(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 102308608 B
(45)授权公告日 2015.05.06

(21)申请号 200980156375.4

(22)申请日 2009.10.01

(30)优先权数据
61/150118 2009.02.05 US

(85)PCT国际申请进入国家阶段日
2011.08.05

(86)PCT国际申请的申请数据
PCT/SE2009/051092 2009.10.01

(87)PCT国际申请的公布数据
WO2010/090569 EN 2010.08.12

(73)专利权人 瑞典爱立信有限公司
地址 瑞典斯德哥尔摩

(72)发明人 L·巴里加 P-A·戴塞纽斯
M·林德斯特伦

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 柯广华 王洪斌

(51)Int.Cl.
H04W 12/04(2006.01)
H04L 9/32(2006.01)
H04W 8/20(2006.01)

(56)对比文件
US 2008/0016230 A1,2008.01.17, 第5页第0086段、第8页第0132段.
WO 2008/006312 A1,2008.01.17, 第11页第3-6、17-19行,第12页第4-26行、第16页第2-5行.

审查员 冷静

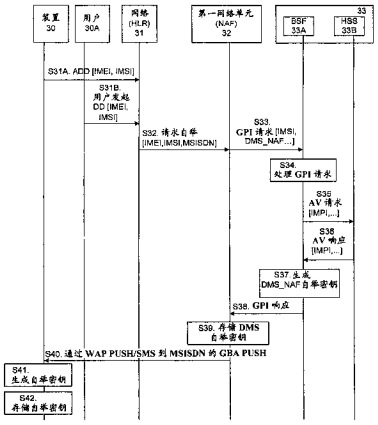
权利要求书2页 说明书6页 附图6页

(54)发明名称

用于在网络中保护自举消息的设备和方法

(57)摘要

本发明的实施例涉及具有第一网络单元和装置形式的设备,并且还涉及用于在装置管理网络系统中实现自举消息保护的方法。该方法包括:在第一网络单元接收自举装置的请求;将对于自举密钥的请求传送到第二网络单元;接收包括自举密钥并且还包括触发信息的消息,以及将触发消息传送到装置以触发在装置中内部生成自举密钥。之后,受保护的自举消息能够从第一网络单元传送到装置,并且在装置验证和/或解密自举消息时,装置管理(DM)会话能够在装置与第一网络单元之间开始。



CN 102308608 B

1. 一种用于实现自举消息保护的装置管理 DM 网络系统的第一网络单元 (500)，所述第一网络单元 (500) 包括 ：

- 接收器 (510)，配置成接收包括自举装置 (600) 的请求的第一消息，所述第一消息包括识别所述装置 (600) 的信息和识别订户的信息 ；

- 传送器 (520)，配置成将包括识别所述订户的所述信息的第二消息发送到第二网络单元，所述第二消息请求所述第二网络单元为所述第一网络单元 (500) 提供基于识别所述订户的所述信息的自举密钥 ；

- 所述接收器 (510) 还配置成从所述第二网络单元接收包括用于实现所述自举消息保护的所述自举密钥的第三消息，所述第三消息还包括触发信息 ；以及

- 所述传送器 (520) 还配置成将所述触发信息传送到所述装置 (600)，以触发在所述装置 (600) 中所述自举密钥的生成。

2. 如权利要求 1 所述的第一网络单元 (500)，还包括配置成存储所述自举密钥的存储部件 (530) ；所述第一网络单元 (500) 还配置成在所述传送器 (520) 将所述受保护的自举消息传送到所述装置 (600) 前，基于所述自举密钥保护所述自举消息。

3. 如权利要求 1 或权利要求 2 所述的第一网络单元 (500)，其中所述传送器 (520) 配置成在通用自举架构 PUSH 信息 GPI 消息中传送所述触发信息，以及其中所述接收器 (510) 配置成在 GPI 响应消息中接收包括所述自举密钥的所述第三消息。

4. 如权利要求 1-3 中任一项所述的第一网络单元 (500)，还配置成使用所述自举密钥作为主密钥以生成额外的密钥，用于在所述自举消息的验证后，在所述装置 (600) 与所述 DM 网络系统之间的至少一个 DM 会话期间保护至少一个消息。

5. 一种能够与用于实现自举消息保护的装置管理 DM 网络系统的第一网络单元 (500) 通信的装置 (600)，所述装置 (600) 包括 ：

- 用于通知所述第一网络单元 (500) 识别所述装置的信息和识别订户的信息的部件 (610) ；

- 接收器 (610)，配置成从所述第一网络单元 (500) 接收触发信息，以触发在所述装置中的自举密钥的生成 ；

- 所述接收器 (610) 还配置成接收受保护的自举消息，所述自举消息基于所述自举密钥受保护 ；以及

- 用于验证和 / 或解密所述受保护的自举消息的部件 (630)。

6. 如权利要求 5 所述的装置 (600)，其中所述接收器 (610) 配置成在通用自举架构 GBA PUSH 信息 GPI 消息中接收所述触发信息。

7. 如权利要求 5 或 6 所述的装置 (600)，还包括配置成存储所述自举密钥的存储部件 (640)。

8. 一种在用于实现自举消息保护的装置管理 DM 网络系统的第一网络单元 (500) 中的方法，所述方法包括 ：

- (401) 在所述第一网络单元接收包括自举装置的请求的第一消息，所述第一消息包括识别所述装置的信息和识别订户的信息 ；

- (402) 将包括识别所述订户的所述信息的第二消息传送到第二网络单元，所述第二消息请求所述第二网络单元为所述第一网络单元提供基于识别所述订户的所述信息的自

举密钥；

- (403) 从所述第二网络单元接收包括用于实现所述自举消息保护的所述自举密钥的第三消息，所述第三消息还包括触发信息；以及

- (404) 将所述触发信息传送到所述装置，以触发在所述装置中所述自举密钥的生成。

9. 如权利要求 8 所述的方法，还包括在将所述自举消息传送到所述装置前，在所述第一网络单元中存储所述自举密钥并基于所述自举密钥保护所述自举消息。

10. 如权利要求 8 或权利要求 9 所述的方法，其中所述触发信息的所述传送 (404) 包括在通用自举架构 PUSH 信息 GPI 消息中传送所述触发信息，以及其中所述第三消息的所述接收 (403) 包括在 GPI 响应消息中接收所述第三消息。

11. 如权利要求 8-10 中任一项所述的方法，还包括使用所述自举密钥作为主密钥以生成额外的密钥，用于在所述自举消息的验证后，在所述装置与所述 DM 网络系统之间的至少一个 DM 会话期间保护至少一个消息。

