(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101883349 B
(45)授权公告日 2012.09.26

(21)申请号 201010156617.4

(22)申请日 2004.10.26

(30)优先权数据
03026069.9 2003.11.12 EP

(62)分案原申请数据
200480040278.6 2004.10.26

(73)专利权人 松下电器产业株式会社
地址 日本大阪府

(72)发明人 詹斯·巴克曼 亚历山大·布格特

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 邸万奎

(51)Int.Cl.
H04L 29/02(2006.01)

(56)对比文件
WO 02/093955 A1,2002.11.21, 说明书第8,77,83-84段,附图7.
CN 1446002 A,2003.10.01, 全文.
US 2002/0059453 A1,2002.05.16, 全文.
WO 03/079700 A1,2003.09.25, 说明书第4页第11-31行,第6页第6-23行.

审查员 吕源

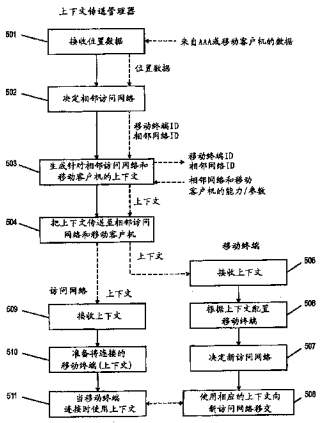
权利要求书 1 页 说明书 15 页 附图 5 页

(54)发明名称

移动终端及其通信方法

(57)摘要

本申请涉及移动终端和该移动终端的通信方法。该移动终端访问多个异构访问网络,并执行所述异构访问网络间的移交,所述移动终端包括:接收单元,从与所述多个异构访问网络共同的访问网络信息传送管理器接收可利用访问网络信息,所述可利用访问网络信息包括所述移动终端相邻的可利用访问网络列表;测量单元,从所述可利用访问网络信息中表示的所述可利用访问网络接收信号;选择单元,从所述可利用访问网络中选择用于移交的访问网络;开始单元,开始对所选择的访问网络的移交。



CN 101883349 B

1. 移动终端中的通信设备，所述移动终端访问多个异构访问网络，并执行所述异构访问网络间的移交，

所述通信设备包括：

接收单元，从与所述多个异构访问网络共同的上下文传送管理器接收上下文，所述上下文包括作为可利用的相邻访问网络的信息的使用了上下文的格式的相邻列表，所述上下文根据存储于数据库中的所述移动终端的能力由所述上下文传送管理器生成；

预配置单元，根据所述上下文预配置对于所述可利用的相邻访问网络接口；

测量单元，从所述可利用的相邻访问网络的信息中所表示的所述可利用的相邻访问网络接收信号；

选择单元，从所述可利用的相邻访问网络中选择用于移交的访问网络；

开始单元，开始对所选择的访问网络的移交。

2. 根据权利要求 1 所述的通信设备，

所述异构访问网络至少包括公众陆地移动网和无线局域网。

3. 根据权利要求 1 所述的通信设备，

所述可利用的相邻访问网络的信息还包括所述可利用访问网络的无线访问网络标识符。

4. 根据权利要求 3 所述的通信设备，

所述信号为所述无线访问网络标识符中所包含的信标消息。

5. 移动终端中的通信方法，所述移动终端访问多个异构访问网络，并执行所述异构访问网络间的移交，

所述通信方法包括以下步骤：

接收步骤，从与所述多个异构访问网络共同的上下文传送管理器接收上下文，所述上下文包括作为可利用的相邻访问网络的信息的使用了上下文的格式的相邻列表，所述上下文根据存储于数据库中的所述移动终端的能力由所述上下文传送管理器生成；

预配置步骤，根据所述上下文预配置对于所述可利用的相邻访问网络接口；

测量步骤，从所述可利用的相邻访问网络的信息中所表示的所述可利用的相邻访问网络接收信号；

选择步骤，从所述可利用的相邻访问网络中选择用于移交的访问网络；

开始步骤，开始对所选择的访问网络的移交。

6. 根据权利要求 5 所述的通信方法，

所述异构访问网络至少包括公众陆地移动网和无线局域网。

7. 根据权利要求 5 所述的通信方法，

所述可利用的相邻访问网络的信息还包括所述可利用访问网络的无线访问网络标识符。

8. 根据权利要求 7 所述的通信方法，

所述信号为所述无线访问网络标识符中所包含的信标消息。

移动终端及其通信方法

[0001] 本申请是以下专利申请的分案申请：

[0002] 申请号：200480040278.6

[0003] 申请日：2004 年 10 月 26 日

[0004] 发明名称：包含多个异构访问网络的通信网络中的上下文传送

发明领域

[0005] 本发明涉及一种在包含多个异构访问网络的通信网络中进行上下文 (context) 传送的方法，其中，把移动终端连接于访问网络之一。另外，本发明还涉及一种执行该方法的上下文传送管理器。而且，本发明还涉及一种专门适用于执行该所提供的用于上下文传送的方法的移动终端。

背景技术

[0006] 与网络连接的每个移动的移动节点在离开旧的覆盖区时可以执行至新网络的移交 (handover) 以维持连接性。如果该移动节点具有通过该连接的正在进行的数据会话，则至少在移交过程时连接将中断。类似 MobileIP（移动 IP）的附加机制可允许把业务 (traffic) 重新路由传输至新的连接点，从而会话可得以恢复。然而，移交持续期是关于会话断开的更低时间限制。

[0007] 因此，恰当的做法是使移交持续期尽可能短。维持其的机制是前摄 (pro-active) 上下文传送。前摄上下文传送允许在移动节点（移动终端）开始向新网络移交之前，在访问路由器 (AR) 或访问点 (AP) 中建立会话状态。通过访问路由器或访问点所连接的主干网络进行传送。主干网络可以为例如因特网。

[0008] 所传送的数据的来源是已经了解该上下文的实体。在前摄上下文传送的替代方案中，当移交已经开始时，启动上下文传送，所谓的后摄 (reactive) 上下文传送。

[0009] 实现前摄上下文传送的重要功能是，在执行移交之前选择上下文所传送至的候选。哪个访问路由器或访问点是下个连接点，通常是不可预知的，因为不知道移动节点的移动模式。总体上，假设访问点的单元覆盖区是重叠的 (overlap)，从而可以进行移交。然而，如果可触及的范围内存在多个新访问点，则也对将加入的新网络的选择过程几乎没有帮助。

[0010] Seamoby CTP 和 CARD

[0011] IETF（因特网工程任务组）工作组 Seamoby 已开发出两种关于上下文传送的协议。这两种协议是：上下文传送协议 (CTP，参见 Loughney 等的“Context Transfer Protocol（上下文传送协议）”，因特网草案，2003 年 10 月，所有因特网草案和 RFC（请求注解）可得于 http://www.ietf.org)；以及候选访问路由器发现 (CARD，参见 Liebsch 等的“Candidate Access Router Discovery（候选访问路由器发现）”，因特网草案，2003 年 9 月）。CTP 用作启动上下文传送及承载上下文数据的协议。CTP 通信中涉及三个部分：移动节点（移动节点）、先前访问路由器 (pAR)、以及下个访问路由器 (nAR)。所有这三个部分，

具有不同的消息类型，都能够启动协议交换。在已与先前访问路由器断开的情况下，如果移动节点希望或者不得不改变其网络访问点，则它至少向下个访问路由器发送请求。如果该移动节点使用某种类型的下个访问路由器预测，可以通过 CARD，则在其自身连接至下个访问路由器之前，其甚至还向先前访问路由器发送启动向所预测的下个访问路由器进行上下文传送的消息。其包含下个访问路由器的 IP 地址、先前访问路由器上的移动节点的旧 IP 地址、将加以传送的上下文数据的列表、下个访问路由器上的可以知道的 IP 地址、以及请求上下文的安全和 / 或可靠传送的标志。然后，在进一步的消息中发送上下文数据，称为“特征上下文”。

[0012] CARD 协议仅由两消息组成 :CARD 请求和 CARD 回复。它们甚至还可以用在两个访问路由器之间，即有可能的下个访问路由器 (nAR) 和称为先前访问路由器 (pAR) 的当前的访问路由器之间，或者在移动节点和先前访问路由器或下个访问路由器之间。在访问路由器之间，CARD 有助于得到下个访问路由器候选的能力信息，需要该信息来选择最适合于上下文传送和以后的移动节点移交的一个。在移动节点和先前访问路由器之间发布要求下个访问路由器候选列表的 CARD 请求。在此请求中，移动节点可以发送任何下个访问路由器数据链路层 (层 2) 标识符，此标识符可能已由某机制检测到，因此，先前访问路由器具有哪个访问路由器处于移动节点的范围内的提示。CARD 草案中未指定先前访问路由器通过其层 2 标识符来标识下个访问路由器的方式。在对移动节点的回复中，先前访问路由器发送带有附属 (belonging) 下个访问路由器能力的下个访问路由器列表，其可能已由先前访问路由器所决定的标准预先加以过滤，以减少移动节点必须作为候选加以处理的下个访问路由器的数目。

[0013] 无线局域网中的上下文传送 (IEEE 802.11f)

[0014] 在无线局域网 (WLAN) 中，交换关于在移交过程中所涉及的访问点 (AP) 之间的客户机或站 (STA) 的信息，这允许了新访问点处的重新关联过程。使用加速此重新关联过程的上下文传送方案。上下文传送中涉及了两功能实体 :访问点和 RADIUS 服务器。对于站 (STA)，管理过程是透明的。RADIUS 服务器履行把所传递的基本服务集合标识符 (BSSID) 映射至访问点的 IP 地址或正式域名 (FQDN) 的任务。此映射暗示访问点是否属于与 RADIUS 服务器相同的扩展服务集 (ESS)。它还根据请求把密码密钥分布至访问点，以允许两个访问点之间的加密通信。此通信包括允许节点间的客户机移动的所有管理数据，并且每次把客户机仅与一个访问点相关联。管理消息可以包含上下文数据。ESS 下属各项 (following) 中的每个访问点均维持其相邻访问点的动态表现。把此表现也称为相邻图。

