

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 12/54 (2006.01)



[12] 发明专利说明书

专利号 ZL 200410097500.8

[45] 授权公告日 2010 年 2 月 24 日

[11] 授权公告号 CN 100592705C

[22] 申请日 2004.11.29

[21] 申请号 200410097500.8

[30] 优先权

[32] 2003.12.17 [33] US [31] 10/738,802

[73] 专利权人 微软公司

地址 美国华盛顿州

[72] 发明人 D·R·西蒙 H·J·王

P·巴尔

[56] 参考文献

US2002/0124169A1 2002.9.5

WO02/063847A2 2002.8.15

CN1395388A 2003.2.5

US2002/0022483A1 2002.2.21

US6571221B1 2003.5.27

A Novel Authentication scheme for Ad hoc Networks. Lakshmi Venkatraman, Dharma P. Agrawal. Wireless Communications and Networking Conference, 2000. WCNC. 2000 IEEE, Vol. 第 3 卷 . 2000

审查员 熊金安

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 谢喜堂

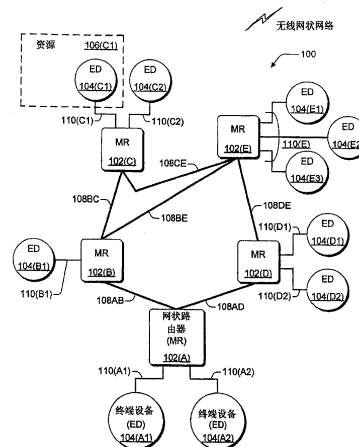
权利要求书 5 页 说明书 22 页 附图 12 页

[54] 发明名称

具有终端设备识别的网状网络

[57] 摘要

一种示例性路由器执行以下行动：从一终端设备接收至少一个证书，该至少一个证书由另一路由器签发；确认该其它路由器是否为预定邻域的成员；确定该至少一个证书是否有效；以及如果该其它路由器被确认为预定邻域的成员，且该至少一个证书被确定为有效，则识别该终端设备为特许。一种示例性网状路由器能够与其它网状路由器建立无线网状网络，该网状路由器还能够指定一邻域管理员网状路由器；该网状路由器适用于当一特定网状路由器是所指定的邻域管理员网状路由器的邻域的成员时，向与由该特定网状路由器签发的特定证书相关联的特定终端设备授予特许状态。



1. 一种用于路由器的方法，其特征在于，它包括：

从一终端设备接收至少一个证书，所述至少一个证书由另一路由器签发；

确认所述另一路由器是否为预定邻域的成员；

确定所述至少一个证书是否有效；以及

如果所述另一路由器被确认为所述预定邻域的成员，且所述至少一个证书被确定为有效，则识别所述终端设备为具有特许状态；所述特许状态涉及服务级别。

2. 如权利要求1所述的方法，其特征在于，还包括：

通过一无线收发器来与终端设备和/或其它路由器进行无线通信。

3. 如权利要求1所述的方法，其特征在于，所述接收动作包括：

从所述终端设备接收所述至少一个证书以及一所述另一路由器的标识。

4. 如权利要求1所述的方法，其特征在于，所述接收动作包括：

从所述终端设备接收所述至少一个证书以及另一证书；其中，所述另一证书与所述另一路由器相关联，并且对应于所述另一证书的公钥的私钥用于签署所述至少一个证书。

5. 如权利要求1所述的方法，其特征在于，所述接收动作包括：

从所述终端设备接收 (i) 所述至少一个证书；(ii) 与所述另一路由器相关联且签署所述至少一个证书的另一证书；(iii) 一指示所述另一路由器是所述预定邻域的成员的成员资格证书；以及 (iv) 一所述预定邻域的邻域管理员证书，其中，所述邻域管理员证书签署所述成员资格证书。

6. 如权利要求1所述的方法，其特征在于，所述确认动作包括：

访问包含在所述路由器中的一数据结构，它枚举作为所述路由器也是其成员的邻域的成员的多个路由器；以及

核查所述另一路由器是否在所述数据结构中枚举。

7. 如权利要求6所述的方法，其特征在于，所述数据结构还将与所述路由器建立的各自的共享机密密钥映射到所述多个路由器的至少一部分的相应的路由器。

8. 如权利要求1所述的方法，其特征在于，所述确认动作包括：

确认所述另一路由器是否为所述预定邻域的成员，其中，所述预定邻域包括所述路由器也是其成员的邻域。

9. 如权利要求1所述的方法, 其特征在于, 所述确认动作包括:

确认所述另一路由器是否为所述预定邻域的成员, 其中, 所述预定邻域包括具有由所述路由器也是其成员的邻域的邻域管理员信任的邻域管理员的邻域。

10. 如权利要求1所述的方法, 其特征在于, 所述确定动作包括:

在所述至少一个证书的签名上执行签名核实过程。

11. 如权利要求1所述的方法, 其特征在于, 所述确定动作包括:

使用来自与所述另一路由器相关联的另一证书的公钥在所述至少一个证书上执行公钥操作。

12. 如权利要求1所述的方法, 其特征在于, 所述识别动作包括:

识别所述终端设备为附属于所述另一路由器, 其中, 所述另一路由器是一邻域成员。

13. 如权利要求1所述的方法, 其特征在于, 所述识别动作包括:

识别所述终端设备为附属于所述另一路由器, 其中, 所述另一路由器是具有与所述路由器是其成员的邻域的互易识别的邻域的成员。

14. 如权利要求1所述的方法, 其特征在于, 所述识别动作包括:

向所述终端设备授予对无线网状网络的优选访问权限。

15. 如权利要求1所述的方法, 其特征在于, 还包括:

如果所述另一路由器不被确认为所述预定邻域的成员, 或所述至少一个证书不被确定为有效, 则向所述终端设备授予对无线网状网络的标准访问权限。

16. 如权利要求1所述的方法, 其特征在于, 还包括:

向一不同的终端设备签发一不同的证书, 所述不同的证书能够由所述另一路由器识别;

其中, 所述路由器和所述另一路由器是无线网状网络内的对等体。

17. 一种启用终端设备识别的装置, 其特征在于, 所述装置包括:

用于从一终端设备接收至少一个证书的接收器装置, 其中, 所述至少一个证书由所述终端设备所附属的路由器向所述终端设备签发;

用于确认所述路由器是否为预定邻域的成员的确认证置;

用于确定所述至少一个证书是否有效的确定装置; 以及

用于响应于所述确认证置和所述确定装置识别所述终端设备为具有特许状态的识别装置。

18. 如权利要求 17 所述的装置, 其特征在于, 所述识别装置适用于: 如果所述确认装置确认所述路由器是所述预定邻域的成员, 且如果所述确定装置确定所述至少一个证书有效, 则识别所述终端设备为具有所述特许状态。

19. 如权利要求 17 所述的装置, 其特征在于, 所述识别装置包括用于响应于所述确认装置和所述确定装置向所述终端设备授予优选访问权限的装置。

20. 如权利要求 17 所述的装置, 其特征在于, 所述确认装置包括:

用于储存邻域成员的数据结构装置; 以及

用于检查所述路由器是否在所述数据结构装置中枚举的访问装置。

21. 如权利要求 17 所述的装置, 其特征在于, 所述确认装置包括:

用于储存可信邻域管理员的数据结构装置; 以及

用于检查由一成员资格证书所指示的所述路由器的邻域管理员是否在所述数据结构装置中枚举的访问装置。

22. 如权利要求 17 所述的装置, 其特征在于, 所述确定装置包括:

用于在所述至少一个证书的签名上执行签名核实过程的核实装置。

23. 如权利要求 17 所述的装置, 其特征在于, 所述确定装置包括:

用于使用来自与所述终端设备所附属的所述路由器相关联的另一证书的公钥在所述至少一个证书上执行公钥操作的操作装置。

24. 如权利要求 17 所述的装置, 其特征在于, 所述装置包括 (i) 一网状路由器以及 (ii) 一个或多个处理器可访问媒质的至少一个。

25. 如权利要求 17 所述的装置, 其特征在于, 所述装置还包括允许与终端设备和/或其他路由器进行无线通信的无线收发器。

26. 一种网状路由器, 其特征在于, 它包括:

用于通过无线链路与一终端设备建立连接的装置;

用于从所述终端设备接收至少一个证书的装置, 所述至少一个证书具有一签名;

用于在所述至少一个证书的签名上执行签名核实过程的装置;

用于在所述签名核实过程成功的情况下向所述终端设备授予优选访问权限的装置; 以及

用于在所述签名核实过程失败的情况下向所述终端设备授予标准访问权限的装置。

27. 如权利要求 26 所述的网状路由器, 其特征在于, 所述网状路由器还包括:
用于接收向所述终端设备签发所述至少一个证书的另一网状路由器的标识符的装置; 以及

用于对于所述标识符确认签发所述至少一个证书的所述另一网状路由器是否为所述网状路由器也是其成员的邻域的成员的装置。

28. 如权利要求 26 所述的网状路由器, 其特征在于, 所述用于接收的装置包括:

用于接收所述至少一个证书和另一证书的装置; 其中, 所述至少一个证书与所述终端设备相关联, 所述另一证书与另一网状路由器相关联。

29. 如权利要求 26 所述的网状路由器, 其特征在于, 所述用于接收的装置包括:

用于从所述终端设备接收至少一个证书的装置; 其中, 所述至少一个证书与所述终端设备相关联, 并且所述签名是使用与另一网状路由器相关联的私钥的私钥操作的结果。

30. 一种路由器, 包括: 用于与其它网状路由器建立无线网状网络的装置; 用于指定一邻域管理员网状路由器的装置; 用于在一特定网状路由器是所指定的邻域管理员网状路由器的邻域的成员时向一与由所述特定网状路由器签发的特定证书相关联的特定终端设备授予特许状态的装置。

31. 如权利要求 30 所述的网状路由器, 其特征在于, 与所述特定终端设备相关联的所述特定证书包括 (i) 所述特定终端设备的名字、(ii) 与所述特定终端设备相关联的公钥—私钥对的公钥、以及 (iii) 由与所述特定网状路由器相关联的公钥—私钥对的私钥签署的签名。

32. 如权利要求 30 所述的网状路由器, 其特征在于, 所述网状路由器还包括用于向所述特定终端授予关于所述网状路由器形成节点的无线网状网络的优选访问权限的装置。

33. 如权利要求 30 所述的网状路由器, 其特征在于, 所述网状路由器还包括用于识别由对等于所述网状路由器以及预定邻域的成员的所述其它网状路由器向终端设备分层次地签发的证书的装置。

34. 如权利要求 31 所述的网状路由器, 其特征在于, 所述预定邻域包括以下的至少一个: (i) 所指定的邻域管理员网状路由器的邻域, 以及 (ii) 具有一可信

邻域管理员网状路由器的邻域。

35. 如权利要求 30 所述的网状路由器, 其特征在于, 所述网状路由器还包括用于在一给定网状路由器是具有可信邻域管理员网状路由器的邻域的成员时向一与由所述给定的网状路由器签发的给定证书相关联的给定终端设备授予特许状态的装置。

36. 一种启用终端设备识别的方法, 其特征在于, 所述方法包括:

从一终端设备接收至少一个证书, 所述至少一个证书由一特定路由器签发;

确认所述特定路由器是否为预定邻域的成员;

如果所述特定路由器不是所述预定邻域的成员, 则向所述终端设备授予标准访问权限;

如果所述特定路由器是所述预定邻域的成员, 则确定所述至少一个证书是否有效; 以及

如果所述至少一个证书有效, 则识别所述终端设备为具有特许状态。

37. 如权利要求 36 所述的方法, 其特征在于, 它还包括:

由所述特定路由器使用所述特定路由器的私钥签署所述至少一个证书; 以及

由所述特定路由器向所述终端设备签发所述至少一个证书。

38. 如权利要求 36 所述的方法, 其特征在于, 它还包括:

由所述终端设备连接到一邻域路由器; 以及

由所述终端设备向所述邻域路由器提供所述至少一个证书和所述特定路由器的证书;

其中, 所述邻域路由器执行所述接收、所述确认、所述确定和所述识别。

39. 如权利要求 36 所述的方法, 其特征在于, 所述确认包括:

访问一枚举以下的至少一个的数据结构: (i) 作为同一邻域的成员的路由器, 以及 (ii) 可信邻域管理员。

40. 如权利要求 36 所述的方法, 其特征在于, 所述确认包括:

访问一参考一成员资格证书枚举可信邻域管理员的数据结构, 所述成员资格证书表示所述特定路由器是具有给定邻域管理员的邻域的成员。

具有终端设备识别的网状网络

技术领域

本揭示一般涉及网状网络，尤其作为示例而非局限，涉及在给定的网状网络邻域中令附属于一个路由器的终端设备能由其它网状路由器识别。

背景技术

无线网络越来越多地用于语音和数据通信。这一无线通信通过从发送器向接收器传播无线信号来完成。发送器和接收器可组成无线网络的节点。例如，传统的蜂窝无线网络中的节点包括固定的基站和移动站。移动站通过固定的基站访问蜂窝无线网络。基站由设计蜂窝网络的网络服务提供商操纵，并能够控制无线网络的访问和/或采用安全措施。换言之，单个实体操作大规模基础上的多个基站，并因此能提供某一程度的组织和安全措施，以及某一级别的对蜂窝无线网络的整体网络管理。

其它类型的无线网络，如自发无线网络，通常不需要这一大规模的计划、组织或管理。例如，特别（ad hoc）无线网络由相互决定共同加入以形成无线网络的节点的多个设备创建，一般在此之前或之后不需要在多个设备的所有者之间的明确同意。因此，没有控制全局的操作员或其它实体来实施网络访问规则、处理安全问题、监控基于标准的需求或确保一般能接受的无线网络行为。因此，这类特别网络的合法和不合法参与方可粗心地、不加选择地或甚至是恶意地行动，而不服从重要的约束或任何真实的相互作用。

因此，需要一种能够将某一程度的控制和/或责任性引入到自发形成的无线网络中的模式和/或技术。

发明内容

在示例性路由器实现中，一路由器包括：至少一个处理器；以及包括能够由该至少一个处理器执行的处理器可执行指令的一个或多个媒质，该处理器可执行指令适用于指导该路由器执行以下行动：从一终端设备接受至少一个证书，该至少一

