(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 102017577 B
(45)授权公告日 2015.02.04

(21)申请号 200980116689.1

(22)申请日 2009.05.06

(30)优先权数据
61/050,829 2008.05.06 US
61/050,845 2008.05.06 US
12/436,090 2009.05.05 US

(85)PCT国际申请进入国家阶段日
2010.11.04

(86)PCT国际申请的申请数据
PCT/US2009/043045 2009.05.06

(87)PCT国际申请的公布数据
WO2009/137625 EN 2009.11.12

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 B·R·库克 J·A·德克 D·萨勒

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈炜 高见

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04W 12/04(2009.01)
H04W 12/06(2009.01)

(56)对比文件
WO 99/26124 A1,1999.05.27, 说明书第5页11-14行,第7页1-13行,第12页16-27行,附图1-4.
EP 1555843 A1,2005.07.20, 全文.
WO 2006/132540 A1,2006.12.14, 全文.

审查员 王伦杰

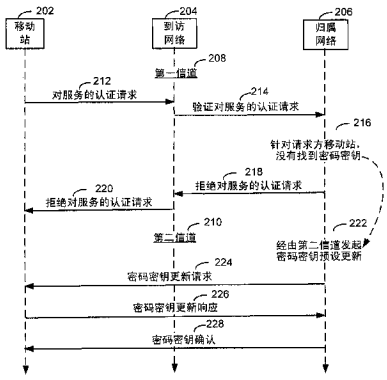
权利要求书2页 说明书14页 附图12页

(54)发明名称

认证到访网络中的无线设备

(57)摘要

提供了用于服务请求的替换性认证办法。对于在不支持对用于合意服务的密码密钥进行传统更新(例如,动态移动IP密钥更新)的到访网络中漫游的移动站,可以不同方式实现此类密码密钥认证。作为在归属网络处未找到移动站的密码密钥时仅仅拒绝服务请求的替代,归属网络发起一过程,藉由该过程,文本消息信道被用来与请求方移动站建立此类密码密钥。替换地,归属网络可利用其他信息——诸如请求方移动站的可验证标识符或凭证(例如,IMSI、MIN等)——连同请求方无线移动站的漫游状况来验证移动站并准许对网络服务的接入,从而允许建立所请求的服务。



CN 102017577 B

1. 一种在无线移动站上操作的用于从到访网络获得服务的方法，所述方法包括：

向到访网络节点发送服务请求以建立需要来自归属网络的认证的数据服务；

在所述无线移动站处，在文本消息接发信道上接收对用于所述数据服务的密码密钥的请求，其中对文本消息接发信道上的密码密钥的所述请求是在需要认证的服务请求被归属网络拒绝时由所述归属网络发起的；以及

在所述文本消息接发信道上发送用于所述数据服务的所述密码密钥。

2. 如权利要求 1 所述的方法，其特征在于，还包括：

在所述无线移动站上生成所述密码密钥。

3. 如权利要求 2 所述的方法，其特征在于，还包括：

在所述文本消息接发信道上发送具有所述密码密钥的认证消息；以及

接收确定对所述数据服务的建立的确认。

4. 如权利要求 1 所述的方法，其特征在于，所述服务请求包括点对点协议 (PPP) 移动网际协议 (MIP) 注册请求 (RRQ) 消息。

5. 如权利要求 1 所述的方法，其特征在于，所述密码密钥包括移动网际协议 (MIP) 密钥。

6. 如权利要求 1 所述的方法，其特征在于，所述数据服务是在与所述文本消息接发信道不同的第一信道上执行的。

7. 如权利要求 6 所述的方法，其特征在于，所述第一信道具有比所述文本消息接发信道更高的数据率。

8. 如权利要求 1 所述的方法，其特征在于，所述密码密钥受所述归属网络的公钥保护地被发送给所述归属网络。

9. 如权利要求 1 所述的方法，其特征在于，所述收到请求是动态移动 IP 密钥更新请求。

10. 如权利要求 1 所述的方法，其特征在于，所述密码密钥作为动态移动 IP 密钥更新响应的部分来发送。

11. 一种在无线移动站上操作的用于从到访网络获得服务的系统，包括：

用于向到访网络节点发送服务请求以建立需要来自归属网络的认证的数据服务的装置；

用于在文本消息接发信道上接收对用于所述数据服务的密码密钥的请求的装置，其中对文本消息接发信道上的密码密钥的所述请求是在需要认证的服务请求被归属网络拒绝时由所述归属网络发起的；以及

用于在所述文本消息接发信道上发送用于所述数据服务的所述密码密钥的装置。

12. 如权利要求 11 所述的系统，其特征在于，所述数据服务是在与所述文本消息接发信道不同的第一信道上执行的。

13. 如权利要求 12 所述的系统，其特征在于，所述第一信道具有比所述文本消息接发信道更高的数据率。

14. 一种在用于归属网络中操作的方法，所述方法用于为在到访网络中漫游的无线移动站认证通信服务，所述方法包括：

从所述到访网络接收关于无线移动站建立需要密码密钥的数据服务的服务请求；

在所述服务请求被归属网络拒绝时使用文本消息接发信道向所述无线移动站发送更

新请求以更新所述密码密钥；以及

经由所述文本消息接发信道从所述无线移动站接收用于所述数据服务的所述密码密钥。

15. 如权利要求 14 所述的方法，其特征在于，还包括：

确定所述无线移动站的密码密钥在所述归属网络处不可用；以及

通过发送所述更新请求发起密钥预设过程。

16. 如权利要求 14 所述的方法，其特征在于，还包括：

一旦接收到所述密码密钥，就向所述到访网络发送认证所述服务请求的消息。

17. 如权利要求 14 所述的方法，其特征在于，所述服务请求是在第一信道上接收到的，但是所述更新请求是在与所述第一信道不同的所述文本消息接发信道上发送的。

18. 如权利要求 14 所述的方法，其特征在于，所述服务请求包括点对点协议 (PPP) 移动网际协议 (MIP) 注册请求 (RRQ) 消息。

19. 如权利要求 14 所述的方法，其特征在于，所述密码密钥包括移动网际协议 (MIP) 密钥。

20. 如权利要求 14 所述的方法，其特征在于，所述数据服务是在与所述文本消息接发信道不同的第一信道上执行的。

21. 如权利要求 20 所述的方法，其特征在于，所述第一信道具有比所述文本消息接发信道更高的数据率。

22. 如权利要求 14 所述的方法，其特征在于，所述更新请求是动态移动 IP 密钥更新请求。

23. 如权利要求 14 所述的方法，其特征在于，所述密码密钥作为动态移动 IP 密钥更新响应的部分被接收。

24. 一种在归属网络中操作的系统，所述系统用于为在到访网络中漫游的无线移动站认证通信服务，所述系统包括：

用于从所述到访网络接收关于所述无线移动站建立需要密码密钥的数据服务的服务请求的装置；

用于在所述服务请求被归属网络拒绝时使用文本消息接发信道向所述无线移动站发送更新请求以更新所述密码密钥的装置；以及

用于经由所述文本消息接发信道从所述无线移动站接收用于所述数据服务的所述密码密钥的装置。

25. 如权利要求 24 所述的系统，其特征在于，所述服务请求是在第一信道上接收到的，但是所述更新请求是在与所述第一信道不同的所述文本消息接发信道上发送的。

认证到访网络中的无线设备

[0001] 背景

[0002] 根据 35U.S.C. §119 的优先权要求

[0003] 本专利申请要求于 2008 年 5 月 6 日提交的题为“Methods and Apparatus forAuthentication of Wireless Device in a Foreign Network Via SMS(用于经由SMS认证外地网络中的无线设备的方法和装置）的临时申请 No.61/050,829 以及于 2008 年 5 月 6 日提交的题为“Methods and Apparatus for Authentication ofWireless Device in a Foreign Network Via IMSI Check(用于经由IMSI核查来认证外地网络中的无线设备的方法和装置）”的临时申请 No.61/050,845，这两个申请被转让给本受让人，并由此通过援引明确纳入于此。

[0004] 领域

[0005] 各个特征涉及保护到访无线通信网络中的数据通信。至少一个特征涉及经由短消息服务 (SMS) 或基于远程设备的唯一性标识符在到访网络中认证该远程设备。

[0006] 背景

[0007] 无线通信服务提供商或承运商常常向具有多个通信接口并在各种通信信道上操作的无线移动站（例如，移动电话等）提供服务。例如，无线移动站可被启用以进行语音信道上的语音通信、用于文本消息接发的短消息业务 (SMS) 和数据通信。通常，SMS 利用最少带宽，语音信道利用中等量的带宽，而数据服务（例如，多媒体内容流送）在这三种无线通信类型中利用最多带宽。承运商可销售能够进行所有三种通信类型的设备。

[0008] 承运商通常还具有与其他承运商的协定，用于允许从一个承运商的网络漫游至另一承运商网络。如果用户具有与特定承运商的服务合同，则属于此承运商的网络被称为归属网络。另一承运商的网络被称为到访网络。

[0009] 无线通信的安全性日益变得重要，尤其因为数据服务变得更普遍。例如，数据服务可被用于财务交易，诸如例如使用移动电话通过因特网购买物品。承运商已建立了用于保护无线通信的系统和方法。如果数据服务将被用在无线通信设备上，则当设备是首次用于数据服务时，通常预设数据服务的安全性。而且，某些服务可能引发生成用于数据服务的安全性的新密码密钥（例如，数据认证凭证）的需要。例如，承运商可发现无线移动站正被用于未授权数据服务。在此情形中，承运商可能希望生成用于该设备的新密码密钥。

[0010] 在多数情形中，在无线移动站售出之前，密码密钥被预设在无线移动站上。动态移动 IP 密钥更新 (DMU) 允许密钥在部署之后将被生成，并且为操作者自动化预设过程。然而，当启用 DMU 的无线移动站在到访网络中首次被用于数据服务或者另外在于到访网络中进行操作的同时需要新密码密钥时，会发生问题。在此情景中，无线移动站可能在已从归属网络获得有效安全性或密码密钥之前在到访网络中被使用。由于无线移动站尚未被预设用于保护数据服务，或者至少不具备正确的密码密钥，因此数据服务可能被其归属网络拒绝。这个问题的一个原因在于，到访网络可能不支持归属网络用来提供密码密钥的密钥预设过程（例如，DMU）。例如，当无线移动站尝试与到访网络建立数据连接时，到访网络联系归属网络以标识该无线通信设备。然而，无线移动站可能不具备数据通信所需的安全性 / 密码

密钥，因此归属网络向到访网络指示无线移动站未被授权来执行数据通信。由于到访网络可能不支持归属网络用来向无线移动站预设安全性 / 密码密钥的密钥预设过程，因此归属网络无法提供此类安全性 / 密码密钥。因而，已对数据服务订立合同的用户可能无法使用数据服务，即使用户应当能够使用数据服务并且如果无线移动站于到访网络中被用于数据服务之前在归属网络中仅已获得正确安全性 / 密码密钥至少一次就将能够使用数据服务。

[0011] 动态移动 IP 密钥更新 (DMU) 是向无线移动设备预设密码密钥的示例。DMU 是用于分发和更新移动 IP 密码密钥的安全且高效的机制，该机制例如可由用于码分多址 (CDMA) 网络的演进数据最优化 (EV-DO)、用于全球移动通信系统 (GSM) 网络的通用分组无线电业务 (GPRS) 和增强型数据率 GSM 演进 (EDGE) 和宽带 CDMA 来实现。DMU 程序可在移动设备与网络认证、授权和计帐 (AAA) 服务器之间实现，并且通过允许个体用户密钥和简化在一个密钥被暴露的情况下密钥的更新来提升网络的安全性。

[0012] 提供一种用于即使在无线移动站正于可能不支持其归属网络的典型密钥预设过程的到访网络中操作时亦能生成并向该无线移动站分发密码密钥及其他安全性特征的方法将会是有价值的。

[0013] 概述

[0014] 向无线移动站提供了用于在到访网络——该到访网络针对合意服务不支持对密码密钥进行传统更新（诸如动态移动 IP 密钥更新）——中漫游时更新其密码密钥的各种办法。

[0015] 根据第一特征，提供了一种在无线移动站上操作的方法，该方法用于从不支持移动站的典型密钥更新协议的到访网络获得服务。移动站可向到访网络节点发送服务请求以建立需要来自归属网络的认证的数据服务。例如，服务请求可包括点对点协议 (PPP) 移动网际协议 (MIP) 注册请求 (RRQ) 消息。作为响应，移动站可在文本消息接发信道上接收对用于数据服务的密码密钥的请求，其中该请求是由归属网络发起的。收到请求可以是例如动态移动 IP 密钥更新请求。移动站可获得或生成密码密钥，并在文本消息接发信道上发送用于数据服务的密码密钥。密码密钥可例如作为动态移动 IP 密钥更新响应的部分来发送。在一种实现中，密码密钥可包括移动网际协议 (MIP) 密钥。移动站可在文本消息接发信道上发送具有密码密钥的认证消息。密码密钥可受归属网络的公钥保护地被发送给归属网络。作为响应，移动站可接收确定数据服务的建立的确认。可在与文本消息接发信道不同的第一信道上执行数据服务。第一信道可具有比文本消息接发信道更高的数据率。

