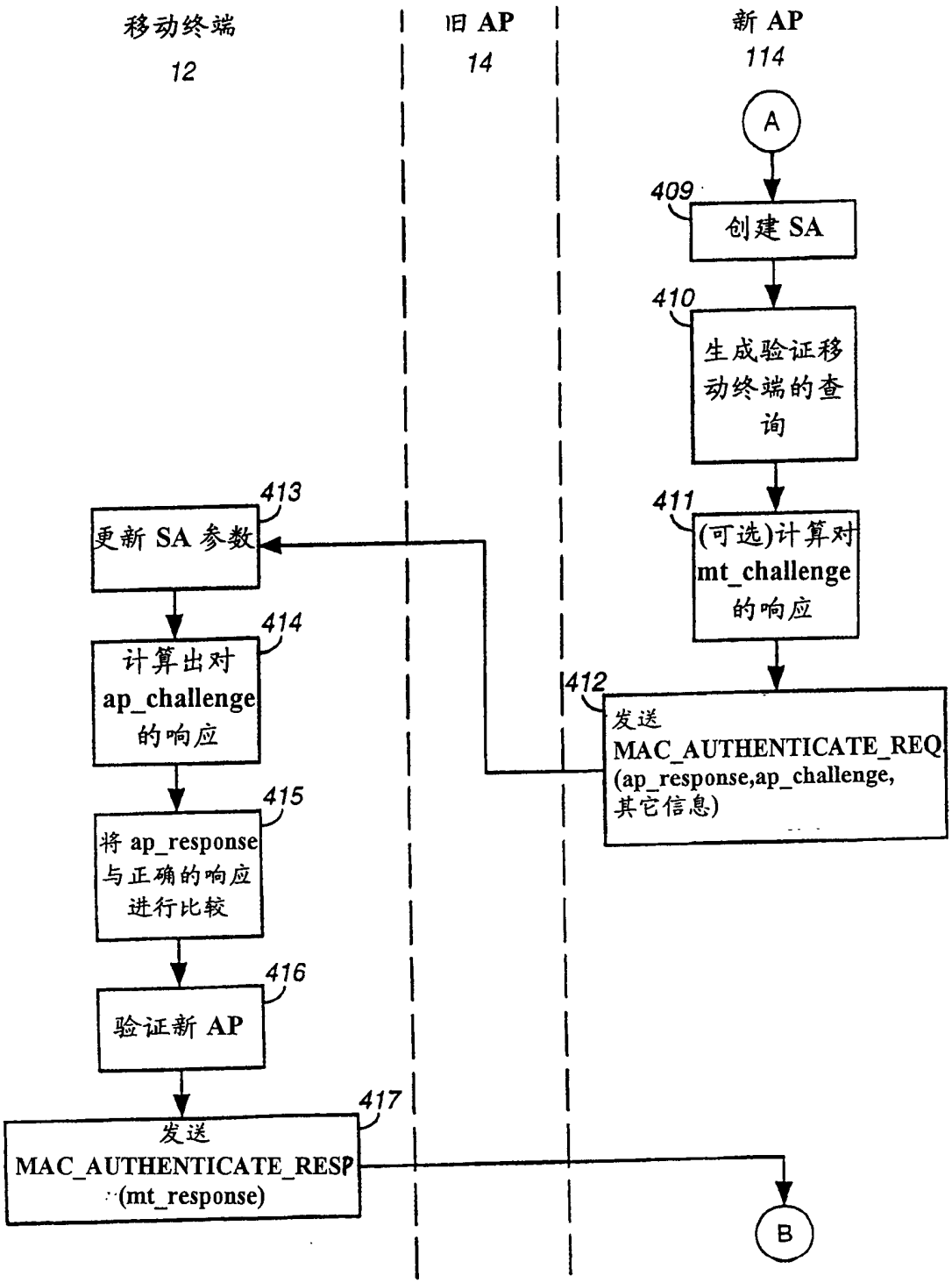

移动终端
12
旧 AP
14
新 AP
114
A
409
创建 SA
410
生成验证移动终端的查询
411
(可选)计算对mt_challenge的响应
412
发送MAC_AUTHENTICATE_REQ(ap_response,ap_challenge,其它信息)
413
更新 SA 参数
414
计算出对ap_challenge的响应
415
将 ap_response与正确的响应进行比较
416
验证新 AP
417
发送MAC_AUTHENTICATE_RESP(mt_response)
B