[0015] 需要加以注意的重要问题是，在 2002 年 1 月的 IEEE 草案 IEEE802.11f-D3“Recommended Practice for Multi-Vendor Access Point ; Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation(多销售商访问点的推荐实践 ;经由支持 IEEE 802.11 操作的跨分布系统的访问点间协议的互操作性)”中，在附录 B 第 B.3.1 节中指出，不能期望具有不同服务模型的媒体之间的上下文传送成功。试图根据 IEEE 802.11 上下文传送机制在蜂窝设备和 IEEE 802.11 访问点之间传送上下文，将会失败，除非蜂窝访问点实施与 802.11 访问点相同的服务集。作为结论，该文献指出，异构技术之间的上下文传送将失败。

[0016] 其它机制

[0017] 对于 CTP 情境 (scenario) 的访问路由器和移动节点，另外，US 2003/0,103,496 A1 中所描述的机制还包含 :服务于检索相邻访问网络 (AN) 的任务的策略服务器 (PS)、以及能够进行上下文传送的访问路由器 (相当于 CARD 机制)。由信标信号中的层 2 信息指示访问网络，所述信标信号由移动节点接收，并且由 PS 在本地数据库中查找。如果相邻策略服务器能够服务于移动节点，则 PS 与该相邻策略服务器进行通信，并且使用它们进行预先认证。此机制的一个缺点是，与 CTP 的情境相比，其需要甚至更多的安全连接 (或者换种说法是安全关联)。其次，在向新的访问网络发送之前，其根据动态和静态部分构造上下文，但不考虑目标网络的任何特征或能力。

[0018] US 2003/0,092,444 A1 描述了这样的机制 :为选择相邻候选，考虑了诸如当前业务负载和用户权利的动态参数。因此，对于每个移动节点，候选列表可能不同。传送过程本身在访问网络的访问路由器之间执行。

[0019] US 2003/0,087,646 A1 中介绍了一种用于发现可用于上下文传送机制的相邻访问路由器的机制，并将其缩写为 GAARD。其允许检测地理上相邻的访问网络，即使在考虑例如 IP 地址的情况下它们不是拓扑相邻的。在该文献中，移动节点具有层 2(数据链路层) 地址和层 3(网络层) 地址的本地高速缓冲存储器。当移动节点使用层 2 地址接收信标信号，并且希望启动向该节点的上下文传送时，该移动节点在其高速缓冲存储器中查找相应的层 3 地址。如果高速缓冲存储器查找失败，则该移动节点请求服务访问路由器查找相应的层 3 地址。访问路由器本身查找其高速缓冲存储器。如果没有发现此地址，则其启动动态发现过程，以导出所请求的层 3 地址。访问路由器把此地址返回给接下来使用它来启动上下文传送的移动节点，或通过其它移交机制返回给所标识的访问路由器。此系统的功能必须存在于希望使用或者支持该系统的每个访问路由器和移动节点中。该机制可用作 CARD 过程的实施。

[0020] 与所有相邻访问路由器甚至可能是移动节点的访问点的一般上下文传送情况相对比，在以合同为基础而共同工作的网络情境中，后面的假设不成立。相邻访问路由器可能属于与移动节点的主操作器 (home operator) 无漫游协议的网络操作器。因此，移动节点接收到异质 (foreign) 网络的信标，但认证过程将失败，因为异质网络中的认证机制不能连接至移动节点的主 AAA(认证、授权以及记账) 服务器，或者至少将不信任此未知的服务器。出于同样的原因，针对这样的网络的上下文传送也将失败。

[0021] 对与移动节点的主操作器无直接漫游协议的网络进行集成的方式是，使用代理 AAA 服务器。访问网络操作器信任操作器的该代理 AAA 服务器，而它自身信任移动节点的主操作器。因此，甚至在异质网络中，也可对移动节点进行授权。

[0022] 针对其它局域网技术，开发类似 WLAN 中上下文传送的机制，也是可能的。拓扑邻接的实体之间的上下文传送具有短距离的优势，从而低潜伏期 (low latency) 传送。

[0023] 与先前问题相关的是异构访问网络结构的事实。很可能不能把移动的移动节点的上下文视为静态数据。它将随新访问点的访问网络基础结构不同于先前的一个而改变。把上下文数据简单地转发至新访问网络将不能解决此问题。

[0024] 上下文传送的总体问题是，上下文传送过程中所涉及的实体之间的信任关系。在具有包含 n 个相邻访问路由器、且彼此之间传送上下文数据的区域的情境中，可得出所有访问路由器之间的 n(n-1)/2 个信任关系的上界。当在技术上由某密码密钥表现的这些关

系在对等体之间交换，以允许加密的通信时，在每个访问路由器 n-1 个数据集的例子中，大数目 n 意味着密钥数据集的大量存储空间。另外，必须在对等体之间可能进行上下文传送之前建立这些关系，这要求管理功能。因此，减小信任关系的数目的方法将会节省存储空间和管理方面的努力。安全数据传送的已经存在的技术是名为信任关系安全关联 (SA) 的 IPSec。

[0025] 大多数情况下，将通过无线链路把移动节点连接至其访问点。通常，这些链路具有低于访问网络的主干部分中有线链路的带宽，并且与不同的访问网络互联。这导致无线域中每数据量的更高的传送开销。

[0026] 另一方面是移动节点的功耗。此功耗与发送至无线链路的包的数目直接相关。这两个方面导致了这样的目标：使管理业务与用户有效载荷业务相比，其量尽可能低。

发明内容

[0027] 本发明的目的是，解决上述问题的至少一个。

[0028] 独立权利要求的主题实现了此目的。本发明的优选实施例为从属权利要求的主题。

[0029] 根据本申请的一个方面，提供了一种移动终端中的通信设备，所述移动终端访问多个异构访问网络，并执行所述异构访问网络间的移交，所述通信设备包括：接收单元，从与所述多个异构访问网络共同的上下文传送管理器接收上下文，所述上下文包括作为可利用的相邻访问网络的信息的使用了上下文的格式的相邻列表，所述上下文根据存储于数据库中的所述移动终端的能力由所述上下文传送管理器生成；预配置单元，根据所述上下文预配置对于所述可利用的相邻访问网络接口；测量单元，从所述可利用的相邻访问网络的信息中所表示的所述可利用的相邻访问网络接收信号；选择单元，从所述可利用的相邻访问网络中选择用于移交的访问网络；开始单元，开始对所选择的访问网络的移交。

[0030] 根据本申请的另一个方面，提供了一种移动终端中的通信方法，所述移动终端访问多个异构访问网络，并执行所述异构访问网络间的移交，所述通信方法包括以下步骤：接收步骤，从与所述多个异构访问网络共同的上下文传送管理器接收上下文，所述上下文包括作为可利用的相邻访问网络的信息的使用了上下文的格式的相邻列表，所述上下文根据存储于数据库中的所述移动终端的能力由所述上下文传送管理器生成；预配置步骤，根据所述上下文预配置对于所述可利用的相邻访问网络接口；测量步骤，从所述可利用的相邻访问网络的信息中所表示的所述可利用的相邻访问网络接收信号；选择步骤，从所述可利用的相邻访问网络中选择用于移交的访问网络；开始步骤，开始对所选择的访问网络的移交。

[0031] 根据本发明的第一实施例，提供了一种在包括多个异构访问网络的通信网络中进行上下文传送的方法。可以把移动终端连接于这些访问网络之一。

[0032] 根据此所建议的方法，上下文传送管理器可以接收位置信息，并且可以根据位置信息决定移动终端的相邻访问网络。另外，上下文传送管理器还可以生成至少一个针对相邻访问网络和移动终端的上下文，并且把上下文传输至每个相邻访问网络和移动终端。

[0033] 考虑到各自的访问技术，至少一个上下文的生成可以基于与移动客户机相关的能力和参数以及与相邻访问网络相关的能力和参数，并且在执行与移动站相关的上下文传送

的通信网络中，上下文传送管理器对于多个异构访问网络可以是公共的。

[0034] 因此，根据第一实施例，本发明允许即使在移动终端使用两不同的访问技术在访问网络之间进行移交的情况下进行上下文传送。另外，当考虑到移动终端可能移动到的候选访问网络，即相邻访问网络，中所使用的访问技术时，可以生成适合于由不同访问技术所使用的相应协议的动态上下文。这也通过在通信网络中使用公共上下文传送管理器来促进，因为在要求甚低的网络中安全关联的不同候选访问网络中，只有公共上下文传送管理器才能够把上下文传送至上下文管理器。以下，将更详细地描述本发明所建议的体系结构的有益之处。

[0035] 根据进一步的实施例，移动终端接收指示存在另一访问网络的信标信号，执行从当前访问网络到从其接收信标信号的新访问网络的移交。

[0036] 针对每个相邻访问网络和移动终端所生成的上下文，可以包括移动终端的静态或临时标识符。例如，新访问网络中的上下文管理器可以使用静态或临时的标识符，来把移动终端与从上下文传送管理器所接收的它的上下文相关联。如果移动终端在传输至新访问网络的数据中包括静态或临时的标识符，则有助于后者。因此，通过把标识符包括在传输至新访问网络中的上下文管理器的消息中，所建议的方法可有助于把（先前）从上下文传送管理器所接收的上下文映射到移动终端。

[0037] 移动终端所接收的上下文，也可由其用来根据从上下文传送管理器所接收的上下文对移动终端进行预配置。因此，例如，通过对网络接口的预配置，当移动终端连接至新访问网络时，不需要执行此过程。

