



(12) 发明专利

(10) 授权公告号 CN 1849837 B

(45) 授权公告日 2010.11.10

(21) 申请号 03826984.8

H04L 12/56(2006.01)

(22) 申请日 2003.08.26

(56) 对比文件

(85) PCT申请进入国家阶段日
2006.02.27US 2003/0159067 A1, 2003.08.21, 全文.
US 2001/0031635 A1, 2001.10.18, 全文.
CN 1430855 A, 2003.07.16, 全文.(86) PCT申请的申请数据
PCT/SE2003/001316 2003.08.26WO 03/056781 A1, 2003.07.10, 全文.
3rd Generation Partnership Project(87) PCT申请的公布数据
W02005/020619 EN 2005.03.03Access security for IP-based
services (Release 5). 3GPP TS 33.203
v5.6.0. 2006, 3(33203560), 12-18.(73) 专利权人 艾利森电话股份有限公司
地址 瑞典斯德哥尔摩

审查员 孙国辉

(72) 发明人 J·M·瓦尔克皮纳
J·A·桑切斯埃雷罗(74) 专利代理机构 中国专利代理(香港)有限公
司 72001

代理人 杨凯 刘杰

(51) Int. Cl.

H04W 48/02(2006.01)

H04L 29/06(2006.01)

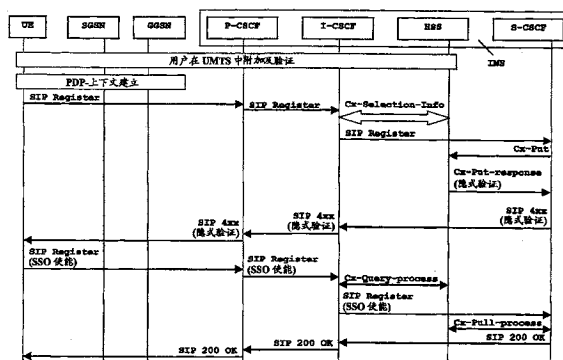
权利要求书 3 页 说明书 11 页 附图 9 页

(54) 发明名称

用于在访问多媒体服务时验证用户的设备及方法

(57) 摘要

本发明提供在接入网域与多媒体域之间对给定用户执行跨域验证的域间验证机制, 这种域间验证机制比现有机制更简单, 并且在用户已经由接入网验证的情况中适用。因此, 根据本发明提供一种新特征、即“多媒体域的隐式验证”, 它可实现为与订户服务器密切配合或者完全集成在所述订户服务器中的专用多媒体验证装置。为此, 提供新装置、新用户设备以及新方法, 它们全部设置用于在不同网络之间或者不同技术域之间再用验证数据, 并借助于根据本标准的多媒体域的其它实体。



1. 一种用于对通过接入网 (UMTS ;WLAN ;GPRS ;CDMA 2000) 访问多媒体域 (IMS) 的用户进行多媒体验证的装置,所述装置供所述接入网的订户服务器 (HSS ;AAA) 使册或者与所述接入网的订户服务器 (HSS ;AAA) 合作,所述订户服务器保存用户的验证数据并且可访问所述多媒体域 (IMS),所述装置的特征在于包括:

用于基于接入网 (UMTS ;WLAN ;GPRS ;CDMA 2000) 对用户的先前验证判定可进行用户与多媒体域 (IMS) 之间的隐式验证、从而省略对显式验证的需要的部件;以及

用于指示负责在多媒体域 (IMS) 中验证用户的在服务实体 (S-CSCF),基于接入网对用户的先前验证可进行所述用户和所述多媒体域 (IMS) 之间的隐式验证的部件。

2. 如权利要求 1 所述的装置,其特征在于,用于判定可进行隐式验证的部件包括用于确定通过所述接入网访问多媒体域的信令路径的潜在安全性的部件。

3. 如权利要求 1 所述的装置,其特征在于,所述用于指示负责在多媒体域中验证用户的在服务实体可进行隐式验证的部件包括用于表明最终判定是在强迫显式验证的用户设备 (UE) 的部件。

4. 如权利要求 1 所述的装置,其特征在于,所述用于指示负责在多媒体域中验证用户的在服务实体可进行隐式验证的部件包括用于表明这是网络采取的最终判定并且不可执行显式验证的部件。

5. 如权利要求 1 所述的装置,其特征在于,还包括用于通知用户设备用于访问多媒体域的用户隐式验证可由网络执行的部件。

6. 如权利要求 1 所述的装置,其特征在于,所述用于基于接入网对用户的先前验证判定可进行用户与多媒体域 (IMS) 之间的隐式验证的部件包括用于接收源自用户设备 (UE) 的隐式验证的建议的部件。

7. 如权利要求 3 所述的装置,其特征在于,还包括用于接收源自用户设备 (UE) 的指示以确认网络提出的隐式验证的接受的部件。

8. 如权利要求 7 所述的装置,其特征在于,还包括用于向负责在多媒体域 (IMS) 中验证用户的在服务实体 (S-CSCF) 表明用户已经确认隐式验证的部件。

9. 如权利要求 8 所述的装置,其特征在于,还包括用于向所述在服务实体 (S-CSCF) 提供附加验证数据的部件,所述附加验证数据包括从包括以下元素的组中选取的至少一个元素:验证类型;访问信息;以及验证时标。

10. 一种用户设备 (UE),能够获得通过接入网 (UMTS ;WLAN ;GPRS ;CDMA 2000) 对多媒体域 (IMS) 的访问权,并且设置成对于接入网执行第一显式验证过程,以及对于多媒体域 (IMS) 执行第二显式验证过程,所述用户设备 (UE) 的特征在于具有用于处理从包括以下通知的组中选取的至少一个通知的部件:

从多媒体域 (IMS) 接收的、表明用户的隐式验证可由网络执行的通知;以及

从用户设备 (UE) 向多媒体域 (IMS) 建议执行所述用户设备与多媒体域之间的隐式验证的通知。

11. 如权利要求 10 所述的用户设备 (UE),其特征在于,所述用于处理从多媒体域 (IMS) 接收的、表明用户的隐式验证可由网络执行的通知的部件包括用于接收和处理最终判定是在强迫显式验证的用户设备 (UE) 上的指示的部件。

12. 如权利要求 11 所述的用户设备 (UE),其特征在于,还包括用于向多媒体域 (IMS)

发送指示以确认网络提出的隐式验证的接受的部件。

13. 如权利要求 12 所述的用户设备 (UE), 其特征在于, 还包括用于向多媒体域 (IMS) 提供附加验证数据的部件, 所述附加验证数据包括从包含以下元素的组中选取的至少一个元素: 验证类型; 访问信息; 以及验证时标。

14. 如权利要求 10 所述的用户设备 (UE), 其特征在于, 所述用于处理从多媒体域 (IMS) 接收的、表明用户的隐式验证可由网络执行的通知的部件包括用于接收和处理隐式验证是网络采取的最终判定并且不可执行显式验证的指示的部件。

15. 一种用于验证通过接入网 (UMTS ; WLAN ; GPRS ; CDMA 2000) 访问多媒体域 (IMS) 的用户的方法, 所述方法包括:

在用户通过其访问的接入网 (UMTS ; WLAN ; GPRS ; CDMA 2000) 中验证用户的步骤, 所述接入网具有包含用户的验证数据并且可访问多媒体域 (IMS) 的订户服务器 (HSS ; AAA); 以及