12. 一种在用于实现自举消息保护的装置管理 DM 网络系统的第一网络单元 (500) 中的设备，所述设备包括：

- 用于在所述第一网络单元接收包括自举装置的请求的第一消息的部件，所述第一消息包括识别所述装置的信息和识别订户的信息；

- 用于将包括识别所述订户的所述信息的第二消息传送到第二网络单元的部件，所述第二消息请求所述第二网络单元为所述第一网络单元提供基于识别所述订户的所述信息的自举密钥；

- 用于从所述第二网络单元接收包括用于实现所述自举消息保护的所述自举密钥的第三消息的部件，所述第三消息还包括触发信息；以及

- 用于将所述触发信息传送到所述装置，以触发在所述装置中所述自举密钥的生成的部件。

用于在网络中保护自举消息的设备和方法

技术领域

[0001] 本发明一般涉及移动通信网络系统或无线通信网络系统的领域，并且更具体地说，涉及用于在装置管理网络系统中装置的自举 (bootstrap) 期间安全地保护自举消息的设备和方法。

背景技术

[0002] 移动装置需要配置有多种设置，以控制和提供多种功能并支持多种服务。为移动装置配置服务有关数据的一种已知方法是经由例如短消息服务 (SMS) 或无线应用协议 (WAP)。这是单向路径，并且为了能够执行双向服务，开放移动联盟 (OMA) 已经规定了用于装置管理 (DM) 的协议、数据模型和政策。例如，在 URL :http://www.openmobilealiance.org 获得的 OMA DM version 1.2.1 enabler release specifications(OMA DM 技术发布规范版本 1.2.1) 定义了如何建立和维持 DM 会话。这些规范的重要功能之一包括自举规范，该规范描述了用于在发起管理会话之前以 OMA DM 设置开通 (provision) 装置的方法。OMA DM 自举技术规范在 OMA DM Bootstrap version 1.2.., OMA-TS-DM_Bootstrap V1_2_1.Open Mobile Alliance, June 2008(OMA DM 自举 (版本 1.2..), OMA-TS-DM_Bootstrap V1_2_1. 开放移动联盟，2008 年 6 月) 中进行了描述。

[0003] 自举是以下这样的过程 :开通移动装置或无线装置的 DM 客户端，以将装置从未开通的空状态转移到它能够发起到 DM 服务器和以后到例如新的 DM 服务器的管理会话的状态。执行自举过程有三种不同方式 :定制的自举 ;服务器发起的自举和从智能卡的自举。

[0004] 在定制的自举过程中，在制造时为装置加载 OMA DM 自举信息。这也称为工厂自举。

[0005] 在服务器发起的自举过程中，服务器配置成经由诸如 WAP PUSH 的某些 PUSH 机制来发出自举信息。对于此过程，服务器必须事先接收装置地址 / 电话号码。

[0006] 在从智能卡的自举过程中，将智能卡 (例如，订户身份模块 (SIM) 或通用 SIM(USIM)) 插入装置中，并且从智能卡自举 DM 客户端。

[0007] 然而，存在与使用这些过程的系统相关联的几个问题和缺陷。定制的自举过程要求在制造时或者在销售装置时知道基本参数。服务器发起的自举过程规定当 DM 服务器通过空中接口执行自举时，必须使用国际移动订户身份 (IMSI) 来编码基本 DM 参数。这通过将带有基本参数的加密 SMS 发送到装置来完成。用于加密的密钥是用于例如第二代 / 第三代网络系统的 IMSI，或者是码分多址 (CDMA) 系统的电子序号 (ESN)。然而，IMSI 或 ESN 一直未设计为机密。这也意味着对从 DM 服务器传送到装置的自举消息的保护弱。因此，攻击者能够创建其自己的自举消息，以自举将锁定到恶意 DM 服务器的装置。另一个缺陷是攻击者能够偷听只受完整性保护的自举消息。由于自举消息可包含诸如用户名和密码的凭证，因此，攻击者可假冒装置。

[0008] 图 1 示出如在上述规范 OMA DM Bootstrap version 1.2.1,OMA-TS-DM_Bootstrap V1_2_1 中定义的服务器发起的自举过程的高级视图。描述服务发起的自举的图 1 的情景显示了装置 10、用户 11、网络 12 及 DM 服务器 (DMS)13。在 OMA-TS-DM_Bootstrap 1_2_1 中，

描述了一旦用户 11 获得装置 10 并将其个性化（例如，通过插入 SIM），则自举过程的前提条件便到位。在装置 10 首次向网络 12 注册时，由例如网络 12 通知或告知 DMS 13 装置 10 的身份、地址或电话号码。在此情况发生时，自举装置 10 的请求能够同装置 10 使用的号码一起从（核心）网络 12 发送到 DMS 13。DMS 13 现在处于它能够发出 OMA DM 自举消息的位置。此自举消息包含使装置 10 能够与发出自举消息的 DMS 13 发起管理会话的信息。

[0009] 上述自举情景的弱保护源于以下事实：如在 OMA Device Management Security 1.2.1(OMA 装置管理安全 1.2.1)，OMA-TS-DM_Security-V1_2_1，OMA，2008 中第 5.7.2.3.1 节中指示的，如上所述只通过非机密密钥 (IMSI 或 ESN) 来保护自举消息。因此，从安全角度而言，IMSI 或 ESN 均未被视为共享机密。类似的 OMA 规范也遇到相同的担保弱的问题，例如 Enable Release Definition for OMA Client Provisioning Specifications version 1.2.(OMA 客户端开通规范的技术发布定义版本 1.2.)OMA-ERELD-ClientProvisioning-V1_1；和 Provisioning Bootstrap 1.1.(开通自举 1.1.)OMA-WAP-ProvBoot-V1_1。

[0010] 应提及的是，这些安全弱点是第三代合作伙伴计划 (3GPP) 中的安全组 (SA3) 已经发布不要使用如 3GPP LS reply S3-080262 中指示的服务器发起的自举方法 / 过程的强烈建议的原因。

[0011] 在美国专利申请 US 2008/0155071 中公开的另一个现有技术提议了用于通信网络中装置的自举的方法和系统。在此现有技术中，服务器发起的自举用于首先使用空中 (OTA) 技术开通装置的智能卡，使得装置能够从智能卡自举。这由组合通过智能卡的自举和 3GPP 自动装置检测 (ADD) 功能来执行。在技术规范 3GPP TS 22.101 中定义的 3GPP ADD 实现了当装置出现在网络中时对该装置的自动检测。然而，此现有技术的方法仍依赖于：如较早所述的、缺乏安全的当前 OMA DM 规定的服务器发起的自举。

发明内容

[0012] 因此，本发明示范实施例的目的是解决上述问题并提供设备和方法，所述设备和方法允许自举消息从 DM 服务器到装置的安全的和受保护的传输，由此防止偷听者和 / 或攻击者假冒装置和 / 或劫持装置的。