[0038] 上下文传送管理器还可以从移动终端接收状态信息，其中，状态信息指示当前访问网络中所达到的服务质量，和/或指示对除当前访问网络之外的至少一个其它访问网络不成功的访问尝试。

[0039] 因此，上下文传送管理器所收集的此信息可由其用于根据此信息来调整上下文传送管理器中的若干决策过程。例如，对相邻访问网络的判断也可以使用可根据来自移动终端的状态信息而调整的选择算法。

[0040] 另一种可能性是，如果客户机报告与特定访问网络的连接失败，则在相邻访问网络的决定过程中可不再考虑后者，和/或可以生成适当的错误消息，访问网络的操作器或上下文传送管理器的操作器可以寻找 (address) 并处理该适当的错误消息。对于后者，上下文传送管理器可以存储关于移动终端所报告的对访问网络的失败的访问尝试的信息。

[0041] 在上下文生成期间所考虑的、与移动客户机相关联的能力与参数，可以包含下列中的至少一个：静态和/或临时终端标识符；对终端通信的要求的用户偏好；所保证的服务质量参数；和/或对服务的访问准许；含有加密密钥、初始值 (seed)、密码和/或头标压缩信息的会话数据；含有与显示器、网络接口、处理能力、所支持的应用和/或视频/音频编码解码器相关的信息的终端能力。显然，可以把能够应对访问网络中不同访问技术的若干访问网络特定的参数用于生成动态上下文。这也适用于相邻访问网络的能力与参数，可以包括下列中的至少一个：含有射频、数据速率、信道、和/或编码方式的访问技术特定的属性；含有各访问网络的加密能力的访问网络特定的属性；访问网络标识符；所支持的服务质量机制；可用的业务类型；本地服务；信息门户 (portal)；和/或公共传输信息。

[0042] 可以在由移动终端根据移动终端和认证服务器之间所执行的认证处理、或者由位

于连接移动终端的访问网络中的实体所传输的寻呼消息中，接收上下文传送管理器所接收的位置信息。第二个例子是，执行访问网络的初始认证处理以与例如相关 AAA 服务器相结合的移动终端，可以向 AAA 服务器提供位置信息。此信息也可用于上下文传送管理器，使得其可以使用来自认证处理的位置信息来决定相邻访问网络。另外，上下文传送管理器还可以响应于移动终端的认证处理，来启动上下文传送。

[0043] 而且，位置信息也可以基于从例如 GPS 接收器的位置决定设备所获得的地理位置、或者根据网络地址和 / 或网络前缀所决定的网络相关位置。以 IP 协议的使用为例，网络地址相应于 IP 地址，而网络前缀将为子网掩码。

[0044] 根据本发明的进一步的实施例，可以当已从与新访问网络相关的上下文传送管理器接收到上下文信息时，执行移动终端的移交。因此，可以通过使用本发明来实现前摄上下文传送。

[0045] 为了描述所生成的上下文，可以使用基于标记语言的数据格式。另外，这种格式还可用于描述从上下文传送管理器传送到所述多个访问网络和移动终端的上下文。

[0046] 在本发明的另一个实施例中，从上下文传送管理器接收上下文的相邻访问网络中的认证服务器可以使用所接收的上下文信息来针对访问网络执行移动终端的登记和 / 或认证处理。而且，移动终端的登记和 / 或认证可以包括移动终端的安全密钥的登记。

[0047] 当连接于其中已登记了安全密钥的相邻访问网络时，移动终端可以把所登记的安全性用于通信。

[0048] 本发明的另一个实施例考虑到这样的情况 ：其中，把移动终端连接于异质通信网络，即所谓的受访通信网络。在此实施例中，上下文传送管理器可以驻留在受访通信网络中。在本发明中，可以把通信网络解释为管理域，即这样的网络，其包含 ：至少一个核心网络以及多个操作器的访问网络或多个具有与操作器的服务级别协议的提供商的访问网络。因此，本实施例与这样的情况相关 ：其中，移动终端驻留在除其主域 (home domain) 之外的另一个管理域中。

[0049] 为了允许受访上下文传送管理器，即受访通信网络中的上下文传送管理器生成针对上下文传送的适当上下文，移动终端的主网络中的上下文传送管理器可以把与至少一个上下文的生成相关的数据传输至受访通信网络的上下文传送管理器。

[0050] 还应该加以注意的是，访问网络中的上下文管理器可以从上下文传送管理器接收上下文，其中，上下文管理器不维持与另一个访问网络中的另一上下文管理器的连接。因此，不同访问网络中的上下文管理器可以不必维持相互间的连接，而且可不必互相直接传送或转发上下文——如果完全可能——但可以从较高层次结构级别上的实体，即上下文传送管理器，接收上下文。

[0051] 本发明的另一个实施例提供了包括多个异构访问网络的通信网络中的上下文传送管理器，其中，移动终端连接于访问网络之一。上下文传送管理器可以包括 ：接收装置，用于接收位置信息 ；处理装置，用于根据位置信息决定移动终端的相邻访问网络 ；上下文生成装置，用于生成针对相邻访问网络和移动终端的至少一个上下文 ；以及传输装置，用于把相应上下文传输至每个相邻访问网络和移动终端。另外，上下文生成装置可适用于根据与移动客户机相关的能力与参数、和考虑到相邻访问网络的相应访问技术的能力与参数，来生成至少一个上下文。而且，通信网络中多个异构访问网络共同的上下文传送管理器可以

执行与移动站相关的上下文传送。

[0052] 上下文传送管理器可适用于执行任何以上所描述的方法。

[0053] 在本发明的进一步的实施例中，提供了一种适合于执行上述方法之一的移动终端。此终端可适用于：其可以向上下文传送管理器信号传送对访问网络的失败的访问尝试；或者，其可以接收以标记语言格式提供的上下文信息。

[0054] 在本发明的进一步的实施例中，提供了移动终端，所述移动终端访问多个异构访问网络，并执行所述异构访问网络间的移交，所述移动终端，包括：接收单元，从与所述多个异构访问网络共同的访问网络信息传送管理器接收可利用访问网络信息，所述可利用访问网络信息包括所述移动终端相邻的可利用访问网络列表；测量单元，从所述可利用访问网络信息中所表示的所述可利用访问网络接收信号；选择单元，从所述可利用访问网络中选择用于移交的访问网络；开始单元，开始对所选择的访问网络的移交。

附图说明

[0055] 以下，将参照附图，更详细地描述本发明。以相同的参照标号标记图中相类似的或相应的细节。

[0056] 图 1 描述了根据本发明的一个实施例，通过受访域的代理从主域至 WLAN 的上下文传送的简化结构；

[0057] 图 2 描述了根据本发明的实施例管理移动节点的上下文传送的通信网络的结构概要；

[0058] 图 3 描述了根据本发明的实施例的上下文生成过程；

[0059] 图 4 描述了根据本发明的实施例从具有上下文传送功能的外部 AAA 服务器到 WLAN 的认证服务器 (AS) 或访问路由器的上下文传送过程；

[0060] 图 5 描述了根据本发明的实施例的上下文传送过程的流程图；以及

[0061] 图 6 描述了根据本发明的实施例的管理连接于受访网络的移动节点的上下文传送的通信网络的结构概要。

具体实施方式

[0062] 图 2 中描述了根据本发明的实施例管理移动节点的上下文传送的通信网络的结构概要。此结构跨越移动节点的主域、移动节点 207 本身、以及访问网络的网络加以分布。

[0063] 可以把上下文传送管理器 (CTM)200 与主域的 AAA 服务器 206 共同放置。上下文传送管理器 200 可以向移动节点的当前位置的相邻访问网络发送适当的、动态创建的上下文数据。这些相邻由从上下文传送管理器 200 得到移动节点 207 的当前位置（例如 IP 地址和网络前缀）的相邻定位器 202 功能来检测，并且返回到相邻列表中。可以把此相邻列表与关于移动节点 207 的用户的信息一起提供至上下文生成器 201。上下文生成器 201 可以维持关于访问网络和移动节点的能力、以及关于上下文格式的数据库（参见用户配置文件 (User Profile) 数据库 203、访问网络上下文数据库 204、相邻能力数据库 205)。根据此信息，可以针对每个相邻访问网络生成一套上下文，例如考虑到不同的终端标识符、预约 (subscription) 信息、用户偏好、终端能力、服务质量参数、加密与压缩信息、访问技术特定的属性或访问网络特定的属性。然后，可以按前摄的方式把此上下文传送至访问网络，其

中，由访问网络 (AN) 的上下文管理器 (CM)209、210、211 对其例示 (instantiate)。也可以使用上下文传送向移动节点 207 上的移动性管理器 208 功能通告相邻网络 220、221、222，包括向它们加速移交所需的信息。根据从上下文传送管理器 200 所接收的上下文，移动节点 207 可以（预）配置其针对下个访问点的网络接口。当移动节点 207 接收到可触及范围内的相邻网络的信标信号时，移动节点 207 本身可以进行移交决策。

[0064] 当移动节点 207 正向异质域漫游时，可以由受访操作器的上下文传送管理器 600 进行上下文传送管理（参见图 6）。上下文传送过程类似于非漫游的情况，仅把来自主上下文传送管理器 200 的管理的移交添加至受访上下文传送管理器 600。

[0065] 以下，将更详细地描述上下文传送管理器 200、600。上下文处理的主示例可以为上下文传送管理器 200、600(CTM)。其可以控制对所需上下文信息进行访问的功能。在此结构中，控制功能可以为上下文生成器 201、相邻定位器 202、访问网络 (AN) 上下文管理器 209、210、211、609、610、611、以及移动性管理器 208 功能。首先，例如，当移动终端 207 接通以及连接于访问网络时，上下文传送管理器 200、600 可以通过与移动性管理器 208 的通信，或者通过标准认证处理，来接收移动节点 207 的当前位置。