把用户注册到多媒体域 (IMS) 中的步骤;

所述方法的特征在于包括:

基于接入网 (UMTS ; WLAN ; GPRS ; CDMA 2000) 中对用户的先前验证判定可进行用户与多媒体域 (IMS) 之间的隐式验证、从而省略对显式验证的需要的步骤; 以及

指示负责在多媒体域 (IMS) 中验证用户的在服务实体 (S-CSCF) 可进行隐式验证的步骤。

16. 如权利要求 15 所述的方法, 其特征在于, 还包括从多媒体域 (IMS) 向用户设备 (UE) 通知可执行用于访问多媒体域的用户隐式验证的步骤。

17. 如权利要求 15 所述的方法, 其特征在于, 所述基于接入网中对用户的先前验证判定可进行用户和多媒体域之间的隐式验证的步骤包括确定通过所述接入网访问多媒体域的信令路径的潜在安全性的步骤。

18. 如权利要求 15 所述的方法, 其特征在于, 所述基于接入网中对用户的先前验证判定可进行用户和多媒体域之间的隐式验证的步骤包括从用户设备 (UE) 向多媒体域 (IMS) 建议在所述用户设备与多媒体域之间执行的隐式验证的步骤。

19. 如权利要求 15 所述的方法, 其特征在于, 所述指示负责在多媒体域中验证用户的在服务实体可进行隐式验证的步骤包括表明这是网络采取的最终判定并且不可执行显式验证的步骤。

20. 如权利要求 15 所述的方法, 其特征在于, 所述指示负责在多媒体域中验证用户的在服务实体可进行隐式验证的步骤包括表明最终判定是在强迫显式验证的用户设备上的步骤。

21. 如权利要求 20 所述的方法, 其特征在于, 还包括从用户设备 (UE) 确认网络提出的隐式验证的接受的步骤。

22. 如权利要求 21 所述的方法, 其特征在于, 还包括向负责在多媒体域 (IMS) 中验证用户的在服务实体 (S-CSCF) 表明用户已经确认隐式验证的步骤。

23. 一种当用户通过先前已经验证所述用户的接入网 (UMTS ; WLAN ; GPRS ; CDMA 2000) 访问多媒体域 (IMS) 时、负责在所述多媒体域 (IMS) 中验证用户的在服务实体 (S-CSCF), 所述在服务实体 (S-CSCF) 的特征在于包括:

用于接收和处理源自权利要求 1 的装置的基于接入网 (UMTS ;WLAN ;GPRS ;CDMA 2000) 对用户的先前验证表明可进行隐式验证的指示的部件 ;以及

用于向用户设备 (UE) 通知用于访问多媒体域 (IMS) 的用户的隐式验证可由网络执行的部件。

24. 如权利要求 23 所述的在服务实体 (S-CSCF), 其特征在于, 还包括用于接收源自所述用户设备 (UE) 的指示以确认网络提出的隐式验证的接受的部件。

25. 如权利要求 23 所述的在服务实体 (S-CSCF), 其特征在于, 还包括用于接收源自权利要求 8 的装置的表明用户已经确认隐式验证的指示的部件。

26. 如权利要求 25 所述的在服务实体 (S-CSCF), 其特征在于, 还包括用于检查分别从权利要求 9 的装置和权利要求 13 的用户设备接收的附加验证数据的匹配、以便提供额外安全性支持的部件。

27. 如权利要求 26 所述的在服务实体 (S-CSCF), 其特征在于, 所述附加验证数据包括从包含以下元素的组中选取的至少一个元素 :验证类型 ;访问信息 ;以及验证时标。

28. 如权利要求 23 所述的在服务实体 (S-CSCF), 其特征在于, 所述用于向用户设备 (UE) 通知用于访问多媒体域的用户的隐式验证可由网络执行的部件包括用于向用户设备 (UE) 表明隐式验证是网络采取的最终判定并且不可执行显式验证的部件。

29. 一种用作用户通过先前已经验证所述用户的接入网 (UMTS ;WLAN ;GPRS ;CDMA 2000) 访问的多媒体域 (IMS) 的入口点的代理实体 (P-CSCF), 其特征在于具有用于处理从包含以下通知的组中选取的至少一个通知的部件 :

向用户设备 (UE) 发送的、表明用于访问多媒体域 (IMS) 的用户的隐式验证可由网络执行的通知 ;以及

从用户设备 (UE) 接收的向多媒体域 (IMS) 建议所述用户设备与多媒体域之间的隐式验证的通知。

30. 如权利要求 29 所述的代理实体 (P-CSCF), 其特征在于, 还包括用于从用户设备 (UE) 接收接受网络提出的隐式验证的指示的部件。

31. 如权利要求 29 所述的代理实体 (P-CSCF), 其特征在于, 还包括用于向用户设备 (UE) 表明隐式验证是网络采取的最终判定并且不可执行显式验证的部件。

32. 一种在多媒体域 (IMS) 中关于已经通过接入网 (WLAN ;GPRS) 访问所述多媒体域的用户查询订户服务器 (HSS ;AAA-3GPP) 的询问实体 (I-CSCF), 所述询问实体具有用于从用户设备 (UE) 接收注册请求的部件以及用于向用户设备确认这种注册的部件, 其特征在于包括 :

用于向用户设备 (UE) 传送用于访问多媒体域 (IMS) 的用户的隐式验证可执行的指示的部件 ;

用于接收源自用户设备 (UE) 以使所述隐式验证能够进行的指示的部件 ;以及

用于从用户设备向从包括权利要求 1 的装置和权利要求 23 的在服务实体 (S-CSCF) 的实体组中选取的至少一个实体传送这种指示的部件。

33. 如权利要求 32 所述的询问实体 (I-CSCF), 其特征在于, 还包括用于向用户设备 (UE) 传送隐式验证是网络采取的最终判定并且不可执行显式验证的指示的部件。

用于在访问多媒体服务时验证用户的设备及方法

[0001] 发明领域

[0002] [0001] 本发明涉及用于验证通过在其中用户已经被验证的接入网来访问多媒体网络的用户的简化程序。

[0003] 背景

[0004] [0002] 许多当前存在的移动网以及由标准化团体定义的可能的未来网络要求终端用户和用户代理在访问网络时,更合适地说,在访问与网络关联的服务时验证其自身。在这方面,如 3GPP 和 3GPP2 标准所定义的 GSM、GPRS、无线局域网 (WLAN) 和多媒体 (IMS) 域都要求用户的设备或终端被设置成在允许用户或用户代理对所述域进行访问之前运行各具体技术域特定的验证程序。特别是,上述技术域以及其它新兴的技术域要求不同的安全等级,使得贯穿不同技术域的访问更为复杂。这种访问贯穿意味着不一定始终需要的额外安全性,因而意味着额外的处理和信令能力以及用户设备或终端中的额外复杂度。

[0005] [0003] 目前,3GPP 多媒体域中的验证过程按照 3G TS 33.203 标准所述以及图 1 中所示、根据基于会话发起协议 (SIP) 的信令流来执行。如图 1 所示以及引用的技术规范所述,总是当用户在多媒体域中注册时会执行多媒体验证,通常是通过发送给定保密和公开身份的 SIP Register (SIP 注册) 消息开始。