[0016] 根据在归属网络服务器上操作的第二特征，当在归属网络处未找到请求方移动站的密码密钥时不是仅仅拒绝服务请求，而是作为替代，归属网络服务器可发起一过程，藉由该过程文本消息接发信道被用于与请求方移动站建立此类密码密钥。提供了一种在归属网络中操作的方法，该方法用于为在到访网络中漫游的无线移动站认证通信服务。在此方法中，再次假定到访网络不向移动站支持用于与归属网络建立或更新其密码密钥的传统方法。归属网络服务器可从到访网络接收关于无线移动站建立需要密码密钥的数据服务的服务请求。服务请求可包括点对点协议 (PPP) 移动网际协议 (MIP) 注册请求 (RRQ) 消息。归属网络可确定无线移动站的密码密钥在归属网络处不可用，并由此可通过发送更新请求发起密钥预设过程。归属网络可在随后使用文本消息接发信道向无线移动站发送更新请求以更新密码密钥。更新请求可以是动态移动 IP 密钥更新请求。作为响应，可经由文本消息接

发信道从无线移动站接收用于数据服务的密码密钥。密码密钥可作为动态移动 IP 密钥更新响应的部分来接收。密码密钥可包括移动网际协议 (MIP) 密钥。一旦接收到密码密钥，归属网络就向到访网络发送认证服务请求的消息。在一个示例中，服务请求可以是在第一信道上接收的，但是更新请求可以是在与第一信道不同的文本消息接发信道上发送的。可在与文本消息接发信道不同的第一信道上执行数据服务。第一信道可具有比文本消息接发信道更高的数据率。

[0017] 在替换性办法中，归属网络可利用其他信息——诸如请求方无线移动站的可验证标识符或凭证（例如，IMSI、MIN 等）——连同请求方无线移动站的漫游状况来验证移动站并向移动站准许对所请求服务的网络接入。

[0018] 因此，另一特征提供在无线移动站上操作的用于从到访网络获得服务的方法。无线移动站可向到访网络节点发送服务请求以建立需要来自归属网络的认证的数据服务。作为响应，无线移动站可接收指示归属网络已准许对所请求的服务的网络接入的消息。然而，此类接入可被准许，而无需移动站首先已与归属网络建立密码密钥。在一个示例中，服务请求可包括无线移动站的唯一性标识符，该唯一性标识符允许归属网络验证移动站是订户。服务请求还可包括到访网络标识符，该到访网络标识符允许归属网络验证无线移动站正在漫游。

[0019] 又一特征提供了一种在归属网络中操作的方法，该方法用于为在到访网络中漫游的无线移动站认证通信服务。归属网络（或其中的一个或多个服务器或实体）可从到访网络接收关于无线移动站建立需要密码密钥的数据服务的服务请求。归属网络可确定无线移动站的密码密钥在归属网络处是否可用。如果针对所请求的服务在归属网络处没有找到有效的密码密钥，但是无线移动站被肯定地验证为归属网络的订户且其正在到访网络中漫游，则归属网络可向到访网络发送向无线移动站准许网络接入的消息。

[0020] 附图简述

[0021] 在结合附图理解下面阐述的详细描述时，本发明各方面的特征、本质和优点将变得更加显而易见，在附图中，相同参考标记始终作相应标识。

[0022] 图 1 是图解网络环境的框图，在该网络环境中可实现用于在到访网络中对移动站进行密钥预设或更新的一个或多个特征。

[0023] 图 2 是图解即使在可能不支持归属网络的典型密钥预设过程的到访网络中操作时可如何用密码密钥来预设移动站的框图。

[0024] 图 3 是图解用于使移动站能在到访网络中经由较低带宽的协议更新用在数据通信信道上的安全性状态——诸如密码密钥——的呼叫流的示图。

[0025] 图 4 是图解用于在到访网络中预设具有数据服务的移动站的替换性方法的示图，移动站在该到访网络中可能未使用此类数据服务通常所需的必要密钥预设过。

[0026] 图 5 是图解移动站 200 的示例的框图，该移动站在到访网络中漫游时可适于根据替换性方法更新其密码密钥。

[0027] 图 6 图解了用于在无线移动站上操作的方法，该方法供在无线移动站在到访网络中漫游时与归属网络建立密码密钥之用。

[0028] 图 7 图解了用于在无线移动站上操作的另一方法，该方法供在无线移动站在到访网络中漫游时与归属网络建立密码密钥之用。

[0029] 图 8 是图解归属网络认证、授权和计帐服务器的一个示例的框图。

[0030] 图 9 图解了在归属网络中操作的方法，该方法用于为在到访网络中漫游的无线移动站认证通信服务。

[0031] 图 10 图解了在归属网络中操作的另一方法，该方法用于为在到访网络中漫游的无线移动站认证通信服务。

[0032] 图 11 是根据一个示例的动态移动 IP 密钥更新服务器的框图。

[0033] 图 12 图解了用于在动态移动 IP 密钥更新服务器中操作的方法，该方法用于通过使用文本消息接发信道向在到访网络中漫游的无线移动站发起密钥更新。

[0034] 详细描述

[0035] 在以下描述中，给出了具体细节以提供对诸实施例的透彻理解。但是，本领域普通技术人员将可理解，没有这些具体细节也可实践这些实施例。例如，可以用框图示出电路以免使这些实施例混淆在不必要的细节中。在其他实例中，公知的电路、结构、和技术可能被具体示出以免与这些实施例相混淆。

[0036] 如本文中所用的，术语“移动站”可以指——但不限于——移动电话、蜂窝电话、通信设备、无线设备、个人数字助理、和 / 或具备无线通信能力的手持计算设备。术语“归属网络”可以指移动站向其订阅以接收服务的服务提供商或无线承运商。“到访网络”可以指不是“归属网络”的服务提供商或无线承运商。术语“数据通信”和 / 或“数据设备”可以指语音信道和 / 或短消息业务信道之外的数据信道。

[0037] 概览

[0038] 根据一个特征，漫游移动站可能在到访网络中尝试数据连接，而没有首先生成密码密钥并与其归属网络交换这些密钥。到访网络可向归属网络通知对数据服务的接入的请求。连接可能被归属网络拒绝（由于针对数据服务，移动站尚未被认证），但是归属网络可触发或发起用于与移动站建立 SMS 信道的过程，通过该 SMS 信道对移动站的认证可向归属网络提供所生成的密钥。归属网络可经由 SMS 信道生成并发送安全性更新请求（即，作为 SMS 消息的部分）。

[0039] 移动站可被配置成通过 SMS（从归属网络）接收安全性更新请求。移动站可识别指示 SMS 消息是安全性更新请求的 SMS 消息的属性。作为将 SMS 解释为给用户的例如文本消息的替代，移动站将 SMS 识别为安全性更新请求消息。这可通过使用例如消息类型标志或其他指示符——SMS 消息与控制信息（例如，安全性更新请求）有关——来实现。安全性更新请求可以是动态移动 IP 密钥更新程序 (DMU) 请求。DMU 是用于在一些网络中分发和更新移动 IP(MIP) 密码密钥的机制。

[0040] 一旦识别到已接收到请求消息，移动站就可生成认证更新消息并经由 SMS 将该认证更新消息发送给其归属网络。归属网络随后处理认证更新消息以提取由移动站生成的密码密钥。在归属网络处，归属认证、授权和计帐服务器 (H-AAA)、归属 SMS 中心 (H-SMSC)、和 DMU 服务器可被通信地耦合，以达成初始密码密钥生成和预设。H-SMSC 在例如 CDMA2000 网络中还可被称为消息中心 (MC)。例如，H-AAA 可经由到访网络接收关于移动站的认证请求。如果移动站尚未在之前获得恰当的密码密钥，则 H-AAA 可拒绝或拒斥认证请求。然而，当发生此类拒绝时，H-AAA 还可通知 DMU 服务器，由 DMU 服务器经由 H-SMSC 发起基于 SMS 的 DMU 请求。移动站识别收到的基于 SMS 的 DMU 请求，并经由 H-SMSC 向 DMU 服务器发送基于 SMS

的 DMU 更新。

[0041] 示例网络环境

[0042] 图 1 是图解网络环境的框图，在该网络环境中可实现用于在到访网络中对移动站进行密钥预设或更新的一个或多个特征。移动站 (MS)102 可能尚未从其归属网络针对数据通信服务被认证和 / 或获得有效密码密钥。移动站 102 在其首次寻求使用数据通信服务时可能正在到访网络 104 中漫游，或者可能需要新密码密钥。移动站 102 可尝试与到访网络 104 中的分组数据服务节点 (PDSN)110 建立数据连接。作为尝试建立数据连接的部分，或者在尝试建立数据连接之前，MS 102 在到访网络 104 中执行认证。例如，MS 102 可向归属网络 116 中的归属位置寄存器 (HLR) 执行认证。换言之，MS 102 向归属网络 116 中的 HLR 118 注册。一旦向 HLR 118 进行了注册，MS 102 就能执行语音呼叫以及发送和接收 SMS 消息。

[0043] 为了尝试建立数据连接，MS 102 与 PDSN 110 创建点对点协议 (PPP) 会话，并且可发送移动 IP(MIP) 注册请求 (RRQ) 消息。PPP 协议是用于在两个网络节点之间建立直接连接的因特网工程任务组 (IETF) 协议。BSC 108 将消息路由至分组数据服务节点 (PDSN)110。分组数据服务节点 110 处置诸如 MS 102 等连接至 BS 106 的移动站的分组数据。PDSN 110 可被连接至因特网 (未示出) 以在移动设备 102 与因特网之间路由分组数据，由此使得移动设备 102 能够与因特网交互。

[0044] PDSN 110 还可被连接至到访认证、授权和计帐服务器 (V-AAA)112。V-AAA 112 将 MS 102 标识为非其网络的成员。V-AAA 112 被连接到 MS 的归属网络 116 中的归属认证、授权和计帐服务器 (H-AAA)114。H-AAA 标识 MS 102 并注意到 MS 102 不具有有效密钥。自 V-AAA 向 H-AAA 的消息可以是移动节点 AAA 授权请求 (MN-AAA AUTH REQ) 消息。由于 MS 102 不具有有效密钥，因此 H-AAA 114 拒绝请求。然而，根据一个特征，H-AAA 114 可被配置成向安全性或密钥服务器 120 通知需要针对到访网络 104 中的 MS 进行密钥更新。安全性服务器 120 可以是动态移动 IP 密钥更新程序 (DMU) 服务器。DMU 是用于在 CDMA2000 网络中分发和更新移动 IP(MIP) 密码密钥的机制。

[0045] DMU 安全性服务器 120 通过在较低带宽信道上——例如在用于 SMS 消息接发的信道上——开始密钥更新过程来响应此对到访网络中的密钥更新的请求。因而，例如，DMU 服务器 120 向 MS 102 发起 SMS 消息以创建新密钥。具体地，MS 102 可创建新密钥，该新密钥将由 H-AAA 114 认证或验证。因此，DMU 服务器 120 通过 SMS 向 MS 102 发送密钥更新请求。密钥更新请求可以是例如短消息对等消息 (SMPP)，该消息具有声明“密钥更新请求”或诸如比方“DMU 请求”等一些类似声明的内容。因此，DMU 服务器 120 将“DMU 请求”消息发送给短消息服务中心 (SMSC)122 以便发送给 MS 102。DMU 服务器 120 可用与 MS 102 相对应的公共密钥来加密该消息。

[0046] SMSC 122 将经加密的 SMS 消息“DMU 请求”路由至 MS 102。V-AAA 112 通过将 SMS 消息发送给移动交换中心 (MSC)124 来继续将 SMS 消息路由至 MS 102。MSC 124 通过将 SMS 消息发送个 BSC 108 来将 SMS 消息路由至 MS102，BSC 108 将该消息发送给 BTS 106，BTS 106 通过空中将 SMS 消息发送给 MS 102。MS 102 接收经加密的消息，解密消息，并通过创建新密钥来作出响应。MS 102 生成经加密消息，该消息包括用网络的公钥加密的新密钥。MS102 通过 SMS 消息将经加密的消息发回给 DMU 服务器。包括新密钥的经加密的消息可以

是 DMU 更新消息。

[0047] DMU 更新消息可以是可在数据信道上使用的确切消息，但是替代地，该消息通过 SMS 来发送。SMS 消息具有最大 160 字节。所生成的新密钥可以是 Rivest Shamir Adleman(RSA)1024 密钥，其长度为 120 字节。如果需要更长的密钥长度，则使用多个 SMS 消息。在 DMU SMS 消息之上使用分段协议。多个 SMS 消息可用于携带 DMU 消息。

[0048] SMSC 122 接收经加密的新密钥并将其转发给 DMU 服务器 120。DMU 服务器 120 将新密钥转发给 H-AAA 114。H-AAA 114 解密该新密钥，并可至少部分地基于来自 MS 102 的经加密消息生成认证确认。H-AAA 114 可用特殊接入拒绝消息来向 DMU 服务器 120 作出响应，而 DMU 服务器 120 将 DMU 更新消息发送给 MS 102。MS 102 可在随后使用已由经认证的 H-AAA 114 确立的新密钥来与 PDSN 110 通信。