图 4B

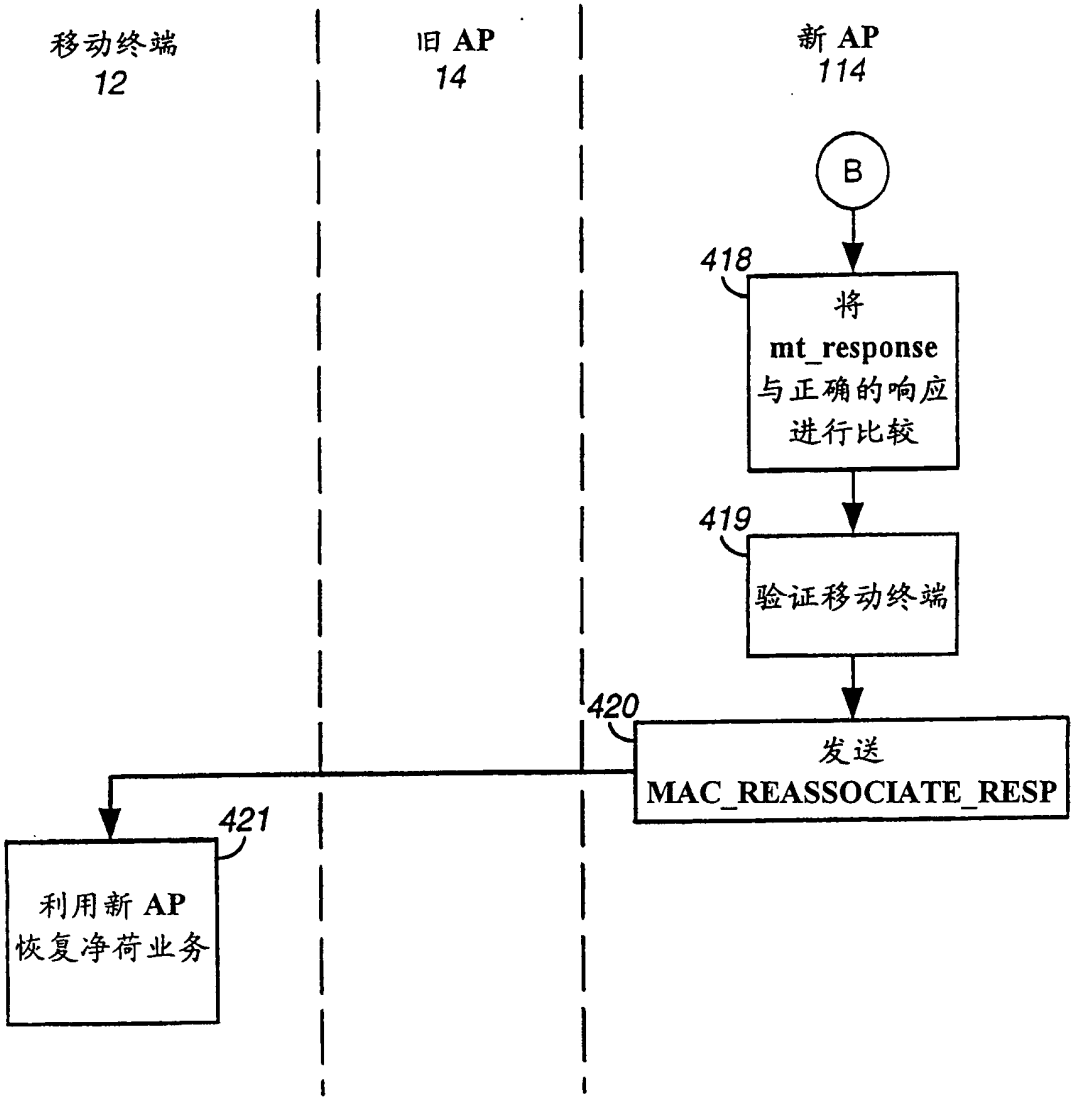

移动终端
12
旧 AP
14
新 AP
114
B
418
将
mt_response
与正确的响应
进行比较
419
验证移动终端
420
发送
MAC_REASSOCIATE_RESP
421
利用新 AP
恢复净荷业务