[0006] [0004] 在开始以上所述流程之前假定的初始条件是,终端用户必须在访问多媒体域之前让数据连接开通。这个连接依据激活了 PDP 上下文可能是 GPRS 连接,或者依据如 IEEE 802.11 标准规定的建立了数据连接可能是 WLAN 连接,或者另一个接入网为用户侧提供数据连接。在这种情况下,终端用户或用户代理已经通过无论是 GPRS 或 WLAN 还是另一个的接入网验证,以便建立这种数据连接并且在向多媒体域发送 SIP Register 之前。

[0007] [0005] 具体来说,当前使用的接入网、即 GPRS 以及 WLAN 提供各自的验证机制,即用于 GPRS 的 SIM/USIM-AKA 以及用于 WLAN 的 EAP-SIM/AKA,而多媒体域当前利用提供与上述接入网类似的安全等级的验证机制,即所谓的 USIM-AKA,它在 SIP Register 消息到达在服务呼叫状态控制功能 (S-CSCF) 实体时被执行,如图 1 所示。在这方面,图 2 说明对于已经访问其中 RADIUS 和 MAP 似乎是最可能的协议备选方案、但是 DIAMETER 也可用于取代 RADIUS 或 MAP 的 WLAN 网络的用户执行 EAP AKA 验证要遵从的动作序列。

[0008] [0006] 目前,希望得到多媒体域的访问权的用户需要预先建立数据连接,这常通过诸如 GPRS 或 WLAN 之类的接入网来执行,因此,首先采用 WLAN 接入网的 EAP-SIM/AKA 验证用户,其次在用户注册到多媒体域时应当采用 USIM-AKA 对其进一步验证。

[0009] [0007] 可以推断,目前没有在诸如 GPRS 或 WLAN 之类的接入网与基于 SIP 的多媒体域之间对给定用户执行跨域验证的验证机制。换言之,不存在能够代表用户或 SIP 用户代理来管理验证数据、并且一旦在用户通过其进行访问的接入网中已经发生验证时、使所述用户或 SIP 用户代理无需在多媒体域中执行验证操作的现有服务或装置,所述接入网可能是 GPRS 或 WLAN。

[0010] [0008] 在这种情况下,如 3G TS 33.203 所述及图 1 所示的多媒体域的验证在无线电路径中添加额外信令,这在一些情况下可能不必要。首先,在 SIP

Register 由 S-SCSF 接收后, S-SCSF 通常向 SIP 用户代理发送 Authentication Challenge(验证查询)消息。如果这个操作成功,则 S-SCSF 将定期向 SIP 用户代理发送 Authentication-Vector-request(验证向量请求), SIP 用户代理又必须以 Authentication-Vector-response(验证向量响应)进行响应。这两种消息对多媒体域增加额外负荷以及更长的注册时间。也就是说, SIP 用户代理应当处理及响应 Authentication-Challenge 和 Authentication-Vector-request。这些消息要求 SIP 用户代理进行的额外处理,这意味着 SIP 用户代理必须利用这个过程的功率而不是利用像可能具有高功耗性质的多媒体服务那么多的功率,并且记住电池的有限电力。

[0011] [0009] 因此,本发明的目的在于提供在接入网域与多媒体域之间为给定用户执行跨域验证的域间验证机制,这种域间验证机制比现有机制简单,并且在用户验证已经由接入网执行的情况中适用。发明内容

[0012] [0010] 根据本发明,通过提供全部设置用于在不同网络之间或者在不同技术域之间再用验证数据的权利要求 1 的装置、权利要求 10 的用户设备以及权利要求 15 的方法,并且借助于均为根据 3GPP 和 3GPP2 标准的多媒体域的实体的权利要求 23 的负责在多媒体域中验证用户的在服务实体以及权利要求 29 的代理实体和权利要求 32 的询问实体,来实现上述目的。因此,根据本发明提供一种新特征,以下称作“多媒体域的隐式验证”,它可实现为与订户服务器密切配合或者完全集成在所述订户服务器中的专用多媒体验证装置。所述订户服务器是在订户验证过程中涉及的订户数据库,例如归属订户服务器(HSS)或者验证-授权-记帐(AAA)服务器,以及多媒体验证装置具有必要的逻辑和组件,以便允许诸如无线局域网(WLAN)、通用分组无线电系统(GPRS)网络、通用移动通信系统(UMTS)或者码分多址(CDMA2000)网络之类的接入网与所述多媒体域之间的验证数据的再用。

[0013] [0011] 根据本发明对于通过接入网访问多媒体域的用户的多媒体验证是有用的装置被设置成在保存用户的验证数据并且可由多媒体域访问的接入网的订户服务器中使用或者与其配合。所述装置包括:用于判定用户或者准确地说是用户设备与多媒体域之间的隐式验证可进行的部件;以及用于指示负责在多媒体域中验证用户的在服务实体可进行隐式验证。这种装置的使用因而省略对于显式验证的需要。

[0014] [0012] 在这种装置中,用于判定可进行隐式验证的部件最好是包括用于确定通过所述接入网访问多媒体域的信令路径的潜在安全性的部件。为此,装置可能还包括设置成评估不同信令路径的安全性的提供和配置数据部件。此外,用于判定可进行隐式验证的部件可包括用于处理源自用户设备的隐式验证的建议的部件。

[0015] [0013] 装置有利地设置成确定隐式验证是否只是对可能强迫显式验证的用户设备的建议,或者是网络采取的最终决定,使得不可执行显式验证。因此,用于指示在服务实体可进行隐式验证的部件包括用于表明最终判定是在用户设备上的部件以及用于表明这是由网络采取的最终判定的部件。

[0016] [0014] 在这个方面,装置还包括用于通知用户访问多媒体域的用户的多媒体验证可由网络执行的部件。然而,这种通知部件也可能驻留在多媒体域的其他实体中。

[0017] [0015] 此外,假定对于是否执行隐式验证的最终判定根据本发明可在用户设备侧,所述装置还包括用于接收源自用户设备侧的指示以便确认网络提出的隐式验证的接受的部件。在接收这种接受确认的情况中,装置还包括用于向负责在多媒体域中验证用户的

在服务实体表明用户设备已经确认隐式验证的部件。装置还可具有用于向所述在服务实体提供附加验证数据的部件,所述附加验证数据包括从包括以下各项的元素组中选取的至少一个元素:验证类型;访问信息;以及验证时标。

[0018] [0016] 按照传统方式,使用户设备能够得到通过接入网对多媒体域的访问权,因而设置成对于接入网执行第一显式验证过程以及对于多媒体域执行第二显式验证过程。接入网包括订户服务器以便保存用户的验证数据,以及为了本发明,所述订户服务器是多媒体域可访问的。根据本发明,用户设备包括用于处理从包括以下各项的通知的组中选取的至少一个通知的部件:来自多媒体域的通知,表明可执行用户的隐式验证;以及送往多媒体域的通知,表明用户设备向网络建议隐式验证。

[0019] [0017] 这种部件可有利地包括用于从多媒体域接收最终判定在可能强迫显式验证的用户设备侧或者它是网络采取的最终判定的指示、使得不可执行显式验证的部件。特别是设置用于最终判定在用户侧的情况,用户设备还包括用于向多媒体域发送确认网络所提出的隐式验证的接受的指示的部件。此外,用户设备可具有用于向多媒体域提供附加验证数据的部件,所述附加验证数据包括从包括以下各项的元素组中选取的至少一个元素:验证类型;访问信息;以及验证时标。