[0049] 到访网络中的安全性预设

[0050] 图 2 是图解即使在可能不支持归属网络 206 的典型密钥预设过程的到访网络 204 中操作时可如何用密码密钥来预设移动站 202 的框图。在一些情形中，用户可购买旨在与第一网络（例如，用户的归属网络 206）联用的无线移动站 202（例如，包括无线通信能力的移动电话、个人数字助理、手持式计算设备、通信设备等）。然而，在通过第一网络 206 激活无线移动站 202 之前，该无线移动站 202 可能被移至其中运作第二网络（例如，到访网络 204）的第二区域。由于移动站 202 尚未通过其归属网络 206 完全激活，因此该移动站 202 可能尚未获得用于特定通信或数据服务的密码和 / 或安全性密钥。如果归属网络 206 已使当前密码或安全性密钥无效而没有向移动站 202 通知此类密钥更新，则可能发生类似问题。当无线移动站 202 在到访网络 204 中尝试接入例如数据服务（例如，网上冲浪等）等特定服务时，该移动站 202 可能被拒绝接入，因为移动站 202 可能针对此服务不具有来自其归属网络 206 的有效认证（例如，其可能尚未获得安全性或密码密钥）。例如，一旦在到访网络 204 中开始操作，移动站 202 就可通过第一信道 208 发送针对特定服务的认证请求 212。到访网络可通过向移动站 202 的归属网络 206 转发该请求来验证认证请求 214。归属网络 206 可探知其针对所请求的服务不能认证移动站，例如，因为针对此服务尚没有安全性 / 密码密钥被提供给移动站 202。结果，对认证请求的拒绝 218 可以从归属网络 206 被发送给到访网络 204，并被转发给移动站 202。

[0051] 然而，诸如 SMS 信道等预先预设的第二信道 210 可被移动站 202 用来与归属网络 206 建立认证，以便获得用于数据服务或信道的安全性 / 密码密钥和其他安全性特征。结果，当归属网络 206 拒绝认证请求时，其可能还通过第二信道 210 发起安全性 / 密码密钥预设和 / 或更新过程 222。归属网络可探知，当来自到访网络的认证请求被拒绝时，应当通过第二信道 210 发起密钥预设过程。此类密钥预设过程可包括使用第二信道 210 来（例如，经由第二网络 204）向移动站 202 发送安全性 / 密码密钥更新请求 224。作为响应，移动站 202 可生成安全性 / 密码密钥并经由安全性 / 密码密钥更新响应 226 将其发送给归属网络。归属网络 206 可在随后认证安全性 / 密码密钥并经由第二信道 210 向移动站 202 发送确认 228。可在随后使用安全性 / 密码密钥来经由第一信道 208 提供认证 / 安全性服务。即，安全性 / 密码密钥可在随后被移动站 202 用于尝试通过第一信道 208 建立服务会话。例如，移动站 202 可再次发送认证请求，但是这次，归属网络 206 成功地验证请求，因为用于移动站 202 的密码密钥已被建立。结果，移动站 202 可经由第一信道建立通信会话。

[0052] 由于诸如 SMS 信道等经预先预设的第二信道 210 被用于预设第一信道 208 的安全性特征，因此，用户可使用无线移动站 202 进行数据服务（通过第一信道），即使归属网络 206 尚未使用用于此类数据服务的安全性 / 密码密钥预设该无线移动站。注意，即使移动站 202 首次在到访网络 204 中使用，也可使用此密钥预设过程。此导致用户减少挫败，以及增大的数据服务的使用。

[0053] 注意，虽然可保护第一信道 208（例如，对于其上的通信和服务需要一些预设的密钥），但是第二信道 210 可以很少或没有认证或安全性的方式使用。根据一些实现，第一信道 208 可以是用于数据服务的高带宽信道，而第二信道 210 相对于第一信道 208 而言是低带宽信道。数据服务或第一信道可对应于码分多址 (CDMA) 通信，诸如例如 CDMA 2000 演进数据最优化 (EV-DO) 通信，其是由第三代伙伴项目 2(3GPP2) 进行标准化的。作为另一示例，通信服务或第一信道可以是无线二进制运行时环境 (BREW™) 服务或应用。BREW™ 是由高通公司 ™ 开发的用于操纵无线通信设备上的软件的专有机制。

[0054] 在又一实施例中，第一信道 208 可仅仅是与提供合意数据服务的更高带宽的第三信道相关联的低带宽控制信道。

[0055] 根据一个示例，无线移动站 202 可以是从承运商 A 处购得的在承运商 A 的网络和其他网络上使用的数据启用蜂窝电话。例如，承运商 A 可以是 Verizon 无线 ™。如果用户已在美国购买了蜂窝电话并签署了国际漫游，则用户可能希望在例如加拿大或欧洲使用该设备。在一些情形中，用户可能甚至在蜂窝电话已被归属网络（在美国）认证用于数据服务（例如，因特网浏览等）之前将该蜂窝电话携带至加拿大或欧洲。因而，当用户尝试在另一网络——承运商 B——中使用移动站时，移动站尝试初始化数据服务。例如，承运商 B 可以是加拿大的 Telus™。如果承运商 A 和承运商 B 具有漫游协定，则用户通常将能够获得语音服务和 SMS 服务，即使数据服务可能未被预设。根据一个特征，图 2 中所例示的过程可用于针对数据服务向移动站提供一个或多个密钥。对（例如，第一信道 208 上的）数据服务的此类预设可以通过 SMS 消息接发（例如，第二信道 210）来执行。例如，虽然服务选项 33(SO33) 可用于执行 Verizon 无线网络中的 DMU 更新（例如，使用 CDMA2000 1xRTT 数据会话），但是此选项在外地网络中可能不可用；因此，DMU 更新可替代地经由 SMS 消息接发来执行。例如，假定承运商 A 和承运商 B 具有 SMS 漫游协定，如果承运商 B 不具备进行动态移动 IP 密钥更新 (DMU) 的能力，则密码密钥和其他安全性特征更新仍可通过使用 SMS 消息经由 SMS 信道来执行，

[0056] 通过 SMS 的 DMU 预设的示例

[0057] 图 3 是图解用于使移动站 300 在到访网络中能经由较低带宽的协议更新用在数据通信信道上的安全性状态——诸如密码密钥——的呼叫流的示图。本文中所描述的概念可使用 EV-DO 数据通信的示例，尽管其他实现是可能的且被构想。移动站 (MS)300 尝试在处于到访网络中时发起数据通信。该尝试可以是去往 VPDSN 304 的 PPP+MIP RRQ 消息 302，如以上参照图 1 所描述的。V-PDSN 304 将 MN-AAA AUTH REQ 306 传达给 V-AAA 308。V-AAA 308 将 MN-AAA AUTH REQ 310 传达给 H-AAA 312。H-AAA 312 在凭证列表中查找 MS 300，并确定 MS 300 不具备有效密码密钥。结果，H-AAA 312 向 V-AAA 发送接入拒绝消息 316，V-AAA 向 V-PDSN 304 发送接入拒绝消息 318，由此阻止 MS 300 获得合意数据服务。

[0058] 然而，伴随着发送接入拒绝消息 316，H-AAA 312 还可通过发送消息 314——向 DMU

服务器 320 通知对于到访网络中的 MS 300 需要密钥更新——来发起生成新安全性 / 密码密钥的过程。DMU 服务器 320 通过向 MS 300 发起关于 DMU 更新（请求）的 SMS 消息 322 来作出响应。将消息发送给 SMSC 324，SMSC 324 将消息 326 路由至 MS 300。MS 300 接收 SMS 消息，该 SMS 消息包括经加密的对密钥更新的请求。例如，请求 326 可用具有相对应的公钥的 Rivest Shamir Adleman(RSA) 私钥来加密。MS 300 可生成密码密钥和认证符，用网络的公钥加密新密钥和认证符，并经由 SMSC 324 和 DMU 服务器 320 将具有经加密的密钥和认证符的消息 328 发回给 H-AAA 312。例如，MS 300 的 MIP 密钥数据可由 MS 300 使用网络的公钥来加密。H-AAA 312 具有相对应的私钥，因此其可解密经加密的消息。SMSC 324 将消息 330 转发给 DMU 服务器 320，该 DMU 服务器 320 将消息 332 转发给 H-AAA 312。H-AAA 312 可通过利用其私钥来解码消息中的新密钥和 / 或认证符。H-AAA 312 可在随后将认证符连同接入接受消息 334 发送给 DMU 服务器 320。DMU 320 将接入接受消息和认证符 336 转发给 SMSC 324，该 SMSC 324 将认证符 338 转发给 MS 300（例如，作为 DMU 确认消息 338 的部分）。一旦接收到认证符，MS 300 就可验证请求新密钥生成的 H-AAA 312 是可信的，因为仅具有正确私钥的实体可正确地解密新密钥消息 328 并正确地获得或提取认证符。因此，即使没有使用数据通信信道来获得经更新密码密钥，MS 300 也可以确定经更新加密密钥是可信的，并且用来与 V-PSDN 304 通信以便与因特网通信是安全的。

[0059] 本文中所描述的系统和方法允许更新密钥（例如，MIP 密钥、安全性密钥、密码密钥等）而无需修改到访 AAA 服务器。可由 MS 或与由 MS 结合归属网络来生成密钥，并经由 SMS 消息接发将其提供给 DMU 服务器。

[0060] 在一个示例中，认证符被包括在 DMU 确认消息 338 中并确保密钥被更新。这向 MS 300 指示密钥被更新，以及可信网络进行了此更新。仅正确实体能够（例如，使用网络的私钥）从 DMU 更新消息 328 来提取密钥，并且用正确认证符来作出答复。

[0061] 本文中例示的示例已在很大程度上描述了 DMU 密钥更新，但是可使用由 MS 发送的任何密钥数据。例如，应用层密钥可由本文中所描述的过程来更新。

[0062] 此外，本文中所例示的示例已在很大程度上描述了使用 SMS 来更新用于数据通信的密钥，但是这些思想可适用于其他通信协议。已被预设的任何协议可用于更新尚未被预设的通信协议的安全性特征。

[0063] 可应用本文中所描述的方法，只要通信提供商或承运商正提供由其自己的密钥保护的服务类型，并且在到访网络中漫游时不能接入此服务，除非移动站已被赋予某些密钥，并且移动站尚未由归属网络用密钥预设。在一些实现中，这些方法仅当移动站漫游到外国网络（例如，CDMA 网络）时才可应用，而在该移动站处在其归属网络（例如，GSM 网络）中时不应用。

[0064] 没有认证凭证的数据漫游 IMSI 核查的示例

[0065] 图 4 是图解用于在到访网络中预设具有数据服务的移动站的替换性方法的示图，移动站在该到访网络中可能未使用此类数据服务通常所需的必要密钥预设过。此办法的初始步骤类似于图 3 的那些。在此办法中，移动站 400 可能不具有诸如用于 MN-AAA 和 / 或移动网络归属代理 (MN-HA) 认证的 MIP 认证凭证。移动站 400 的国际移动订户身份 (IMSI) 或移动标识号码 (MIM)（或其等效物）可被归属网络用来对移动站准许接入而不用建立密码密钥。一旦对网络的接入被准许接入，可在 DMU 服务器与移动站之间建立密码密钥。

[0066] 类似于图 3，移动站 (MS)400 尝试在处于到访网络中时发起数据通信。该尝试可以是去往 VPDSN 404 的 PPP+MIP RRQ 消息 402，如以上参照图 1 所描述的。V-PDSN 404 将 MN-AAA AUTH REQ 406 传达给 V-AAA 408。V-AAA408 将 MN-AAA AUTH REQ 410 传达给 H-AAA 412。此 MN-AAA AUTH REQ410 可包括空白分组数据认证凭证（例如，默认凭证或无效凭证）。MN-AAAAUTH REQ 410 还可包括移动站 400 的国际移动订户身份 (IMSI) 或移动标识号码 (MIN)。IMSI 或 MIN 可最初例如从 MS 400 的空中链路记录中获得。另外，MN-AAA AUTH REQ 410 还可包括到访网络的承运商 ID。

[0067] 首先，一旦接收到认证请求 410，H-AAA 412 可基于密码密钥尝试执行对 MS 400 的典型认证 414。由于 MS 尚未从 DMU 服务器 420 获得此类密钥，因此此典型认证将失败。然而，H-AAA 412 还可被配置成执行替换性认证过程，其中可基于 MS 400 的 IMSI/MIN 和当前漫游状况来认证 MS 400416。

[0068] 在此办法中，H-AAA 412 使用承运商 ID 来探知请求方 MS 400 正在到访网络中漫游。当接收到此请求，H-AAA 还在凭证列表中查找 MS400 并确定 MS 400 不具有有效密码密钥（例如，其尚未执行 DMU）。与如图 3 中的拒绝请求不同，H-AAA 412 可基于 IMSI 或 MIN 以及该请求指示 MS 400 是处于不支持 DMU 的到访网络中这个事实允许继续数据服务请求。即，H-AAA 412 可基于请求 410 中接收到的 IMSI 或 MIN 确定 MS 400 为归属网络的订户。另外，由于探知 MS 400 已漫游至到访网络，因此 H-AAA 412 可使用此信息来允许继续或准许数据服务请求。结果，H-AAA 412 可基于 IMSI 或 MIN 以及 MS 400 正在漫游这个事实来认证该 MS 400。即使 MS 400 不提供正确认证凭证（例如，MN-AAA 口令或 MN-HA 口令），也可发生此类认证。注意，因为 IMSI 或 MIN 来自空中链路（从 MS 400 至到访网络基站），因此由于由于归属位置寄存器 (HLR) 认证将失败而不可能进行哄骗。