[0013] 根据本发明示范实施例的第一方面，借助于用于实现自举消息保护的 DM 网络系统的第一网络单元，解决了上述问题。第一网络单元包括：配置成接收包括自举装置的请求的第一消息的接收器，消息包括识别装置的信息和识别订户的信息。第一网络单元还包括：配置成将包括识别订户的信息的第二消息发送到第二网络单元的传送器，第二消息请求第二网络单元为第一网络单元提供基于识别订户的信息的自举密钥。接收器还配置成从第二网络单元接收包括用于自举消息保护的自举密钥的第三消息。第三消息还包括触发信息，其被传送到装置以触发在装置中的自举密钥的生成。

[0014] 在从第一网络单元接收触发信息时，装置内部生成自举密钥。在第一网络单元和装置均拥有自举密钥时，第一网络单元基于自举密钥保护自举消息，并将受保护的自举消息传送到装置。这样，由于机密自举密钥仅为 DM 网络和装置所知，因此，攻击者不能劫持或假冒装置。

[0015] 根据本发明示范实施例的另一个方面，借助于在用于实现自举消息保护的 DM 网络的第一网络单元中的方法，解决了上述问题。该方法包括：接收包括自举装置的请求的第

一消息，第一消息包括识别装置和订户的信息。方法还包括：将包括识别订户的信息的第二消息传送到第二网络单元，请求第二网络单元为第一网络单元提供基于识别订户的信息的自举密钥。方法还包括从第二网络单元接收包括用于实现自举消息保护的自举密钥的第三消息，第三消息还包括触发信息。方法还包括：将触发信息传送到装置，以触发装置中的自举密钥的生成。

[0016] 根据本发明示范实施例的又一个方面，借助于能够与用于实现自举消息保护的 DM 网络系统的第一网络单元通信的装置，解决了上述问题。该装置包括：用于通知第一网络单元识别装置和订户的信息的部件。装置还包括：配置成从第一网络单元接收触发信息以触发装置中的自举密钥的生成的接收器。接收器还配置成接收基于自举密钥保护的、受保护的自举消息，并且装置包括用于验证和 / 或解密受保护的自举消息的部件。

[0017] 本发明示范实施例的优点是防止了攻击者劫持装置和 / 或假冒装置。

[0018] 本发明示范实施例的另一优点是确保了使用仅网络和装置知道的、真正机密的自举密钥。

[0019] 结合附图，本发明实施例的又一些优点、目的和特征将从下面详细描述中变得显然，然而，要注意的事实是下面的附图只是图示性的，并且可在示出的特定实施例中进行多种修改和改变，如在所附权利要求的范围之内描述的那样。还应理解的是，附图不必按比例绘制，并且除非另有说明，否则它们只是要从概念上示出本文描述的结构和过程。

附图说明

[0020] 图 1 是在服务器发起的自举过程期间涉及的信令的现有技术高级视图。

[0021] 图 2 是根据本发明一示范实施例的、用于实现装置的安全的服务器发起的自举的流程图。

[0022] 图 3 是根据本发明另一个示范实施例的、用于装置的安全的服务器发起的自举的另一个流程图。

[0023] 图 4 是示出根据本发明示范实施例的、用于在第一网络单元中使用的方法的流程图的简图。

[0024] 图 5 示出了根据本发明示范实施例的、示范网络单元的框图。

[0025] 图 6 示出了根据本发明示范实施例的、示范装置的框图。

具体实施方式

[0026] 在下面的描述中，为解释而不是限制的目的阐述了特定细节，例如，具体的架构、情景、技术等，从而提供对本发明的详尽理解。然而，从下面将明显的是，本发明及其实施例可在脱离这些特定细节的其它实施例中实践。

[0027] 本发明示范实施例在本文中通过参照具体示例情景的方式进行了描述。具体而言，在装置管理 (DM) 网络系统中与服务器发起的自举情景有关的非限制性通用上下文中描述了本发明，装置管理网络系统包括与根据 3GPP 技术规范 TS 33.223 中 GBA PUSH 规范的通用自举架构 (GBA) 交互的 DM 服务器 (DMS)。DMS 在下文中表示为第一网络单元。然而，注意到第一网络单元可以是能够实现本发明示范实施例的、任何适合的网络单元或节点。此类网络单元例如能够由 DM 代理而不是 DMS 表示。

[0028] 参照图 2，其中示出了根据本发明一示范实施例的、用于实现在网络系统中装置的安全的服务器发起的自举的流程图。示出的实体是：装置 20、网络实体（一个或多个）21（例如，归属位置寄存器 (home location register))、第一网络单元 22 及第二网络单元 23。如后面将示出和描述的那样，额外的节点 / 功能也能用于装置的安全自举的目的。

[0029] 如图 2 所示，装置 20 通知网络 21 其可用性 (S21)。这能由用户 / 订户打开尝试附接到网络 21 的装置 20 来完成。例如，经由如在 3GPPTS 22.101 中公开的、已知的自动装置检测 (ADD) 方法或经由如在 GBA Push 3GPP TS 33.223 中描述的、已知的用户发起的过程，网络 21 检测装置 20 的存在 / 可用性 (S22)。在附接到网络 21 时，装置 20 发送识别装置的信息，即，其装置身份（例如，IMEI），并还发送识别订户的信息（例如，IMSI/ESN）。在自举请求 (S23) 中，网络 21 请求第一网络单元 22 自举装置 20。在自举请求 (S23) 中，网络 21（例如，HLR) 包括识别装置的信息 (IMEI) 和识别订户的信息（即，IMSI/ESN、MSISDN 等）。在第一网络单元 22 接收到请求时，并基于识别装置和用户 / 订户的信息，第一网络单元 22 确定 GBA PUSH 是否能朝向装置使用。如果能够使用，则第一网络单元 22 将消息 (S24) 传送到第二网络单元 23，请求第二网络单元 23 为第一网络单元 22 提供自举密钥。是 GBA 子系统一部分的第二网络单元 23 包括自举服务器功能 (BSF) 和归属订户服务器 (HSS)。

[0030] 应提及的是，如果第一网络单元 22 确定 GBA PUSH 能够朝向装置使用，则第一网络单元 22 的网络应用功能 (NAF) 配置成使用 GBA PUSH 过程联系 BSF，以使用消息 (S24) 请求至少触发信息和自举密钥。触发信息对应于 GBA PUSH 信息 (GPI)。消息 (S24) 还包括 NAF 身份。然而，注意第一网络单元 22 配置成选择用于自举装置 20 的方法，因而是安全方法中基于 GBA PUSH 的一种方法。如果选择 GBA PUSH，则基于识别装置和订户的信息，第一网络单元 22 的 NAF 处理安全自举过程。在下面描述了当 GBA PUSH 能够朝向装置 20 使用——即请求消息 (S24) 到达第二网络单元 23 时的情况。