[0020] [0018] 还提供一种用于在多媒体域中当用户通过接入网对其访问时验证用户的方法,该方法传统上包括:在接入网中验证用户的步骤,所述接入网具有包含用户的验证数据并且是多媒体域可访问的订户服务器;以及把用户注册到多媒体域中的步骤。

[0021] [0019] 根据本发明,这种方法还包括:

[0022] - 判定用户与多媒体域之间的隐式验证可进行、因而省略对显式验证的需要的步骤;以及

[0023] - 指示负责在多媒体域中验证用户的在服务实体可进行隐式验证的步骤。

[0024] [0020] 这种方法还可包括从多媒体域向用户设备通知访问多媒体域的用户隐式验证可被执行的步骤。

[0025] [0021] 在这种方法中,判定可进行隐式验证的步骤最好是包括确定通过所述接入网访问多媒体域的信令路径的潜在安全性的步骤。此外,判定可进行隐式验证的上述步骤还可包括从用户设备向多媒体域建议要在所述用户设备与多媒体域之间执行隐式验证的步骤。

[0026] [0022] 另外在这种方法中,指示在服务实体可进行隐式验证的步骤最好是包括表明最终判定是在可能强迫显式验证的用户设备上还是最终判定由网络采取、使得不可执行显式验证的步骤。另外,特别是对于最终判定在用户侧的情况,该方法还可包括从用户设备确认网络所提出的隐式验证的接受的步骤。此外并且与上述步骤结合,该方法还可包括向负责在多媒体域中验证用户的在服务实体表明用户已经确认隐式验证的步骤。

[0027] [0023] 本发明还提供负责在多媒体域中当用户通过先前已经验证所述用户的接入网对多媒体域访问时验证用户设备的在服务实体。根据本发明,这种在服务实体包括:用于从上述装置接收表明可进行隐式验证的指示的部件;以及用于通知用户设备访问多媒体域的用户隐式验证可由网络来执行的部件。

[0028] [0024] 这种在服务实体有利地以下列方式设置:用于通知用户隐式验证可由网络来执行的部件包括用于向用户表明隐式验证是否是网络采取的最终判定并且不可执行

显式验证、或者隐式验证是来自网络的、用户可能接受或者通过强迫显式验证拒绝的建议的部件。

[0029] [0025] 在隐式验证是网络的建议的情况中,在服务实体有利地包括用于接收源自用户设备、确认网络提出的这种隐式验证的接受的指示的部件。此外,这种在服务实体最好是包括用于从上述装置接收用户已经确认隐式验证的这种指示的部件。

[0030] [0026] 这种在服务实体可有利地包括用于检查分别从上述装置和用户设备接收的附加验证数据的匹配、以便提供额外安全性支持的其它部件。这些附加验证数据包括包含以下各项的元素组中的至少一个元素:验证类型;访问信息;以及验证时标。

[0031] [0027] 本发明还通过提供其它一些实体、如代理和询问实体以便针对遵循 3GPP 或 3GPP2 标准的典型拓扑来补充。

[0032] [0028] 根据 3GPP 和 3GPP2 标准,代理实体意在用作用户通过已经对用户进行验证的接入网访问的多媒体域的入口点。根据本发明,这种代理实体包括用于处理从包括以下各项的通知的组中选取的至少一个通知的部件:

[0033] - 向用户设备发送以表明访问多媒体域的用户隐式验证可由网络来执行的通知;以及

[0034] - 从用户设备接收以向多媒体域提出所述用户设备与多媒体域之间的隐式验证的通知。

[0035] [0029] 这种代理实体还经过有利地设置,使得用于通知用户隐式验证可由网络来执行的部件包括用于向用户表明隐式验证是网络采取的最终判定并且不可执行显式验证、还是隐式验证是来自网络的用户可能接受或者通过强迫显式验证拒绝的建议的部件。

[0036] [0030] 在隐式验证是网络建议的情况中,代理实体有利地包括用于从用户设备接收接受网络提出的这种隐式验证的指示的部件。

[0037] [0031] 根据 3GPP 和 3GPP2 标准,询问实体用来查询多媒体域中的订户服务器关于用户已经通过另一个接入网访问所述多媒体域。这种询问实体包括:用于从用户接收注册请求的部件;以及用于向用户确认这种注册的部件,以及根据本发明,询问实体还包括用于向用户设备传送访问多媒体域的用户隐式验证可被执行的指示的部件。

[0038] [0032] 为了实现本发明提供的其它有利特征,询问实体最好是包括:用于接收源自用户设备的、确认网络提出的隐式验证的接受或者其本身提出这种隐式验证的指示的部件;以及用于向从包括上述装置和在服务实体的实体组中选取的至少一个实体传送用户接受的这种确认的部件。

[0039] [0033] 此外以及为了实现本发明提供的其它有利特征,询问实体还包括用于向用户设备传送隐式验证是网络采取的最终判定并且不可执行显式验证的指示的部件。

[0040] 附图概述

[0041] [0034] 通过结合附图阅读本说明,本发明的特征、目的和优点将变得明显,其中:

[0042] [0035] 图 1 说明根据 3GPP TS 33.203 在多媒体域中的验证流程的基本示意图。

[0043] [0036] 图 2 说明在通过 WLAN 接入网、遵循 EAP-AKA 机制的用户的验证过程中的体系结构组件和信令流的概览。

[0044] [0037] 图 3 说明流序列,描述用于再用已经通过 GPRS 或 UMTS 网络访问多媒体

域的用户的先前验证的当前优选实施例,其中,用户设备接收这方面的通知并被提供接受或不接受隐式验证的可能性。

[0045] [0038] 图 4 说明流序列,描述图 3 所示实施例的备选实施例,在其中,用户设备接收这方面的通知,并且没有被提供接受或不接受隐式验证的可能性,而是收到关于已经发生这种隐式验证的通知。

[0046] [0039] 图 5 说明备选流序列,描述图 3 和图 4 所示实施例的备选实施例,在其中,用户设备在定位过程中接收对多媒体域进一步执行隐式验证的邀请,因而对用户接受或不接受隐式验证的可能性。

[0047] [0040] 图 6 说明对图 5 所示实施例的备选流序列,在其中,用户设备通过短消息业务 (SMS) 接收对多媒体域进一步执行隐式验证的邀请,因而对用户接受或不接受隐式验证的可能性。

[0048] [0041] 图 7 说明流序列,描述用于再用已经通过 WLAN 网络访问多媒体域的用户先前验证的当前优选实施例,在其中,用户设备接收这方面的通知并被提供接受或不接受隐式验证的可能性。

[0049] [0042] 图 8 说明流序列,描述用于由 CDMA 2000 网络再用用户的先前验证的另一个优选实施例,用户通过分组数据业务网络访问多媒体域,在其中,用户设备接收这方面的通知并被提供接受或不接受隐式验证的可能性。

[0050] [0043] 图 9 说明对图 5 和图 6 所示的那些实施例的备选流序列,在其中,用户设备不分别通过 Update Location Answer (更新位置应答) 消息或者通过短消息业务 (SMS) 接收邀请以便进一步执行隐式验证,而是用户设备向网络产生隐式验证的建议。

[0051] 优选实施例的详细说明

[0052] [0044] 下面描述用于为用户提供在通过已经对用户进行验证的接入网进行访问时由多媒体域隐式验证的可能性的设备、用户设备及方法的当前优选实施例。接入网最好是无线局域网 (WLAN)、通用分组无线电系统 (GPRS) 网络、全球移动通信系统 (GSM) 网络、通用移动通信系统 (UMTS) 网络或者码分多址网络 (CDMA 2000)。