[0069] 一旦执行此替换性认证过程，H-AAA 就可向到访网络发送接入准许消息 418 和 422。这允许向移动站 400 准许所请求的服务。在一个示例中，此接入可以是临时接入，该临时接入允许 MS 400 通过 V-PDSN 404 进行操作和接入。然而，一旦 MS 400 在归属网络中操作，就仍必需与 DMU 服务器 420 建立其密码密钥。

[0070] 示例移动站

[0071] 图 5 是图解移动站 500 的示例的框图，该移动站在到访网络中漫游时可适于根据替换性方法更新其密码密钥。移动站 500 可包括用于通过空中传送和接收无线通信的天线 502。无线网络接口 504（例如，射频 (RF) 前端）可包括用于将数字信号调制到 RF 信号的调制器和用于将收到的 RF 信号解调成数字信号的解调器。网络接口 504 可被耦合至处理器 506。处理器 506 可包括至少两个通信模块，即，无线数据通信模块 520、语音通信模块 524、和 / 或低带宽通信模块，诸如 SMS 模块 522。通信模块可适于执行以上参照图 1-4 描述的 SMS 和数据通信功能。例如，无线数据模块 520 可发起对数据服务的请求，如以上所描述的。此外，SMS 模块 522 可接收由归属网络 DMU 服务器 120 发送的 SMS DMU 更新请求并经由 SMS 用 DMU 更新消息进行答复。

[0072] 处理器 506 还可包括安全性模块 516。安全性模块 516 可适于保护移动站 500 与其他实体之间的通信。除按需更新密码密钥、以及认证其他实体和执行其他有关任务之外，安全性模块 516 可加密移动站 500 的消息。安全性模块 516 可包括密钥发生器模块 518。密钥发生器模块 518 可按需生成新密码密钥或安全性密钥。例如，密钥发生器模块 518 可

生成由 DMU 服务器 120 所请求的新密钥，如以上参照图 1 所描述的。移动站 500 还可包括用于为移动站 500 存储数据和指令的存储设备 508。例如，与其他实体的通信的内容可被存储在存储设备 508 中。例如，通过 SMS 接收到的 DMU 更新请求可被存储在存储 508 中。移动站 500 还可包括用户接口 510，该用户接口用于向用户显示或播放诸如音频、视频或文本之类的输出，以及用于接收来自用户的输入。用户接口 510 可包括用于向用户显示视频、图像和文本的显示器 512。用户接口 510 可包括用于接收来自用户的输入的键区 514。诸如扬声器、麦克风等其他用户接口设备未被示出，但是可被包括在移动站 500 上。

[0073] 当在处于到访网络的同时寻求建立数据服务时，移动站 500 可能尚未获得用于与其归属网络进行认证的必需密钥。结果，移动站 500 可被配置成执行一种或多种替换性方法，这些方法允许该移动站在于到访网络中漫游时并且在之前针对数据服务还未被归属网络认证的情况下获得数据服务。

[0074] 图 6 图解了用于在无线移动站上操作的方法，该方法供在无线移动站在到访网络中漫游时与归属网络建立密码密钥之用。在此方法中，假定移动站可能尚未获得或建立用于合意服务的必需密码密钥或安全性密钥。此方法可在已漫游至到访网络的移动站——诸如图 5 中所例示的移动站 500——上操作。到访网络可能不支持归属网络用来与其移动站建立密钥的典型密钥预设过程。

[0075] 当在到访网络中漫游时，移动站可向到访网络节点发送服务请求，以建立需要来自归属网络的认证的数据服务 (602)。服务请求可包括在点对点协议 (PPP) 上发送的 MIP 注册请求。

[0076] 作为响应，可在文本消息接发信道上接收对用于数据服务的密码密钥的请求，其中该请求是由归属网络发起的 (604)。收到请求可以是动态移动 IP 密钥更新请求。通过此办法，移动站可适于针对具有指示消息为密码密钥请求的消息类型或代码的消息来监视文本消息接发信道。在知晓可能通过文本消息接发信道接收到此类消息的情况下，移动站可监视此类信道。

[0077] 移动站可在随后生成用于数据服务的密码密钥并在文本消息接发信道上发送该密码密钥 (606)。密码密钥可例如包括或者基于移动网际协议 (MIP) 密钥。密码密钥可作为具有密码密钥的认证消息的部分在文本消息接发信道上发送。例如，密码密钥可作为动态移动 IP 密钥更新响应的部分来发送。

[0078] 作为响应，可由移动站接收确定密钥生成过程完成的确认 (608)。移动站可在随后再次使用密码密钥建立数据服务会话 (610)。

[0079] 注意，可在与文本消息接发信道不同的第一信道上执行数据服务。第一信道可具有比文本消息接发信道更高的数据率。

[0080] 图 7 图解了用于在无线移动站上操作的另一方法，该方法供在无线移动站在到访网络中漫游时与归属网络建立密码密钥之用。在此方法中，由归属网络基于移动站的凭证及其漫游状况“认证”移动站，而无需首先建立其密码密钥。当在到访网络中漫游时，移动站可向到访网络节点发送服务请求，以建立需要来自归属网络的认证的数据服务 (702)。请求可包括无线移动站的唯一性标识符或凭证，诸如 IMSI 或 MIN，该唯一性标识符或凭证允许归属网络验证该无线移动站事实上是归属网络的运营商的订户。另外，该请求（或由到访网络转发的消息）还可包括到访网络的标识符，该标识符允许归属网络验证无线移动站

事实上正在漫游和 / 或处在不支持其典型密钥更新协议的到访网络中。

[0081] 作为响应，可接收指示网络接入已被归属网络准许的消息，尽管无线移动站无法针对所请求的服务与归属网络建立密码密钥 (704)。归属网络可基于将移动站标识为合法订户以及探知其正在另一网络中漫游来探知或准许此类接入。此响应消息可准许移动站通过到访网络进行通信。结果，移动站可在不使用经认证的密码密钥的情况下建立数据服务会话 (706)。然而，在一个示例中，被准许的网络接入可以是临时的，或者被限于到访网络，因为移动站尚未与归属网络建立其密码密钥。因此，当移动站再次在归属网络内操作时，其将需要建立其用于数据服务的密码密钥。

[0082] 示例归属网络 AAA 服务器。

[0083] 图 8 是图解归属 AAA 服务器的一个示例的框图。H-AAA 800 可包括用于与诸如到访网络等其他网络以及归属网络中的其他服务器——诸如 DMU 服务器——通信的网络接口 804。网络接口 804 可被耦合至处理器 806，该处理器 806 可包括密钥状态核查模块 820、密钥更新请求模块 822 和接入拒绝模块 824。密钥状态核查模块 820 可从移动站（即，归属网络的订户）在其中漫游的到访网络或外地网络接收对数据服务认证的请求。服务器 800 可核查请求方移动站是否具有有效密码密钥。对数据服务认证的请求可包括请求方移动站的标识，诸如例如电子序列号 (ESN)、IMSI 和 / 或 MIN。

[0084] H-AAA 服务器 800 还可包括存储设备 808，凭证列表 830 可被存储在该存储设备中。凭证列表 830 可存储归属网络的用户或订户的凭证。此类凭证列表 830 可尤其指示订户的密钥状态 828。在一个示例中，密钥状态 828 可以是 MIP 密钥状态。MIP 密钥状态可指示每个移动站是否具有当前或有效密码密钥。此类密码密钥可与特定类型的服务相关联，因此不同的服务可具有不同的密钥。密钥状态核查模块 830 可在凭证列表 828 中搜索和 / 或寻找请求方移动站的密钥状态，以确定请求方移动站是否具有用于所请求服务的有效密码密钥。如果请求方移动站的 MIP 密钥状态 828 指示移动站不具有用于合意服务的有效密码密钥，则密钥状态核查模块 820 可触发密钥预设过程。

[0085] 在图 8 中所例示的第一办法中，H-AAA 服务器 800 可发起一过程，藉由该过程文本消息接发信道被用来与请求方移动站建立此类密码密钥。此类文本消息接发信道可不同于用于所请求的服务的信道。一旦发现请求方移动站不具有有效密码密钥，接入拒绝模块 824 就生成接入拒绝消息，该拒绝消息可通过网络接口 804 被发送给到访网络。另外，密钥更新请求模块 822 还可适于向请求方移动站发起和 / 或发送密钥更新请求（经由文本消息接发信道）以获得密码密钥。

[0086] 在图 9 中所例示的第二办法中，H-AAA 服务器 800 可使用其他信息，诸如请求方移动站的可验证标识符（例如，IMSI、MIN 等）连同该请求方移动站的漫游状况来认证移动站。即，即使没有（如在第一办法中那样）发起获得密码密钥的过程，然而如果 H-AAA 服务器 800 可验证该移动站标识符 (IMSI/MIN) 对应于有效订户、移动站在之前尚未获得有效密码密钥、以及移动站正在到访网络中漫游，则 H-AAA 服务器 800 也可用接入准许消息来作出响应。

[0087] 图 9 图解了在归属网络中操作的方法，该方法用于为在到访网络中漫游的无线移动站认证通信服务。此方法可以在归属网络的一个或多个服务器或节点（例如，H-AAA、DMU 服务器、H-SMSC 等）中操作。

[0088] 从到访网络接收关于移动站建立需要密码密钥的数据服务的服务请求 (902)。服务请求可包括点对点协议 (PPP) 移动网际协议 (MIP) 注册请求 (RRQ) 消息。

[0089] 归属网络可确定移动站的密码密钥在归属网络处不可用 (904)。结果，归属网络可通过向移动站发送更新请求来发起密钥预设过程。这可涉及使用文本消息接发信道向移动站发送更新请求以更新密码密钥 (906)。例如，可使用 SMS 消息，因为 SMS 信道可被预设而无需对密码密钥的认证。更新请求可以是动态移动 IP 密钥更新请求。作为响应，归属网络可经由文本消息接发信道从移动站接收用于数据服务的密码密钥 (908)。在一个示例中，密码密钥可包括或者基于移动网际协议 (MIP) 密钥。密码密钥可作为动态移动 IP 密钥更新响应的部分来接收。接着，归属网络可经由文本消息接发信道来向移动站发送 (910)。

[0090] 然后，归属网络可从到访网络接收关于移动站建立需要密码密钥的数据服务的第二服务请求 (912)。归属网络现在可确定移动站的密码密钥在归属网络处可用 (914)。结果，归属网络可向移动站准许服务请求 (916)。

[0091] 注意，服务请求可在第一信道上接收，但是更新请求是在与第一信道不同的第二信道（即，文本消息接发信道）上发送的。在一些实现中，可在与文本消息接发信道不同的数据信道上执行数据服务。数据信道可具有比文本消息接发信道更高的数据率。

[0092] 图 10 图解了在归属网络中操作的方法，该方法用于为在到访网络中漫游的无线移动站认证通信服务。与如图 9 中那样发起替换性认证过程不同，归属网络可替代地利用其他信息来出于所请求服务的目的执行认证。从到访网络接收关于移动站（在到访网络上）建立需要密码密钥的数据服务的服务请求 (1002)。注意，收到服务请求可包括到访网络的网络标识符以及移动站的唯一性节点标识符或凭证。归属网络可确定移动站的密码密钥在归属网络处不可用 (1004)。另外，归属网络可通过使用请求方移动站的唯一性节点标识符或凭证来验证该请求方移动站是否是归属网络的订户。例如，移动站的唯一性节点标识符或凭证（例如，IMSI 或 MIN）可作为服务请求的部分被接收。可将此唯一性节点标识符或凭证与归属网络的已知订户列表作比较以作出此确定。归属网络还可探知请求方移动节点是否正在到访网络中漫游 (1008)。如果没有找到与移动站相关联的有效密码密钥，但是请求方漫游移动站是归属网络的订户，则可由归属网络向到访网络发送接入准许消息 (1010)。

[0093] 向移动站准许接入可意味着移动站在有限或无限时间量上具有对到访网络上的服务的（有限或无限）接入。根据一个实现，一旦移动站再次在归属网络（或支持 DMU 的另一网络）内操作，则其必需与归属网络建立其密码密钥。

[0094] 示例归属网络 DMU 服务器

[0095] 图 11 是诸如参照图 1 所示和描述的 DMU 服务器 120 等 DMU 服务器 1100 的框图。DMU 服务器 1100 具有用于与 H-AAA 114 以及与 SMSC 122 通信的网络接口 1104。网络接口 1104 被连接至处理器 1106，该处理器包括 DMU 请求模块 1120 和文本消息接发接口模块 1122（例如，SMSC 模块）。DMU 服务器 110 可适于接收对访网络中的移动站的密钥更新请求。作为响应，DMU 服务器 1100 可生成将被发送给移动站的 DMU 请求。由 DMU 请求模块 1120 生成的请求可被发送给文本消息接发接口模块 1122，该文本消息接发模块在将被发送给归属网络的 SMS 中心的 SMS 消息中打包该请求。作为响应，DMU 服务器 1100 可从移动站接收具有密码密钥的 DMU 更新消息。DMU 可在随后更新其凭证列表以反映移动站现在具有有效密