[0066] 然后，上下文传送管理器 200、600 可以使用相邻定位器 202、602 来决定移动节点 207 的所有相邻访问网络 220、221、222、620、621、622。接下来，上下文传送管理器 200、600 可以信号传送上下文生成功能 201、601，以检索与移动节点 207 的相邻访问网络 220、221、222、620、621、622 所使用的上下文相关的用户信息。信号传送可以包括用户 ID 和相邻网络 220、221、222、620、621、622 的可用网络 ID，例如网络前缀。包括在上下文中的另一个参数可以是用户的附加的唯一静态或临时标识符，访问网络以后可以使用其来离线或在线地对所传递的服务进行收费。可以想像把 GSM 或 UMTS 中的 IMSI（国际移动订户标识）、或者也可以假名 NAI（网络访问标识符，参见 Aboba 等的“Network Access Identifier（网络访问标识符）”，RFC 2486，1999 年 1 月）分别用作静态或临时标识符。

[0067] 在把此信息集成于上下文数据之后，上下文传送管理器 200、600 可以向访问网络上下文管理器 209、210、211、609、610、611 发送上下文数据和向移动客户机 207（移动终端）的移动性管理器 208 发送此所生成的上下文信息的某些部分。信息的这些部分可以使移动节点 207 能够配置其网络接口，以及能够在接下来的相邻网络访问尝试中使用正确的标识符。

[0068] 除了移动节点 207 的追踪信息之外，上下文传送管理器 200、600 还可以从移动性管理器 208 接受状态信息。在状态信息中，移动节点 207 可以信号传送当前网络中所到达的服务质量 (QoS)，或者对另一个访问网络的访问的完全失败。这可以允许在相邻列表中针对最适合的访问网络进行选择算法的动态调整，从而有助于在同一区域中移动的其它移动节点选择适当的新访问网络。在此方式下，移动节点 207 可以用作收集关于网络状态的信息的网络探测器。如果在单个访问网络中许多移动性管理器信号传送上下文辅助移交的失败，则上下文传送管理器 200、600 可以向管理和操作功能通知其拥有的网络，以进一步调查此错误，或者也可以向操作器通知访问网络。

[0069] 另外，以下将更详细地讨论上下文生成器 201 中的上下文生成功能。如以上所描述的，当在异构网络中或在不同管理域中的网络中实现时，基本 Seamody CTP 方案具有某些限制。这属于‘上下文’的创建。上下文可以不仅为单独一组纯用户相关的数据，例如标识、

口令或加密密钥。特别是，其还可以描述从客户机角度所观察的网络的状态。关于网络状态的信息可以例如包括对网络服务的访问权、所传送数据的加密算法、用户数据的路由策略、赋予用户会话业务的业务类型、或可访问的网络实体 (DNS 服务器、默认的网关等)。在单个管理域中，如果操作器要求，则可以在整个网络上保持此数据为静态。跨越边界到达其它域，此数据可能在变化，或者因此可以说，可以变为动态。为了防止，如果可能的话，可能需要操作器之间极为紧密的耦合。因此，由本发明所建议的方案进行适合于这些动态的上下文传送，具有优点并且解决了上述问题。

[0070] 图 3 中描述了根据本发明的实施例的上下文生成过程。可以把此上下文创建过程划分成四个部分 :两个源数据对象、一个处理功能以及一个结果数据对象。两个静态数据对象代表用户参数 301(包括终端参数与能力) 和网络参数 302 及能力。根据这两个参数集合，处理功能 303 可以导出结果数据对象，即动态上下文 304。由于网络相关参数还依赖于相应访问网络中所使用的访问技术，所以具有不同访问技术的访问网络的上下文可能变化。例如，设想产生会话加密密钥、状态标志或用户 ID 句柄的处理功能内部的多种算法。针对用户参数的数据对象可以包括 :包含临时标识的用户标识的描述、诸如 QoS 要求的用户偏好或所允许的会话类型 (例如，视频、语音)、加密密钥或初始值以及所安装的密码以及诸如屏幕分辨率、处理能力、音频 / 视频编码解码器和可用应用、网络接口等的终端能力。

[0071] 不仅可以把与上下文相关的数据包括在数据对象中。这有助于把最终存在的一般用户数据存储用于其它目的 (例如，3GPP 的一般用户配置文件 GUP)。针对网络参数的数据对象可以包括关于以后结果上下文可传送到的特定访问网络的信息。

[0072] 考虑到用户特定的和 / 或终端特定的参数以及依赖于下个访问网络的相应访问技术的参数，在移动终端 207 访问新网络的情况下，可以创建防止上下文传送失败的动态上下文。其可以为诸如包括在网络信标中的所支持的加密算法或 WLAN SSID(服务集合标识符) 等的数据，有助于移动节点 207 标识所要选择的 WLAN。同样，不仅可以把上下文相关数据包括在数据对象 304(上下文) 中，而且还可以把属于使用该对象的其它应用的数据集合包括在数据对象 304 中。总体上，可以使用 XML 导出语言来描述例如用于 GUP 或用于构成能力 / 偏好配置文件 (profile)(CC/PP) 的上下文数据。可以使用用于 XML 文档和 XSL 内数据搜索和选择的 W3C 语言 Xpath 和 XQuery。XSL 可用于把 XML 文档以及它们的后过程转换为任意输出格式。另外，可以以安全和容易的、保持与较旧描述兼容的方式来使用描述上下文信息的标记语言，以扩展数据描述。由于应请求的上下文生成可以解决向不一致的网络进行上下文传送的问题，所以还可以提供保持某些或全部用户或网络参数动态的能力。用户可以改变他 / 她的用户偏好，通信网络中即将到来的下个上下文传送可以立即适应新的偏好 (较高的会话 QoS、新的加密方式等)。

[0073] 另外，移动终端 207 中的移动性管理器 208 还可以控制网络接口并可以追踪移动节点 207 的移动。因此，最佳位置可以是移动节点 207。或者，当从一个访问点改变到另一个访问点时，访问网络还可以根据终端的移动来追踪移动节点的位置。在把移动性管理器 208 定位在移动节点 207 处的情况下，可以把状态信息包括在从移动客户机 207 传输到上下文传送管理器 200 的寻呼 (paging) 消息中。移动性管理器 208 可以把移动节点 207 的移动和位置信号传送至上下文传送管理器 200。因此，可以使用由诸如 GPS(全球定位系统) 接收器的内置的位置决定设备、或者例如通过估计所接收的网络信标、或所接收的路由器

广告所收集的信息。

[0074] 可以由地理的或虚拟的，即网络相关的位置，来代表位置。可以支持用于描述移动终端 207 的位置的多种格式，以允许在移动节点 207 中实现不同的技术，并且允许从不同的位置表现来获取不同的信息。这受这样的事实所激励：单一的技术不能满足所有的需求。例如，GPS 可以提供关于终端的位置的高精确的位置信息，但为了进行位置计算，需要至 GPS 卫星的直瞄准线。特别是，在具有高地平线的城市中，有时这是不可能做到的。又例如，移动节点 207 的网络相关位置（例如网络地址和前缀）可有助于收集关于移动节点 207 连接到的网络的信息（例如，获取访问服务器的地址）。然而，移动节点 207 的单一的网络地址不必类似于地理上邻接的网络的地址。因此，也可以使用另外的机制来计算给定网络地址的相邻（例如，相邻图）。

[0075] 可以使移动性管理器 208 的网络控制部分能够根据从上下文传送管理器 200 接收的上下文内信息，来预配置移动节点 207 的一或多个网络接口。网络控制部分可以把任何信号传送的相邻访问网络的不同配置的预设置保存在本地高速缓冲存储器内部，并且当其检测到移交状况时，可以例示适当的一个。如果决定需要进行切换，例如应用可能需要更高的带宽，或当前连接可能衰减，则移动性管理器 208 可以主动开始移交。

[0076] 移动性管理器 208 还可以解决把用户对网络连接的偏好或服务质量要求方面的变化通信传送给上下文传送管理器 200 的任务。这些偏好影响着对适当网络相邻的选择和上下文生成过程。

[0077] 访问网络上下文管理器 209、210、211、609、610、611(AN 上下文管理器）可以处理所接收的上下文数据。在此过程中，可以针对可能移动的移动节点 207 来配置访问控制实体，即访问网络 220、221、222、620、621、622 中的访问服务器 212、213、214、612、613、614（参见图 2 和 6）。对于外部网络和对于发送上下文的上下文传送实体，配置过程可以是透明的。唯一的要求可能是使用所定义的模板，该模板描述了上下文传送管理器 200、600 中的上下文生成器 201、601 可以填充的、以及访问网络上下文管理器 209、210、211、609、610、611 可以理解和例示的上下文格式。可以包括关于网络的内部信息，因为双方都具有防止滥用上下文传送数据的信任关系。访问网络上下文管理器 209、210、211、609、610、611 的内部访问网络配置可以包括允许加速域内移交的访问网络范围的上下文传送机制。

[0078] 相邻定位器 202、602 可以检索移动节点 207 的相邻访问网络。相邻定位器 202、602 可以预先从上下文传送管理器 200、600 获得移动节点的位置。使用位置信息，其可以查找存储相邻关系的网络表现（参见图 2 中的数据库 203、204、205 以及图 6 中的数据库 603、604、605）。此表现可以为动态的，也可以为静态的。

[0079] WLAN 被视为公共和公司领域中的一种针对无线带宽访问的新兴技术，3GPP 标识 WLAN 和 3GPP 蜂窝网络之间相互操作机制的需求。因此，3GPP 定义了 6 种不同的情境，描述了与 3GPP 网络相互操作的 WLAN 所支持的服务级别。