[0031] 再参照图 2，当第二网络单元 23 接收请求消息 (S24) 时，它生成自举密钥 (S25)，并且在此处表示为 GPI 响应的响应消息 (S26) 中将自举密钥和至少 GPI 发送或递送到第一网络单元 (22)。由于第一网络单元 22 拥有 GPI 响应，因此，它将触发信息（即 GPI 响应中的 GPI 部分）传送或转发到装置 20(S27)。第一网络单元 22 也能够在将 GPI 传送到装置 20 前存储自举密钥。GPI 或触发信息能够通过 SMS、WAP、HTTP、SIP PUSH 或适于载运触发信息的任何载体传送，以触发在装置 20 中的自举密钥的生成。一旦接收到 GPI，装置 20 就使用适合的标准过程生成自举密钥 (S28)。

[0032] 在 GBA Push 3GPP TS 33.223 中，公开了 GPI 受保护。这称为 GPI 完整性保护和 GPI 秘密性保护。而且在 GBA 中，自举密钥表示 Ks_NAF，并且此密钥也称为密钥材料或建钥材料。在上述现有技术 GBA Push 3GPP TS 33.223 中引用的 3GPP TS 33.220 V8.5.0 中描述了 Ks_NAF。在通篇描述中，自举密钥用于指 Ks_NAF 或密钥材料 / 建钥材料。

[0033] 再参照图 2，在装置 20 生成自举密钥 (S28) 时，它存储自举密钥。随后，能够由第一网络单元 22、通过保护和传送基于自举密钥保护的自举消息 (S29)，来执行安全的自举。第一网络单元 22 能够使用自举密钥直接保护自举消息，或者能够使用自举密钥得到进一步的密钥，并使用这些密钥保护自举消息。注意，如果第一网络单元 22 在将自举消息传送到装置 20 前已将它加密，则装置 20 需要首先将自举消息解密，然后验证消息。可以不是 IMSI/ESN 的自举密钥能够用于完整性保护和 / 或能够用于秘密性保护。在装置的成功和安

全的自举之后，DM 会话能在装置 20 与第一网络单元 22 之间开始。注意，自举密钥也能够用做主密钥，以在自举消息的成功验证 / 解密后进一步生成能够用于保护在装置 20 与第一网络单元 22 之间一个或多个 DM 会话的密钥（例如，鉴权 (authentication)）。

[0034] 参照图 3，其中示出了根据本发明另一个示范实施例的、用于实现在网络系统中装置的安全的服务器发起的自举的流程图。类似于图 2，网络系统包括 :装置 30、网络 31（例如，HLR）、第一网络单元 32（例如，带有 NAF 的 DMS）及包括 BSF 33A 和 HSS 33B 的第二网络单元 33。图 3 也描绘了用户 30A。在 (S31A) 中，在附接到网络 31 时，装置 30 发送识别装置的信息 IMEI，并且还发送识别用户 / 订户的信息（例如，IMSI）。如更早所提及的那样，这能够使用某一形式的 ADD 过程和 / 或用户发起的过程完成。应提及的是，用户 / 订户 30A 能够备选地关于 IMEI 和 IMSI 通知网络 31(S31B)。这能够由在销售控制台位置处的销售员或由终端用户自己经 web 接口或使用例如 DMTF 音来执行。

[0035] 在 (S32) 中，在网络 31 检测到通过例如 IMSI/ESN、MSISDN 及 IMEI 识别的装置 / 用户 / 订户时，网络 31 将自举装置 30 的请求发送到第一网络单元 32（例如，DMS(NAF)），并且在请求中包括 IMEI、IMSI（或 ESN) 和 MSISDN。如更早所提及的那样，第一网络单元 32 或第一网络单元 32 的 NAF 首先基于装置和用户 / 订户信息确定 GBA PUSH 是否能够朝向装置 30 使用。如果能够使用，则第一网络单元 32 的 NAF 部分使用 GBA PUSH 过程将 GPI 请求 (S33) 发送到第二网络单元 33 的 BSF 33A，以请求 GPI 响应。请求 (S33) 包括诸如 IMSI 的识别订户的信息和至少 NAF 的身份 (DMS_NAS_Id)。在 BSF 33A 接收请求时，它处理请求 (S34) 并识别用户 / 订户。之后，BSF 33A 将请求 (S35) 发送到第二网络单元 33 的 HSS 33B，向 HSS 33B 请求用于装置 30 的鉴权向量 (AV)。在 AV 请求 (S35) 中，指示了 IMPI。在 (S36) 中，HSS 33B 在 AV 响应中返回请求的 AV。然后，BSF 33A 生成 (S37) 自举密钥并存储密钥，该密钥是 DMS NAF 自举密钥。BSF 33A 在 (S38) 中将包括自举密钥和包含 GPI 参数的至少一 GPI 的 GPI 响应发送到第一网络单元 32。第一网络单元 32 存储自举密钥 (S39) 并准备包括触发信息（即，GPI) 的 GPI 包，之后将 GPI 包发送到装置 30(S40)。如更早所提及的那样，任何适合的载体能够用于将 GPI 载运到装置 30，例如，通过 WAP PUSH 或 SMS 或 SIP 等的 GPI。MSISDN 能够用于寻址装置 30。

[0036] 在装置 30 接收 GPI 时，装置 30 内部生成 DMS NAF 自举密钥 (S41)，并且装置 30 存储自举密钥 (S42)。之后，自举消息由第一网络单元 32 基于自举密钥进行保护，并且将受保护的自举消息传送到装置 30（未示出）。然后，装置验证和 / 或解密自举消息。如果验证和 / 或解密成功，则 DM 会话在装置与第一网络单元之间开始（未示出）。这样，只有第一网络单元和装置知道自举密钥，由此防止偷听者和攻击者劫持装置或假冒装置。

[0037] 类似于前面描述的示范实施例，第一网络单元和装置均能够使用自举密钥生成进一步的密钥。第一网络单元使用该进一步的密钥保护自举消息，并且装置能够使用该进一步的密钥来验证和 / 或解密自举消息。

[0038] 参照图 4，其中示出了根据本发明前面描述的示范实施例的、在第一网络单元中用于实现自举消息保护的方法或过程的主要步骤。如图 4 中所示，方法的主要步骤包括 :