码密钥。在一个示例中，密码密钥可以是 MIP 密钥或可以基于 MIP 密钥。

[0096] 图 12 图解了用于在 DMU 服务器中操作的方法，该方法用于通过使用文本消息接发信道向在到访网络中漫游的无线移动站发起密钥更新。此方法可假定到访网络不支持直接使用 DMU 更新用于合意服务的密钥。因此，可使用替换性办法，其中 DMU 更新可替代地经由文本消息接发信道来执行。由 DMU 服务器接收对到访网络中的移动站的密钥更新请求 (1202)。DMU 服务器可在随后生成对移动站的 DMU 请求 (1204)。DMU 请求可被发送给文本消息接发模块，以使得该请求可经由文本消息接发信道发送给移动站 (1206)。作为响应，DMU 服务器可从移动站接收包括密码密钥的文本消息 (1208)。DMU 服务器可在凭证列表中存储密码密钥以反映移动站具有有效密码密钥 (1210)。

[0097] 应认识到，一般而言，本公开中所描述的绝大多数处理可以用类似的方式来实现。(诸) 电路或电路段中的任何电路或电路段可单独实现或者与一个或更多个处理器组合地实现为集成电路的一部分。这些电路中的一个或更多个可以在集成电路、先进 RISC 机 (ARM) 处理器、数字信号处理器 (DSP)、通用处理器等上实现。

[0098] 还应注意，这些实施例可能是作为被描绘为流程图、流图、结构图、或框图的过程来描述的。尽管流图可能会把诸操作描述为顺序过程，但是这些操作中有许多能够并行或并发执行。另外，这些操作的次序可以被重新安排。过程在其操作完成时终止。过程可对应于方法，函数，规程，子例程，子程序等。当过程对应于函数时，它的终止对应于该函数返回调用方函数或主函数。

[0099] 如在本申请中所使用的，术语“组件”、“模块”、“系统”等旨在指示计算机相关实体，无论其是硬件、固件、软硬件组合、软件，还是执行中的软件。例如，组件可以是但不被限定于在处理器上运行的进程、处理器、对象、可执行件、执行的线程、程序、和 / 或计算机。作为解说，在计算设备上运行的应用和该计算设备两者皆可以是组件。一个或更多个组件可驻留在进程和 / 或执行的线程内，且组件可以局部化在一台计算机上和 / 或分布在两台或更多台计算机之间。此外，这些组件能从其上存储着各种数据结构的各种计算机可读介质来执行。各组件可借助于本地和 / 或远程进程来通信，诸如根据具有一个或更多个数据分组的信号 (例如，来自通过该信号与本地系统、分布式系统中的另一组件交互、和 / 或跨诸如因特网之类的网络与其它系统交互的一个组件的数据)。

[0100] 不仅如此，存储介质可以代表用于存储数据的一个或更多个设备，包括只读存储器 (ROM)、随机存取存储器 (RAM)、磁盘存储介质、光学存储介质、闪存设备、和 / 或其他用于存储信息的机器可读介质。术语“机器可读介质”包括，但不被限定于，便携或固定的存储设备、光学存储设备、无线信道以及能够存储、包含或承载指令和 / 或数据的各种其它介质。

[0101] 此外，诸实施例可以由硬件、软件、固件、中间件、微代码、或其任何组合来实现。当在软件、固件、中间件或微码中实现时，执行必要任务的程序代码或代码段可被存储在诸如存储介质或其它存储之类的机器可读介质中。处理器可以执行这些必要的任务。代码段可表示规程、函数、子程序、程序、例程、子例程、模块、软件包、类，或是指令、数据结构、或程序语句的任何组合。通过传递和 / 或接收信息、数据、自变量、参数、或存储器内容，一代码段可被耦合到另一代码段或硬件电路。信息、自变量、参数、数据等可以经由包括存储器共享、消息传递、令牌传递、网络传输等任何合适的手段被传递、转发、或传输。

[0102] 附图中所解说的组件、步骤、和 / 或功能中的一个或更多个可以被重新编排和 / 或

组合成单个组件、步骤、或功能，或可以实施在数个组件、步骤、或功能中而不会影响伪随机数发生的操作。还可添加额外的元件、组件、步骤、和／或功能而不会脱离本发明。附图中所解说的装置、设备和／或组件可以被配置成执行在这些附图中所描述的方法、特征、或步骤中的一个或更多个。本文中描述的新颖算法可以在软件和／或嵌入式硬件中高效率地实现。

[0103] 本领域技术人员将可进一步领会，结合本文中公开的实施例描述的各种解说性逻辑框、模块、电路、和算法步骤可被实现为电子硬件、计算机软件、或两者的组合。为清楚地解说硬件与软件的这一可互换性，各种解说性组件、框、模块、电路、和步骤在上面是以其功能性的形式作一般化描述的。此类功能性是被实现为硬件还是软件取决于具体应用和强加于整体系统的设计约束。

[0104] 本文中所描述的本发明的各种特征可实现于不同系统中而不会脱离本发明。例如，本发明的一些实现可用移动或静态移动站（例如，接入终端）和多个移动或静态基站（例如，接入点）来执行。

[0105] 应注意，以上实施例仅是示例，且并不被解释成限定本发明。这些实施例的描述旨在成为解说性的，而并非旨在限定权利要求的范围。由此，本发明的教导能现成地应用于其他类型的装置，并且许多替换、改动、和变形对于本领域技术人员将是明显的。

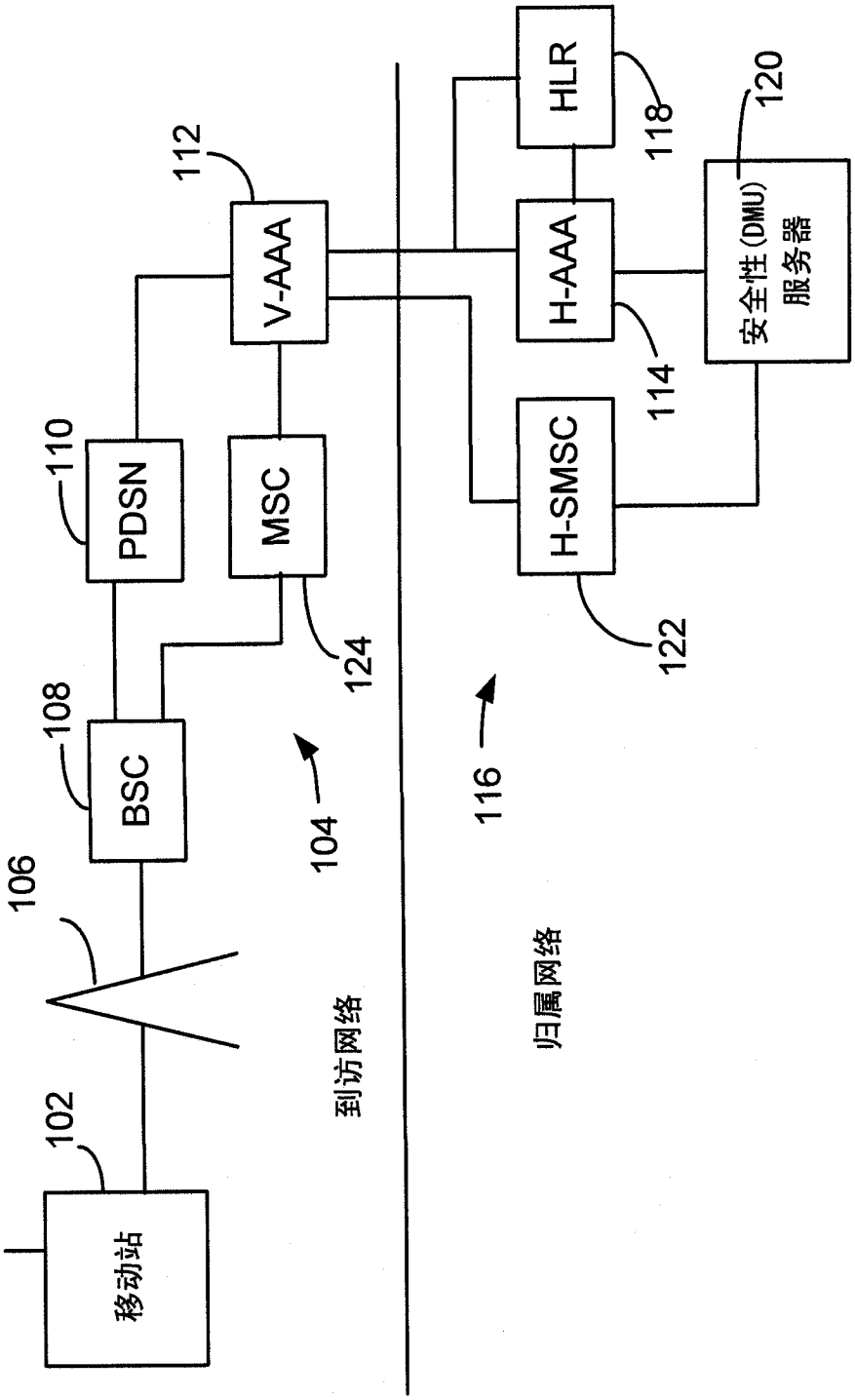

HLR
118
120
112
V-AAA
H-AAA
安全性 (DMU)
服务器
114
110
PDSN
MSC
H-SMSC
124
122
108
BSC
104
116
106
到访网络
归属网络
102
移动站

图 1

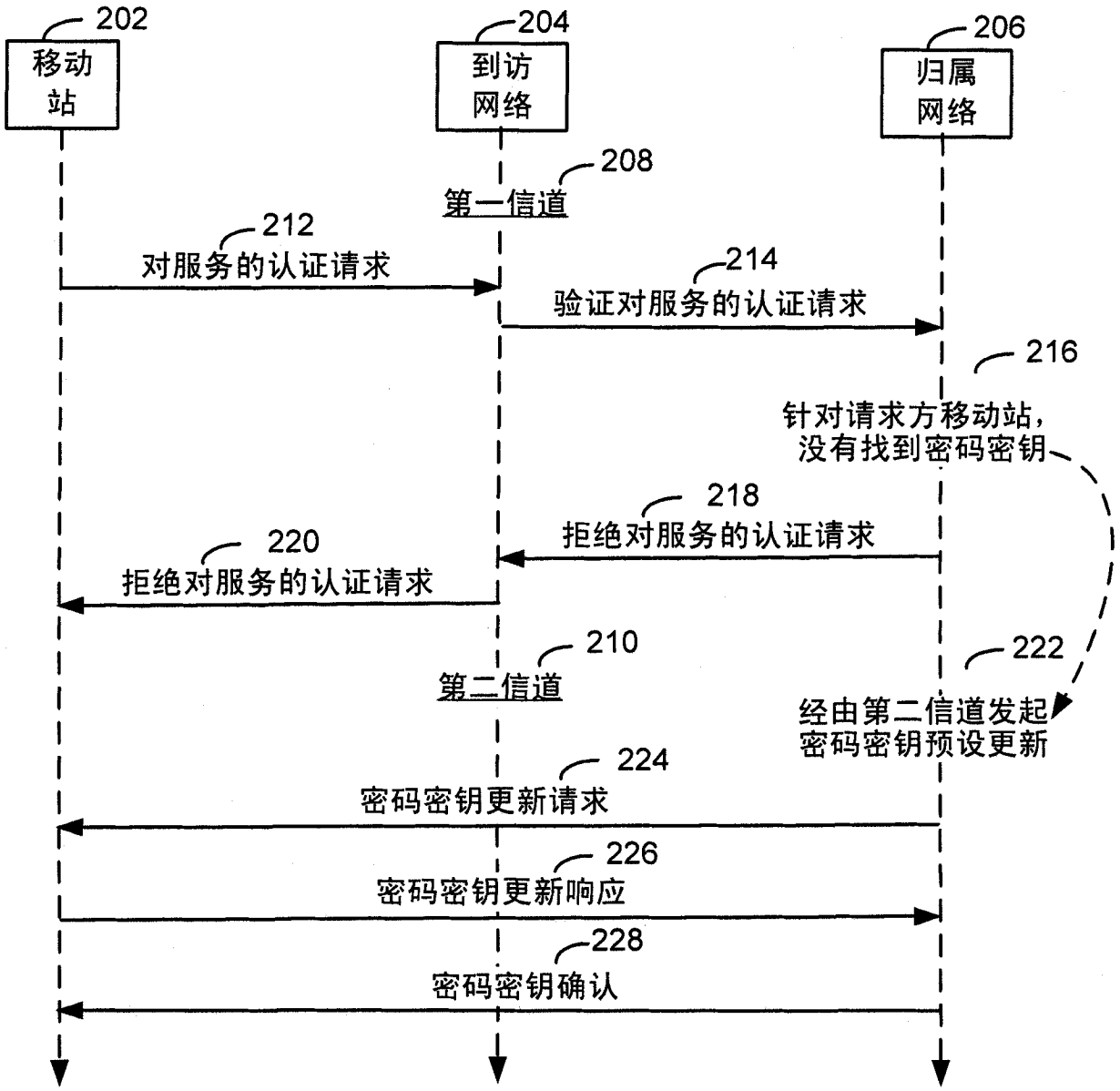

202
移动站
204
到访网络
206
归属网络
208
第一信道
212
对服务的认证请求
214
验证对服务的认证请求
216
针对请求方移动站，没有找到密码密钥
218
拒绝对服务的认证请求
220
拒绝对服务的认证请求
210
第二信道
222
经由第二信道发起密码密钥预设更新
224
密码密钥更新请求
226
密码密钥更新响应
228
密码密钥确认