图 4C

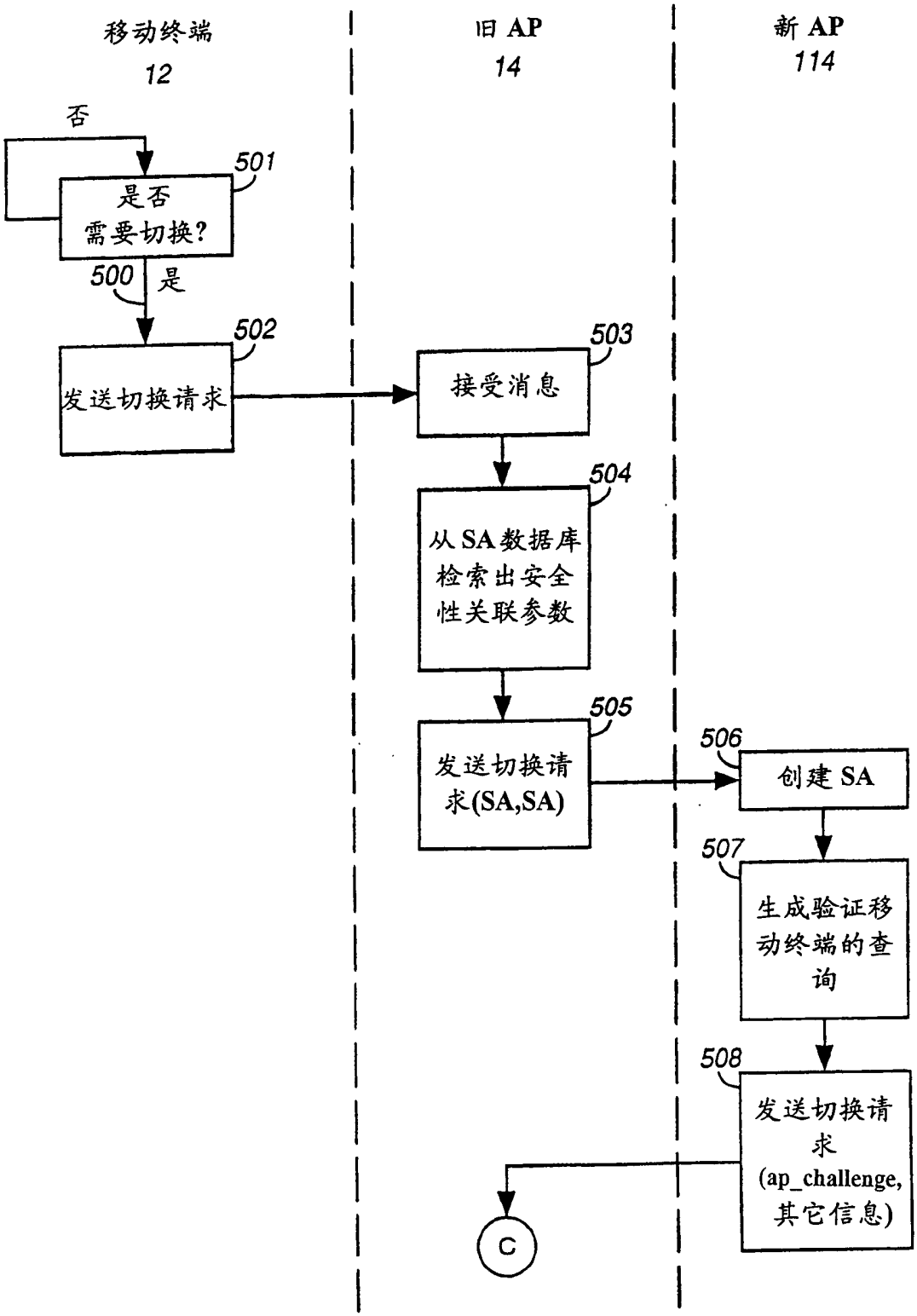

移动终端
12
旧 AP
14
新 AP
114
否
501
是否
需要切换?
500
是
502
发送切换请求
503
接受消息
504
从 SA 数据库
检索出安全
性关联参数
505
发送切换请
求(SA,SA)
506
创建 SA
507
生成验证移
动终端的查
询
508
发送切换请
求
(ap_challenge,
其它信息)
C