个证书由另一路由器签发；确认其它路由器是否为预定邻域的成员；确定该至少一个证书是否有效；如果确认其它路由器为预定邻域的成员，且确定该至少一个证书是有效的，则识别该终端设备为具有特许的状态；该特许状态涉及服务级别。

在示例性网状路由器实现中，一网状路由器能够与其它网状路由器建立无线网状网络，该网状路由器还能够指定一邻域管理员网状路由器；该网状路由器适用于当特定的网状路由器是指定的邻域管理员网状路由器的邻域的成员时，向与由该特定的网状路由器签发的特定证书相关联的特定的终端设备授予特许状态。

在另一示例性网状路由器实现中，一网状路由器被配置成执行以下行动：通过无线链路和一终端设备建立连接；从该终端设备接收至少一个证书，该至少一个证书具有签名；在该至少一个证书的签名上执行签名核实过程；如果签名核实过程成功，则向该终端设备授予优选的访问权限；如果签名核实过程失败，则向该终端设备授予标准访问权限。

本发明将描述其它方法、系统、方式、装置、路由器、设备、媒质、过程、方案等实现。

附图说明

贯穿附图，相同的标号表示相同和/或相应的方面、特征和组件。

图 1 是包括网状路由器层和终端设备层的示例性无线网状网络。

图 2 示出了网状路由器层的示例性公钥基础结构（PKI），其中，每一网状路由器与一证书相关联。

图 3 示出了网状路由器层的 PKI 对分组通信的示例性使用。

图 4 示出了对无线网状网络的示例性邻域建立。

图 5 示出了对于违法网状路由器/证书的示例性排除机制的一个方面。

图 6 示出了对于违法网状路由器/证书的示例性排除机制的另一方面。

图 7 所示是用于在无线网状网络中实现排除能力的示例性方法的流程图。

图 8 示出了对于终端设备的示例性识别机制的一个方面。

图 9 示出了对于终端设备的示例性识别机制的另一方面。

图 10 所示是用于在无线网状网络中实现终端设备识别的示例性方法的流程图。

图 11 示出了对于参与邻域间移动的终端设备的另一示例性识别机制。

图 12 示出了能够（全部或部分地）实现本发明所描述的网状网络的至少一个方面的示例性计算（或通用装置）操作环境。

具体实施方式

图 1 是包括网状路由器层和终端设备层的示例性无线网状网络 100。网状路由器层由网状路由器 102 形成，它创建了无线网状网络 100 的网状路由器网络部分。终端设备层由终端设备 104 形成。终端设备 104 可通过网状路由器网络的一个或多个网状路由器 102 彼此通信。

如图所示，五个网状路由器 102(A)、102(B)、102(C)、102(D)和 102(E)形成了网状路由器网络，以实现多跳（multihop）无线网络的至少一部分。然而，两个或多个网状路由器 102（可能是几十个、几百个或几千个等）可形成网状路由器网络。每一网状路由器 102 能够使用如无线发送器和/或接收器（如，收发器）进行无线通信。

网状路由器 102(A)具有与网状路由器 102(B)的无线链路 108AB，以及与网状路由器 102(D)的无线链路 108AD。网状路由器 102(B)另外还有分别与网状路由器 102(C)和 102(E)的无线链路 108BC 和 108BE。类似地，网状路由器 102(C)也通过无线链路 108CE 与网状路由器 102(E)进行无线通信，网状路由器 102(E)也通过无线链路 108DE 与网状路由器 102(D)进行无线通信。

尽管示出每一网状路由器 102 与一到三个终端设备 104 进行无线通信，然而其每一个可选地与任意数量个终端设备 104 进行通信。网状路由器 102(A)分别通过无线链路 110(A1)和 110(A2)与两个终端设备 104(A1)和 104(A2)进行无线通信。网状路由器 102(B)通过无线链路 110(B1)与一个终端设备 104(B1)进行无线通信。网状路由器 102(C)通过分别通过无线链路 110(C1)和 110(C2)与两个终端设备 104(C1)和 104(C2)进行无线通信。类似地，网状路由器 102(E)具有与三个终端设备 104(E1)、104(E2)和 104(E3)的无线链路 110(E)。网状路由器 102(D)具有分别与两个终端设备 104(D1)和 104(D2)的无线链路 110(D1)和 110(D2)。

在所描述的实现中，从操作观点来看，网状路由器 102 包括一组相对标准的设备。例如，每一网状路由器 102 具有类似的（或甚至是同样）的硬件和/或软件。硬件能够进行无线通信并执行软件（包括固件）。

网状路由器 102 由实体设计和/或制造成具有至少一组基线互操作能力。例如，

从第一版本的硬件和软件观点来看，第一产品可得到同样的网状路由器 102。可用（如，包括硬件的软件）更新可得到提供可任选额外能力的第二及随后的版本。第二产品可得到不同于先前的版本但仍可向后兼容的较新版本的网状路由器 102。简言之，生产网状路由器 102 的实体具有某些关于其硬件和软件组件的确定标准。

相反，终端设备 104 包括一组相对多样的设备，这些设备可具有拥有偶然可操作能力的任意的硬件和软件。终端设备 104 的每一个可以是膝上计算机、移动电话、个人数字助理（PDA）、家庭计算机、娱乐设备或其它设备等等。终端设备 104 可执行各种操作系统、应用程序、管理程序编码等的任一个。尽管有所不同，这些终端设备 104 能够使用接受的协议通过网状路由器 102 访问无线网状网络 100。

生产网状路由器 102 的实体创建它们，以使一稳定且可预测的网状路由器网络被相对自动地建立。当然，无线网状路由器网络的稳定性和可预测性受无线通信的反复无常的行为所限制，这是由于受发送器和接收器之间的距离、干扰、无线媒质的变化等的影响。然而，当网状路由器 102 被激活时，它试图通过与范围内的任何网状路由器 102 通信来加入无线网状网络 100。建立无线网状网络 100 在后文具体参考图 2 和 3 进一步描述。由于生产网状路由器 102 的实体确定其可操作能力、因此可某一程度上减少恶意或不适当的网络行为。

另一方面，终端设备 104 实际上能够执行任意和/或系统的恶意行动，因为其可操作能力不被集中式控制。然而，可在某一程度上限制终端设备 104 的行动，因为终端设备 104 通过网状路由器 102 连接到无线网状网络 100，如由无线链路 110 所示的。应当注意，支配 (i) 用于终端设备 104 到网状路由器 102 的通信的无线链路 110，以及 (ii) 用于网状路由器 102 之间的通信的无线链路 108 的无线访问协议可以相同或不同。

作为示例，如果终端设备 104(A1)试图向终端设备 104(C1)发送通信，则终端设备 104(A1)通过无线链路 110(A1)向网状路由器 102(A)发送通信。网状路由器 102(A)通过网状路由器 102(B)或网状路由器 102(D)和 102(E)将该通信路由到网状路由器 102(C)。网状路由器 102(C)然后通过无线链路 110(C1)将该通信发送到终端设备 104(C1)。

如图所示，终端设备 104(C1)包括资源 106(C1)。尽管仅示出了一个资源 106，然后在无线网状网络 100 中在同一或不同的网状路由器 102 上可存在多个资源

106。例如，每一资源 106 可以是本地服务器或信息储存库（如，用于细分）、因特网接入点（ITap）、多媒体数据集合（如，小团体所感兴趣的）等等。

图 2 示出了网状路由器层上的示例性公钥基础结构（PKI），其中，每一网状路由器 102 与一证书 202 相关联。具体示出了三个示例性网状路由器 102(A)、102(B) 和 102(C)。如图所示，每一网状路由器 102 包括证书 202、公钥（PbK）204、私钥（PvK）206、根钥 208。每一证书 202 包括名字 210、签名 212 和对应的公钥 204。网状路由器“A”102(A)特别地用于描述网状路由器层上的示例性 PKI 的这些通用方面。

在网状路由器 102(A)的所描述的实现中，生产实体与签署密钥（未示出）和根密钥 208 相关联，它们共同形成了用于该生产实体的公钥—私钥对。生产实体通过在名字 A 210(A)上执行操作来签署私钥来签署证书 202(A)，以创建签名 212(A)。证书 202(A)证明公钥 204(A)被绑定到名字 A 210(A)，它是网状路由器 102(A)的名字。例如，名字 A 210(A)可以是网状路由器 102(A)的序列号。

证书 202(A)表示网状路由器 102(A)是由与根钥 208 相关联的生产实体证明的有效网状路由器 102。因此，证书 202(A)表明网状路由器 102(A)应当被允许加入无线网状网络 100（图 1）。除证书 202(A)之外，网状路由器 102(A)包括（如，储存）公钥 204(A)、私钥 206(A)和根钥 208(A)。私钥 206(A)对应于公钥 204(A)，并且与其共同形成了与网状路由器 102(A)相关联的公钥—私钥对。根钥 208(A)是储存在网状路由器 102(A)上的生产实体的根钥 208 的副本。

简言之，每一网状路由器 102 用一关联的证书 202 “出厂”。因此，网状路由器“B”102(B)包括证书 202(B)，网状路由器“C”102(C)包括证书 202(C)。证书 202(B)包括名字 B 210(B)、签名 212(B)和公钥 204(B)，以表明网状路由器 102(B)是来自生产实体的有效网状路由器 102，并且它被绑定到对应于公钥 204(B)的私钥 206(B)。同样，证书 202(C)包括名字 C 210(C)、签名 212(C)和公钥 204(C)，以表明网状路由器 102(C)是来自生产实体的有效网状路由器 102，并且它被绑定到对应于公钥 204(C)的私钥 206(C)。

当网状路由器 102 被激活时，它试图联系其它网状路由器 102 以建立（如，加入）无线网状网络 100。当已被激活的网状路由器 102 联系另一网状路由器 102 时，已被激活的网状路由器 102 和其它网状路由器 102 执行验证/密钥交换协议。这两个网状路由器 102 通过签名核实过程使用根钥 208 交换证书，以向对方表明其

每一个都是来自生产实体的有效网状路由器 102。

网状路由器 102 之一或两者然后使用另一个的公钥 204 以建立仅已被激活的网状路由器 102 和另一网状路由器 102 可共享的机密对称密钥。该机密密钥可通过密钥传输过程或密钥协定过程来建立。共享的机密密钥然后用于彼此验证每一网状路由器 102。共享机密密钥也可用于确保两个网状路由器 102 之间的通信中的信息的保密性。

作为示例，在网状路由器 102(A)被激活之后，它查找并找出在范围内且可能为近邻的其它网状路由器 102。对于网状路由器 102(B)，网状路由器 102(A)和 102(B)交换证书 202(A)和 202(B)。在机密密钥建立过程之后，密钥 AB 214 被创建并在网状路由器 102(A)和 102(B)之间共享。

在网状路由器 102(A)处，密钥 AB 214(A)结合网状路由器“B”储存和/或映射到网状路由器“B”。例如，这些网状路由器—密钥映射可被储存在一数据结构中。在网状路由器 102(B)处，密钥 AB 214(B)结合网状路由器“A”储存和/或映射到网状路由器“A”。密钥 AB 214 可用于向网状路由器 102(B)验证网状路由器 102(A)，并且反之亦然，也可任选地通过加密来确保通信内容的保密性。

同样，网状路由器 102(A)和 102(C)交换证书 202(A)和 202(C)。在机密密钥建立过程之后，密钥 AC 216 被创建并在网状路由器 102(A)和 102(C)之间共享。密钥 AC 216(A)被映射到网状路由器 102(A)处的网状路由器“C”，密钥 AC 216(C)被映射到网状路由器 102(C)处的网状路由器“A”。网状路由器 102(A)和 102(C)之间的这一验证/密钥交换协议和密钥建立过程可在无线网状网络 100 的网状路由器网络部分出现（如，通过诸如网状路由器 102(B)等一个或多个网状路由器 102），即使网状路由器 102(A)和 102(C)不在对方的无线范围内。类似地，在交换了证书 202(B)和 202(C)以及密钥建立过程之后，密钥 BC 218 被创建并在网状路由器 102(B)和 102(C)之间共享。密钥 BC 218(B)被映射到网状路由器 102(B)处的网状路由器“C”，密钥 BC 218(C)被映射到网状路由器 102(C)处的网状路由器“B”。

图 3 示出了网状路由器层上的 PKI 对分组 302 的通信的示例性使用。网状路由器 102(A)正在向预期的接收方网状路由器 102(B)发送分组 302。分组 302 可由网状路由器 102(A)从另一网状路由器 102、从终端设备 104(A)等接收；可最初在网状路由器 102(A)处制定；等等。网状路由器 102(A)用消息验证码 (MAC) 为分组 302 加标签。

由于分组 302 被从网状路由器 102(A)发送到网状路由器 102(B)，网状路由器 102(A)在数据结构（如，表）中查找网状路由器“B”，并确定在它们之间共享的机密密钥。在本示例中，网状路由器 102(A)所检索的共享机密密钥是密钥 AB 214(A)。因此，网状路由器 102(A)使用密钥 AB 214(A)来创建 MAC-AB 302(AB)。MAC-AB 302(AB)然后在发送之前被作为标签加到分组 302 上。在接收分组 302 后，网状路由器 102(B)访问其机密密钥数据结构的网状路由器“A”的条目，以检索被映射到其上的共享机密密钥—密钥 AB 214(B)。网状路由器 102(B)使用密钥 AB 214(B)以及 MAC-AB 302(AB)来验证分组 302 是从网状路由器 102(A)发送的，该网状路由器 102(A)是有效且未泄密的网状路由器 102。

在本示例中，分组 302 最终的目的地是终端设备 104(C1)上的资源 106(C1)，终端设备 104(C1)在网状路由器 102(C)处耦合至无线网状网络 100（并可被认为是其一部分）。具有用于无线网状网络 100 的路由能力的网状路由器 102(B)确定分组 302 要被发送到网状路由器 102(C)。因此，网状路由器 102(B)确定密钥 BC 218(B)被映射到网状路由器“C”，并使用密钥 BC 218(B)来创建 MAC-BC 302(BC)。MAC-BC 302(BC)被作为标签加到分组 302 上，并发送到网状路由器 102(C)。网状路由器 102(C)使用其储存的密钥 BC 218(C)来验证分组 302 是从已知且可信的网状路由器 102(B)接收的。