图 2

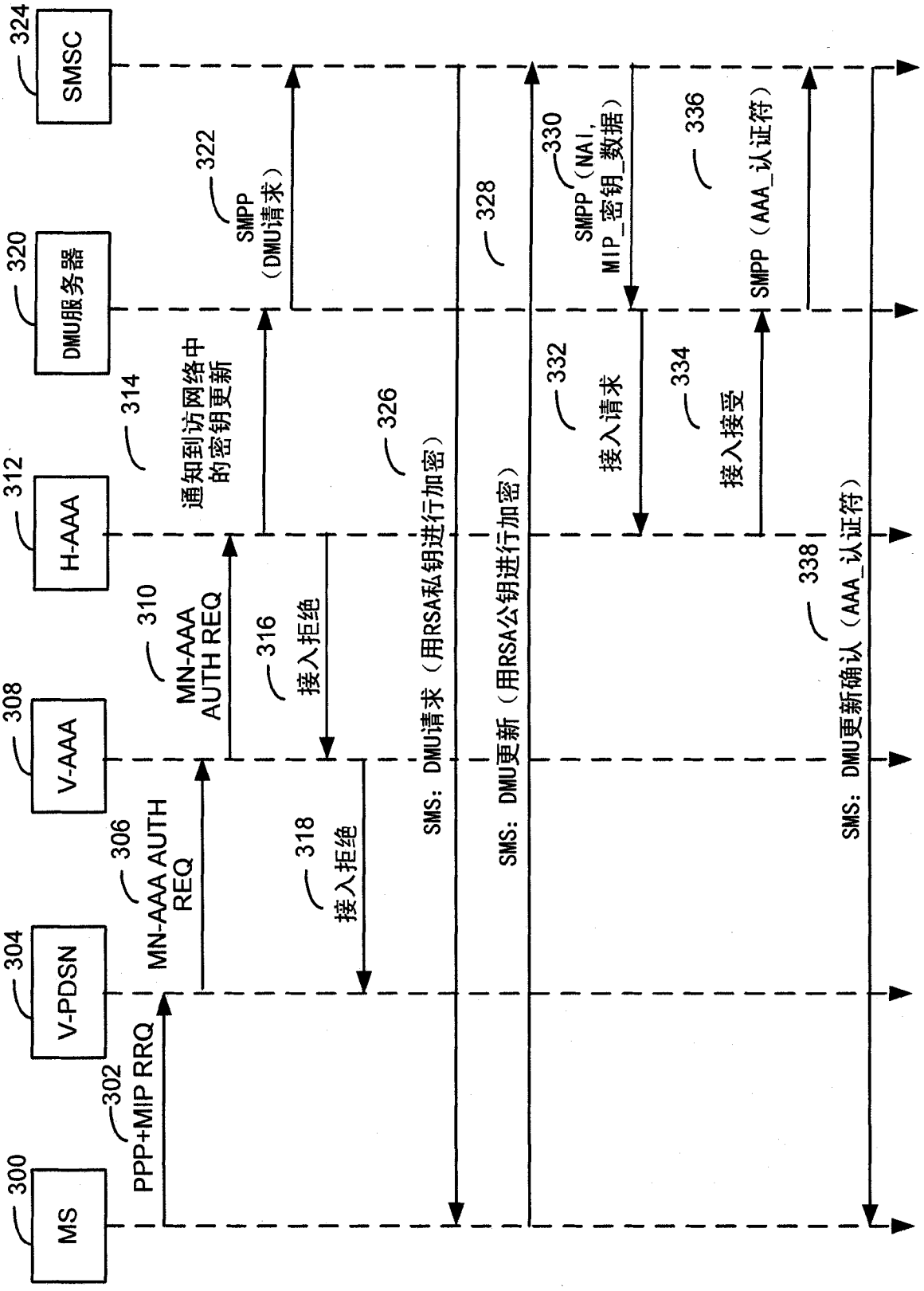

MS
300
V-PDSN
304
V-AAA
308
H-AAA
312
DMU服务器
320
SMSC
324
302
PPP+MIP RRQ
306
MN-AAA AUTH REQ
310
MN-AAA AUTH REQ
314
通知到访网络中的密钥更新
316
接入拒绝
318
接入拒绝
322
SMPP（DMU请求）
326
SMS：DMU请求（用RSA私钥进行加密）
328
SMS：DMU更新（用RSA公钥进行加密）
330
SMPP（NAI，MIP_密钥_数据）
332
接入请求
334
接入接受
336
SMPP（AAA_认证符）
338
SMS：DMU更新确认（AAA_认证符）

图 3

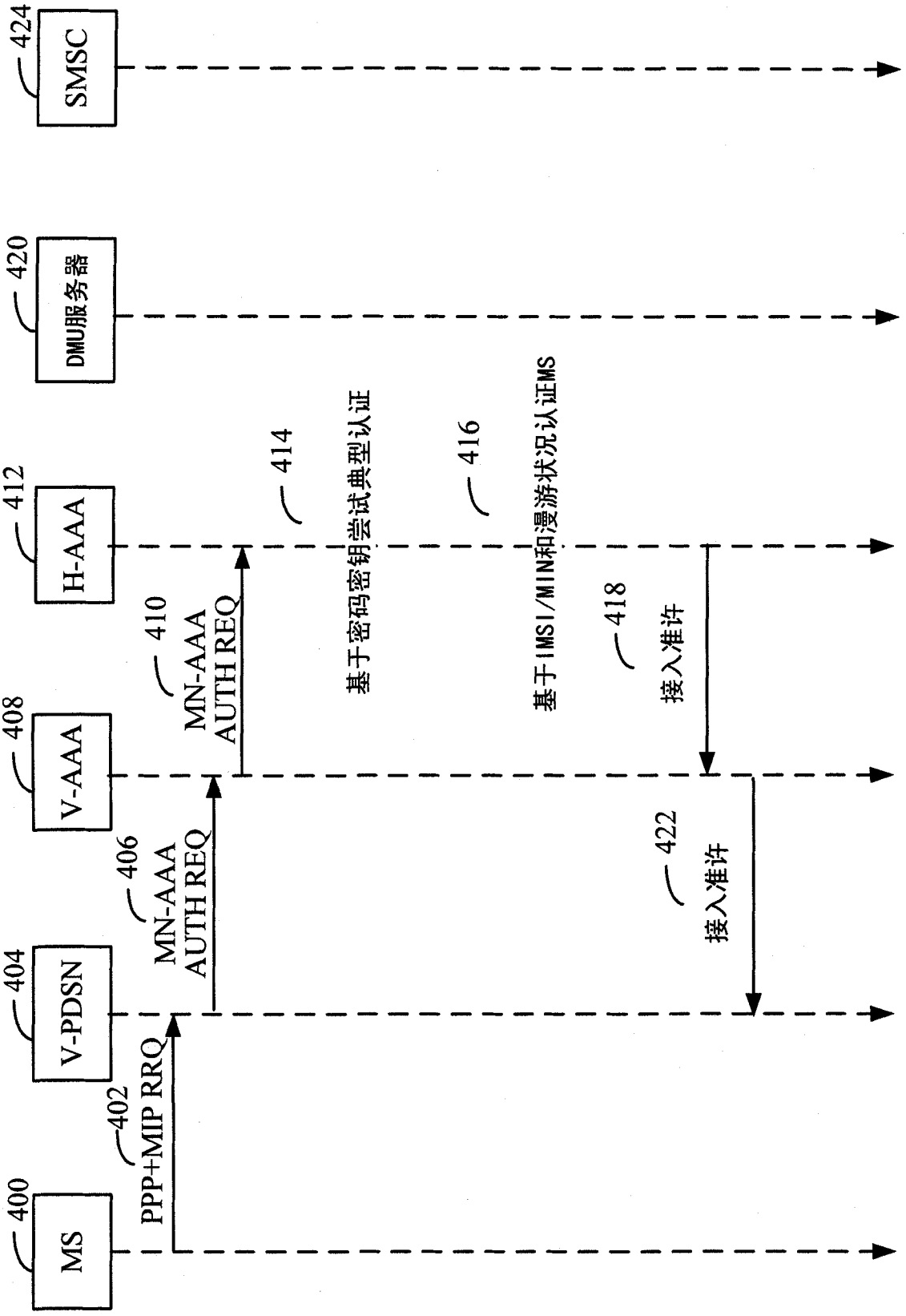

424
SMSC
420
DMU服务器
412
H-AAA
414
基于密码密钥尝试典型认证
416
基于IMSI/MIN和漫游状况认证MS
408
V-AAA
410
MN-AAA
AUTH REQ
418
接入准许
406
MN-AAA
AUTH REQ
422
接入准许
404
V-PDSN
402
PPP+MIP RRQ
400
MS

图 4

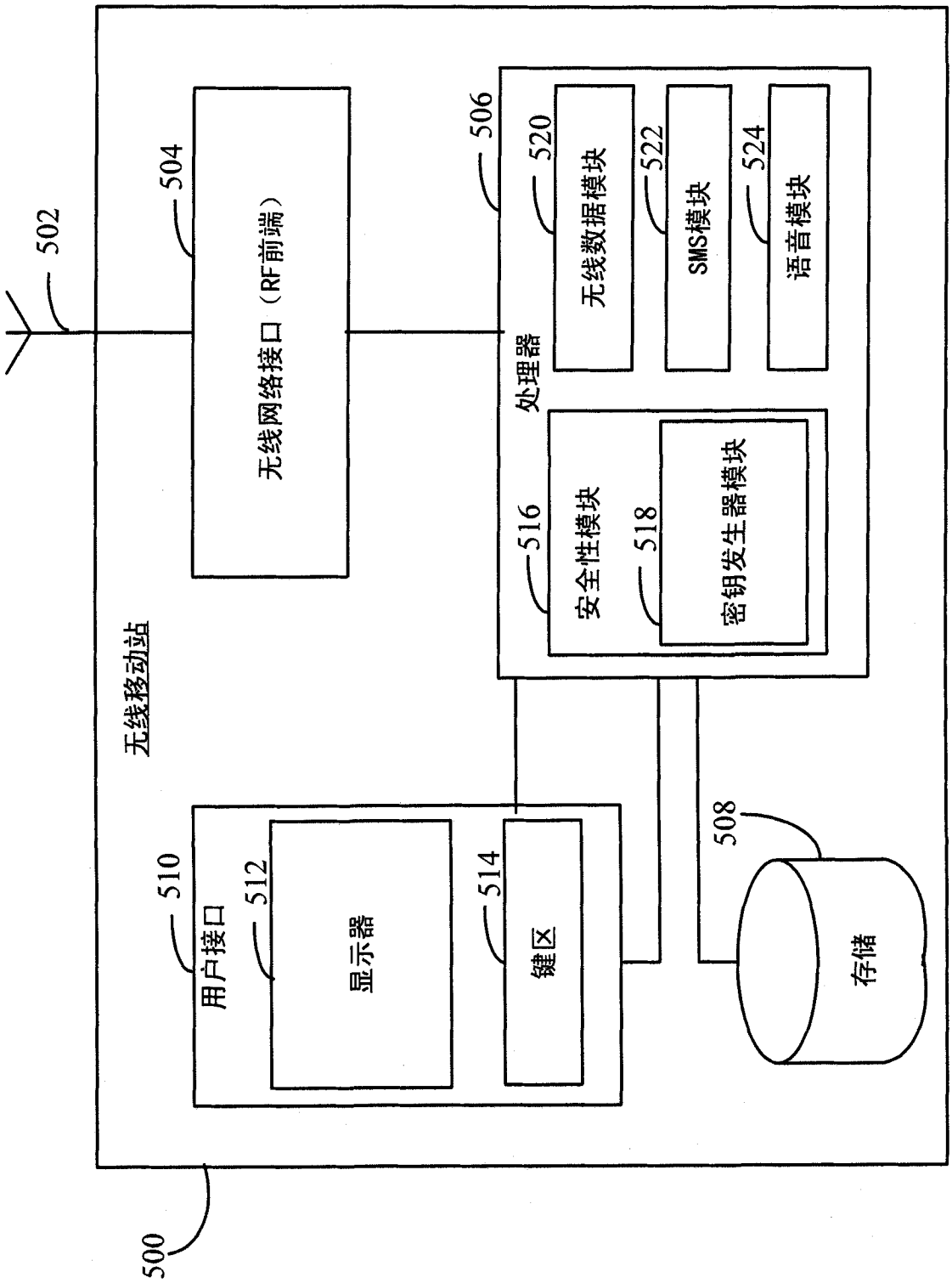

500
无线移动站
502
504
无线网络接口（RF前端）
506
处理器
520
无线数据模块
522
SMS模块
524
语音模块
516
安全性模块
518
密钥发生器模块
508
存储
510
用户接口
512
显示器
514
键区