图 5A

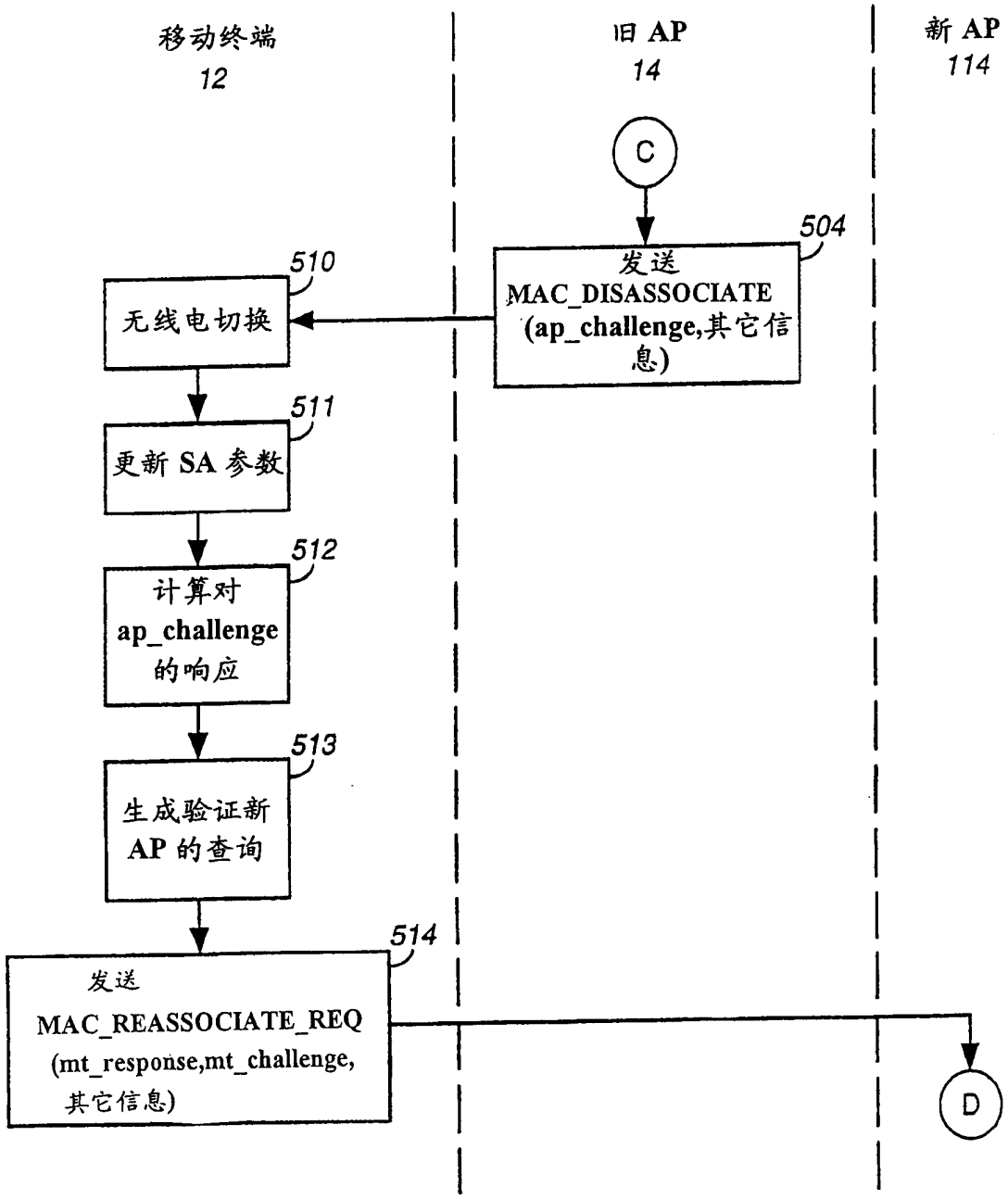

移动终端
12
旧 AP
14
新 AP
114
C
504
发送
MAC_DISASSOCIATE
(ap_challenge,其它信息)
510
无线电切换
511
更新 SA 参数
512
计算对
ap_challenge
的响应
513
生成验证新
AP 的查询
514
发送
MAC_REASSOCIATE_REQ
(mt_response,mt_challenge,
其它信息)
D