由此，验证是在逐段转接（hop-by-hop）的基础上执行的。也可在逐段转接的基础上执行通信信息内容的保密（如，通过加密），使得每一通信由每一对相邻的网状路由器 102 的共享机密密钥来加密。可选地，加密可在端对端的基础上执行。例如，由于网状路由器 102(A)和 102(C)建立了共享机密密钥 AC 216，则分组 302 的内容可使用密钥 AC 216 来加密。因此，干预诸如网状路由器 102(B)等网状路由器 102 无法理解分组 302 的内容，因为它用端对端加密在无线网状网络 100 中路由的。

图 4 示出了对无线网状网络 100 的示例性邻域建立。无线网状网络 100 最初可以任意速率不受控制地增长，至一较大的、实际上无边界的尺寸。此外，没有集中式的整体网络管理员来确保网络能继续平滑地其作用。因此，授权网状路由器 102 在任命或指定意见一致的邻域管理员 404 的相对民主的基础上建立准官方邻域。

如图 4 所示，网状路由器 102(A)也建立与网状路由器 102(D)的共享机密密钥

AC 402。密钥 AD 402(A)被映射到网状路由器 102(A)处的网状路由器“D”，密钥 AD 402(D)被映射到网状路由器 102(D)处的网状路由器“A”。每一网状路由器一机密密钥映射数据结构中包括的椭圆表示可能存在额外条目。这一额外的条目可被定向到图 4 所示的其它网状路由器 102 和图 4 中未具体包括的其它网状路由器 102。

在描述的实现中，网状路由器 102(C)将其本身呈现或提供为无线网状网络 100 中用于若干网状路由器 102 的邻域管理员 404。每一网状路由器 102 具有一个人管理员（未示出），如管理最初由生产实体提供并启用的准许能力的界限（有希望地）之内的各自的网状路由器 102 的功能的所有者。

网状路由器 102 的每一个人管理员可选择指定邻域管理员。尽管未在图 4 中示出，邻域管理员可能不物理地位于所管理的邻域中；例如，邻域管理员实际上可以是互联网服务。无论物理位置如何，邻域管理员可被信任来管理对于管理决策的至少一个子集的局部邻域。该管理决策子集包括违法网状路由器 102/证书 202 的排除，如后文具体参考图 5-7 进一步描述的。局部邻域的大小可由邻域管理员的预定（但可改变）数量的中继段来界定。

在图 4 的示例中，网状路由器 102(C)是可用的邻域管理员 404。网状路由器 102(A)、102(B)、102(D)和 102(E)的每一个分别在 406A、406B、406D 和 406E 处将网状路由器“C”指定为邻域管理员。因此，在邻域管理员指定取消之前，网状路由器 102(A)、102(B)、102(D)和 102(E)对管理决策的子集听从网状路由器 102(C)。可任选地，每一相应的个别的个人管理员还可标识相应的网状路由器 102 要向听从的管理决策子集的所选择的之一。

图 5 示出了对于违法网状路由器/证书的示例性排除机制的一个方面。网状路由器 102 可以在规定的网络行为的边界之外恶意并故意地、不经意地并偶然地、其某一组合等行动。在任一情况下，参与所禁止的网络行为的网状路由器 102 可被认为是违法的。因此，与该违法的网状路由器 102 相关联的证书 202 也被认为是违法的。

在描述的实现中，违法行为包括但不限于：(i) 超出允许速率发送；(ii) 试图在给定时间周期内在网状网络上发送超出最大允许数量的分组；(iii) 拒绝与有效网状路由器通信；(iv) 丢弃，包括不转发合法分组；(v) 发动对网络的攻击；(vi) 其组合，等等。可任选地，本地邻域和/或邻域管理员可选择性地确定被承认为违法的活动，尤其是来自生产实体所公布列表的那些活动。例如，违法网状路

由器可使用安全跟踪路由、物理测量、通信流量监控、专用网状管理工具（如，统计分析）、来自其它邻域管理员的通知、其某一组合等等来发现。

在图 5 所示的示例中，网状路由器 102(A)被发现为违法。因此，网状路由器 102(C)如 502(C)处所示的排除证书 202(A)。排除指示与网状路由器“A”相关联和/或被映射到网状路由器“A”。排除指示可包括在储存共享机密密钥的同一数据结构或不同的数据结构中。

生产实体最初签发证书 202(A)以表明网状路由器 102(A)的有效性，并向其绑定其公私钥。然而，证书 202(A)的排除导致网状路由器 102(C) (i) 为无线网状网络 100 目的考虑证书 202(A)无效，以及 (ii) 拒绝从相关联的网状路由器 102(A)路由通信量。

作为邻域管理员 404 的网状路由器 102(C)具有向其邻域中的网状路由器 102 传播排除确定的能力（如果不是责任的话）。网状路由器 102(C)向其邻域中的网状路由器 102 广播排除消息 504。排除消息—网状路由器 A 504 包括网状路由器 202(A)和/或证书 202(A)的标识符。该标识符包括，例如所有或部分证书 202(A)的名字—A 210(A)（图 2），等等。

如图 5 所示，网状路由器 102(B)、102(D)和 102(E)接收排除消息—网状路由器 A 504。可任选地，可向网状路由器 102(A)发送排除消息—网状路由器 A 504* 以向网状路由器 102(A)及其个人管理员通知证书 202(A)的排除以及网状路由器 102(A)的排除。排除消息—网状路由器 A 504 可选地可适用某一带外途径发送到网状路由器 102 和/或其个人管理员。这一途径包括电子邮件、常规邮件、即时消息、电话呼叫等等。

图 6 示出了对于违法的网状路由器 102(A)/证书 202(A)的示例性排除机制的另一方面。如上文参考图 5 所描述的，网状路由器 102(B)、102(D)和 102(E)的每一个从网状路由器 102(C)接收排除消息—网状路由器 A 504。响应于接收排除消息—网状路由器 A 504，网状路由器 102(B)、102(D)和 102(E)的每一个分别将排除指示与 502(B)、502(D)和 502(E)处的网状路由器“A”和/或证书 202(A)相关联和/或将排除指示映射到网状路由器“A”和/或证书 202(A)。

如果在接收排除消息—网状路由器 A 504 之前已建立了与网状路由器 102(A)的共享机密密钥，则该共享机密密钥将在未来被忽略。例如，在排除指示 502(B)和 502(D)上，密钥 AB 214(B)和密钥 AD 402(D)可被呈现为不相关的。可任选地，

如果这些密钥随后不用于例如跟踪目的，则密钥 AB 214(B)和密钥 AD 402(D)可被删除。

如截断无线链路 108AB 和 108AD 所表示的，网状路由器 102(A)被从网状路由器 102(C)为邻域管理员 404 的邻域中排除。例如，如果网状路由器 102(B)接收用 MAC-AB 302(AB)加标签的分组 302，则网状路由器 102(B)拒绝进一步路由分组 302（至另一网状路由器 102 或终端设备 104(B1)）。

另一方面，如果在接收排除消息—网状路由器 A 504 之前尚未建立与网状路由器 102(A)的共享机密密钥，则该排除揭示可被映射到网状路由器 102(A)和/或证书 202(A)的标识符（如果在消息中提供）。例如，该标识符可以是名字—A 210(A)（图 2），或证书 202(A)的全部或部分。如图 6 所示，网状路由器 102(E)的数据结构的条目 602(E)将网状路由器“A”的标识符映射到排除指示 502(E)。如果网状路由器 102(A)随后试图与网状路由器 102(E)通信并提供证书 202(A)作为有效性和可信性的指示，则网状路由器 102(E)拒绝执行与网状路由器 102(A)的验证/密钥交换协议。

图 7 所示是用于在无线网状网络中实现排除能力的示例性方法的流程图 700。流程图 700 包括六个（6）块 702-712。尽管块 702-712 的行动可在其它实现和环境执行，然而图 2-6 特别地用于阐明该方法的某些方面。例如，流程图 700 被划分成两个部分：网状路由器“C” 102(C)和网状路由器“B” 102(B)。如图所示，网状路由器“C” 102(C)执行三个（3）块 702-706 的行动，网状路由器“B” 102(B)执行三个（3）块 708-712 的行动。

在块 702，建立邻域管理员状态。例如，网状路由器“C” 102(C)可提议为邻域管理员 404，并且至少一个其它网状路由器 102 将网状路由器“C” 102(C)指定为邻域管理员 404。例如，有价值的资源 106 的所有者可提议其自己的网状路由器 102 为邻域管理员 404。

在块 704，检测违法网状路由器。例如，可通过上文描述的机制的一个或多个检测网状路由器 102(A)为违法的。在块 706，向邻域网状路由器通知违法的网状路由器。例如，网状路由器“C” 102(C)可如通过在消息中包括证书 202(A)来广播标识网状路由器 202(A)的排除消息—网状路由器 A 504。排除消息—网状路由器 A 504 可通过无线网状网络 100 或通过某一带外途径发送。

对于网状路由器“B” 102(B)，由网状路由器在块 708 指定邻域管理员。例如，

网状路由器“B”102(B)可将网状路由器“C”102(C)指定为其被指定的邻域管理员406B。实行该指定的通信交换向网状路由器“C”102(C)通知网状路由器“B”102(B)已加入其邻域。结果，由网状路由器“C”102(C)提供（如发送）的排除通知被定向到网状路由器“B”102(B)。

在块710，网状路由器从指定的邻域管理员接收违法网状路由器的通知。例如，网状路由器“B”102(B)可从网状路由器“C”102(C)接收标识网状路由器102(A)的证书202(A)的排除消息—网状路由器A504。排除消息—网状路由器A504可由网状路由器“C”102(C)签署，使得网状路由器“B”102(b)可验证排除通知始发于其指定的邻域管理员404。

在块712，网状路由器基于与标识的违法网状路由器相关联的证书排除所标识的违法网状路由器。例如，网状路由器“B”102(B)可拒绝与网状路由器102(A)通信，包括拒绝转发或路由用证书202(A)或与其建立的机密密钥所验证的分组。

证书202(A)由网状路由器102的生产实体向网状路由器102(A)签发。网状路由器102(C)向网状路由器102(B)通知证书202(A)的排除状态。网状路由器102(B)因此基于该通知排除证书202(A)。该排除影响网状路由器102(A)或试图将证书202(A)呈现为有效性和可信性的指示的任一网状路由器102。由此，网状路由器102(B)基于来自网状路由器102(B)指定具有该排除权限的非签发实体，即网状路由器102(C)的通知，有效地将证书202(A)处理为废除和/或无效。

图8示出了对于终端设备104(B1)的示例性识别机制的一个方面。终端设备104(B1)通过无线链路110(B1)与网状路由器102(B)通信。示例性识别机制令终端设备104(B1)能够由给定邻域内的多个网状路由器102特别地识别。例如，终端设备104(B1)附属于作为网状路由器102(C)的邻域的成员的网状路由器102(B)。当终端设备104(B1)移动到作为同一邻域的一部分的另一网状路由器102，如网状路由器102(E)时，该其它网状路由器102将终端设备104(B1)识别为特许的终端设备104。这一移动到网状路由器102(E)并由其识别在后文参考图9更详细描述。

如图8所示，网状路由器102(E)被明确地示出为包括证书202(E)。证书202(E)包括名字—E210(E)、签名212(E)和公钥204(E)。公钥204(E)对应于网状路由器102(E)的私钥206(E)（未明确示出）。证书202在上文已参考图2一般描述。终端设备104(B1)被示出为包括证书202(B1)和证书202(B)（的副本）。

在所描述的实现中，网状路由器102(C)是对给定邻域所建立的邻域管理员

404. 网状路由器 102(C)的邻域包括网状路由器 102(B)、网状路由器 102(E)、网状路由器 102(D) (如, 图 1、4 和 5)、网状路由器 102(A) (如, 如果未排除) 以及未具体示出的可能的其它网状路由器 102。网状路由器 102(C)的邻域的网状路由器 102 在 406 指定网状路由器 “C” 为它们的邻域管理员。

形成邻域是能够实现上文描述的排除能力的一种方法。邻域形成也能够给定邻域的网状路由器 102 之间和之中实现另一种协作。例如, 可由网状路由器 102 向附属于同一邻域的其它网状路由器 102 的终端设备 104 给予特许访问。

在描述的实现中, 终端设备 104 被授予不同特许/优先级别上对无线网状网络 100 (如图 1) 的访问。例如, 可向终端设备 104 授予标准访问权限或优选访问权限。默认访问情形令任一终端设备 104 能够以标准访问级别访问无线网状网络 100。提升的访问情形令附属于给定邻域的特定网状路由器 102 的终端设备 104 能够以优选访问级别访问给定邻域的任一网状路由器 102。至少部分地使用网状路由器层的 PKI 提供终端设备 104 附属于给定邻域的特定网状路由器 102 的证明。

终端设备 104(B1)附属于网状路由器 102(B)。例如, 网状路由器 102(B)的个人管理员可知道或实际上就是终端设备 104(B1)的所有者。因此, 个人管理员可希望向终端设备 104(B1)授予至少通过网状路由器 102(B)对无线网状网络 100 的优选访问权限。为向终端设备 104(B1)提供这一附属的证明, 网状路由器 102(B)向终端设备 104(B1)签发由证书 202(B)签署的证书 202(B1)。

换言之, 向终端设备 104(B1)签发由证书 202(B)签署的证书 202(B1), 并将其与证书 202(B1)相关联。因此, 证书 202(B1)的名字标识终端设备 104(B1)。证书 202(B1)的公钥对应于私钥, 所得的公钥—私钥对与终端设备 104(B1)相关联。证书 202(B1)的签名由私钥操作使用网状路由器 102(B)的私钥 206(B) (图 2) 生成。终端设备 104(B1)可使用证书 202(B1)以及证书 202(B)来向网状路由器 102(B)证明它附属于网状路由器 102(B)。

向终端设备 104 签发的证书, 如证书 202(B1)可用到期日来签发, 因为它们不如由生产实体向网状路由器 102, 如网状路由器 102(B)签发的证书安全。网状路由器 102(B)也可向终端设备 104(B1)委托证书签发权限。终端设备 104(B1)随后可向其它终端设备 104 签发额外的证书 202, 以创建证书链。证书链可用于证明终端设备 104 的附属, 并保护来自非附属网状路由器 102 的识别。