图 5

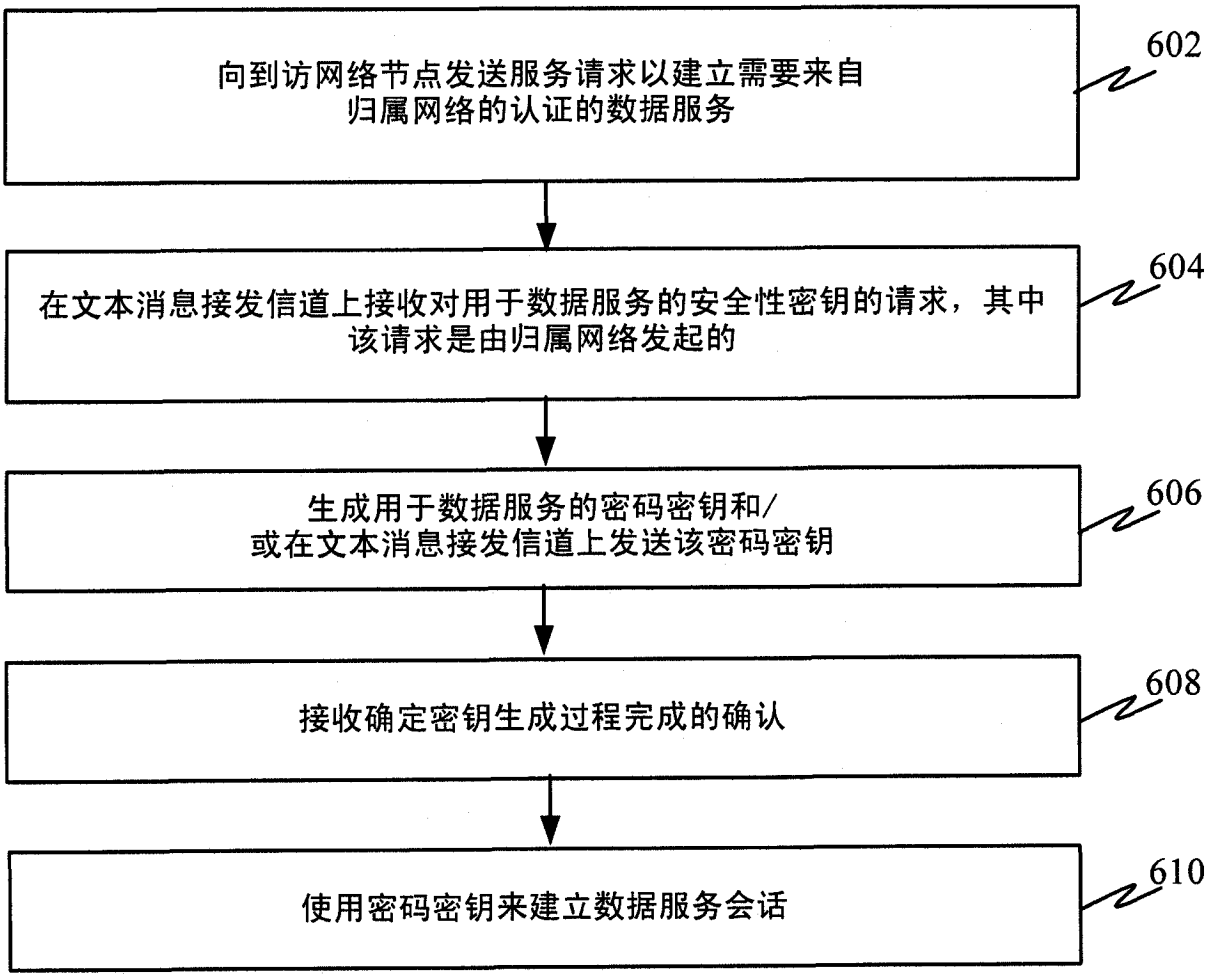

向到访网络节点发送服务请求以建立需要来自归属网络的认证的数据服务
602
在文本消息接发信道上接收对用于数据服务的安全性密钥的请求，其中该请求是由归属网络发起的
604
生成用于数据服务的密码密钥和/或在文本消息接发信道上发送该密码密钥
606
接收确定密钥生成过程完成的确认
608
使用密码密钥来建立数据服务会话
610

图 6

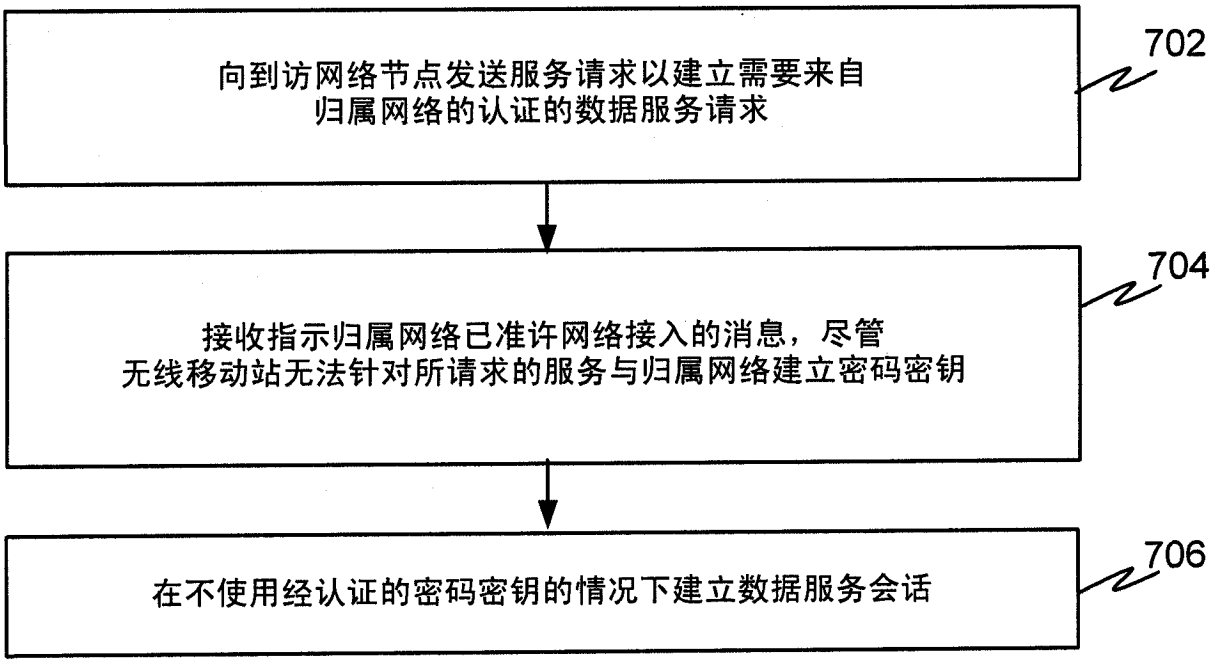

向到访网络节点发送服务请求以建立需要来自
归属网络的认证的数据服务请求
702
接收指示归属网络已准许网络接入的消息，尽管
无线移动站无法针对所请求的服务与归属网络建立密码密钥
704
在不使用经认证的密码密钥的情况下建立数据服务会话
706

图 7

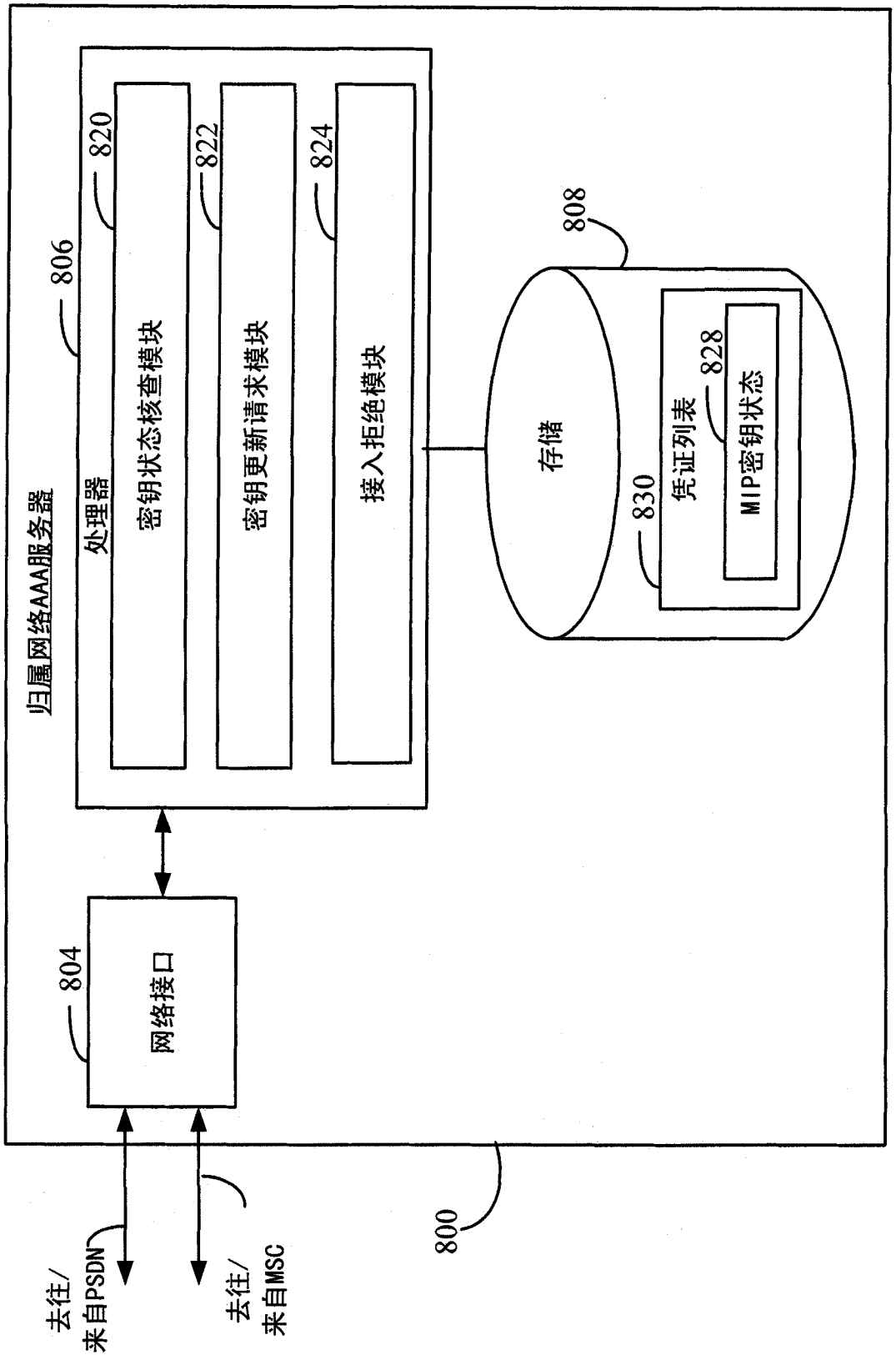

归属网络AAA服务器
806
处理器
820
密钥状态核查模块
822
密钥更新请求模块
824
接入拒绝模块
808
存储
828
凭证列表
MIP密钥状态
830
804
网络接口
800
去往/
来自PSDN
去往/
来自MSC

图 8

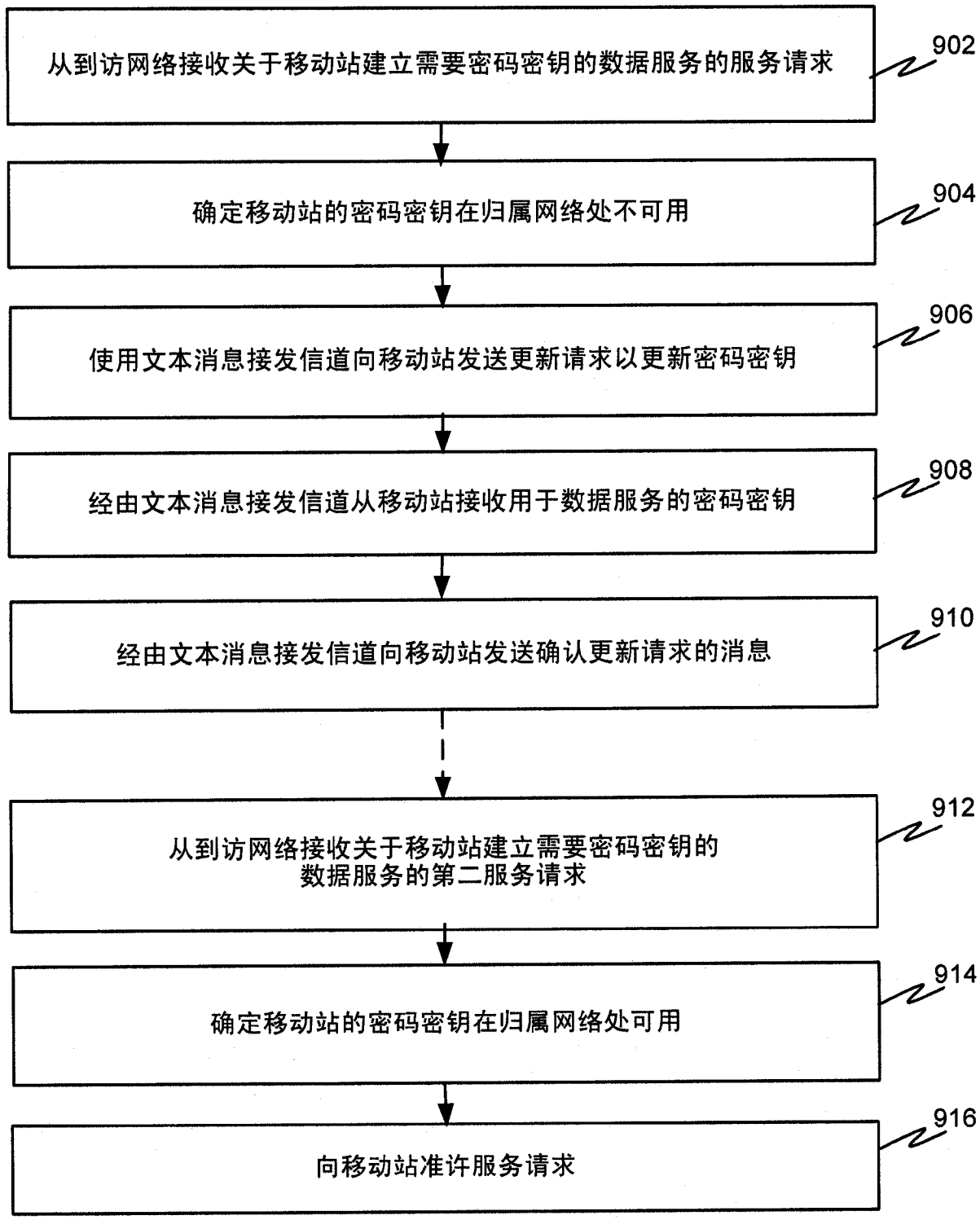

从到访网络接收关于移动站建立需要密码密钥的数据服务的服务请求
902
确定移动站的密码密钥在归属网络处不可用
904
使用文本消息接发信道向移动站发送更新请求以更新密码密钥
906
经由文本消息接发信道从移动站接收用于数据服务的密码密钥
908
经由文本消息接发信道向移动站发送确认更新请求的消息
910
从到访网络接收关于移动站建立需要密码密钥的
数据服务的第二服务请求
912
确定移动站的密码密钥在归属网络处可用
914
向移动站准许服务请求
916