[0080] 在 3G-WLAN 相互操作的情境中，存在着具有 Diameter 服务器的集中化 AAA 结构。此结构还具有为了安全地进行上下文传送而可重新使用的安全关联 (SA)，此处，为受访公共陆地移动网络 (VPLMN)、主公共陆地移动网络 (HPLMN) 和 WLAN 访问网络之间。本发明可以在主和受访上下文传送管理器之间提供连锁的信任关系，使得可以向异质网络进行成功的上下文传送。因此，针对此情境的上下文传送方案可实现针对上下文传送的代理功能，建

立针对层次结构的上下文传送的系统。图 1 描述了从主域（例如 HPLMN）经由受访域（例如，VPLMN）的代理到其中对上下文进行处理和例示的 WLAN 的上下文传送的简化结构。

[0081] 因此，可以改变访问路由器到访问路由器的上下文传送情境，即，从先前访问路由器 (pAR) 到下个访问路由器 (nAR) 的上下文传送。

[0082] 现在，所涉及的根据本发明的 3 种实体，可以为移动节点 207、下个访问路由器以及 AAA 服务器 206。移动节点 207 可以把上下文传送请求传输至 AAA 服务器 206。此时，AAA 服务器 206 可以把移动节点 207 的上下文传送至下个访问路由器。这可以在下个访问路由器和 AAA 服务器 206 之间推荐信任关系，如果 WLANAR 操作器与 AAA 服务器 206 操作器之间具有漫游协议，则此信任关系已经存在。假设 m 为漫游伙伴的数目，则这将导致 n 个访问路由器的每个具有 m 个安全关联，全部为 n·m 个安全关联。

[0083] 此数目应明显低于访问路由器到访问路由器的上下文传送情境。另一个有益之处是，当 AAA 服务器 206 发现相邻时，不再需要访问路由器中的类似 CARD 的功能。在访问路由器中可以仅存在上下文传送代理器。总体上，对于网络，相邻发现功能是不可见的，因此可以按销售商特定的方式加以实现。通过模仿先前访问路由器的 AAA 服务器 206，甚至可以更有效地面对两个访问路由器之间、至少在不同管理域之间的纵向移交时期待的上下文数据不兼容的问题。

[0084] 在 AAA 服务器 206 通过相邻发现过程而准确了解下个访问路由器能力的情况下，其可动态地使上下文适应于作为目标的下个访问路由器的能力。具有对完整用户配置文件的访问，与仅具有缩减信息集的访问路由器间上下文传送相反，可以创建适当的特征上下文。

[0085] 漫游在异质或受访域（例如，VPLMN）中的移动节点 207 可以不由主上下文传送管理器 200 直接协助，因为上下文传送管理器 600 可能还不具有、或不具有充分的关于异质域的访问网络 621、622 的信息。主上下文传送管理器 200，即移动客户机 207 中的主域中的上下文传送管理器 200，可能不能够生成针对访问网络的上下文数据。因此，移动节点 207 可能由异质域中的上下文传送管理器 600，即由受访的上下文传送管理器 600(VCTM) 协助。为了允许 VCTM 600 进行协助，主上下文传送管理器 200(HCTM) 可以把移动节点的或用户配置文件的所需要的部分传递至 VCTM 600。

[0086] 图 6 描述了控制个别访问网络的主和受访域的网络结构。受访域 (VPLMN) 中的上下文传送管理器 600 可具有针对作为目标的访问点或访问网络而调整所接收的数据的可能性。与主操作器的上下文传送管理器 200 一样，VCTM 600 也可以维持与具有与其拥有的操作器的服务级别协议 (SLA) 的访问网络 621、622 相关的、以及与它们的能力和它们所需的上下文格式相关的数据库 603、604、605。另外，受访上下文传送管理器 600 还可以从 AAA 服务器 606 检索信息。服务于移动节点 207 的 VPLMN(VCTM) 中的上下文传送管理器 600 和其移动性管理器 208 的差别，可以是针对漫游移动节点 207 的非永久性存储的用户配置文件。

[0087] 此配置文件的替代物可以是在上下文传送管理器之间所传送的。对一般用户配置文件 (GUP) 或者 CC/PP 的派生的使用，有助于信号传送。然而，所传送的数据可以不是位于主上下文传送管理器 200 的数据库中的原始用户配置文件的直接拷贝。至少可以由临时假名来替代用户的标识，该临时假名允许对用户的会话进行标识并且允许针对假名对所传递

的服务进行计帐，但不允许关于用户习惯或跨越多个会话的移动模式的信息收集。另外，可以从主上下文传送管理器 200 传送至受访上下文传送管理器 600 的临时配置文件剥离对上下文生成过程无影响的所有数据。

[0088] 可以利用加密来确保临时用户配置文件的安全传送。加密过程可以提供保密性以及完整性保护。单独保密性仍可能允许攻击者把假的数据插入用户配置文件，从而可用作服务的拒绝 (DoS) 攻击。使用存在于两个操作器之间的安全关联，可以建立安全连接自身。可能不需要针对数据的特定应用协议。

[0089] 当时间方面不严格时，所推荐的上下文传送模式可以为前摄模式。然而，使用后摄模式也是可行的。在此情况下，移动节点 207 在移交过程开始之后请求上下文传送。上下文传送管理器 200、600 可以通过新访问网络 221、621 接收此请求，并且可以把移动节点 207 的上下文返回给访问网络上下文管理器 209、210、211、609、610、611。上下文传送管理器 200、600 能够通过追踪移动节点 207 的移动和通过对相邻的上下文进行预处理和高速缓冲存储，来使响应时间保持较短。

[0090] 以下，将参照图 4，给出从具有上下文传送功能的外部 AAA 服务器 (CTM、上下文生成器 201 等) 到 WLAN 的认证服务器 (AS) 或访问路由器的上下文传送过程的例子。

[0091] 针对此例子可做出下列假设 ：允许移动节点根据 WLAN 和 3GPP 操作器之间的协议来使用 WLAN。移动节点的主操作器具有关于存储在数据库中的 WLAN 的能力的充分信息，并且具有导出所需加密数据的技术能力。移动节点处于被连接至访问网络并且尚未开始向新访问网络移交的状态。另外，使 WLAN 中的认证服务器 (AAA) 能够把 IAPP.CACHE-NOTIFY 消息发送至访问点，请求 AP 把移动节点的上下文条目插入其高速缓冲存储器，通常按 IEEE802.11f-D5 在两个访问点之间的网络交换的消息，IEEE 802.11f-D5 为 2003 年 1 月的 IEEE 草案“Recommended Practice for Multi-Vendor Access point ;Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation(多销售商访问点的推荐实践 ;经由支持 IEEE 802.11 操作的跨分布系统的访问点间协议的互操作性)”。

[0092] AAA 服务器可以把适当的上下文传送 401 至相邻选择过程作为相邻所检测的 WLAN 的认证服务器。接下来，AAA 服务器可以通过当前链路向 UE(即，移动终端中的移动性管理器) 通知其与其它访问网络的下个可能的连接的上下文参数 (例如，WLAN 的成对主密钥、SSID 等)。上下文参数还可用于 WLAN 内“特征上下文”。也可以包括其它独立的上下文字段。

[0093] 接收具有有效数据的上下文的每个相邻认证服务器可以启动针对含有所接收的上下文的所有相关访问点的 IAPP.CACHE-NOTIFY 消息 403。每个 WLAN 访问点可具有读取 IAPP.CACHE-NOTIFY 消息中的所传递上下文并且把该上下文插入 PMK SA 表的应用，其中所述上下文在我们的情况下可以是成对主密钥 (PMK) 安全关联 (SA)。对于访问点，其现在似乎为已通过了密钥建立过程的移动节点，通常在访问访问网络的新客户机上执行该密钥建立过程。

[0094] 当移动节点或客户机与访问点相关联 404，而且为其已通过先前连接而接收到上下文数据时，可以直接发送鲁棒安全网络 (RSN) 信息元素内的 PMKID，其中列出了关联请求的密钥密码、认证以及由 STA 所支持的密钥管理算法 (参见 IEEE 802.11i-D5 中的 7.3.2.9

节“媒体访问控制 (MAC) 安全增强”，IEEE 草案，2003 年 8 月）。

[0095] 然后，访问点可以识别由 PMKID 所参照的 PMK，并且围绕初始 EAPOL 过程直接启动与客户机的 4 路握手 405。这既节省了访问点和访问服务器之间的认证握手，又节省了 WLAN 访问服务器和 AAA 服务器之间的认证握手。

[0096] 客户机和访问点之间的 4 路握手生成了刷新的临时成对和组密钥 (PTK 和 GTK)，以确保接下来的单播和多播用户数据传送的安全。如果客户机在扩展的服务集 (ESS) 内进一步漫游 406，则 WLAN 中正在进行的上下文传送可以在无远距离 AAA 服务器的交互的情况下，由内部机制加以完成。

[0097] WLAM 中 AAA 服务器和认证服务器之间的上下文传送过程与 HPLMN 和 VPLMN AAA 服务器相同。此可以通过主和受访域中的上下文传送管理器之间的上下文传送管理的移交而完成。WLAM 认证服务器不可能从代理上下文传送管理器对原始和后处理上下文进行区分。其仅可以在来自不可信或可信源的上下文数据之间进行区分。

[0098] 由于访问点的 PMK 安全关联高速缓冲存储器中的安全关联超时，或者向 WLAN 的上下文传送完全失败，则所列过程可能失败。在此情况下，4 路握手失败，而启动使用诸如可扩展认证协议 (EAP) 握手的正常认证处理。对于此握手，可以使用允许互相认证的 EAP 机制。在我们的所给出的例子中，可以使用 IETF 草案 EAP-SIM 和 EAP-KAK 中所描述的机制（参见 Haverinen 等的“EAP SIM Authentication（认证）”，IETF 因特网草案，2003 年 10 月；以及 Arkko 等的“EAP AKA Authentication（认证）”，IETF 因特网草案，2003 年 10 月），而提供互相认证。它们使用了用于用户标识和密钥生成的 SIM（订户标识模块）或 USIM(UMTS SIM) 卡中的加密功能。