[0039] (401) 接收包括识别装置的信息和识别订户的信息的第一消息（即，自举装置的请求）；

[0040] (402) 将包括识别订户的信息的第二消息（即，GPI 请求）传送到第二网络单元，

请求第二网络单元为第一网络单元提供基于识别订户的信息的自举密钥；

[0041] (403) 从第二网络单元接收包括用于实现自举消息保护的自举密钥和触发信息（即，GPI）的第三消息（即，GPI 响应）；

[0042] (404) 将触发信息传送到装置以触发在装置中内部生成自举密钥。

[0043] 对第一网络单元的额外方法步骤和功能已经进行了讨论，因此不再重复。

[0044] 参照图 5，其中示出了根据本发明前面描述的示范实施例的、用于实现自举消息保护的 DM 网络系统的示范第一网络单元 500（例如，DMS）的框图。如图 5 中所示，第一网络单元 500 包括配置成接收包括自举装置的请求的第一消息的接收器 510(RX)。第一消息包括识别装置和订户的信息。第一网络单元 500 还包括传送器 520(TX)，其配置成将包括识别订户的信息的第二消息（即，GPI 请求）传送到第二网络单元（例如，BSF+HSS），请求第二网络单元为其提供自举密钥。第一网络单元 500 的接收器 510 还配置成接收包括用于实现自举消息保护的自举密钥的第三消息（即，GPI 响应）。第三消息还包括触发信息（即，GPI）。第一网络单元 500 的传送器 520 还配置成将触发信息传送到装置，以触发在装置中的自举密钥的生成。第一网络单元 500 还包括用于存储自举密钥的存储部件 530。第一网络单元 500 还包括配置成确定 GBA PUSH 是否能够朝向装置使用的处理逻辑 / 单元 540，并且还配置成基于自举密钥生成进一步的 / 额外的密钥和保护自举消息。存储部件 530 和处理逻辑 / 单元 540 示为是处理系统 550 的一部分，虽然这不是必需的。

[0045] 虽然图 5 示出第一网络单元 500 的示范组件，但在其它实现中，第一网络单元 500 可包含与图 5 中描绘的相比更少、不同或额外的组件。在又一些实现中，单元 500 的一个或多个组件可执行描述为由第一网络单元 500 的一个或多个其它组件来执行的任务。

[0046] 参照图 6，其中示出了根据本发明一些示范实施例的、装置 600 的示范组件的简图。如示出的，装置 600 包括收发器 610，收发器包括用于将识别装置和订户的信息通知 DM 网络系统的（图 5 的）第一网络单元的部件，用于实现自举消息的保护。用于通知的部件能够视为是收发器 610 的传送器。收发器 610 还包括配置成从第一网络单元接收触发信息（即，GPI），以触发在装置中内部生成自举密钥的接收器。收发器 610 的接收器还配置成接收第一网络单元基于自举密钥保护的受保护的自举消息。天线 620 还示为连接到收发器 610。装置 600 还包括用于验证和 / 或解密受保护的自举消息的部件。装置 600 的处理单元 / 部件 630 配置成生成自举密钥，并执行受保护的自举消息的验证 / 解密。装置 600 可包括几根天线（仅示出一根天线 620）、用于存储自举密钥的存储器或存储部件 640、输入装置（一个或多个）650、输出装置（一个或多个）660 及总线 670。虽然图 6 示出装置 600 的示范组件，但在其它实现中，装置 600 可包含与图 6 中描绘的相比更少、不同、或额外的组件。

[0047] 本发明及其示范实施例能以许多方式实现。例如，本发明的一个实施例包括具有存储其中的程序指令的计算机可读媒体，程序指令可由第一网络单元的计算机执行，以执行如前面所述本发明示范实施例的方法步骤。

[0048] 虽然本发明已根据几个优选实施例进行了描述，但预期的是，本领域技术人员一旦阅读本说明书及研究附图，就将明白优选实施例的备选、修改、置换及等同物。因此，意在使所附权利要求包括落入本发明范围之内的此类备选、修改、置换及等同物。