图 5B

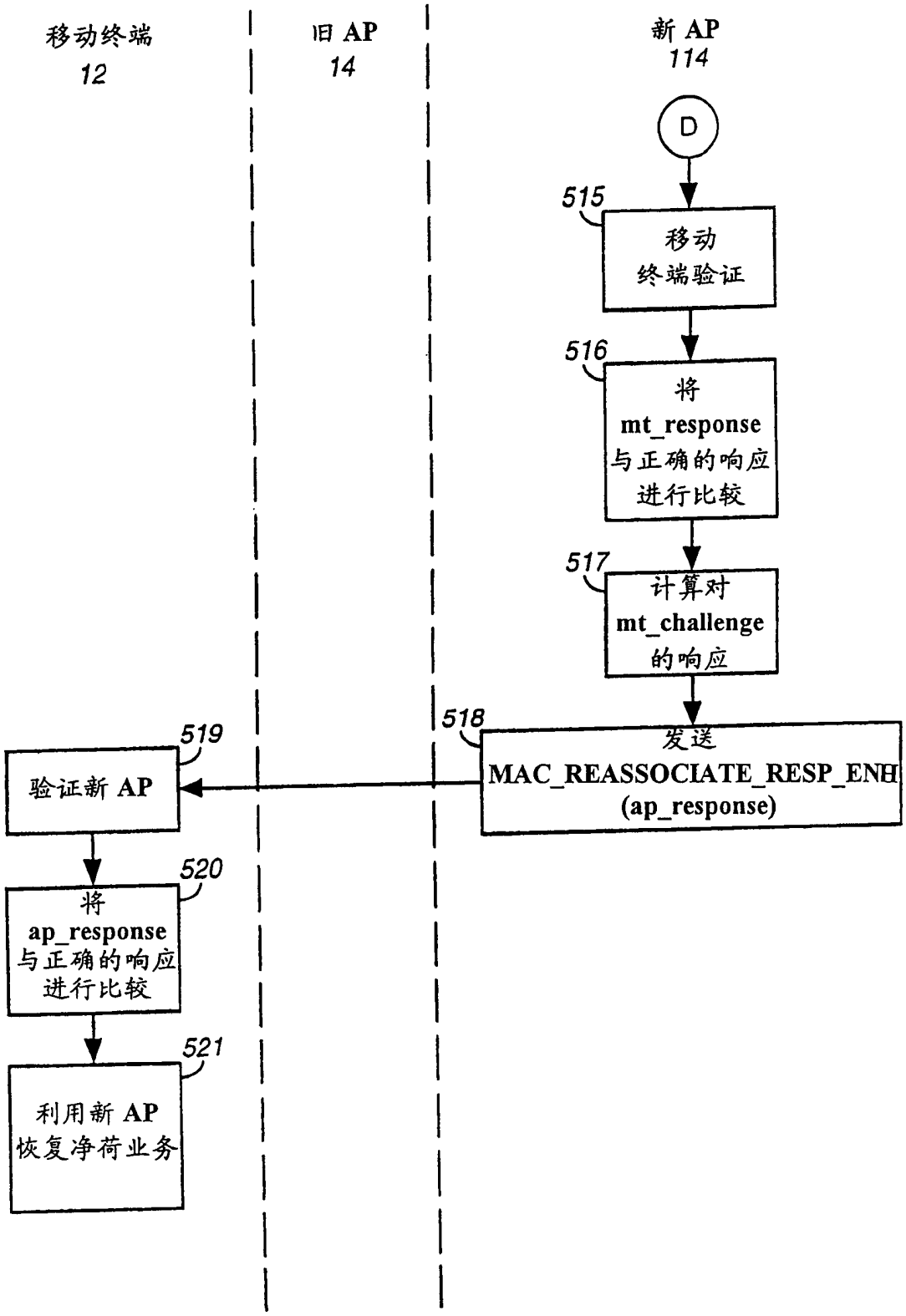

移动终端
12
旧 AP
14
新 AP
114
D
515
移动
终端验证
516
将
mt_response
与正确的响应
进行比较
517
计算对
mt_challenge
的响应
518
发送
MAC_REASSOCIATE_RESP_ENH
(ap_response)
519
验证新 AP
520
将
ap_response
与正确的响应
进行比较
521
利用新 AP
恢复净荷业务