如果给定网状路由器 102 个人管理员认识到由其给定的网状路由器 102 签发

的特定终端设备证书 202 是可疑的（如，由于关联的终端设备 104 被泄密），则个人管理员或其给定的网状路由器 102 请求排除该可疑的终端设备证书 202。该请求对邻域管理员 404 作出，邻域管理员 404 然后可广播标识该可疑终端设备证书 202 的排除通知消息。

终端设备 104(B1)可使用证书 202(B1)以及证书 202(B)来证明它也被授予对网状路由器 102(C)的邻域中的非附属网状路由器 102 的优选访问权限。例如，如果网状路由器 102(B)是非功能性的，和/或如果终端设备 104(B1)移动出网状路由器 102(B)的范围，则可出现这一情况。例如，终端设备 104(B1)可移动到网状路由器 102(E)的范围之内。

图 9 示出了对于终端设备 104(B1)的示例性识别机制的另一方面。与图 8 相比，终端设备 104(B1)移动到网状路由器 102(E)的范围之内。终端设备 104(B1)通过无线链路 110 (E/B1) 与网状路由器 102(E)通信。示例性识别机制令终端设备 104(B1)能够由作为网状路由器 102(C)的邻域的一部分的网状路由器 102(E)特别地识别。

网状路由器 102(E)包括列出或枚举作为邻域成员的网状路由器 102 的数据结构 902。在本示例中，枚举的邻域成员是在 406B、406E 等处将网状路由器 102(C)指定为其邻域管理员的那些网状路由器 102。数据结构 902 列出网状路由器 “B” [102(B)]；网状路由器 “C” [102(C)]，它可被标识为邻域管理员 (NA)；网状路由器 “D” [102(D)]；等等。

数据结构 902 可以是其它数据结构的一部分和/或包括其它数据结构，如储存共享机密密钥的那些数据结构、储存排除指示的那些数据结构等等。尽管未在图 9 中示出，作为网状路由器 102(C)的邻域的成员的每一网状路由器 102（如网状路由器 102(B)）也包括类似于数据结构 902 的数据结构。

在操作中，终端设备 104(B1)和网状路由器 102(E)建立其之间的无线链路 110(E/B1)。终端设备 104(B1)向网状路由器 102(E)提供证书 202(B)和证书 202(B1)。基于证书 202(B)，网状路由器 102(E)访问数据结构 902 以确认命名的网状路由器—网状路由器 102(B)—是否为网状路由器 102(E)所属的网状路由器 102(C)的邻域的成员。如果数据结构 902 包括被排除的网状路由器 102，则网状路由器 102(E)也检查以确保网状路由器 102(B)未被排除。

由于网状路由器 102(B)是网状路由器 102(C)的邻域的成员，并由此在邻域成员数据结构 902 中列出，则网状路由器 102(E)分析证书 202(B)。如果网状路由器

102(E)和网状路由器 102(B)先前已执行了证书/密钥建立过程, 并且如果网状路由器 102(E)储存了证书 202(B)的副本, 则网状路由器 102(E)可仅将储存的证书 202(B)的副本与由终端设备 104(B1)提供的证书 202(B)的副本相比较, 以确保证书 202(B)的合法性。如果不是, 则网状路由器 102(E)使用其储存的根钥 208(E) (未明确示出) 在证书 202(B)上执行签名核实过程, 以确认证书 202(B)。

在网状路由器 102(E)确认网状路由器 102(B)是同一邻域的成员, 且呈现的证书 202(B)合法/有效之后, 网状路由器 102(E)分析证书 202(B1)。分析证书 202(B1)以确保证书 202(B1)由与证书 202(B)相关联的网状路由器 102(B)签发。由此, 网状路由器 102(E)使用证书 202(B)的公钥 204(B)在证书 202(B1)的签名上执行签名核实过程, 以核实证书 202(B1)的签名由邻域成员网状路由器 102(B)的对应的私钥 206(B)签署。

如果该签名核实过程成功, 则网状路由器 102(E)确定证书 202(B1)有效, 且终端设备 104(B1)附属于作为网状路由器 102(C)的邻域的邻域成员的网状路由器 102(B)。因此, 网状路由器 102(E)向终端设备 104(B1)授予优选访问权限而非标准访问权限。网状路由器 102(E)和终端设备 104(B1)也可执行密钥建立过程以建立共享的机密密钥, 用于两个节点之间的验证/加密通信。

特许状态涉及诸如被授予优选访问权限而非仅标准访问权限的服务级别。优选访问和标准访问分别可包括较快的数据率以及较慢的数据率、有保证的吞吐量和最佳成果吞吐量、发送/接收的较高优先级和发送/接收的较低优先级、其某一组合等等。服务级别也可包括两个以上不同的服务/状态级别。

应当注意, 传递的信息量的优选访问和标准访问 (或更多的不同服务级别) 可贯穿无线网状网络 100 通过对通信量加标签来兑现。例如, 路由器 102 可按其个别确定的类别 (如, “标准访问速率” 或 “优选访问速率”) 对其发送的分组加标签。结果, 可贯穿无线网状网络 100 考虑分组中的差异, 而非仅在终端设备 104 将分组引入到无线网状网络 100 且作出分类确定的路由器 102 上考虑。

因此, 该示例性识别机制令附属于特定网状路由器 102(B)的终端设备 104(B1)能够由作为由网状路由器 102(C)管理的同一邻域的成员的其他网状路由器 102 特别地识别。结果, 第一层的对等体 (如, 网状路由器 102) 可分层次地向可由第一层的其他对等体识别的第二不同层 (如, 向终端设备 104) 签发证书 202。

图 10 所示是用于在无线网状网络中实现终端设备识别的示例性方法的流程图

1000。流程图 1000 包括十个 (10) 块 1002-1020。尽管块 1002-1020 的行动可在其它实现和环境中执行,然而图 2、8 和 9 用于特别地阐明本方法的某些方面。例如,流程图 1000 被划分成三个部分:网状路由器“B”102(B)、网状路由器“B”的终端设备 104(B1)和网状路由器“E”102(E)。如图所示,网状路由器“B”102(B)执行块 1002 的行动,网状路由器“B”的终端设备 104(B1)执行五个 (5) 块 1004-1012 的行动,网状路由器“E”102(E)执行四个 (4) 块 1014-1020 的行动。

在块 1004,终端设备与所附属的网状路由器连接。例如,终端设备 104(B1)可通过无线链路 110(B1)与网状路由器 102(B)连接。如果网状路由器 102(B)的个人管理员知道或信任终端设备 104(B1)的所有者/操作者,则终端设备 104(B1)可附属于网状路由器 102(B)。

在块 1002,所附属的网状路由器向终端设备签发终端设备证书,它由所附属的网状路由器的网状路由器证书签署。例如,网状路由器 102(B)可使用其关联的证书 202(B)来签署向终端设备 104(B1)签发的证书 202(B1)。两个证书—证书 202(B)和 202(B1)都可通过无线链路 110(B1)从网状路由器 102(B)提供给终端设备 104(B1)。

在块 1006,终端设备证书和网状路由器证书由终端设备储存。例如,证书 202(B1)和证书 202(B)可由终端设备 104(B1)储存。在块 1008,终端设备移动到一个新位置。例如,在从网状路由器 102(B)断开之后,终端设备 104(B1)可从网状路由器 102(B)的范围内移动到网状路由器 102(E)的范围内。如星号 (*) 所示的,这是可任选的行动,因为终端设备 104(B1)可从单个位置同时位于网状路由器 102(B)和 102(E)的范围之内,并能够无线地与它们通信。

在块 1010,终端设备与邻域(但非附属)网状路由器连接。例如,终端设备 104(B1)可通过无线链路 110(E/B1)与网状路由器 102(E)连接。网状路由器 102(E)是与终端设备 104(B1)所附属的网状路由器 102(B)的同一邻域的成员。换言之,网状路由器 102(B)和网状路由器 102(E)指定了网状路由器 102(C)中的同一邻域管理员 404。

在块 1012,终端设备提供终端设备证书以及用于向非附属邻域网状路由器签署终端设备证书的网状路由器证书。例如,终端设备 104(B1)可向网状路由器 102(E)提供证书 202(B1)和证书 202(B)。可选地,如果网状路由器 102(E)储存了其邻域中每一网状路由器 102 的关联的证书 202 的副本,则终端设备 104(B1)可仅向网状路

由器 102(E)发送证书 202(B1)和网状路由器 102(B)的标识符,该标识符可包括在证书 202(B1)中。

在块 1014,邻域网状路由器确认与网状路由器证书相关联的网状路由器是否为邻域成员。例如,网状路由器 102(E)可访问邻域成员数据结构 902 以确定是否存在定向到/包括网状路由器 102(B)的实体。如果没有,则在块 1020,邻域网状路由器授予终端设备标准访问权限。例如,网状路由器 102(E)可向终端设备 104(B1)授予标准访问权限。

另一方面,如果邻域网状路由器确实确认了与网状路由器证书相关联的网状路由器为邻域成员(在块 1014),则方法继续到块 1016。在块 1016,邻域网状路由器确定终端设备是否有效。例如,网状路由器 102(E)可能结合对证书 202(B)的分析来分析证书 202(B1),以确定证书 202(B1)是否由合法网状路由器 102(B)的私钥 206(B)签发。该分析可涉及证书 202(B1)的签名上的签名核实过程的至少一个公钥 204(B)操作。

如果未确定终端设备证书有效(在块 1016),则在块 1020 由邻域网状路由器向终端设备授予标准访问权限。另一方面,如果邻域网状路由器确实确定终端设备证书有效(在块 1016),则方法继续到块 1018。在块 1018,邻域网状路由器向终端设备授予优选访问权限。例如,网状路由器 102(E)可向终端设备 104(B1)授予优选访问权限。由此,该示例性方法实现了无线网状网络中的终端设备识别,使得终端设备可从作为该终端设备所附属的网状路由器的同一邻域的成员的非附属网状路由器接收特许的访问。

图 11 示出了对于参与邻域间移动的终端设备 104(B1)的另一示例性识别机制。终端设备 104(B1)可从具有所附属的网状路由器 102(B)作为其成员的第一邻域移动到第二邻域。采用图 11 所示的这一其它示例性识别机制,终端设备 104(B1)可由作为第二邻域的成员的网状路由器 102 特别地识别。

如图所示,在 404C 指示网状路由器“C”102(C)为第一邻域的邻域管理员。网状路由器 102(B)是网状路由器 102(C)的第一邻域的成员。在 404G 指示网状路由器“G”102(G)为另一第二领域的领域管理员。网状路由器 102(F)是网状路由器 102(G)的第二邻域的成员。网状路由器 102(F)在 406F 指定网状路由器“G”为邻域管理员。网状路由器 102(F)与证书 202(F)相关联,网状路由器 102(G)与证书 202(G)相关联。

在所描述的实现中,网状路由器 102(C)和 102(G)各自的邻域管理员 404C 和 404G 同意互易识别 1102。换言之,网状路由器 102(C)和网状路由器 102(G)的每一个同意特别地识别附属于彼此的成员网状路由器 102 的终端设备 104。可选地,识别协定可以是单边的而非互易或双边的。

网状路由器 102(G)通过无线链路 108FG 与网状路由器 102(F)通信。通过无线链路 108FG,网状路由器 102(G)向网状路由器 102(F)发送可信网状路由器“C”消息 1104。换言之,网状路由器 102(G)表明网状路由器 102(C)操作较好和/或可信的邻域。网状路由器 102(G)也指令网状路由器 102(F)特别地识别附属于网状路由器 102(C)的邻域的网状路由器 102 的终端设备 104,以履行作为网状路由器 102(G)的邻域中正确的网状路由器 102 的义务。

网状路由器 102(F)包括列出或枚举将被信任的邻域管理员的数据结构 1106。响应于可信网状路由器“C”消息 1104,网状路由器 102(F)添加包括/标识网状路由器“C”[102(C)]的条目。数据结构 1106 也可包括由椭圆指示的额外条目。此外,可信邻域管理员数据结构 1106 也可与其它数据结构相组合,包括本发明中另外描述的数据结构。尽管未在图 11 中示出,网状路由器 102(B)也包括当识别协定 1102 互易时枚举网状路由器“G”[102(G)]的类似的可信邻域管理员数据结构 1106。

在描述的实现中,在时刻 $T=X$,终端设备 104(B1)通过无线链路 110(B1)与网状路由器 102(B)通信。终端设备 104(B1)与由证书 202(B)签署的证书 202(B1)相关联并包括该证书,它也由终端设备 104(B1)储存。网状路由器 102(B)也向终端设备 104(B1)提供由证书 202(C)签署的成员资格证书 202(CB)。成员资格证书 202(CB)和证书 202(C)从网状路由器 102(C)提供到网状路由器 102(B)。

数字证书也可用于证明实体具有特定属性。表示实体具有某一属性的证书被称为属性证书。当属性是成员资格时,属性证书可用术语成员资格证书来称呼。成员资格证书 202(CB)表示网状路由器 102(B)是网状路由器 102(C)的邻域的成员。成员资格证书 202(CB)由作为邻域管理员 404C 的网状路由器 102(C)用证书 202(C)来签署。

在时刻 $T=X+1$,终端设备 104(B1)从网状路由器 102(C)的邻域的网状路由器 102(B)的范围之内移动到网状路由器 102(G)的邻域的网状路由器 102(F)的范围之内。网状路由器 102(F)和终端设备 104(B1)通过无线链路 110(F/B1)建立连接。通过无线链路 110(F/B1),终端设备 104(B1)向网状路由器 102(F)发送证书 202(B1)、证

书 202(B)、成员资格证书 202(CB)和证书 202(C)。在替换的实现中,成员资格证书 202(CB)和/或证书 202(C)可从网状路由器 102(G)提供到网状路由器 102(F)。

网状路由器 102(F)使用证书 202(B1)和证书 202(B)通过签名核实过程来确保终端设备 104(B1)是实际上附属于网状路由器 102(B)的有效网状路由器 102。网状路由器 102(F)使用成员资格证书 202(CB)和证书 202(C)来确保网状路由器 102(B)实际上是网状路由器 102(C)的邻域的成员。