[0053] [0045] 本发明提供与具体可由密切配合订户服务器的独立装置来执行或者由订户服务器本身来执行的特征“多媒体域的隐式验证”驻留的位置有关的若干方面。

[0054] [0046] 此外,本发明还提供与用户设备、即用户终端或 SIM 或 USIM 或者其组合有关的若干方面,取决于判定度是保留在用户侧还是保留在网络侧。

[0055] [0047] 根据本发明的第一方面,具体可能是 3GPP 中的 HSS 或者 3GPP2 标准和 CDMA 2000 网络中的 AAA 服务器的订户服务器本身或者为特定用户支持对多媒体域的访问的多媒体验证装置根据用户通过其中进行访问的接入网所执行的先前订户验证,以及根据多媒体信令的安全承载通过接入网来执行的假设,来确定多媒体域的显式验证可能是不必要的。这种安全承载可能是例如在执行订户验证时 GPRS 作为接入网的情况中的 PDP 上下文或者 WLAN 作为对于归属网络的接入网的情况中的安全隧道。

[0056] [0048] 根据本发明,订户服务器或者专用多媒体验证装置向负责验证用户的在服务实体、即在服务呼叫状态控制功能 (S-CSCF) 提供表明可根据通过接入网的先前承载验证对访问多媒体域的所述用户执行隐式验证过程的验证策略。

[0057] [0049] 除了由用户正访问的网络对用户进行验证之外,3GPP 验证过程还支持由

用户对网络的验证。因此,根据本发明的另一个方面,订户服务器或专用多媒体验证装置能够可选地向用户设备表明另一个验证策略,以便建议用户可能或者可能不接受的一种可能的相互隐式验证。

[0058] [0050] 由于“多媒体域的隐式验证”特征,减少了由用户或者由用户设备以及由网络执行的验证操作的量,因而实现多媒体域中的可避免信令消息的减少,同时保持所需安全等级,从而实现本发明的一个目的。

[0059] [0051] 本发明适用于不同情况,在其中,用户利用特定的接入网来访问多媒体域,从而产生本发明的不同实施例。另外,可从一个实施例到另一个实施例引入若干变更,而没有实质上背离本发明的范围。

[0060] [0052] 出现第一种情况,其中,用户由 UMTS 网络进行了验证,并且还通过 GPRS 网络访问多媒体域。

[0061] [0053] 在这种情况下,根据图 3 所示的本发明的第一实施例,提供一种用于在多媒体域中验证用户的简化机制,其中,通知用户关于可能的隐式验证。用户、确切地说是用户设备侧 (UE) 在收到这个通知时可能接受隐式验证,或者根据多媒体域的适用标准强迫显式验证,如图 1 所示。此外,这种隐式验证可适用于由网络对用户的验证以及由用户对网络的验证。另外,所述隐式验证可能如图 3 所示由订户服务器、如负责 UMTS 网络中的用户的先前验证的归属用户服务器 (HSS) 来触发,或者由与所述订户服务器配合工作的专用多媒体验证装置来触发。

[0062] [0054] 因此,根据图 3 所示的这个第一实施例,终端用户或用户设备在 UMTS 中被附加并验证,并且让 GPRS PDP 上下文开通。在这个阶段,终端用户和用户代理通过发起 SIP 注册过程得到对多媒体域的访问权。

[0063] [0055] 这个 SIP 注册过程包括从用户侧 (UE) 向代理呼叫状态控制功能 (P-CSCF) 以及从这个实体向询问呼叫状态控制功能 (I-CSCF) 发送 SIP Register 消息。I-CSCF 对归属订户服务器 (HSS) 发起通常所说的 Cx-Selection-Info (Cx 选择信息) 过程,以便识别当前负责用户的在服务呼叫状态控制功能 (S-CSCF)。一旦识别了这种 S-CSCF, I-CSCF 向 S-CSCF 发送相应的 SIP Register 消息。接收这种注册消息的 S-CSCF 对归属订户服务器 (HSS) 发起通常所说的 Cx-Put 过程。

[0064] [0056] 假定 HSS 先前已经通过与在服务 GPRS 支持节点 (SGSN) 交换了用户简档和验证向量来参与用户的 GPRS 接入验证,则 HSS 除了其它网络拓扑信息之外还采用它的关于订户所在的 SGSN 的信息,来确定通过所述接入网访问多媒体域的信令路径的潜在安全性。因此,根据本发明, HSS 本身或者专用多媒体验证装置可为用户决定隐式验证。为此, HSS 在对 S-CSCF 的 Cx-Put-response 中包括“隐式验证”的指示。

[0065] [0057] 当网关 GPRS 支持节点 (GGSN) 属于与 HSS 相同的归属域并且 GGSN 因而被认为是安全及可信的时,有利地作出向 S-CSCF 发送这个消息的决定。一种特别适合的情况是当 HSS 也信任订户所在的 SGSN 时,因为例如它们两者都属于相同的网络运营商,并且与是否为用户提供进一步拒绝所建议的隐式验证的可能性无关。

[0066] [0058] 另外,特征“多媒体域的隐式验证”可包括基于订户的数据提供和数据配置,使得当用户让这种服务提供并且用户是可信的时, HSS 本身或者专用多媒体验证装置可为该用户确定隐式验证。在这个方面以及考虑到可能在多媒体域中为特定用户提供多个用

户标识符,以下涉及并在不同实施例中描述的隐式验证可应用于多媒体域中的全部或者特定的用户标识符。

[0067] [0059] 另外,其它相关信息也可在 Cx-Put-response 消息中向 S-CSCF 发送,诸如验证类型、例如 IP 地址和联络信息之类的访问信息、验证时标以及其它重要数据,以便提供额外的安全性支持。

[0068] [0060] 因此,对于上述的本发明的一个方面,可通知用户关于网络提出的、用于让用户接受或不接受的隐式验证。因此,S-CSCF 以即时规定向 SIP 用户代理发送称作“SIP 4xx 隐式验证”的新 SIP 消息,使得 SIP 用户代理在发现可接受时内部禁用传统上被执行的显式多媒体验证过程。也就是说,SIP 用户代理不会等待或预计接收 3G TS 33.203 中所述的 Authentication-Challenge 消息或者验证向量。此外,SIP 用户代理或者更一般地说是用户设备将认为支持多媒体域的网络经过隐式验证。另一方面,SIP 用户代理可能认为隐式验证是不可接受的,在这种情况下,在任何附图中均未示出的适当否定确认被发送给网络,以便根据上述适用标准强迫传统的显式验证机制。

[0069] [0061] 仍然参照图 3,一旦 SIP 用户代理已经接受隐式验证,则采用新的 SIPRegister 消息来响应这个消息。

[0070] [0062] 在这个阶段,大家可能知道,由于根据本发明、通过对来自置信接入网的多媒体域验证数据进行再用所执行的隐式验证,本发明还提供一种有利的解决方案来支持在访问所述多媒体域之前已经由接入网验证的用户在多媒体域的单次登录 (SSO)。