图 5C

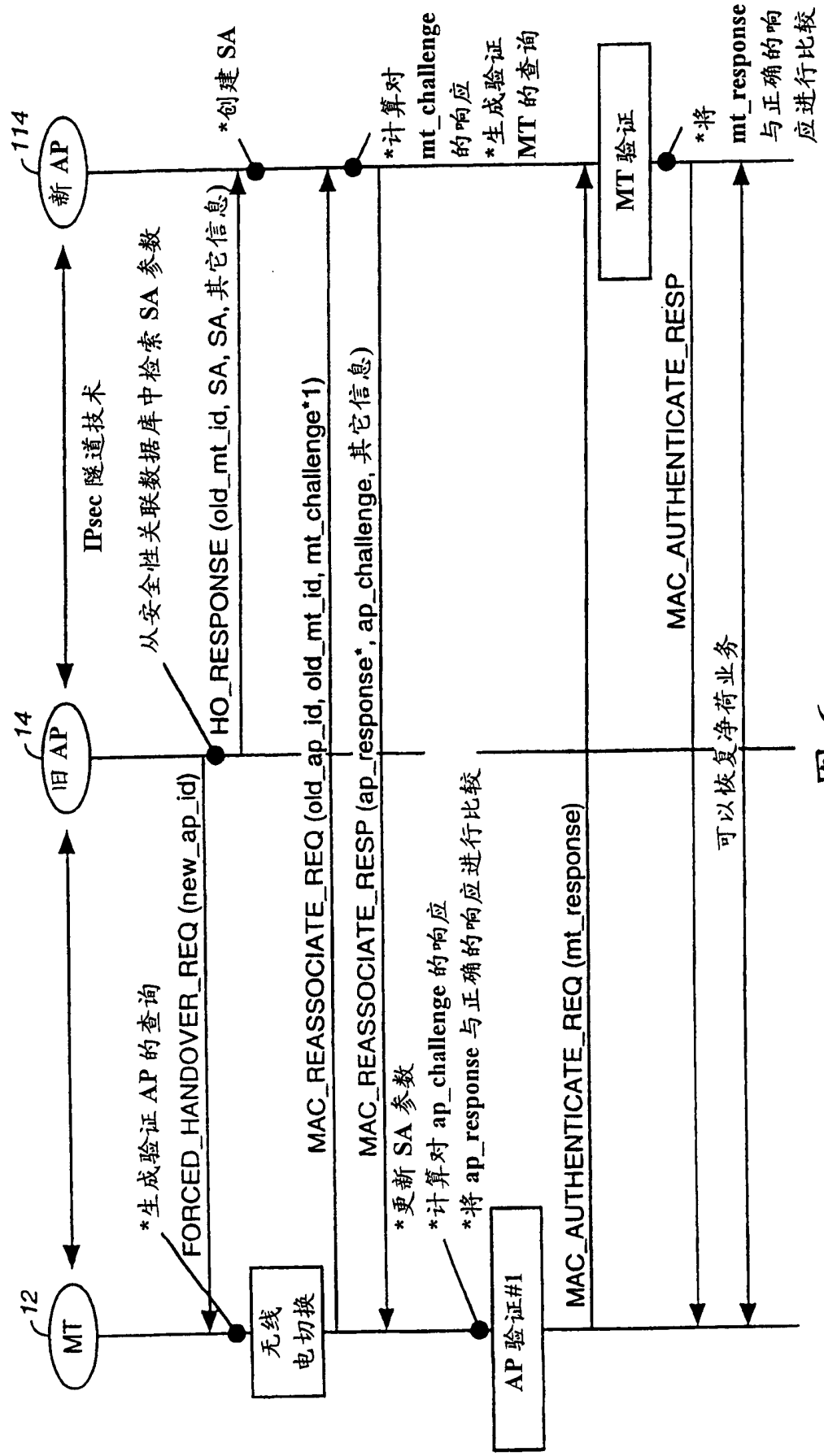

MT
12
旧 AP
14
新 AP
114
IPsec 隧道技术
*生成验证 AP 的查询
FORCED_HANDOVER_REQ (new_ap_id)
从安全性关联数据库中检索 SA 参数
HO_RESPONSE (old_mt_id, SA, SA, 其它信息)
*创建 SA
无线电切换
MAC_REASSOCIATE_REQ (old_ap_id, old_mt_id, mt_challenge*1)
MAC_REASSOCIATE_RESP (ap_response*, ap_challenge, 其它信息)
*计算对 mt_challenge 的响应
*生成验证 MT 的查询
*更新 SA 参数
*计算对 ap_challenge 的响应
*将 ap_response 与正确的响应进行比较
AP 验证#1
MAC_AUTHENTICATE_REQ (mt_response)
MT 验证
MAC_AUTHENTICATE_RESP
*将 mt_response 与正确的响应进行比较
可以恢复净荷业务