[0099] 以下各节中将更详细地解释 PMK 安全关联数据的生成。标准的机制使用散列函数 (Hash Function)(HMAC-SHA1-128) 来创建 PMKID。此散列函数是单向函数，因此不能直接用于检索针对散列算法的源信息。散列函数仅允许检查带有未知输入参数的散列函数是否会得到与带有已知输入参数的参照散列函数相同的结果。如果结果相同，则输入参数一定也相同。对于 PMKID 生成，可以把值 PMK、PMK 名、BSSID（基本服务集合标识）以及客户机的 MAC 地址用作散列函数的输入值。当把客户机连接于访问点时，这些值可用于访问点。因此，访问点可创建完整的 PMK 安全关联条目。在我们的例子中，不能够由本地访问点创建此条目，而可由上下文传送管理器 200 创建该条目。在客户机漫游的访问网络中，上下文传送管理器 200 可以通过其访问网络能力数据库来了解 WLAN 的 SSID，但其不了解访问点，特别是它们的 BSSID。这意味着，在使用 HMAC-SHA1 算法计算 PMKID 的过程中，上下文传送管理器 200 不可使用 BSSID。

[0100] 一种方案是，可以推迟 PMKID 的计算，从而在切换到访问网络之前推迟向该访问网络的上下文传送，直至客户机已通过信标消息收到 BSSID 和 SSID。然后，移动性管理器 208 可以把所检测到的 BSSID 和 SSID 发送回上下文传送管理器 200，上下文传送管理器 200 根据 SSID 决定访问网络。

[0101] 根据本发明的另一个实施例，上下文传送管理器 200 可以计算 PMKID，并且进行向访问网络的上下文传送管理器 200 的上下文传送，并且通过其传送至具有所检测到的 BSSID 的访问点。上下文很可能不能到达访问点，这将再次导致后摄上下文传送，可以针对访问网络中每个访问点发送单个上下文消息。这可能要求对上下文传送管理器 200 的 WLAN

基础结构有完全的了解，而这是不能够期待的。

[0102] 解决生成 PMK 安全关联问题的另一种方案是，把 PMKID 的处理委托给 WLAN 中的上下文管理器 209、210、211。上下文管理器 209、210、211 可以把所计算的 PMKID 与从上下文传送管理器 200 所接收的客户机附加上下文一起发送至访问点。客户机本身可能已根据从上下文传送管理器 200 通过移动性管理器 208 接收到的访问网络的信息、和 WLAN 信标中所检测到的 BSSID，计算出同样的 PMKID。此方案把 PMKID 计算的负担从上下文传送管理器 200 卸下，并将其分布至 WLAN 上下文管理器 209、210、211 以及移动客户机 207，从而可能仅导致性能问题。如果上下文传送失败，则客户机应能够以任何方式进行计算。

[0103] 对于 WLAN，PMKID 仅用作用于从高速缓冲存储器选择 PMK 安全关联的唯一且不可预测的标识符。可以使用在对等体之间永不交换的 PMK，在具有质询 / 响应技术的 4 路握手（参见图 4）内部检查安全关联本身的有效性。因此，对于欺诈 (rogue) 客户机的 PMKID 的权利猜测依然不会危及成对主密钥的安全。这可允许便捷地解决我们的不能计算正确 PMKID 的问题。上下文传送管理器 200 可以在不使用散列函数的情况下，生成随机的 128 位数作为 PMKID。此捷径可意味着两个问题：首先，可通过 WLAN 上下文管理器 209、210、211 把 PMKID 从上下文传送管理器 200 传播至访问点，其次，存在着随机产生的 PMKID 和访问点的本地 PMK 安全关联高速缓冲存储器中的条目之间发生冲突的可能性。以下诸节给出了对这种冲突可能性的估计：

[0104] 可以假设 HMAC-SHA1 算法创建了等同分布的散列值。PMKID 具有 128 位，这导致了 $3.4 \cdot 10^{38}$ 个可能的值，并且给出了针对将产生不同值的 $P(X) = 2.9 \cdot 10^{-39}$ 种可能性。对于我们的情况，这意味着我们随机计算的 PMKID 与包含此 $P(\text{碰撞}) = P(X) = 2.9 \cdot 10^{-39}$ 可能性的一个条目的高速缓冲存储器中的 PMKID 条目相匹配。如果我们假设高速缓冲存储器大小为 n 个 PMKID 条目，则碰撞的可能性为 $P(\text{碰撞}) = n \cdot P(X) = n \cdot 2.9 \cdot 10^{-39}$。对于 1000 个高速缓冲存储器条目，这将产生 $P(\text{碰撞}) = 2.9 \cdot 10^{-36}$ 可能性，仍是非常小的可能性。

[0105] 有益的是，上下文传送管理器 200 可以预先分布 PMKID，无论是客户机还是 WLAN 上下文管理器 209、210、211，都必须自行计算 PMKID，从而节省了处理时间和能力，并且可能缩短来自客户机的关联请求准备好向访问点发送之前的时间。对于 WLAN 上下文管理器 209、210、211，这可能意味着把相同的上下文数据集发送至所有所需的访问点，并且不计算针对任何访问点的特定上下文。

[0106] 以下，将参照图 5 中所示的流程图，对本发明根据另一个实施例所提出的上下文传送机制进行总的概述。上下文传送管理器 200 可以从移动节点 207 或可由上下文传送管理器 200 访问的 AAA 接收 501 将加以估计的位置信息。当从传递源接收到位置信息时，上下文传送管理器 200 可以把此信息传送至功能或装置，该功能或装置根据移动节点的位置来决定 502 在移交的情况下移动节点 207 可以连接的相邻访问网络。例如，可以通过图 2 和 6 中所示的相邻定位器 202 来实现此功能。

[0107] 例如，由标识符标识移动节点 207 将可以连接的相邻访问网络，如先前所概要性描述的。另外，也可以把移动节点的标识符包括在传递至下个处理步骤的信息中。根据标识相邻网络和移动节点 207 的 ID，接下来，上下文传送管理器 200 可以使用上下文生成功能或装置来动态地生成 503 对于相邻访问网络和移动节点 207 的适当上下文。重要的是，应注意，取决于相邻网络的访问技术，上下文传送管理器 200 所生成的上下文在其参数方面

可能不同。移动节点 207 还可以接收特别调整为移交所需的信息的上下文，如先前所概要性描述的。

[0108] 当已经针对相邻网络和移动节点 207 生成了不同的上下文时，上下文传送管理器 200 可以把所有上下文传送 504 至相应的访问网络和移动节点 207。

[0109] 当在移动节点 207 处接收 505 上下文时，示例性地假设向下个访问网络的移交尚未执行，移动节点 207 可以根据包含在从上下文传送管理器 200 所接收的上下文中的信息，来预配置 506 其网络设备。例如，在 IPv6 网络中，在使用 WLAN 接口的情况下，移动节点 207 可以使用新 IP 地址、新默认网关等对网络接口进行预配置，使得当决定 507 接下来将加入的访问网络时，以及当向其进行移交时，可以接管预配置设置，并且可以使用网络接口的新配置立即启动 508 与新访问网络的通信。

[0110] 从上下文传送管理器 200 接收 509 上下文的访问网络还可以使用其中的信息来准备 510 可能连接移动客户机 207 的访问网络。为了能够关联连接移动客户机 207 的特定配置，可以把标识符包括在将传输至相邻访问网络中的上下文管理器 209、210、211 的上下文中，从而允许它当移动节点 207 连接于该网络时标识移动节点 207，并且利用通信 511 的上下文信息。