[0071] [0063] 与这个有利的解决方案配合,图 3 说明最终从用户设备的 SIP 用户代理发送到 S-CSCF 的 SIP Register 包括“SSO 使能”的指示,用于向网络表明隐式验证被接受。网络向 S-CSCF 提交这种 SIPRegister 消息,S-CSCF 又向用户设备回送成功结果“SIP 200 OK”。终端用户这时注册到多媒体域,而没有按照传统方式在终端用户的多媒体注册中出现那些额外定期验证过程。

[0072] [0064] 一般来说,对于这个实施例并且也适用于进一步描述的其它实施例,以及只要存在来自用户设备关于隐式验证的通知,在服务实体 (S-CSCF) 可能还检查分别包含在 SIP Register 以及 Cx-Put-response 中的其它相关数据是否与隐式验证和单次登录访问一致。所述相关数据可能是例如验证类型、如 IP 地址和联络信息之类的访问信息、验证时标或者它们的组合以及其它重要数据,以便提供额外的安全性支持。

[0073] [0065] 仍然在用户已经由 UMTS 网络进行验证并且进一步通过 GPRS 网络访问多媒体域的上述情况下,以及根据图 4 所示的第二实施例,提供一种用于在多媒体域中验证用户的更简化机制,其中,只是通知用户由网络采取的执行隐式验证的决定。在这个第二实施例中,用户附加到 UMTS 网络,并且在其中被验证,其中有归属订户服务器 (HSS) 的参与,PDP 上下文采用 GPRS 实体 (SGSN、GGSN) 来激活,以及 SIP Register 消息被发送给呼叫状态控制功能 (P-CSCF、I-CSCF、S-CSCF) 实体,以便以第一实施例中进行的相似方式注册到多媒体域中。第一和第二实施例之间的差别在于,HSS 本身或者专用多媒体验证装置作出为用户执行隐式验证的最终决定。为此,HSS 在对 S-CSCF 的 Cx-Put-response 中包括“由网络进行的隐式验证”的指示。

[0074] [0066] 然后,在已经完成 S-CSCF 与 HSS 之间的“Cx-Pull-process”之后,并且没有请求用户的接受,S-CSCF 通过在特定的“SIP2xx OK”响应中包括指示“由网络进行的

隐式验证”而不是采用上述新的“SIP 4xx”消息,来通知用户网络已经主动执行隐式验证。

[0075] [0067] 在收到带有指示“由网络进行的隐式验证”的所述“SIP2xx OK”响应时,SIP 用户代理不会等待或预计接收 3G TS 33.203 中所述的 Authentication-Challenge 消息或者验证向量。此外,SIP 用户代理或者更一般地说是用户设备可能认为支持多媒体域的网络经过隐式验证,只要用户设备配置成执行网络的这种验证。

[0076] [0068] 终端用户这时注册到多媒体域,而没有按照传统方式在终端用户的多媒体注册中出现的那些额外定期验证过程,并且具有比第一实施例所述的更简单的机制。

[0077] [0069] 出现第二种情况,在其中,在 GSM 附加以及位置更新过程之后,用户由 UMTS 网络进行了验证,并且还通过 GPRS 网络访问多媒体域。在这个方面,并且为了清楚起见,UMTS 网络的归属订户服务器 (HSS) 包括所有基本功能性,并且用作 GSM 网络的传统归属位置寄存器 (HLR),再加上用作多媒体域中的订户服务器所需的所有功能性。然而,如果传统 HLR 功能性驻留在与多媒体域的订户服务器不同的实体中,则两种实体、即 GSM HLR 与多媒体域的订户服务器之间的附加接口用来共享用户验证数据。

[0078] [0070] 图 5 中说明在上述第二种情况下的第三实施例,其中,新的字段在 GSM 附加和位置更新过程中返回给用户设备的 SIP 用户代理。因此,多媒体域的订户服务器 (HSS) 在对于接入网中的在服务 GPRS 支持节点 (SGSN) 的 GSM 操作“插入订户数据”中包含“隐式验证”的指示。然后,SGSN 还在对 SIP 用户代理的 GSM 操作“更新位置应答”中包含“隐式验证”的这个指示。

[0079] [0071] 这个指示可应用于多媒体域中的所有或特定用户标识符,并且被用户设备 (UE) 理解为用户设备可能或者可能不接受的启用对多媒体域的单次登录 (SSO) 访问的隐式邀请。只要隐式验证由于不需要额外安全性而对于终端用户 (UE) 是可接受的,则 SIP Register 消息发送到多媒体域 (P-CSCF、I-CSCF),SIP Register 消息包括用于向网络表明隐式验证被接受的“SSO 使能”的指示。

[0080] [0072] 在询问呼叫状态控制功能 (I-CSCF) 实体中收到这种 SIPRegister 消息时,“SSO 使能”的指示被加入采用多媒体域订户服务器 (HSS) 所保存的所谓“Cx-Selection-Info”过程中包含的“Cx-Query”消息的新字段。这时,HSS 本身中或者专用多媒体验证装置中的特征“多媒体域的隐式验证”处理“SSO 使能”的指示,以便在请求时进一步提供用户的验证数据。

[0081] [0073] “SSO 使能”的指示还被加入从 I-CSCF 向当前选择用于为用户提供服务的在服务呼叫状态控制功能 (S-CSCF) 实体发送的 SIP Register。如在前面的实施例中那样,图 5 所示的本实施例也说明从 S-CSCF 对 HSS 所执行的“Cx-Put”操作。因此,HSS 采用“Cx-Put-response”操作来指示 S-CSCF,其中包括“隐式验证由用户确认”的指示,以便排除终端用户的进一步验证以及避免为所述终端用户发送验证向量。S-CSCF 又可能还检查 SIP Register 中以及 Cx-Put-response 中分别包含的其它相关数据是否与隐式验证和单次登录访问一致,相关数据例如包括验证类型、如 IP 地址和联络信息之类的访问信息、验证时标或者其组合以及其它重要数据,以便提供额外的安全性支持。

[0082] [0074] 最后,在已经结束 S-CSCF 与订户服务器 (HSS) 之间的“Cx-Pull-process”之后,S-CSCF 向用户返回对于用户设备的 SIP 用户代理的传统成功结果“SIP 200OK”。

[0083] [0075] 图6说明在上述第二种情况下的第四实施例,其中,与图5所示的先前第三实施例的唯一差别在于,“隐式验证”的指示以从短消息服务中心(SMSC)发送的短消息返回给用户设备的SIP用户代理,如先前由订户服务器(HSS)本身或者由专用多媒体验证装置所指示的那样,以及一旦GSM附加和验证过程结束,而不是在位置更新过程中进行。在附图中为清楚起见,图5中的GPRS实体对SGSN和GGSN在图6中用所谓的“GSN”实体来代替。对于上述实施例,“隐式验证”的这种指示也可应用于多媒体域中的所有或特定用户标识符。一旦用户设备知道已经接收“隐式验证”的这个指示,并且只要发现这种隐式验证是可接受的,则用户设备处理该消息,并且在被发送以访问多媒体域(P-CSCF、I-CSCF)的SIP Register消息中包括“SSO使能”的指示,“SSO使能”的指示用于向网络表明隐式验证被用户设备接受。从这一点开始,信令流可与先前的第三实施例中相同。

[0084] [0076] 同样在这个第二种情况下的实施例中,终端用户注册到多媒体域,而没有按照传统方式在终端用户的多媒体注册中出现的那些额外定期验证过程,并且具有比按照传统方法所执行的更简单的机制。