在访问可信邻域管理员数据结构 1106 并定位了包括/定向到网状路由器 “C” [102(C)]的条目之后,网状路由器 102(F)确定附属于作为网状路由器 102(C)的邻域的成员的网状路由器 102 的终端设备 104 将被授予专门的识别。因此,网状路由器 102(F)向终端设备 104(B1)A 授予特殊识别。例如,终端设备 104(B1)可被授予优选的访问状态。

参考图 8-10,应当注意,属性证书 202 也可用于邻域内移动实现来替代邻域成员数据结构 902 方法。例如,在图 9 的移动的这一实现中,终端设备 104(B1)除证书 202(B1)和证书 202(B)之外向网状路由器 102(E)发送成员资格属性证书 202(CB) (并可能发送证书 202(C))。网状路由器 102(E)然后分析证书 202 来替代访问 (或储存) 数据结构 902。

图 1-11 的路由器、设备、行动、方面、特征、组件等在被划分成多个块的图中示出。然而,描述和/或示出图 1-11 的顺序、互连、相互关系、布局等并不意味着被解释为局限,任意数量的块可以实现用于网状网络实现的一个或多个系统、方法、设备、过程、媒体、应用编程接口 (API)、装置、排列等的方式被修改、组合、重排列、增加、省略等等。此外,尽管本发明的描述包括对具体实现 (以及下文图 12 的示例性操作环境) 的参考,然而所示出和/或所描述的实现可以任一合适的硬件、软件、固件或其组合,并使用任一合适的设备、体系结构、编码范例、通信途径、无线空中接口模式等来实现。

图 12 示出了能够 (完全或部分地) 实现用于本发明所描述的网状网络实现的至少一个系统、路由器、设备、装置、组件、排列、协议、途径、方法、过程、媒体、API、其某一组合等的示例性计算 (或通用设备) 操作环境 1200。操作环境 1200 可在下文描述的计算机和网络体系结构中使用。

示例性操作环境 1200 仅为环境的一个示例,并非暗示对适用的设备 (包括计算机、诸如路由器或终端设备等网络节点、娱乐设备、移动设备、一般电子设备等)

体系结构的使用范围或功能的局限。也不应将操作环境 1200（或其设备）解释为对图 12 所示的任一组件或其组合具有依赖或需求。

另外，网状网络实现可用众多其它通用或专用装置（包括计算或无线系统）环境或配置来实现。适合适用的众所周知的装置、系统、环境和/或配置的示例包括但不限于，个人计算机、服务器计算机、薄客户机、厚客户机、个人数字助理(PDA)或移动电话、手表、手持式或膝上设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费者电子产品、视频游戏机、游戏控制台、便携式或手持式游戏单元、网络 PC、小型机、大型机、有线或无线网络节点（包括通用或专用路由器）、包括上述系统或设备的任一个的分布式或多处理计算环境、其某一组合等等。

对网状网络的实现可在处理器可执行指令的一般上下文中描述。一般而言，处理器可执行指令包括例程、程序、模块、协议、对象、接口、组件、数据结构等，它们执行和/或启用特定的任务和/或实现特定的抽象数据类型。本发明的某些实施例中所描述的网状网络实现也可在分布式处理环境中实现，其中，任务由通过通信链路和/或网络连接的远程链接处理设备执行。尤其但非穷尽地在分布式计算环境中，处理器可执行指令可位于单独的存储媒质上、由不同的处理器执行、和/或通过传输媒质传播。

示例性操作环境 1200 包括计算机 1202 形式的通用计算装置，它可包括具有计算/处理能力的任一（如，电子）设备。计算机 1202 的组件可包括但不限于，一个或多个处理器或处理单元 1204、系统存储器 1206 以及将包括处理器 1204 的各种系统组件耦合至系统存储器 1206 的系统总线 1208。

处理器 1204 不受形成它们的材料或本发明所采用的处理机制的限制。例如，处理器 1204 可包括半导体和/或晶体管（如，电子集成电路（IC））。在这一上下文中，处理器可执行指令可以是电可执行指令。可选地，处理器 1204 以及计算机 1202 的机制可包括但不限于，量子计算、光学计算、机械计算（如，使用纳米技术）等等。

系统总线 1208 表示众多类型的有线或无线总线结构的任一种的一个或多个，包括存储器总线或存储器控制器、点对点链接、交换光纤、外围设备总线、加速图形端口以及使用各种总线体系结构的任一种的处理器或局部总线。作为示例，这类体系机构可包括工业标准体系结构（ISA）总线、微通道体系结构（MCA）总线、增强 ISA（EISA）总线、视频电子技术标准协会（VESA）局部总线、外围部件互

连 (PCI) 总线 (也称为 Mezzanine 总线)、其某一组合等等。

计算机 1202 通常包括各种处理器可访问媒质。这类媒质可以是可由计算机 1202 或另一 (如, 电子) 设备访问的任一可用媒质, 并包括易失和非易失媒质、可移动和不可移动媒质、以及存储和传输媒质。

系统存储器 1206 包括易失存储器 (如, 随机存取存储器 (RAM) 1240) 和/或非易失存储器 (如, 只读存储器 (ROM) 1212) 形式的处理器可访问存储媒质。基本输入/输出系统 (BIOS) 1214 包含如在启动时帮助在计算机 1202 内的元件之间传输信息的基本例程, 通常储存在 ROM 1212 中。RAM 1210 通常包含处理单元 1204 立即可访问或者当前正在操作的数据和/或程序模块。

计算机 1202 也可包括其它可移动/不可移动和/或易失/非易失存储媒质。作为示例, 图 12 示出了用于 (通常) 对不可移动、非易失磁媒质 (未单独示出) 进行读写的硬盘驱动器或盘驱动器阵列 1216; (通常) 用于对可移动、非易失磁盘 1220 (如, “软盘”) 进行读写的磁盘驱动器 1218; 以及 (通常) 用于对诸如 CD、DVD 或其它光媒质等可移动、非易失光盘 1224 进行读写的光盘驱动器 1222。硬盘驱动器 1216、磁盘驱动器 1218 和光盘驱动器 1222 的每一个都通过一个或多个存储媒质接口 1226 连接到系统总线 1208。可选地, 硬盘驱动器 1216、磁盘驱动器 1218 和光盘驱动器 1222 可通过一个或多个其它单独或组合的接口 (未示出) 连接到系统总线 1208。

盘驱动器及其关联的处理器可访问媒质为计算机 1202 提供了诸如数据结构、程序模块和其它数据等处理器可执行指令的非易失存储。尽管示例性计算机 1202 示出了硬盘 1216、可移动磁盘 1220 和可移动光盘 1224, 可以理解, 其它类型的处理器可访问媒质可储存可由设备访问的指令, 如磁带盒或其它磁存储设备、闪存卡、光盘 (CD)、数字多功能盘 (DVD) 或其它光存储、RAM、ROM、电可擦除可编程只读存储器 (EEPROM) 等等。这类媒质也可包括所谓的专用或硬布线 IC 芯片。换言之, 任一处理器可访问媒质可用于实现示例性操作环境 1200 的存储媒质。

任意数量的程序模块 (或其它单元或指令/代码集) 可储存在硬盘 1216、磁盘 1220、光盘 1224、ROM 1212 和/或 RAM 1240 中, 作为一般的示例包括操作系统 1228、一个或多个应用程序 230、其它程序模块 1232 和程序数据 1234。这类指令可包括用于加入并参与用于实现将 PKI 扩展到终端设备层、映射数据结构等排除机制、模块的无线网状网络、模块的模块。

用户可通过输入设备,如键盘 1236 和定位设备 1238 (如,“鼠标”)向计算机 1202 输入命令和/或信息。其它输入设备 1240 (未具体示出)可包括麦克风、操纵杆、游戏垫、圆盘式卫星天线、串行端口、扫描仪和/或其类似物。这些和其它输入设备通过耦合至系统总线 1208 的输入/输出接口 1242 连接到处理单元 1204。然而,输入设备和/或输出设备可替代地通过其它接口和总线结构连接,如并行端口、游戏端口、通用串行总线(USB)端口、红外端口、IEEE 1394 (“火线”)接口、IEEE 802.11 或其它通用无线接口、Bluetooth® (蓝牙)接口等等。

监视器/视图屏幕 1244 或其它类型的显示设备也通过接口,如视频适配器 1246 连接到系统总线 1208。视频适配器 1246 (或另一组件)可以是或可包括用于处理图形密集型计算和用于处理高要求的显示需求的图形卡。通常,图形卡包括图形处理单元(GPU)、视频 RAM (VRAM) 等,以方便图形的快速显示和图形操作的执行。除监视器 1244 之外,其它数据外围设备可包括诸如扬声器(未示出)和打印机 1248 等组件,可通过输入/输出接口 1242 连接到计算机 1202。

计算机 1202 可以在使用到一个或多个远程计算机,如远程计算装置 1250 的逻辑连接的网络化环境中操作。作为示例,远程计算装置 1250 可以是个人计算机、便携式计算机(如,膝上计算机、图形输入板计算机、PDA、移动站等等)、掌上或袖珍计算机、手表、游戏设备、服务器、路由器、网络计算机、对等设备、另一网络节点、或上文列出的另一设备类型等等。然而,示出远程计算装置 1250 为便携式计算机,它可包括本发明参考计算机 1202 所描述的许多或所有元件和特征。

计算机 1202 和远程计算机 1250 之间的逻辑连接被描述为局域网(LAN)1252 和一般广域网(WAN)1254。这类网络环境常见于办公室、企业范围计算机网络、内联网、因特网、固定和移动电话网络、特别(ad-hoc)和基础结构无线网络、其它无线网络、游戏网络、其某一组合等等。这类网络和通信连接是传输媒质的示例。

当在 LAN 网络环境中实现时,计算机 1202 通常通过网络接口或适配器 1256 连接到 LAN 1252。当在 WAN 网络环境中实现时,计算机 1202 通常包括调制解调器 1208 或其它组件,用于通过 WAN 1254 建立通信。调制解调器 1258 可以对计算机 1202 是内置或外置的,可通过输入/输出接口 1242 或任一其它合适的机制连接到系统总线 1208。可以理解,所示的网络连接是示例性的,也可采用用于在计算机 1202 和 1250 之间建立通信链路,包括无线链路的其它方式。

在诸如用操作系统 1200 所示出的网络化环境中,相对计算机 1202 所描述的

程序模块或其它指令或其部分可完全或部分地储存在远程媒质存储设备中。作为示例，远程应用程序 1260 驻留在远程计算机 1250 的存储器组件中，但也可通过计算机 1202 使用或访问。同样，为说明目的，应用程序 1230 和其它处理器可执行指令，如操作系统 1228 被示出为离散的块，但是可以认识到，这类程序、组件和其它指令在不同的时刻驻留在计算装置 1202（和/或远程计算装置 1250）的不同存储组件中，并由计算机 1202 的处理器 1204（和/或远程计算装置 1250 的处理器）执行。

尽管以对结构、逻辑、算法和功能特征和/或图表专用的语言描述了系统、媒体、路由器、设备、方法、过程、装置、技术、API、模式、途径、程序、排列和其它实现，应当理解，所附权利要求书中所定义的本发明不必要限于所描述的具体特征或图表。相反，揭示了具体特征和图表作为实现本发明的示例性形式。