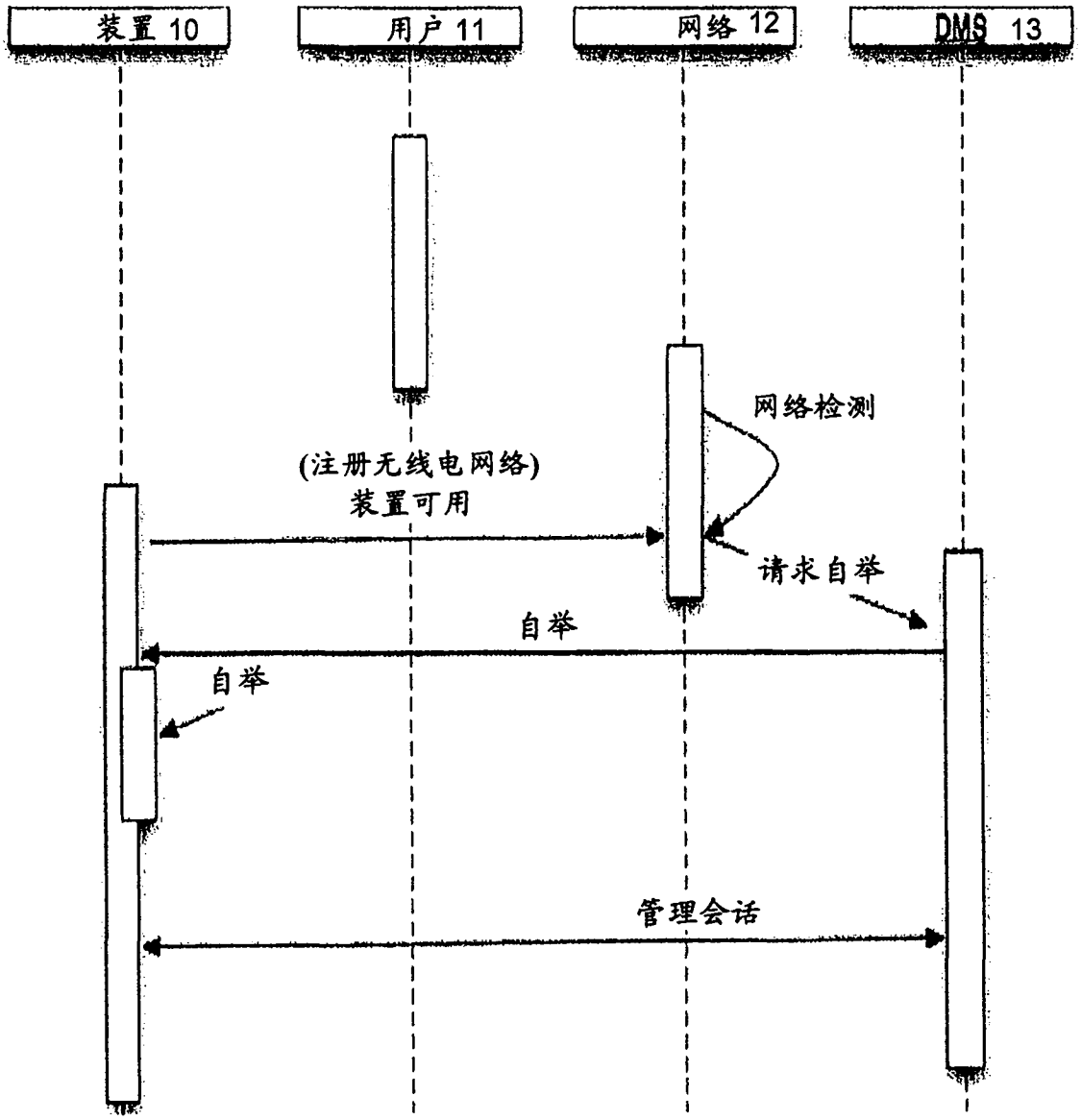


图 1

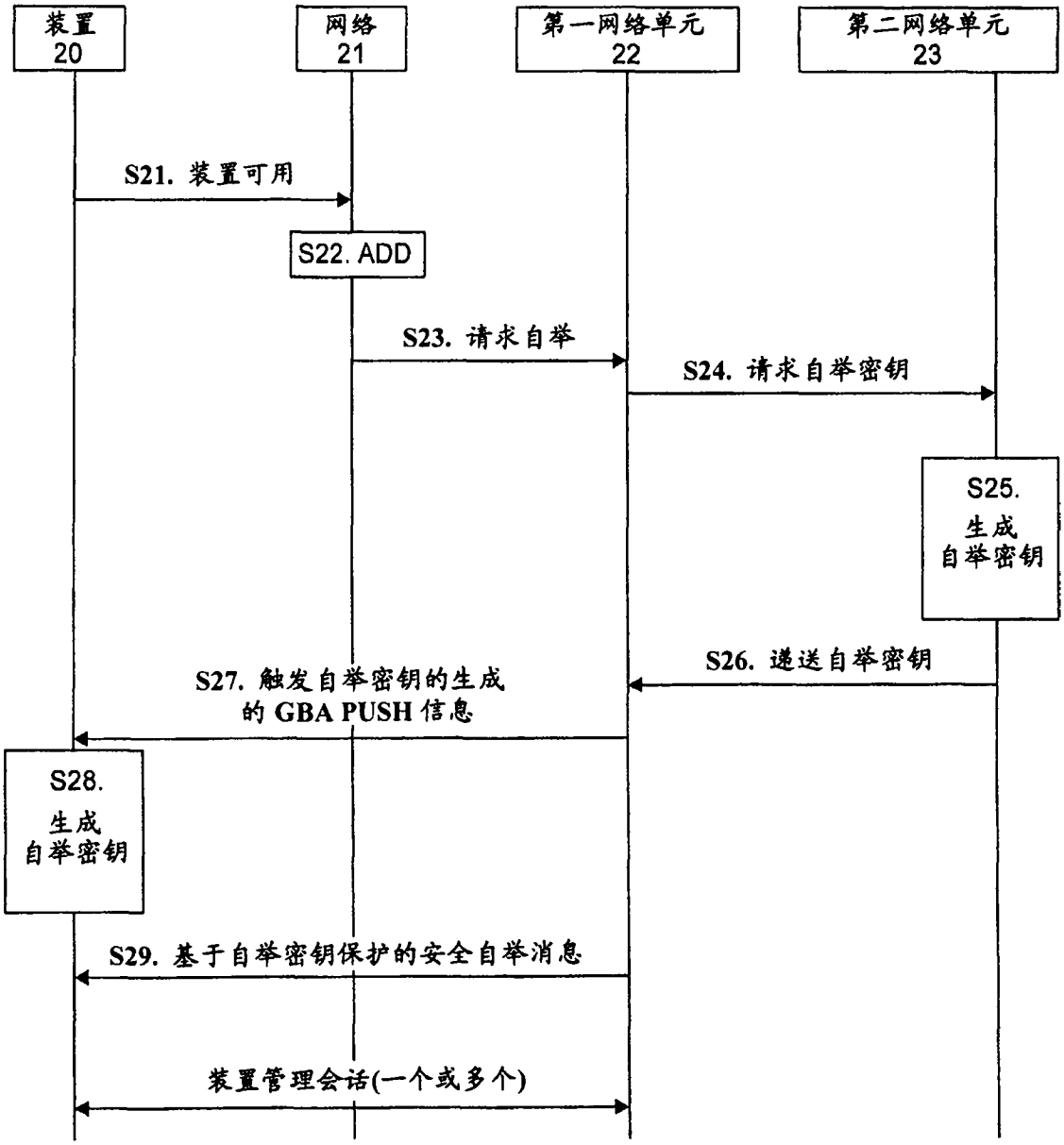

装置
20
网络
21
第一网络单元
22
第二网络单元
23
S21. 装置可用
S22. ADD
S23. 请求自举
S24. 请求自举密钥
S25.
生成
自举密钥
S26. 递送自举密钥
S27. 触发自举密钥的生成
的 GBA PUSH 信息
S28.
生成
自举密钥
S29. 基于自举密钥保护的安全自举消息
装置管理会话(一个或多个)