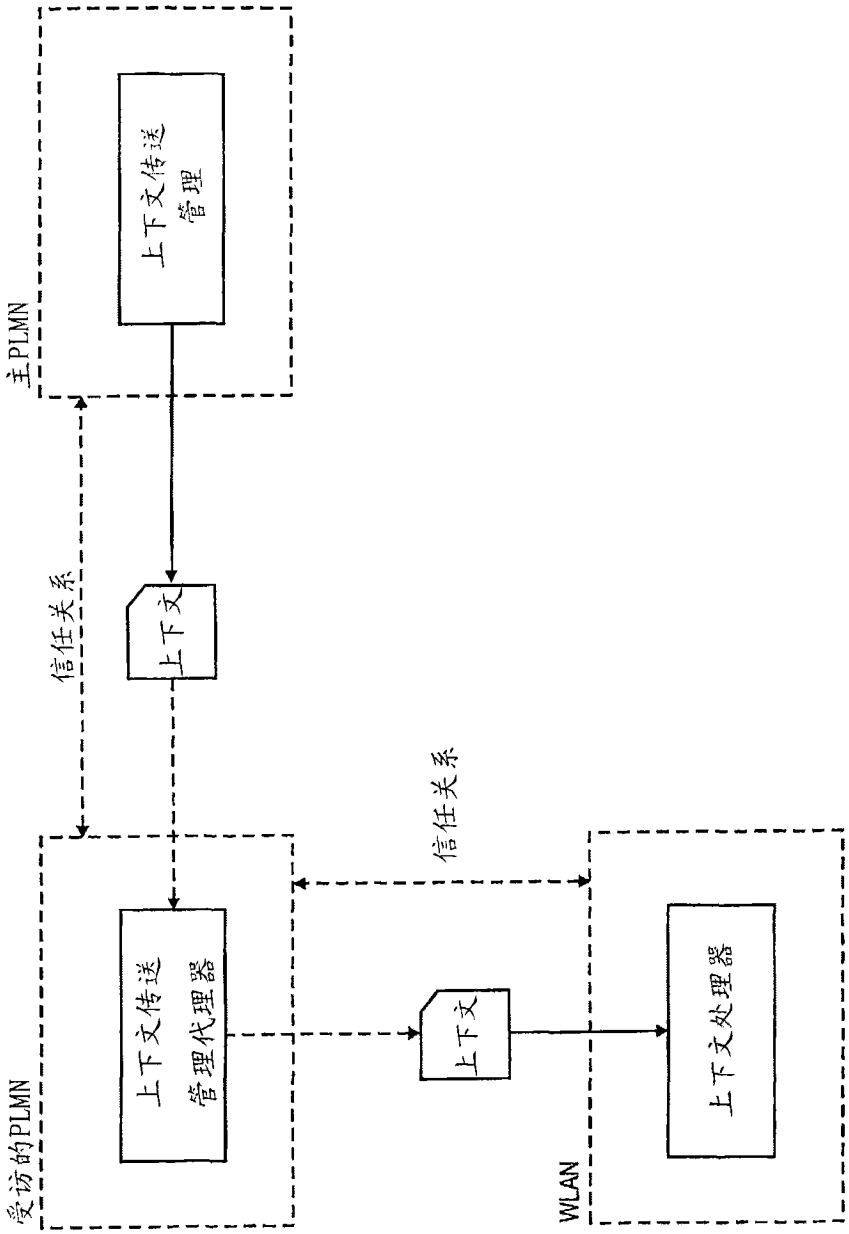

主PLMN
上下文传送管理
信任关系
上下文
受访的PLMN
上下文传送管理代理器
信任关系
上下文
WLAN
上下文处理器

图 1

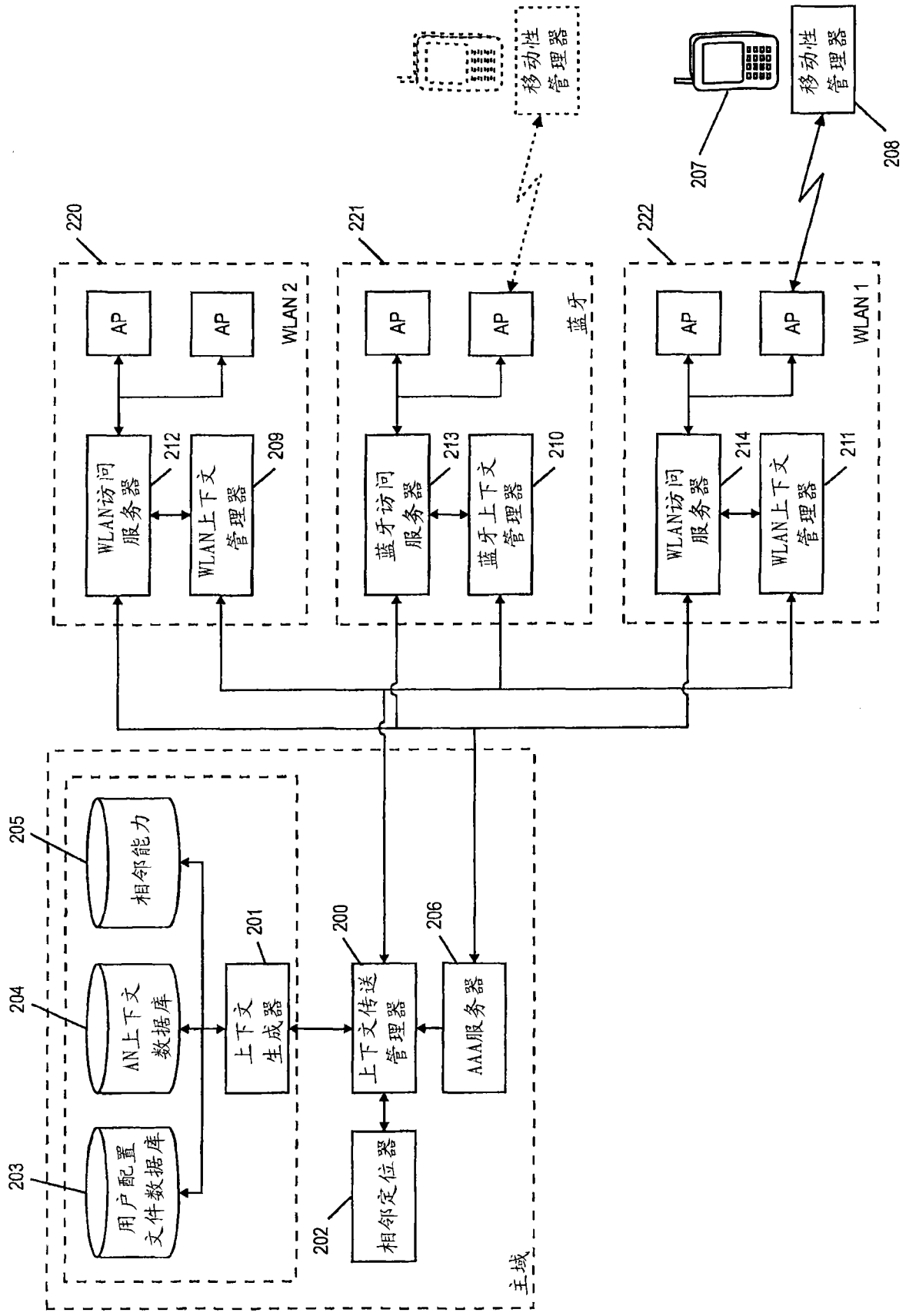

移动性管理器
207
208
移动性管理器
220
221
222
AP
AP
AP
AP
AP
AP
WLAN 2
蓝牙
WLAN 1
WLAN访问服务器
212
WLAN上下文管理器
209
蓝牙访问服务器
213
蓝牙上下文管理器
210
WLAN访问服务器
214
WLAN上下文管理器
211
205
相邻能力
204
AN上下文数据库
203
用户配置文件数据库
201
上下文生成器
200
上下文传送管理器
206
AAA服务器
202
相邻定位器
主域

图 2

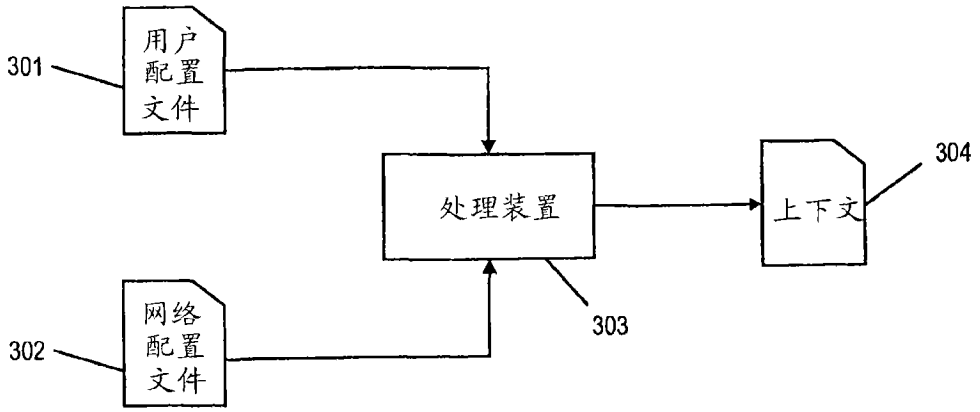

用户配置文件
301
网络配置文件
302
处理装置
303
上下文
304

图 3

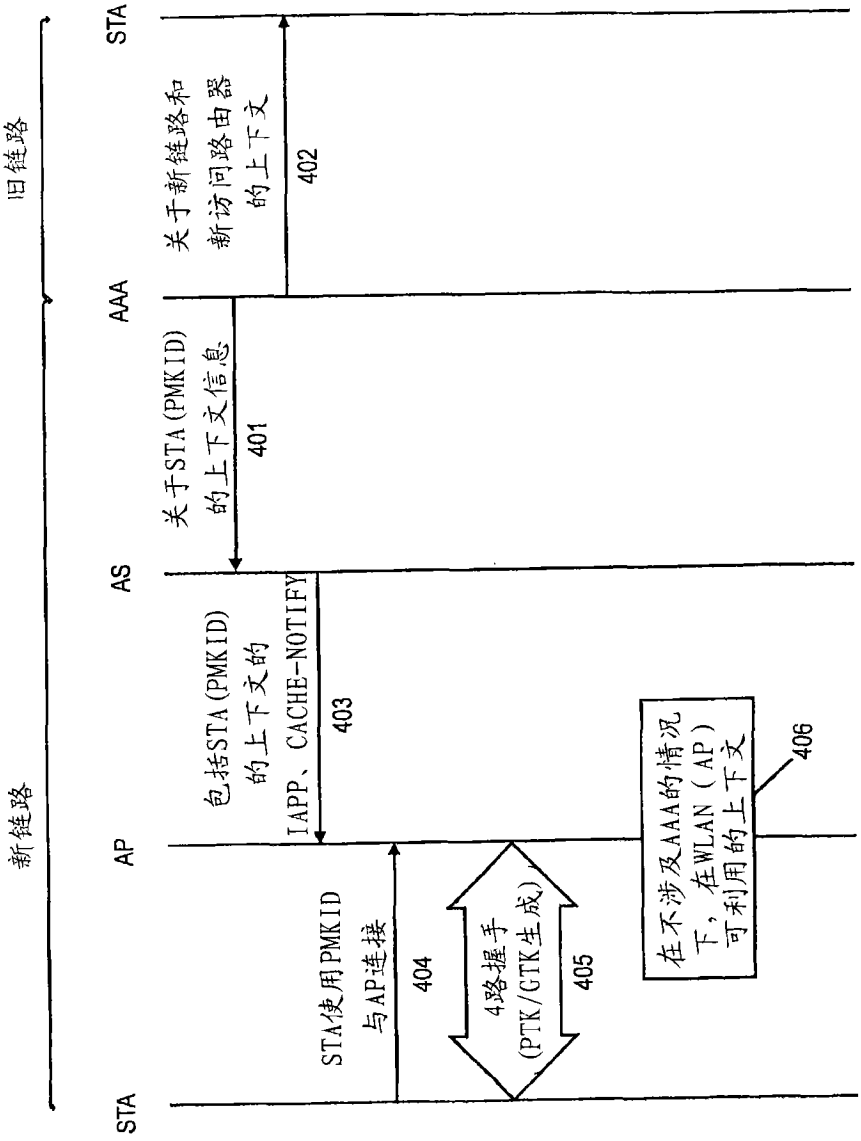

旧链路
新链路
STA
AAA
AS
AP
STA
关于新链路和新访问路由器的上下文
402
关于STA(PMKID)的上下文信息
401
包括STA(PMKID)的上下文的IAPP、CACHE-NOTIFY
403
STA使用PMKID与AP连接
404
4路握手(PTK/GTK生成)
405
在不涉及AAA的情况下，在WLAN(AP)可利用的上下文
406