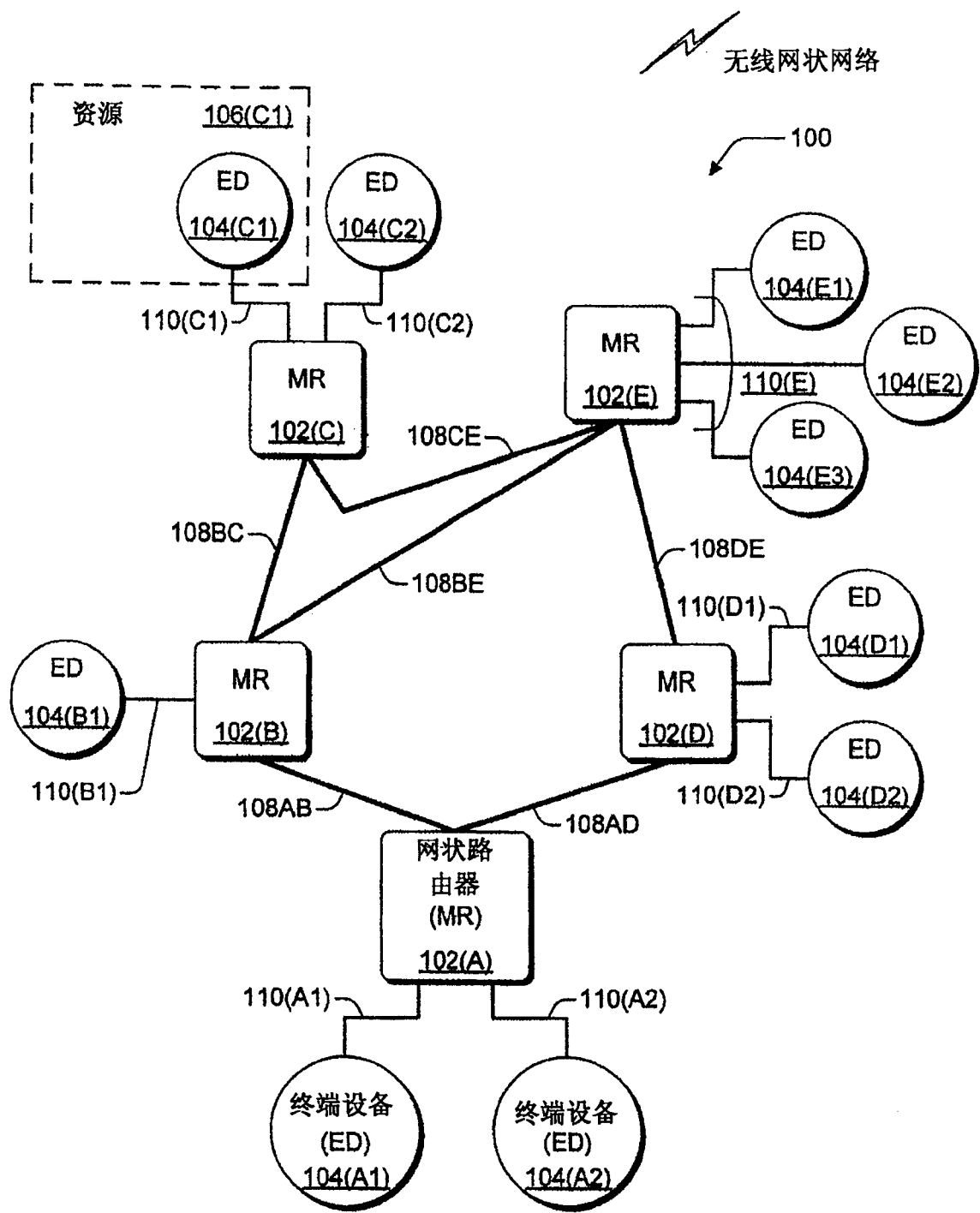


图 1

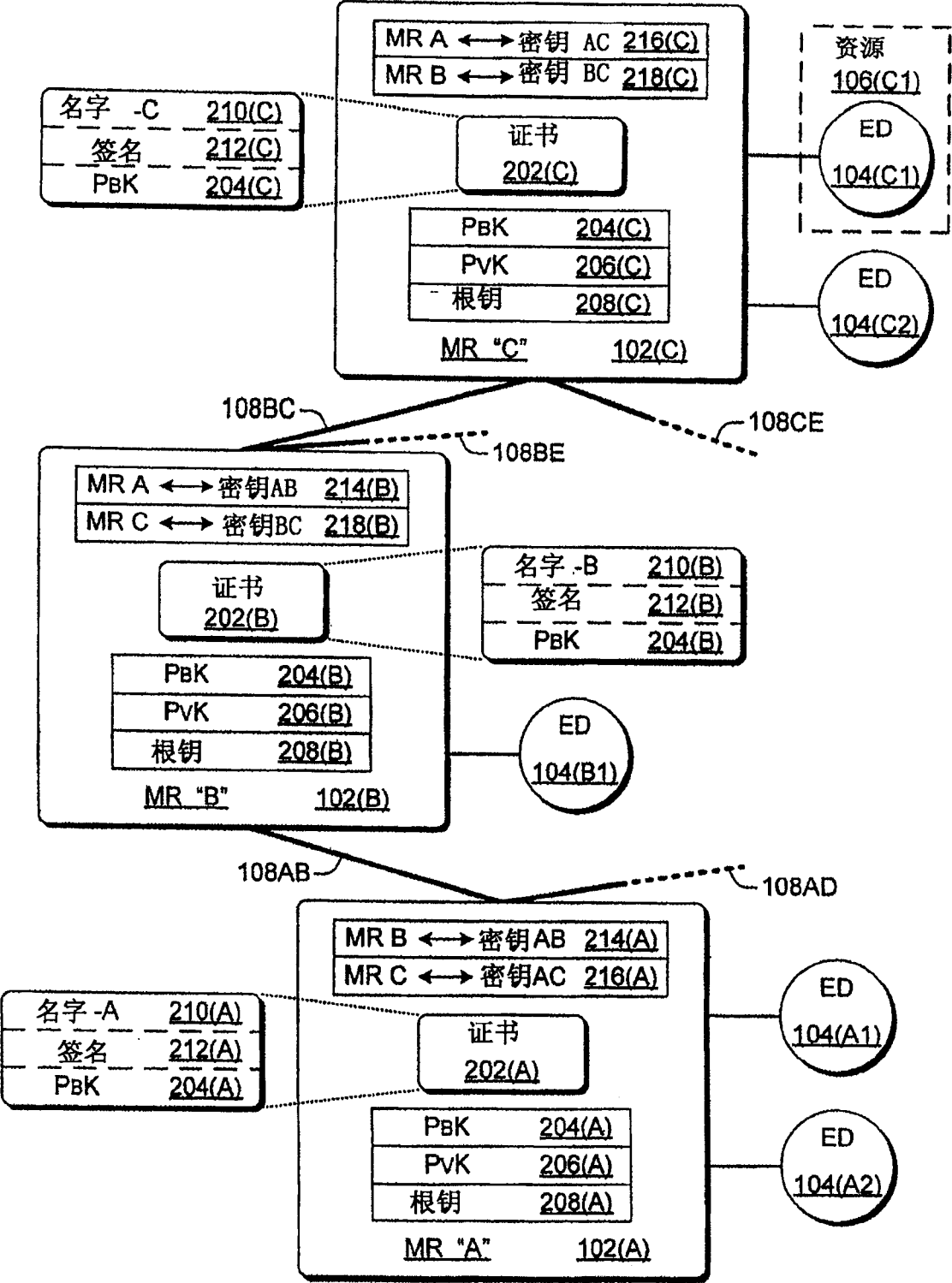


图 2

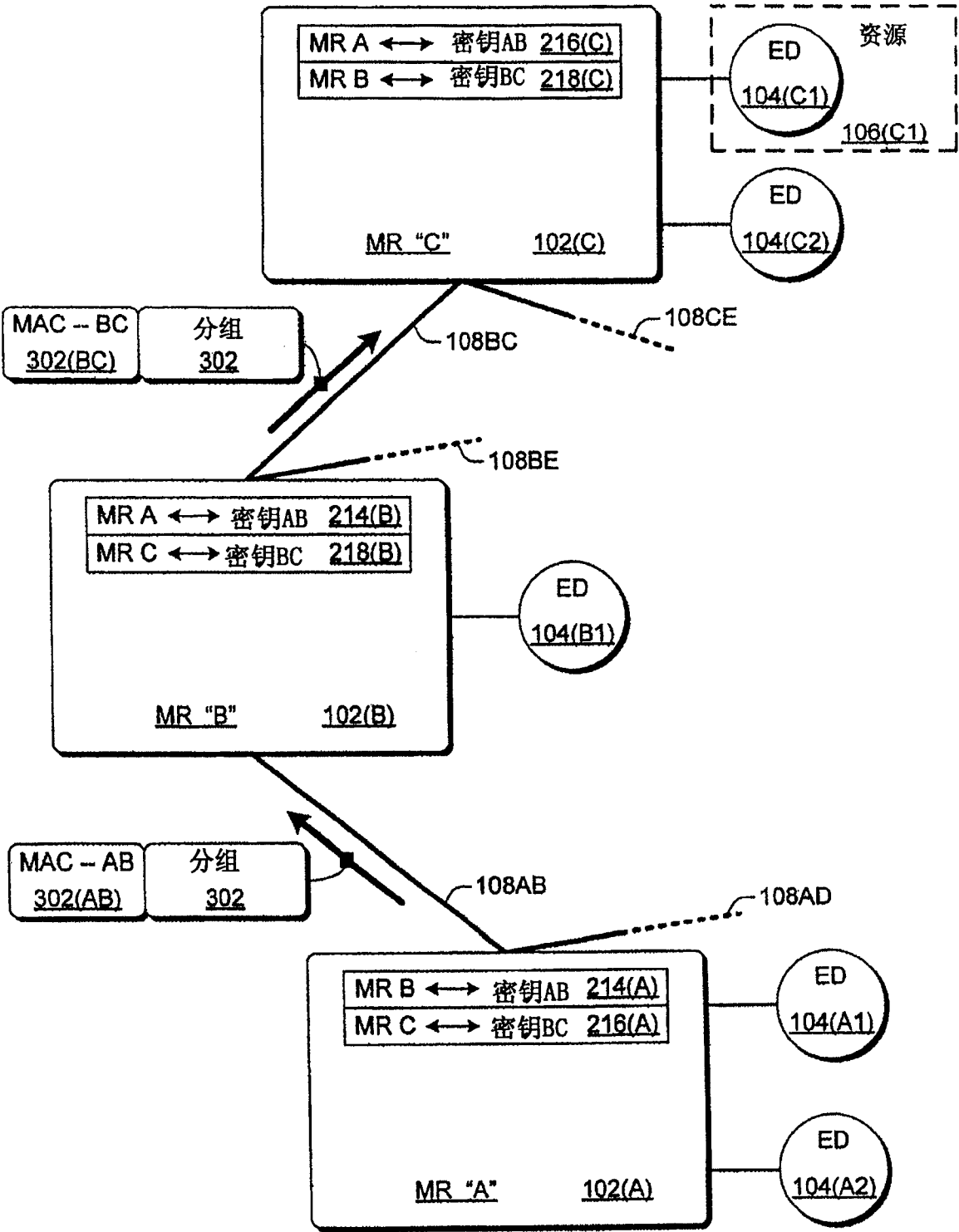


图 3

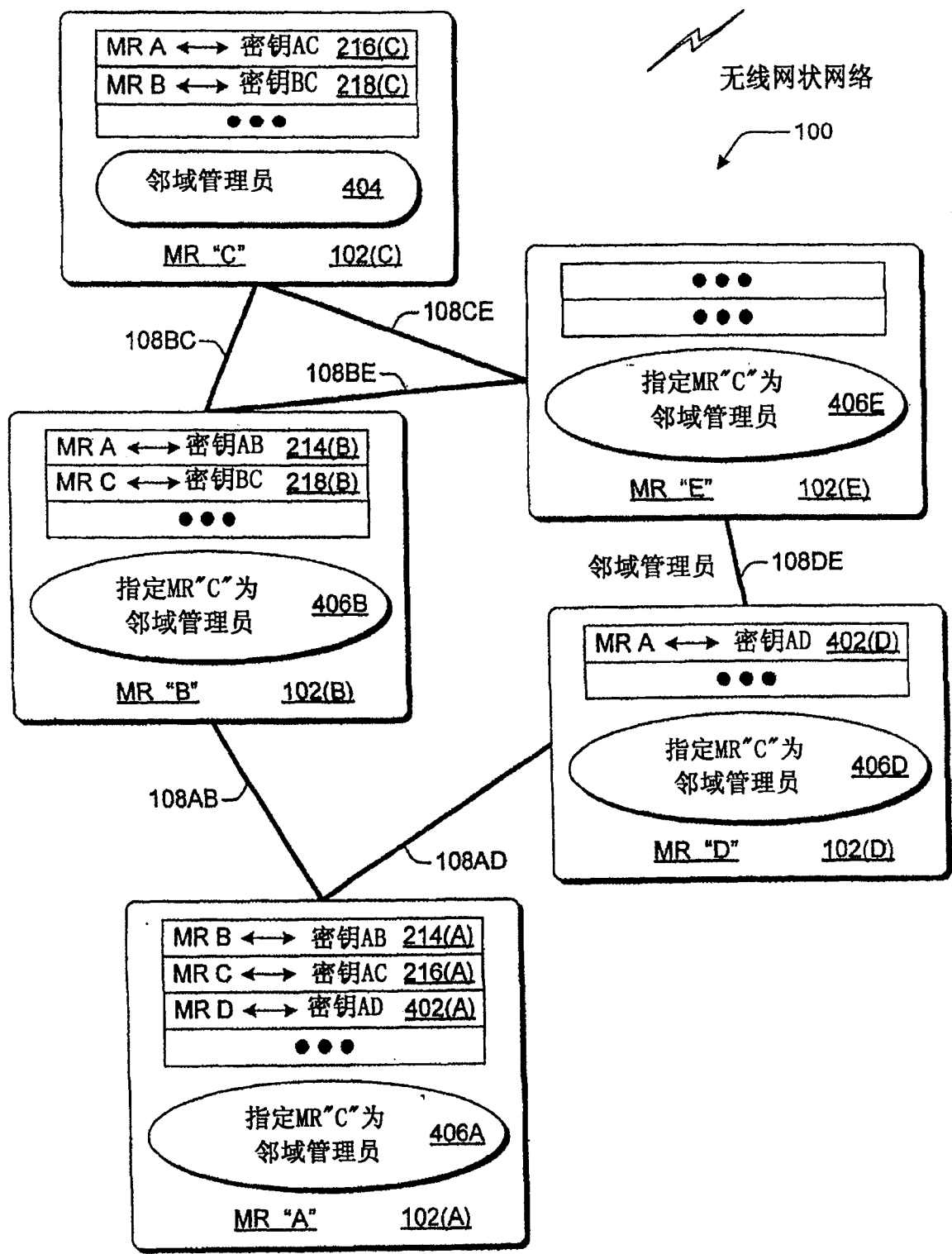


图 4