图 2

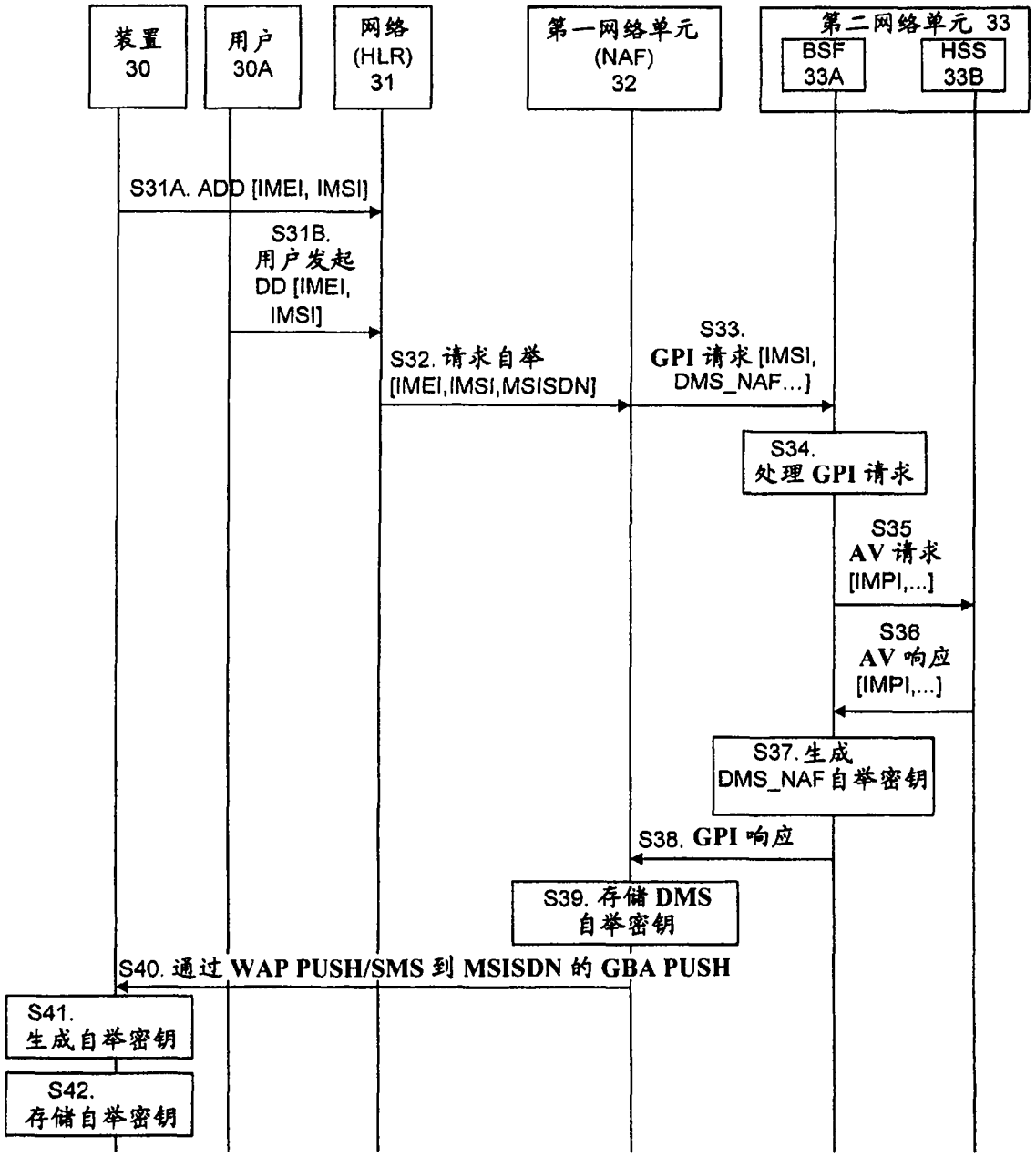

装置
30
用户
30A
网络
(HLR)
31
第一网络单元
(NAF)
32
第二网络单元 33
BSF
33A
HSS
33B
S31A. ADD [IMEI, IMSI]
S31B.
用户发起
DD [IMEI,
IMSI]
S32. 请求自举
[IMEI,IMSI,MSISDN]
S33.
GPI 请求 [IMSI,
DMS_NAF...]
S34.
处理 GPI 请求
S35
AV 请求
[IMPI,...]
S36
AV 响应
[IMPI,...]
S37. 生成
DMS_NAF 自举密钥
S38. GPI 响应
S39. 存储 DMS
自举密钥
S40. 通过 WAP PUSH/SMS 到 MSISDN 的 GBA PUSH
S41.
生成自举密钥
S42.
存储自举密钥

图 3

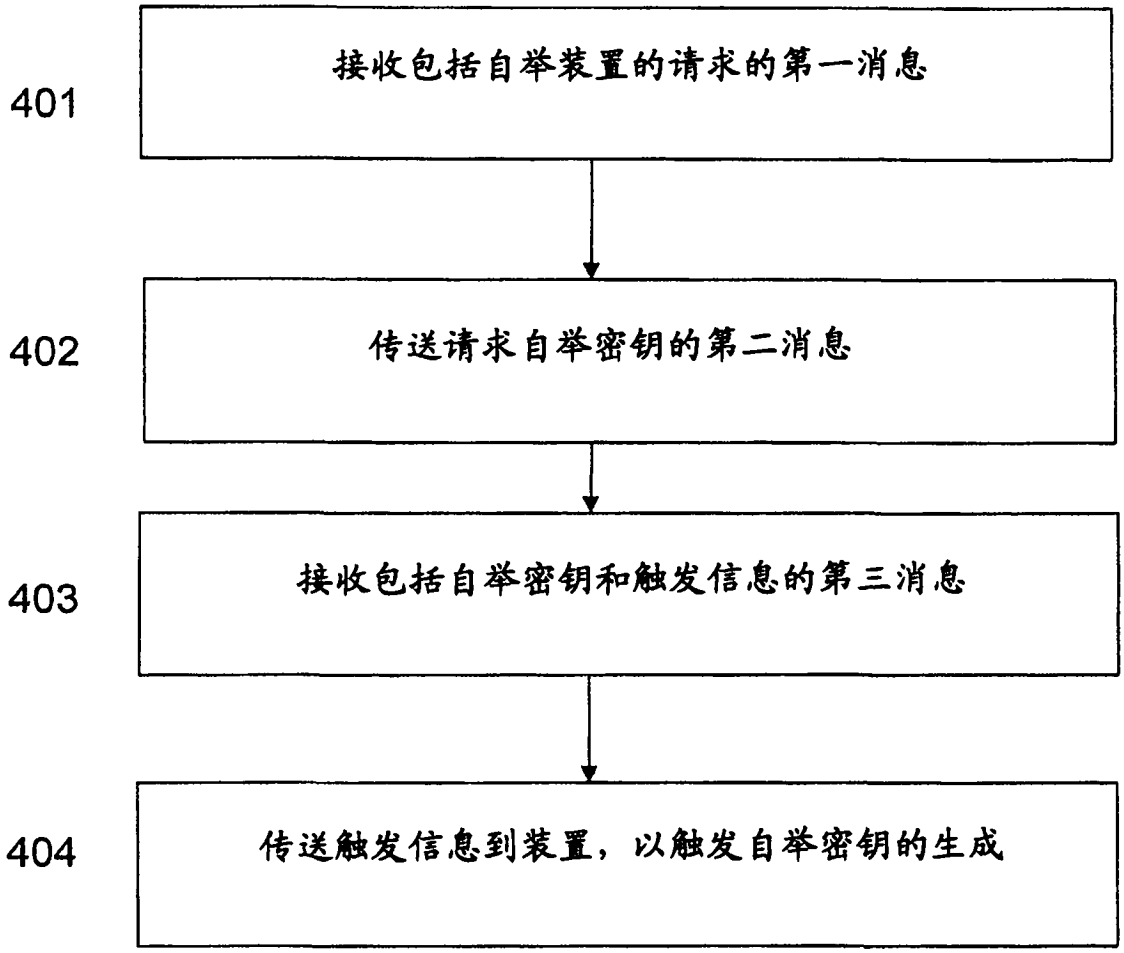

401
接收包括自举装置的请求的第一消息
402
传送请求自举密钥的第二消息
403
接收包括自举密钥和触发信息的第三消息
404
传送触发信息到装置，以触发自举密钥的生成