图 9

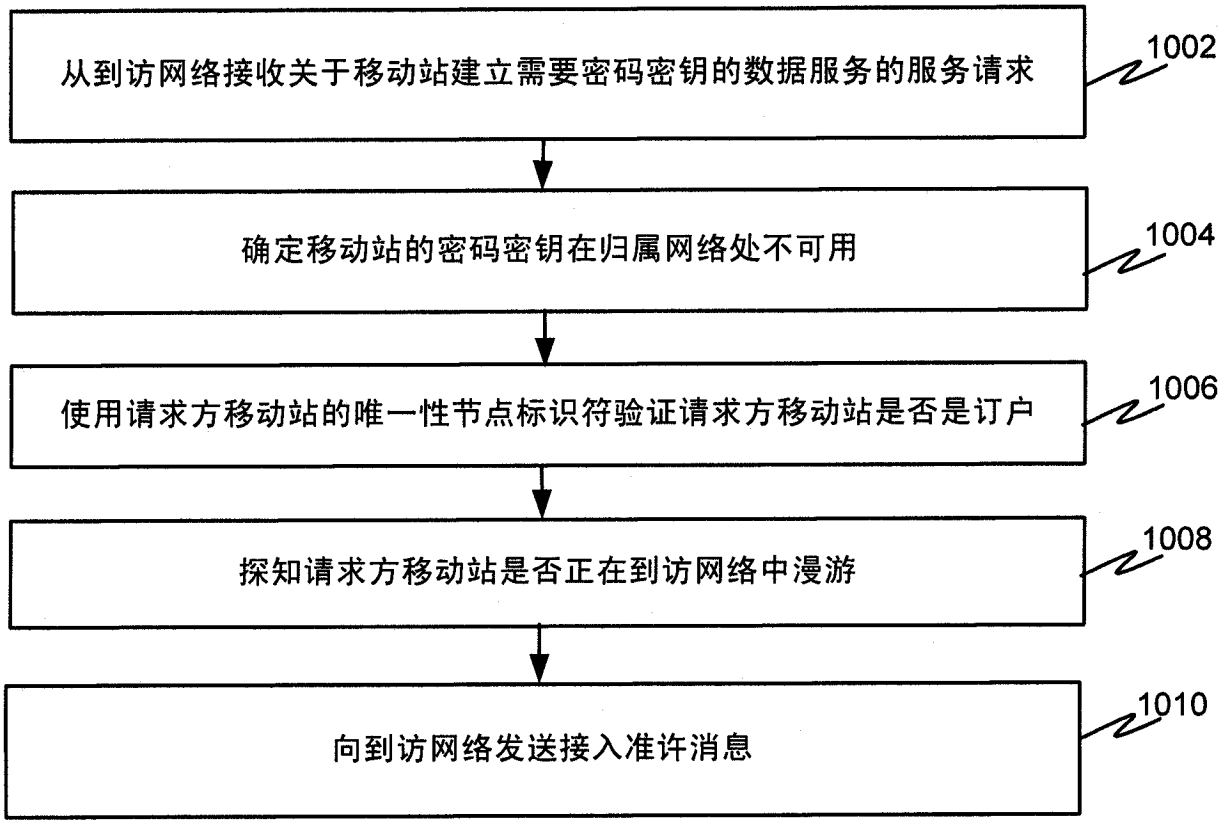

从到访网络接收关于移动站建立需要密码密钥的数据服务的服务请求
1002
确定移动站的密码密钥在归属网络处不可用
1004
使用请求方移动站的唯一性节点标识符验证请求方移动站是否是订户
1006
探知请求方移动站是否正在到访网络中漫游
1008
向到访网络发送接入准许消息
1010

图 10

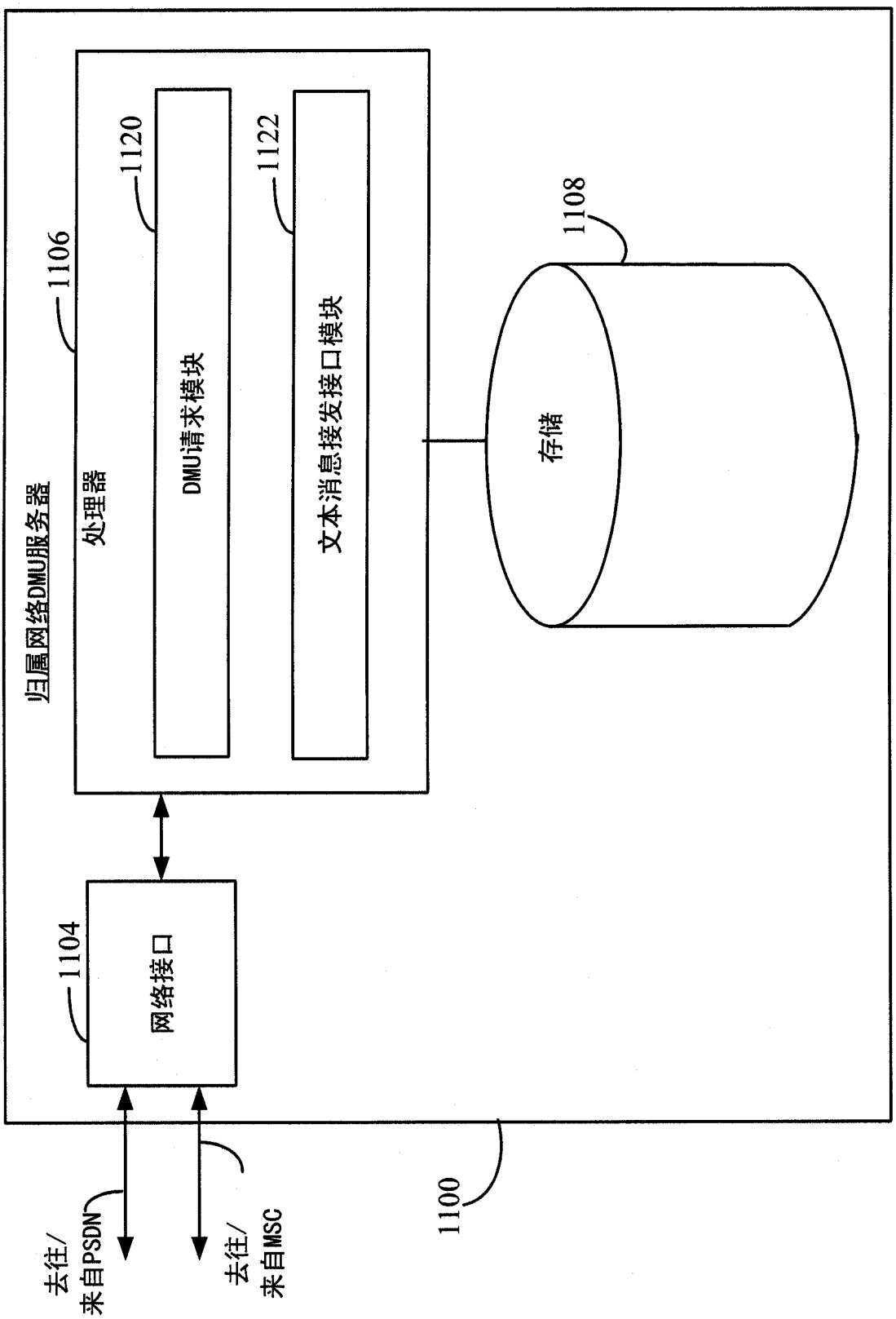

归属网络DMU服务器
1100
处理器
1106
DMU请求模块
1120
文本消息接发接口模块
1122
存储
1108
网络接口
1104
去往/
来自PSDN
去往/
来自MSC

图 11

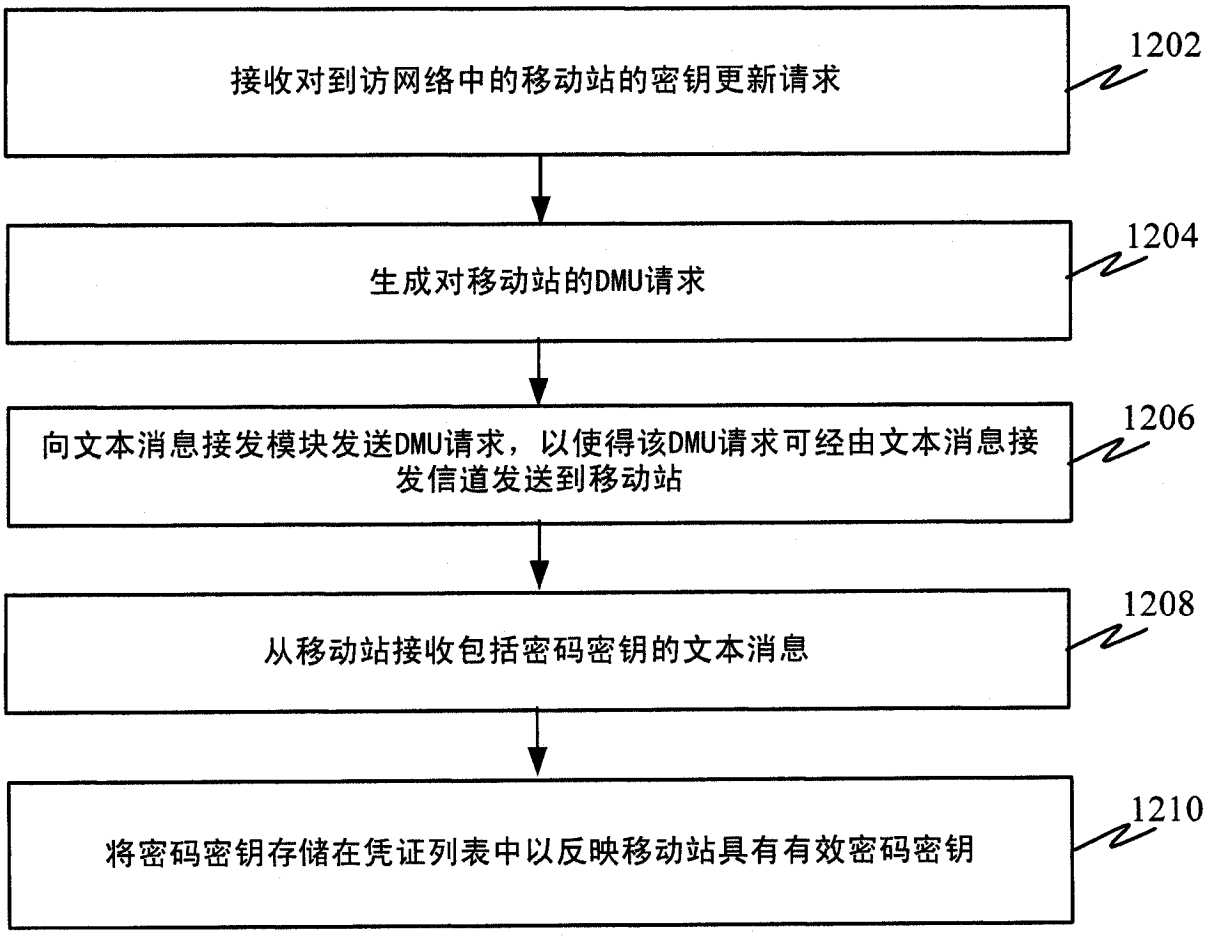

接收对到访网络中的移动站的密钥更新请求
1202
生成对移动站的DMU请求
1204
向文本消息接发模块发送DMU请求，以使得该DMU请求可经由文本消息接发信道发送到移动站
1206
从移动站接收包括密码密钥的文本消息
1208
将密码密钥存储在凭证列表中以反映移动站具有有效密码密钥
1210

图 12