图 6

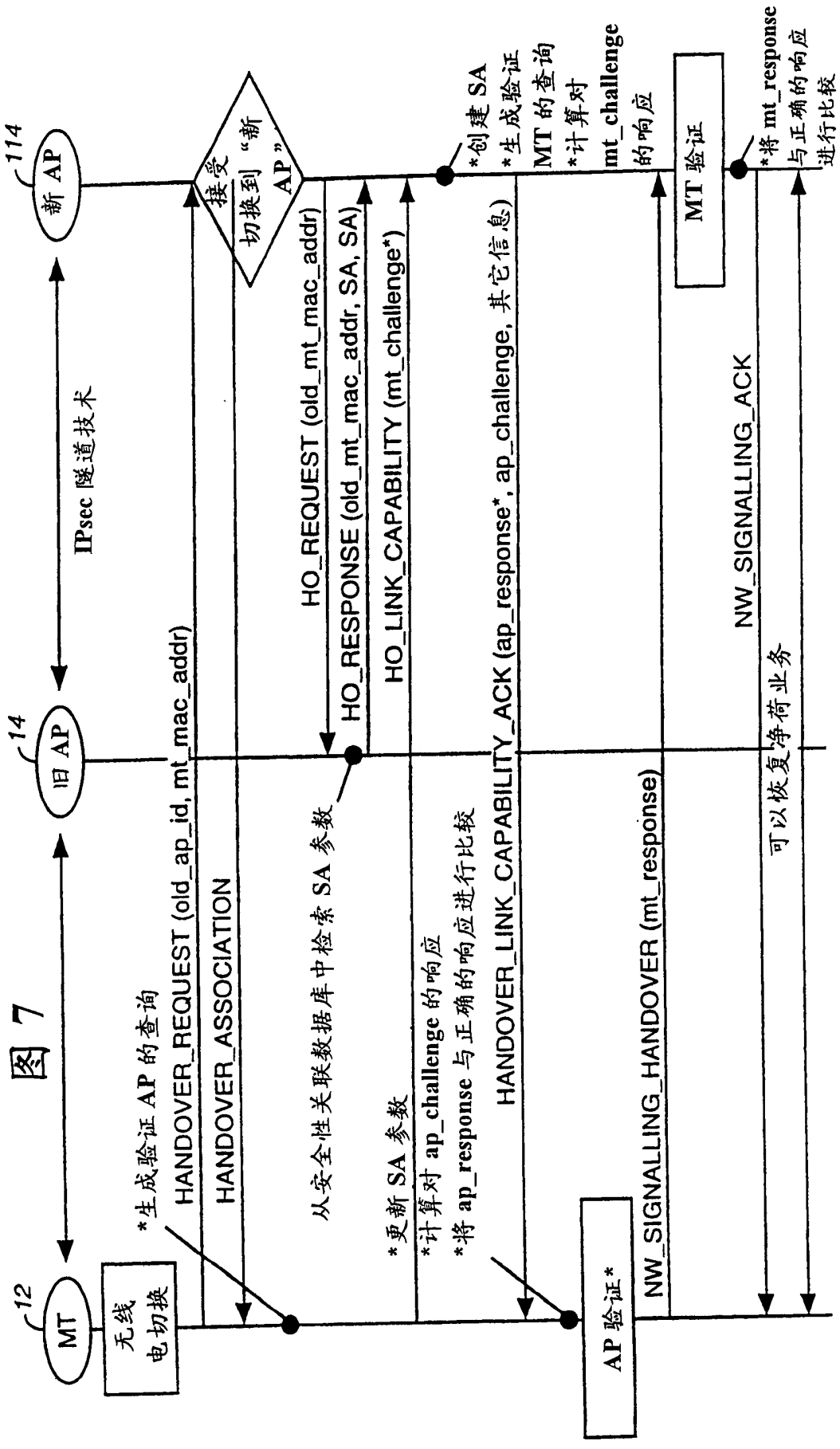

MT
12
旧 AP
14
新 AP
114
无线电切换
IPsec 隧道技术
*生成验证 AP 的查询
HANDOVER_REQUEST (old_ap_id, mt_mac_addr)
HANDOVER_ASSOCIATION
接受切换到“新 AP”
HO_REQUEST (old_mt_mac_addr)
从安全性关联数据库中检索 SA 参数
HO_RESPONSE (old_mt_mac_addr, SA, SA)
*更新 SA 参数
HO_LINK_CAPABILITY (mt_challenge*)
*计算对 ap_challenge 的响应
*将 ap_response 与正确的响应进行比较
*创建 SA
*生成验证 MT 的查询
*计算对 mt_challenge 的响应
HANDOVER_LINK_CAPABILITY_ACK (ap_response*, ap_challenge, 其它信息)
MT 验证
*将 mt_response 与正确的响应进行比较
AP 验证*
NW_SIGNALLING_HANDOVER (mt_response)
NW_SIGNALLING_ACK
可以恢复净荷业务

图 7