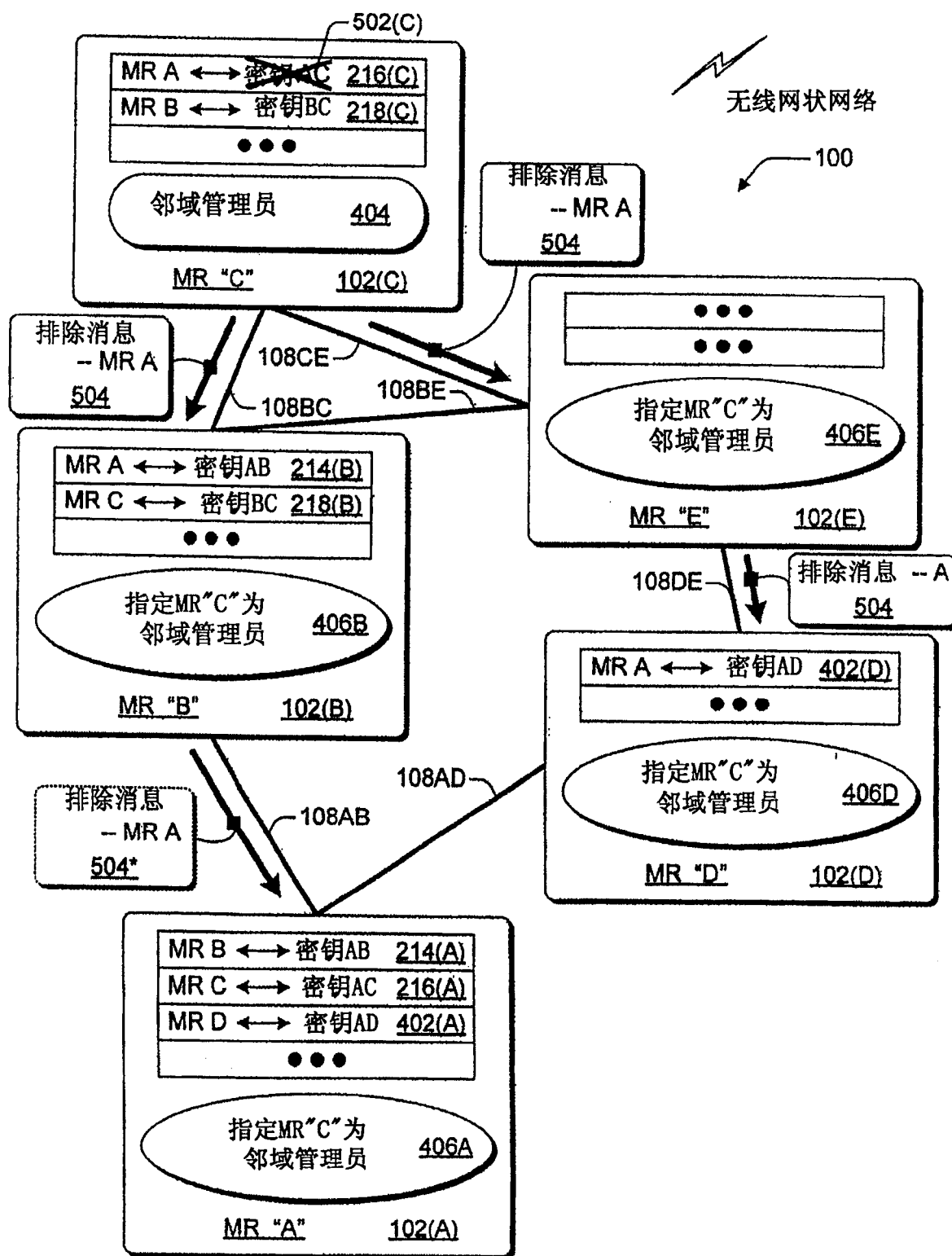


图 5

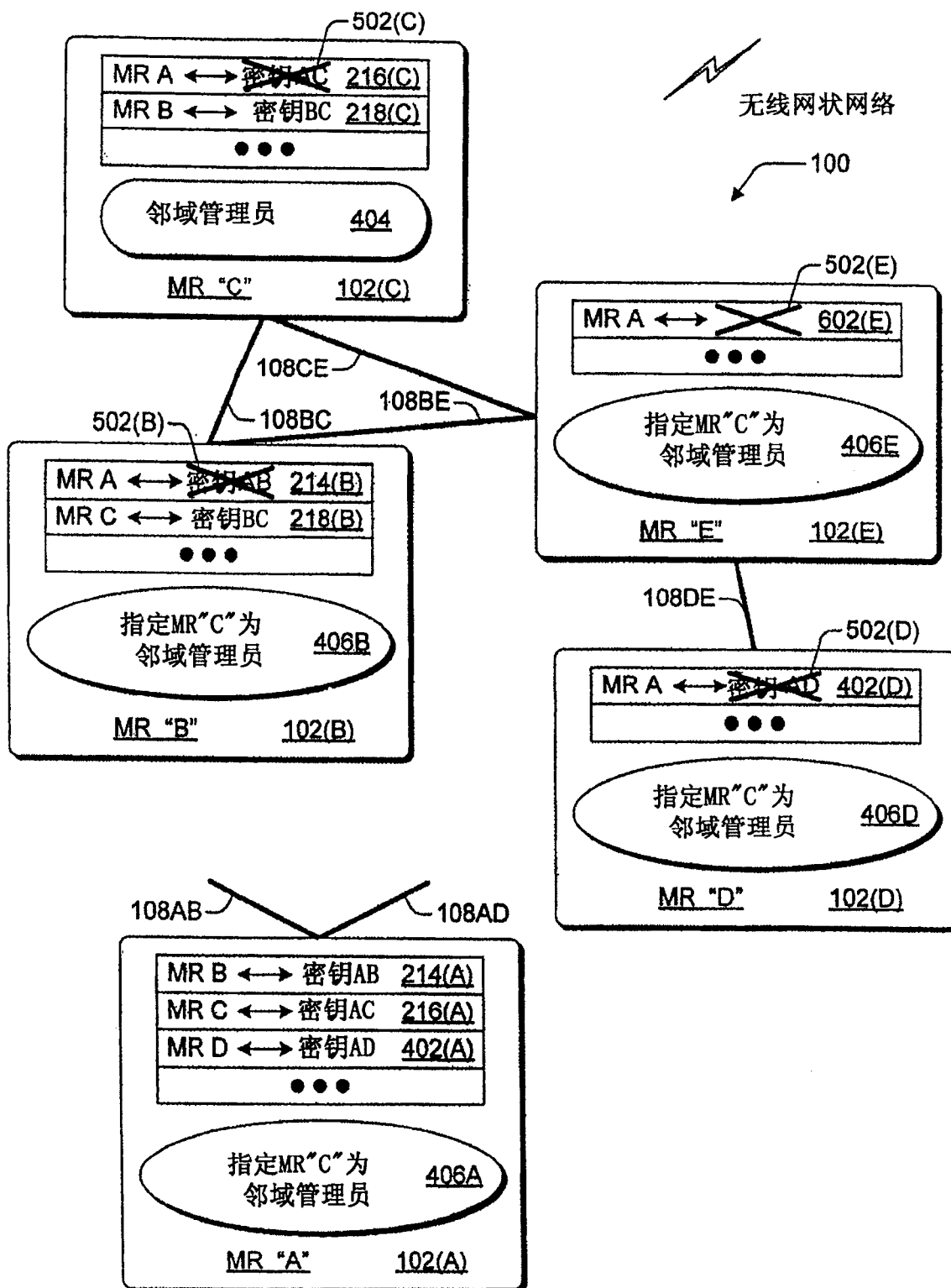


图 6

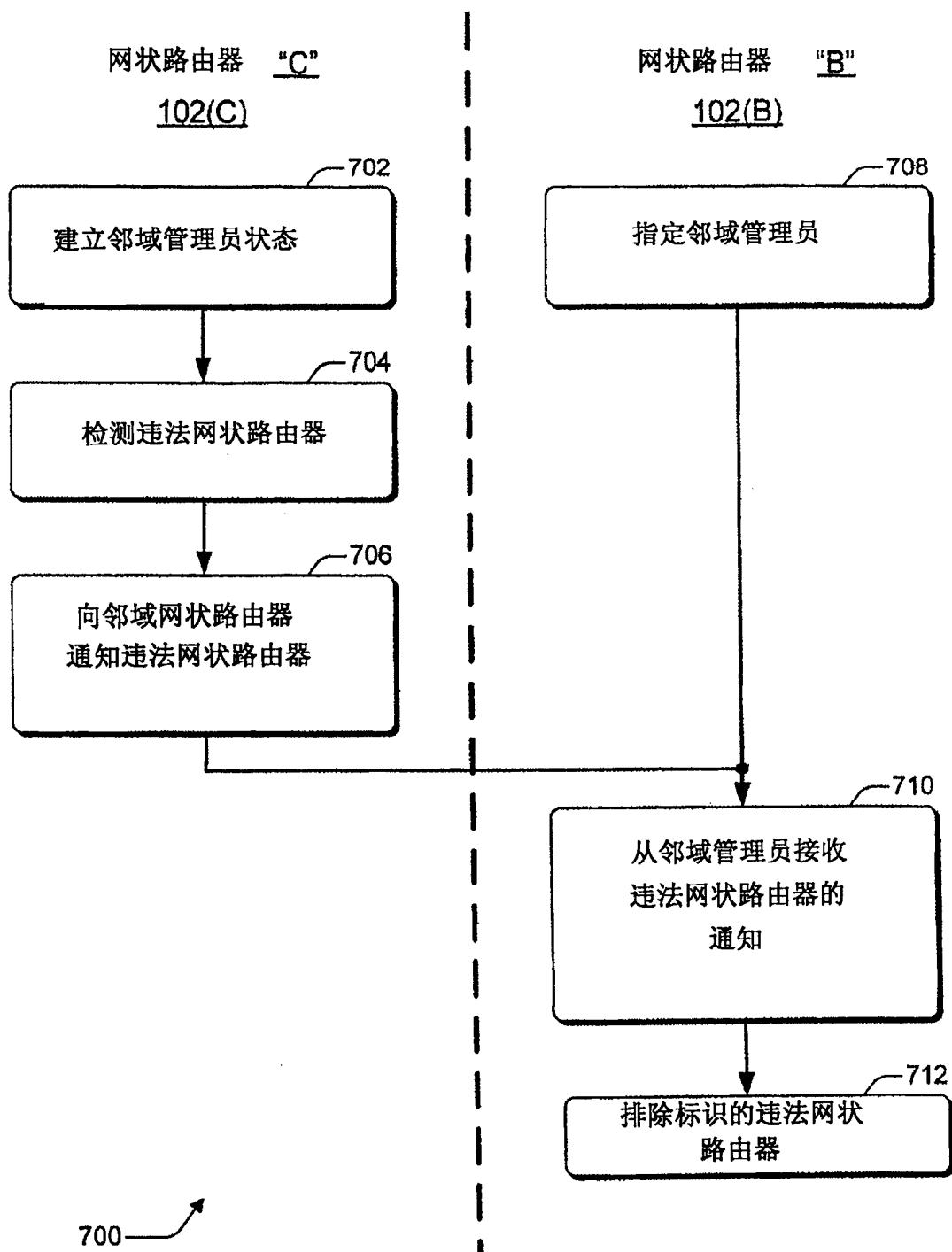


图 7

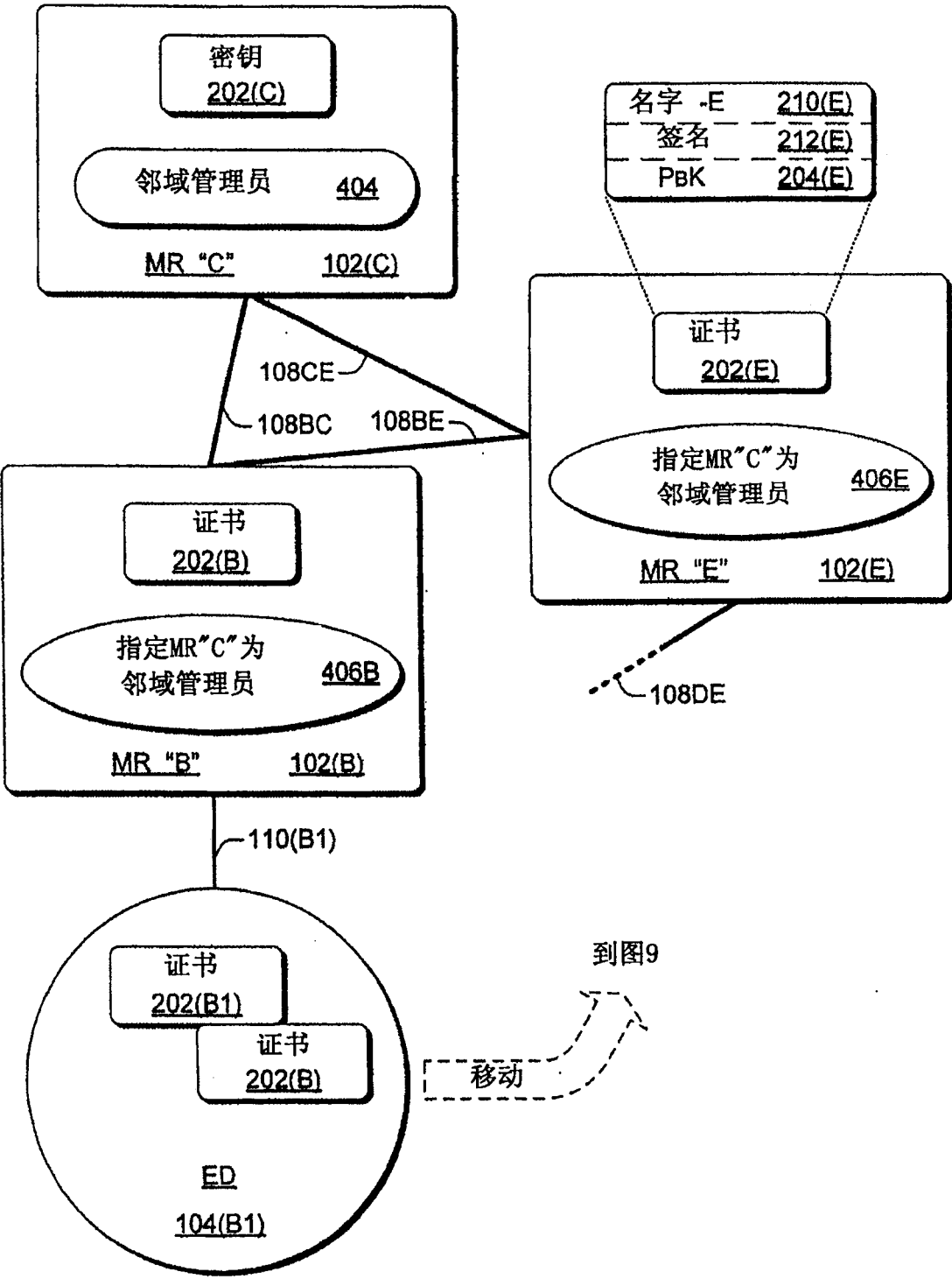
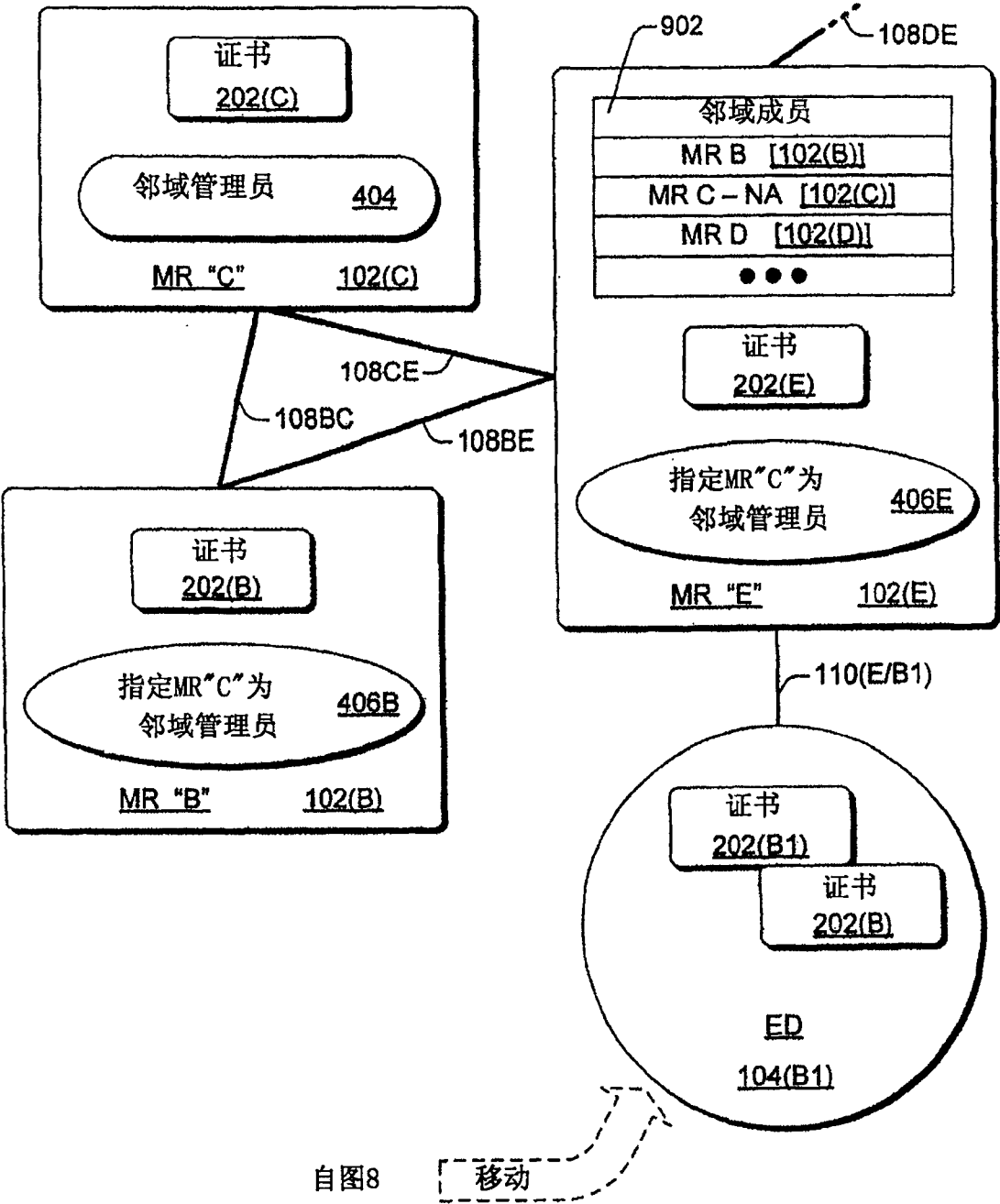