图 4

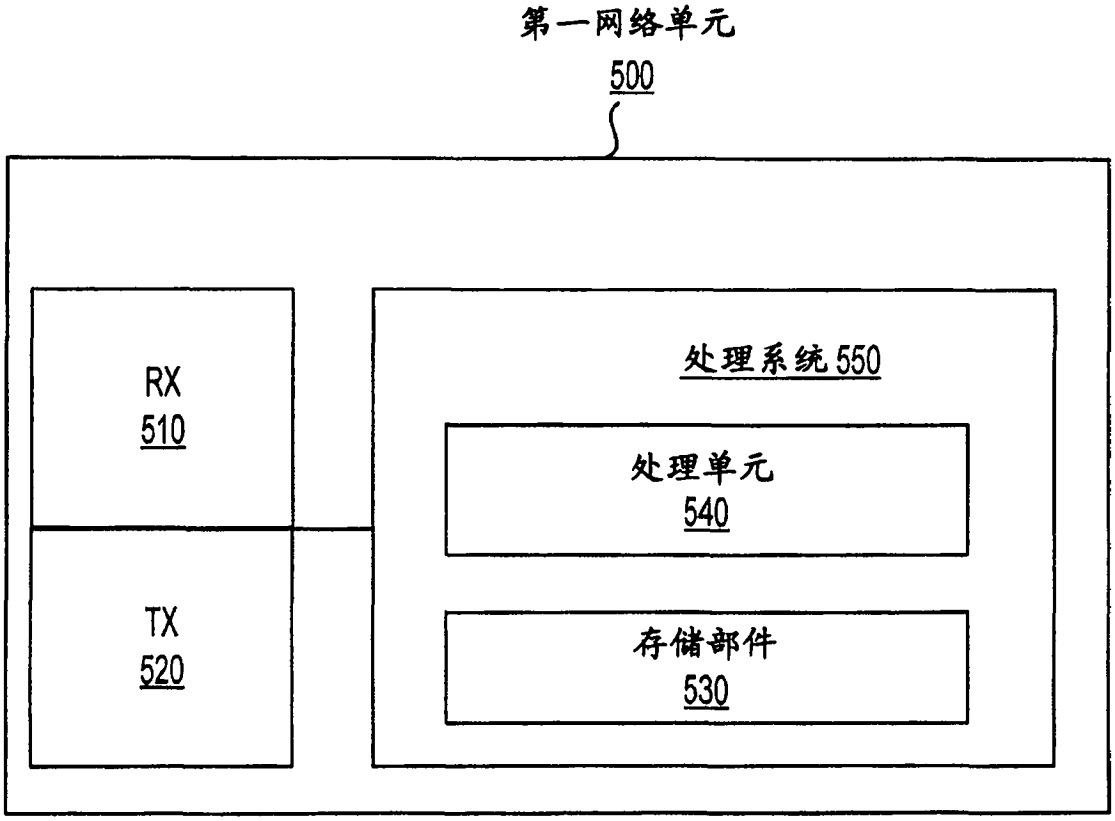


图 5

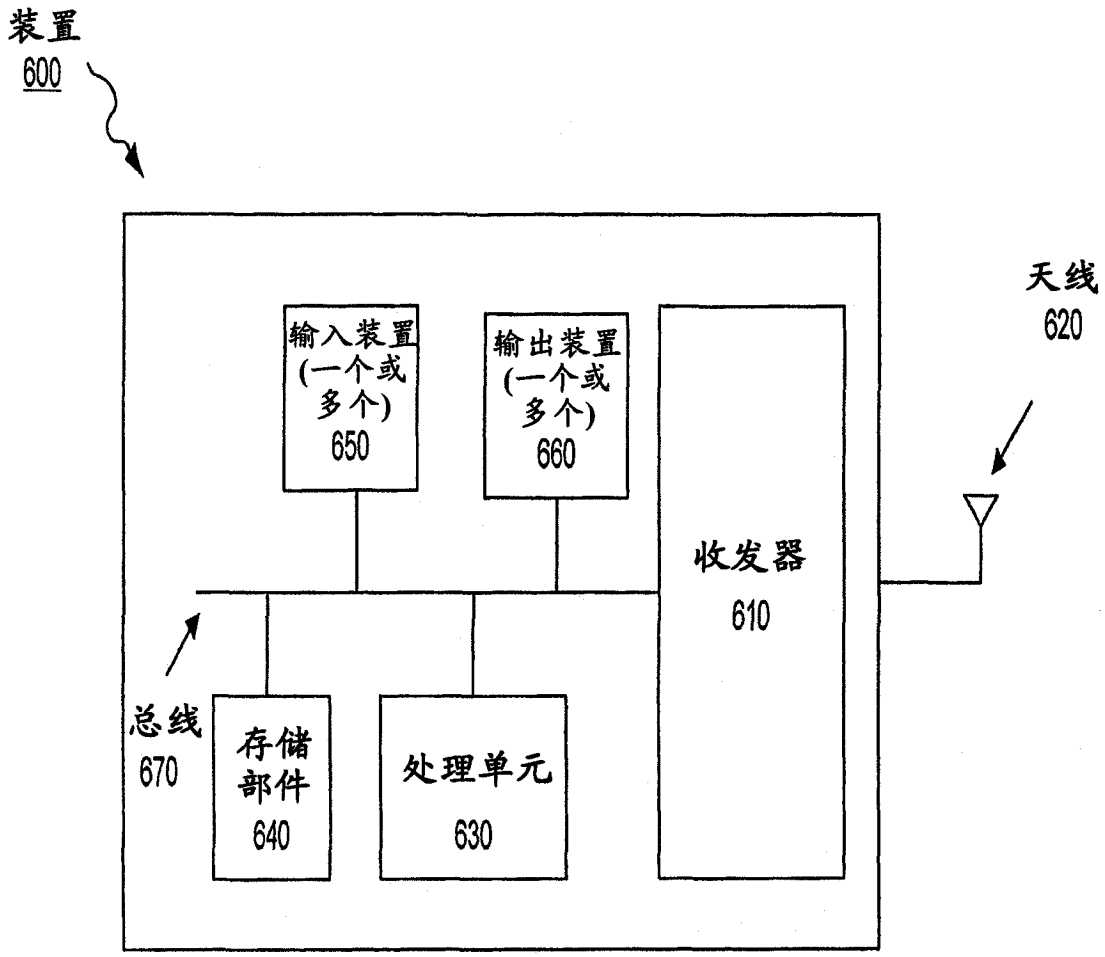

装置
600
输入装置
(一个或
多个)
650
输出装置
(一个或
多个)
660
收发器
610
天线
620
总线
670
存储
部件
640
处理单元
630

图 6