[0085] [0077] 出现第三种情况,在其中,通过无线局域网进行访问的用户由UMTS网络进行了验证,并且还通过这个无线局域网(WLAN)访问多媒体域。

[0086] [0078] 根据图7所示的第五实施例,在这个第三种情况下,终端用户在WLAN中附加并由UMTS网络进行验证,终端用户、确切地说是用户设备(UE)已经最好是通过利用到归属网络的通常所说的安全隧道使IP会话开通。这种安全隧道最好是通过在加密消息净荷中封装来自上述IP会话的数据、一般为IP地址,在用户设备与分组数据网关(PD-GW)之间建立,同时没有与IP会话相关的外部IP地址用于用户设备(UE)与分组数据网关(PD-GW)之间。

[0087] [0079] 这时,通过与图3所示的第一实施例相似的方式,图7中的信令流说明终端用户和SIP用户代理、即用户设备(UE)如何通过从用户例(UE)向多媒体域(P-CSCF、I-CSCF)发送SIP Register消息来获得对多媒体域的访问权。

[0088] [0080] 询问呼叫状态控制功能(I-CSCF)实体对归属订户服务器(HSS)、即多媒体域中的订户服务器发起通常所说的“Cx-Selection-Info”过程,以便识别当前负责用户的在服务呼叫状态控制功能(S-CSCF)。一旦识别了这种S-CSCF,I-CSCF向S-CSCF发送相应的SIP Register消息。接收这种注册消息的S-CSCF对归属订户服务器(HSS)发起通常所说的Cx-Put过程。

[0089] [0081] 假定HSS先前已经通过与符合3GPP标准的所谓“验证、授权和记帐”服务器(以下称作AAA-3GPP)交换用户简档和验证向量来参与用于WLAN访问的用户的验证,如图2所示,则HSS除了其它网络拓扑信息之外还采用它的关于安全隧道的信息,来确定通过所述接入网访问多媒体域的信令路径的潜在安全性。因此,根据本发明,HSS本身或者专用多媒体验证装置可为所述用户决定隐式验证。当分组数据网关(PD-GW)属于与HSS相同的归属域时,或者在PD-GW被认为安全且可信的其它情况中,有利地作出这种决定。此外,如前面的实施例中那样,特征“多媒体域的隐式验证”可包括基于订户的数据提供和数据配置,使得当用户让这种服务提供并且用户是可信的时,HSS本身或者专用多媒体验证装置可为该用户确定隐式验证。

[0090] [0082] 因此,HSS在对S-CSCF的“Cx-Put-response”中加入“隐式验证”的指

示。有利地并且为了安全起见,其它相关信息也可在“Cx-Put-response 消息”中向 S-CSCF 发送,例如验证类型、如 IP 地址和联络信息之类的访问信息、验证时标以及其它重要数据,以便提供额外的安全性支持。

[0091] [0083] 图 7 中的这个第五实施例与图 3 的第一实施例一致,并且这两个实施例均按照上述本发明的一个方面,其中,可通知用户关于网络提出的、用于让用户接受或不接受的隐式验证。

[0092] [0084] 因此, S-CSCF 以即时规定向 SIP 用户代理发送称作“SIP4xx 隐式验证”的新 SIP 消息,使得 SIP 用户代理在发现可接受时内部禁用在传统上被执行的显式多媒体验证过程。也就是说, SIP 用户代理不会等待或预计接收 3G TS 33.203 中所述的 Authentication-Challenge 消息或者验证向量。

[0093] [0085] 一旦 SIP 用户代理已经接受隐式验证,则采用包括用于向网络表明隐式验证被接受的“SSO 使能”的指示的新 SIP Register 消息来响应这个“SIP 4xx 隐式验证”消息。网络 (P-CSCF、I-CSCF) 向 S-CSCF 提交这种 SIP Register 消息, S-CSCF 又向用户设备 (UE) 回送成功结果“SIP 200 OK”。已经通过 WLAN 网络进行访问的终端用户这时注册到多媒体域,而没有通常在终端用户的多媒体注册中出现的那些额外定期验证过程。

[0094] [0086] 图 7 中所示的第五实施例的描述尽可能地与图 3 所示的第一实施例匹配。类似地,来自其中 GPRS 为接入网的图 4 所示的第二实施例的理论可方便地适用于其中 WLAN 为接入网的另一个实施例,后者由于上述实施例而无需进一步说明。

[0095] [0087] 另一方面,其中 GPRS 为接入网的上述第三实施例实际上也适用于其中 WLAN 为接入网的另一个实施例,因为发送给用户设备的相关验证指示作为特定属性值对 (AVP) 包含在 WLAN 访问所采用的 RADIUS 或 Diameter 协议的相应消息中。

[0096] [0088] 最后,其中 GPRS 为接入网的上述第四实施例也适用于其中 WLAN 为接入网的另一个实施例,假定对 WLAN 中的短消息业务 (SMS) 的支持,或者通过在具有双终端作为用户设备的情况下把 GPRS 基础结构的电路交换技术用于 SMS 来进行。

[0097] [0089] 出现第四种情况,在其中,在分组数据业务附加过程之后,用户由 CDMA 2000 网络进行验证,并且还通过分组数据业务网络访问多媒体域。图 8 说明与第一种情况下图 4 中的实施例一致的第六实施例,其中,验证、授权和记帐服务器 (AAA) 用作 CDMA 2000 网络的订户服务器。在这个方面,并且为了清楚起见,CDMA 2000 网络的验证、授权和记帐服务器 (AAA) 包括允许对 CDMA 2000 网络中的分组数据业务进行访问所需的所有基本功能性以及用作多媒体域中的订户服务器所需的所有功能性。

[0098] [0090] 然而,只要访问 CDMA 2000 分组数据业务的传统已知 AAA 功能性驻留在与多媒体域的订户服务器不同的实体中,则两种实体、即传统 CDMA 2000 AAA 与多媒体域的订户服务器之间的附加接口用来共享用户验证数据。

[0099] [0091] 除了这些考虑之外,上述实施例也适用于涉及 CDMA2000 网络的这种情况,假定相关信息可采用对当前 RADIUS 和 Diameter 接口的扩展来传输。

[0100] [0092] 在上述示范的第一种情况下提供又一个实施例,并且如图 9 所示,其中,隐式验证的建议 (SSO 建议) 实际上从用户设备 (UE) 本身被触发,并且没有接收来自多媒体域 (IMS) 的先前邀请。因此,图 9 中的流序列提供对图 5 和图 6 中的那些实施例的备选实施例,其中,用户设备 (UE) 直接向多媒体域 (IMS) 提交它对隐式验证的建议 (SSO 建议),

而没有通过更新位置应答消息或者通过短消息业务 (SMS) 接收先前邀请,以便在所述用户设备与多媒体域之间执行这种隐式验证。

[0101] [0093] 这种新的方法可能还适用于修改其它上述实施例,并且与应用情况无关。

[0102] [0094] 以上以说明性而非限制性方式关于若干实施例描述了本发明。显然,根据上述理论,本发明的修改和变更是可行的,以及落入权利要求的范围之内的对实施例的任何修改意在包含于其中。