图 8



自图8

移动

图 9

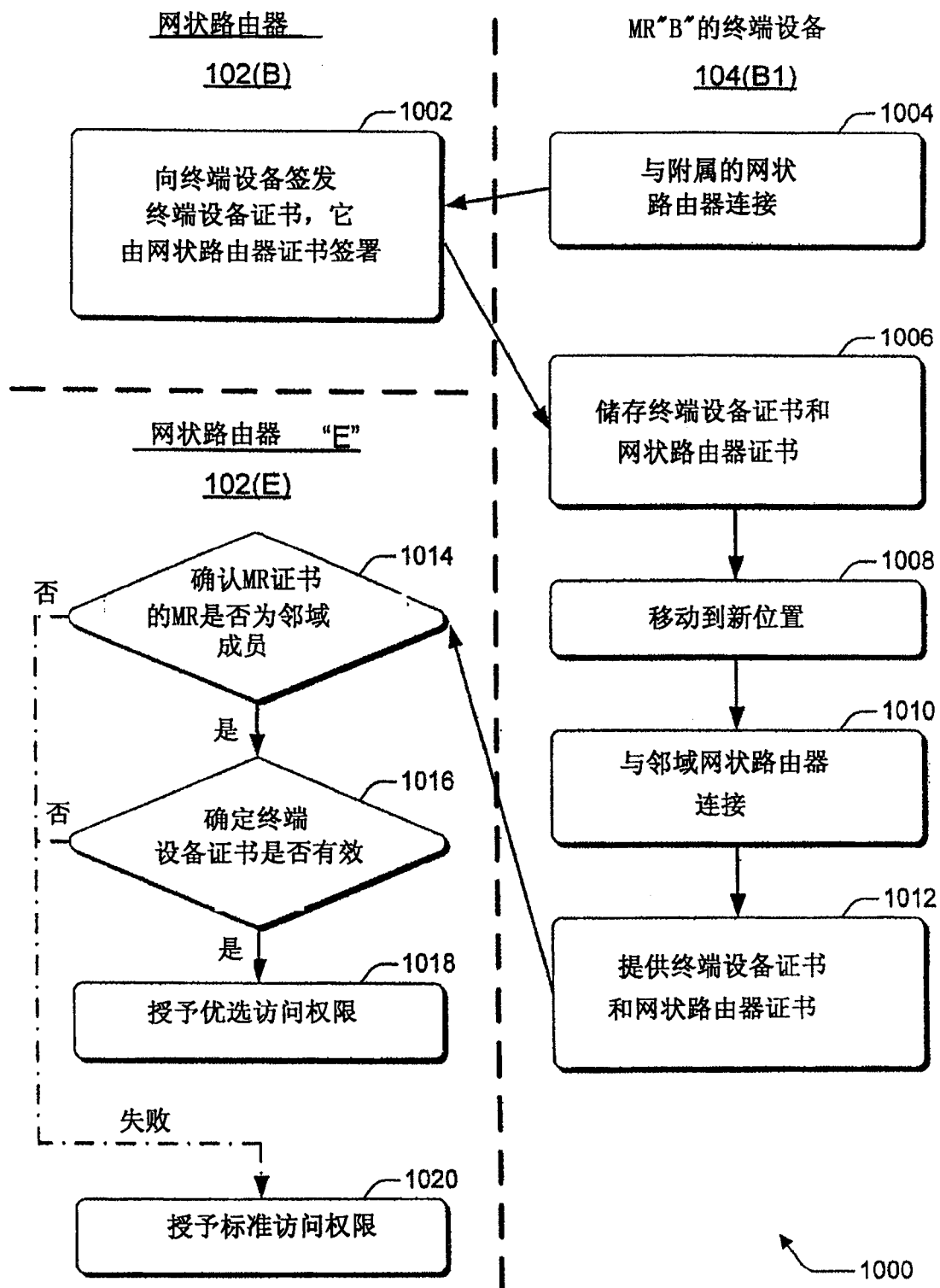


图 10

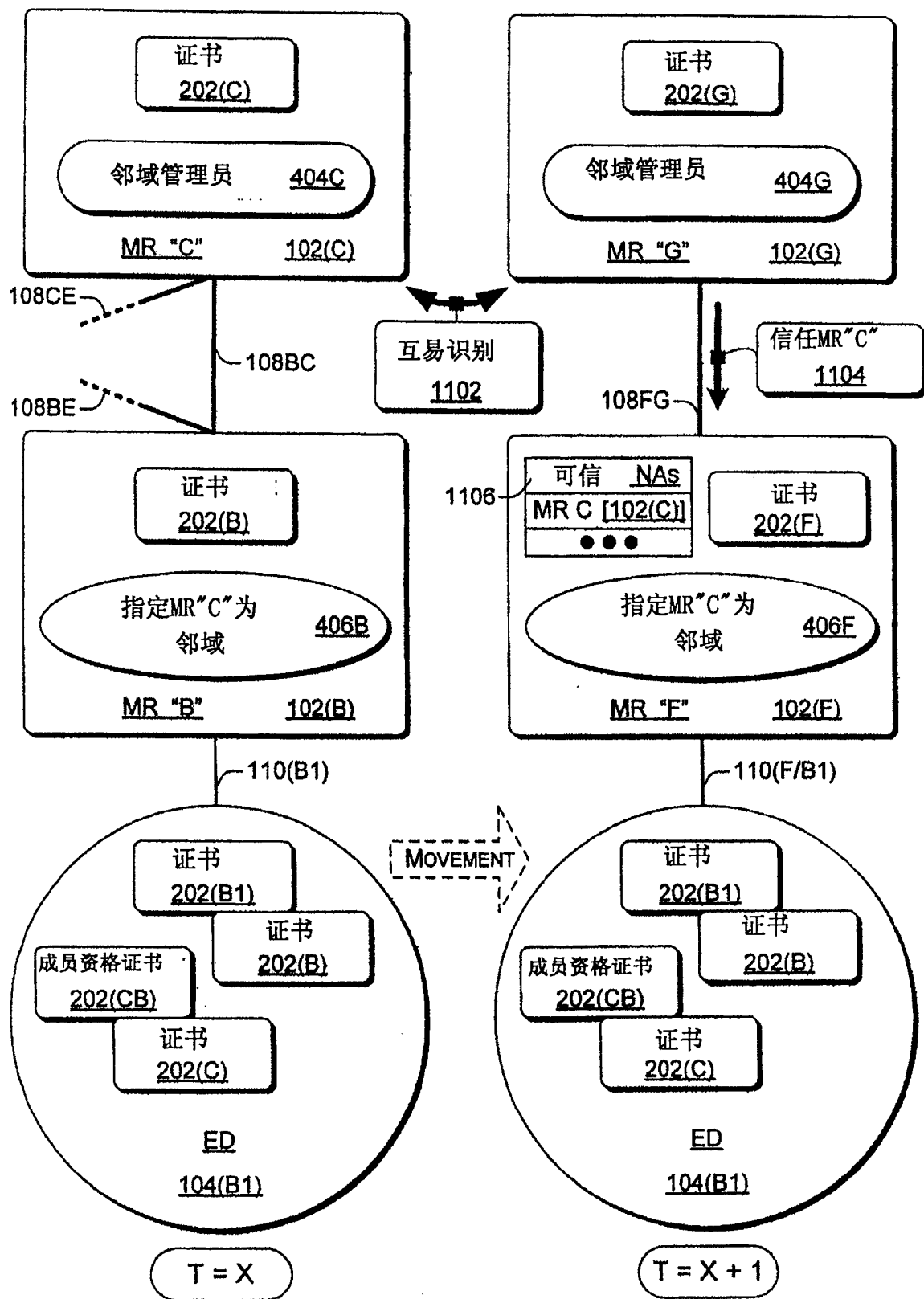


图 11

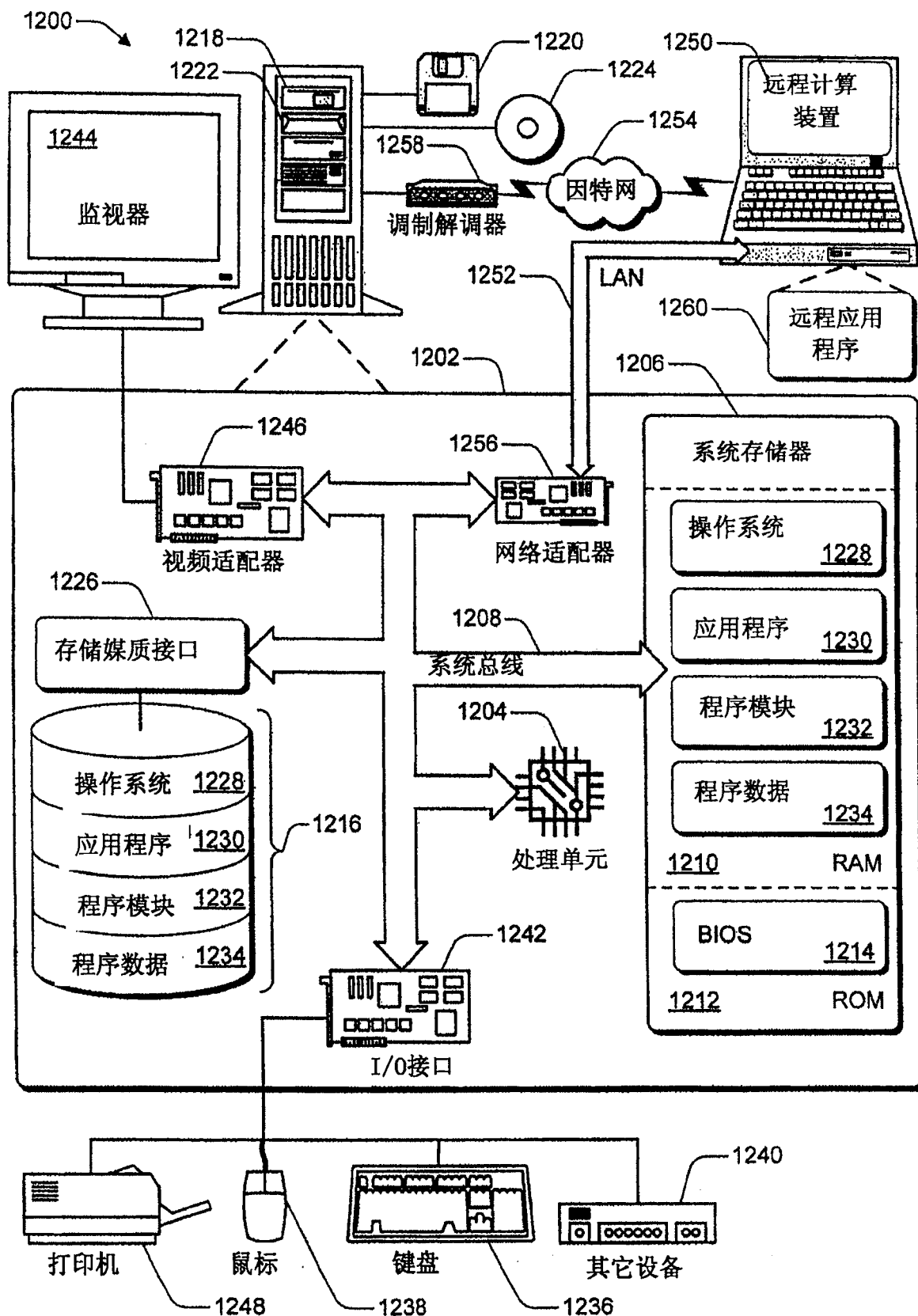


图 12