图 4

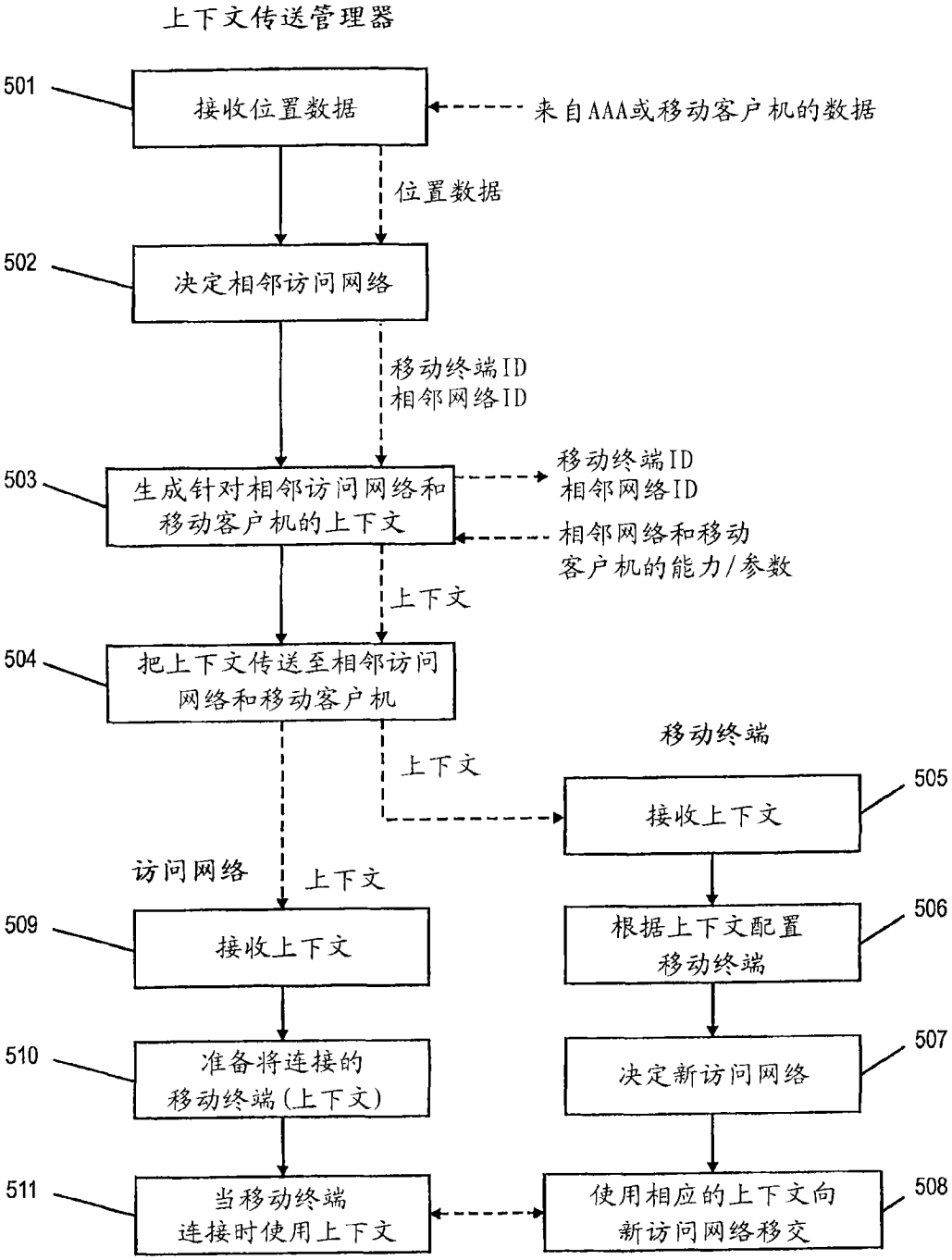

上下文传送管理器
501
接收位置数据
来自AAA或移动客户机的数据
位置数据
502
决定相邻访问网络
移动终端ID
相邻网络ID
503
生成针对相邻访问网络和移动客户机的上下文
移动终端ID
相邻网络ID
相邻网络和移动客户机的能力/参数
上下文
504
把上下文传送至相邻访问网络和移动客户机
移动终端
上下文
505
接收上下文
访问网络
上下文
509
接收上下文
506
根据上下文配置移动终端
510
准备将连接的移动终端(上下文)
507
决定新访问网络
511
当移动终端连接时使用上下文
使用相应的上下文向新访问网络移交
508

图 5

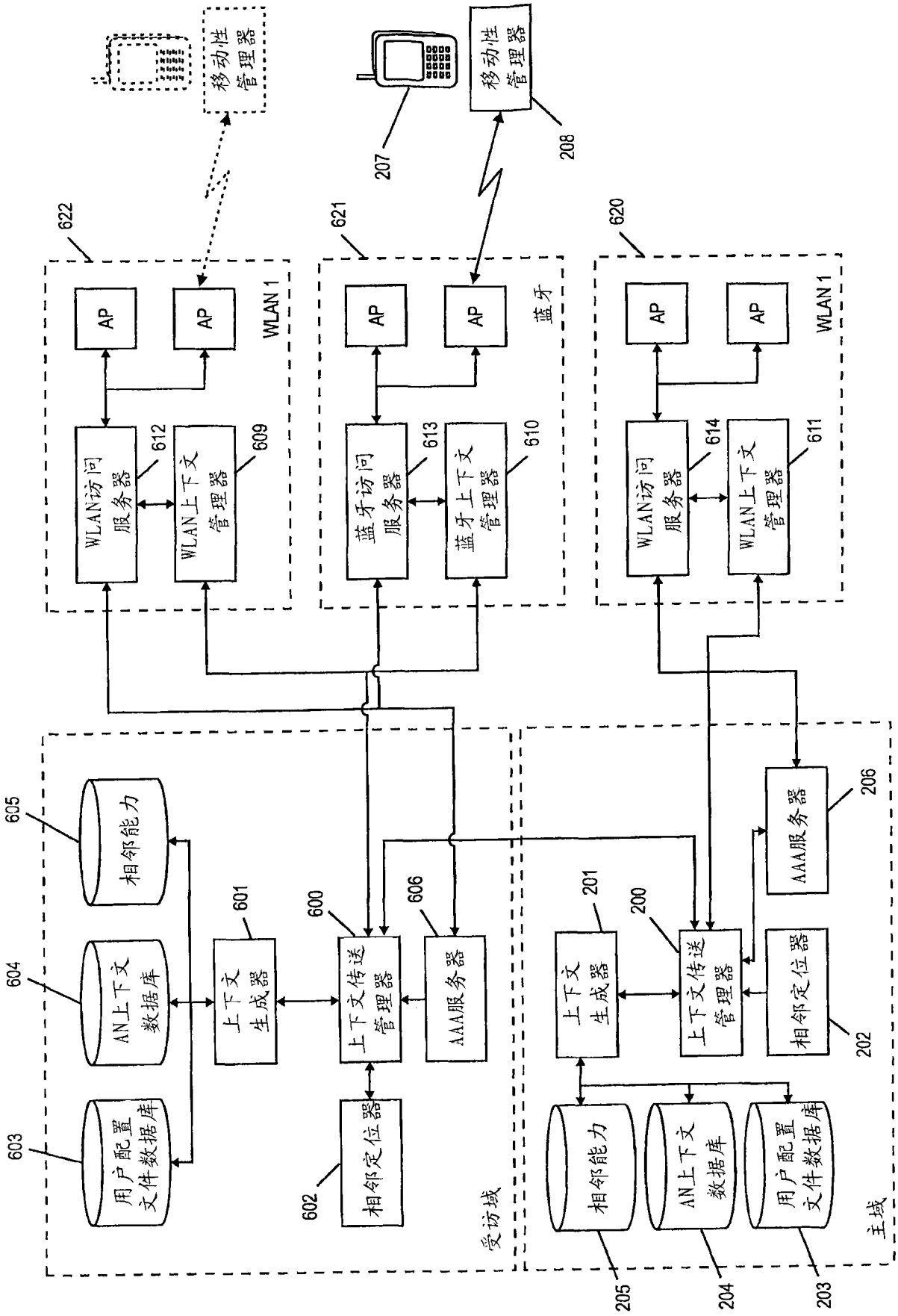

移动性管理器
移动性管理器
207
208
622
621
620
AP
AP
AP
AP
AP
AP
WLAN 1
蓝牙
WLAN 1
WLAN访问服务器
612
WLAN上下文管理器
609
蓝牙访问服务器
613
蓝牙上下文管理器
610
WLAN访问服务器
614
WLAN上下文管理器
611
605
相邻能力
604
AN上下文数据库
603
用户配置文件数据库
601
上下文生成器
600
上下文传送管理器
606
AAA服务器
602
相邻定位器
受访域
201
上下文生成器
200
上下文传送管理器
206
AAA服务器
202
相邻定位器
205
相邻能力
204
AN上下文数据库
203
用户配置文件数据库
主域

图 6