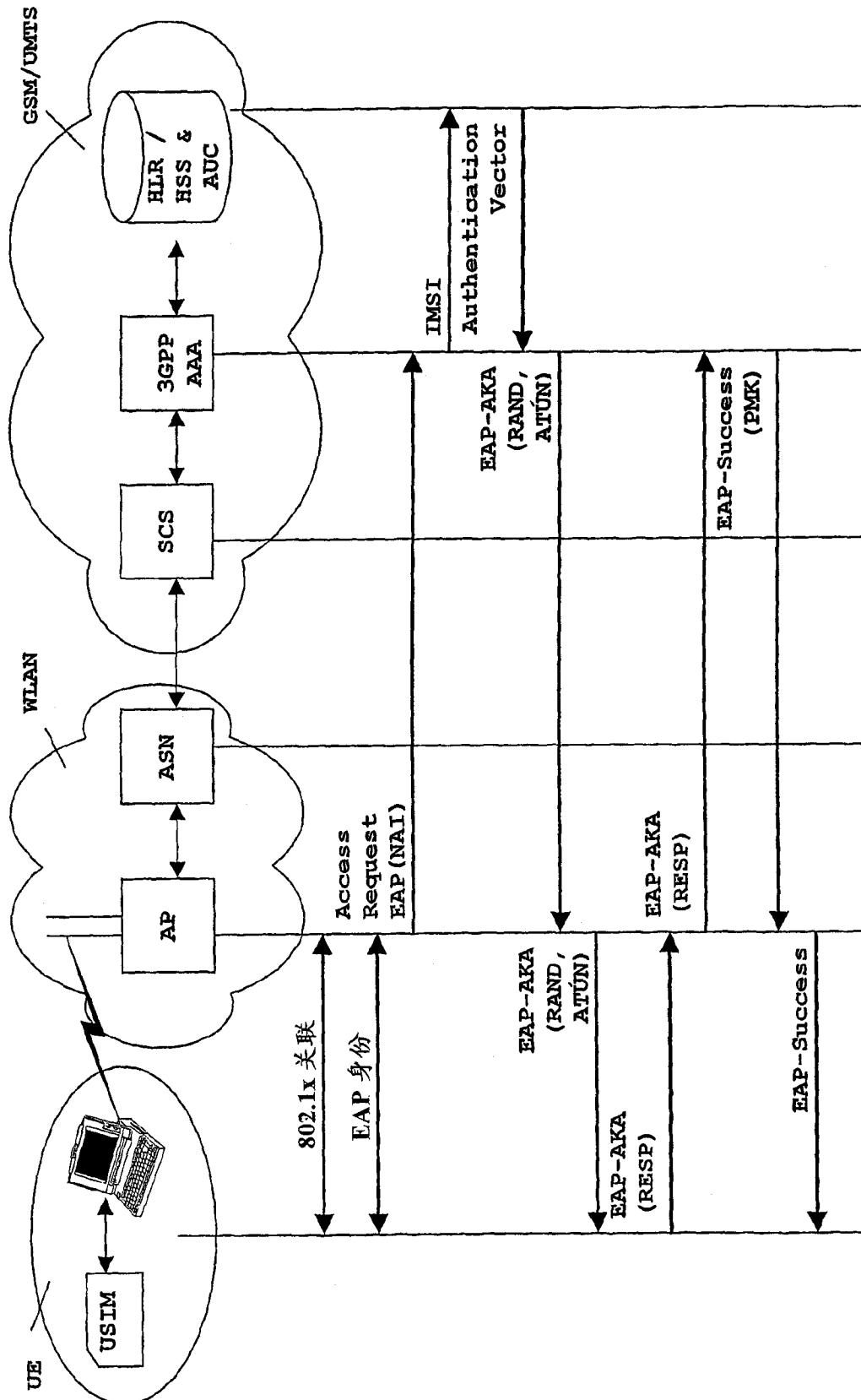
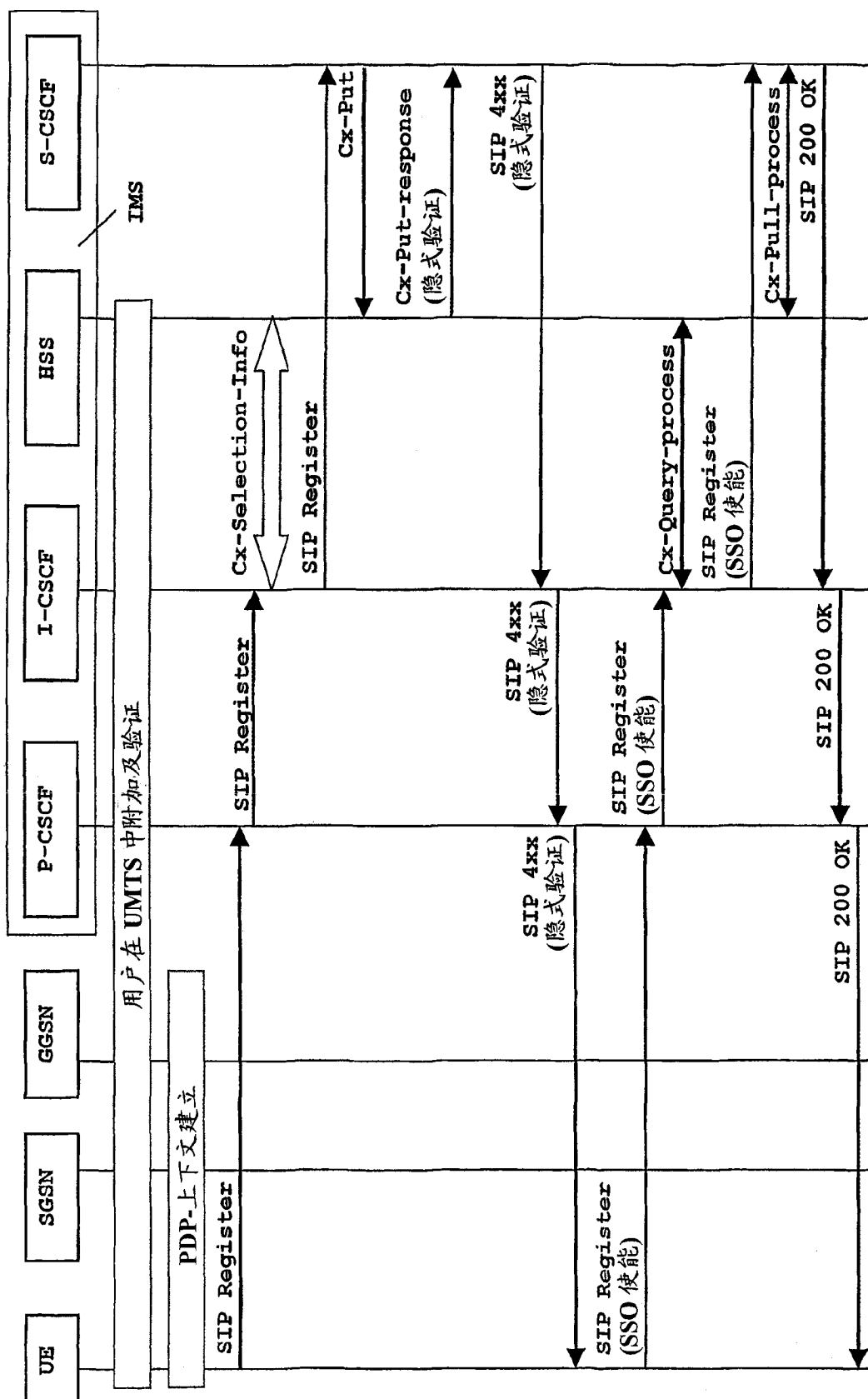
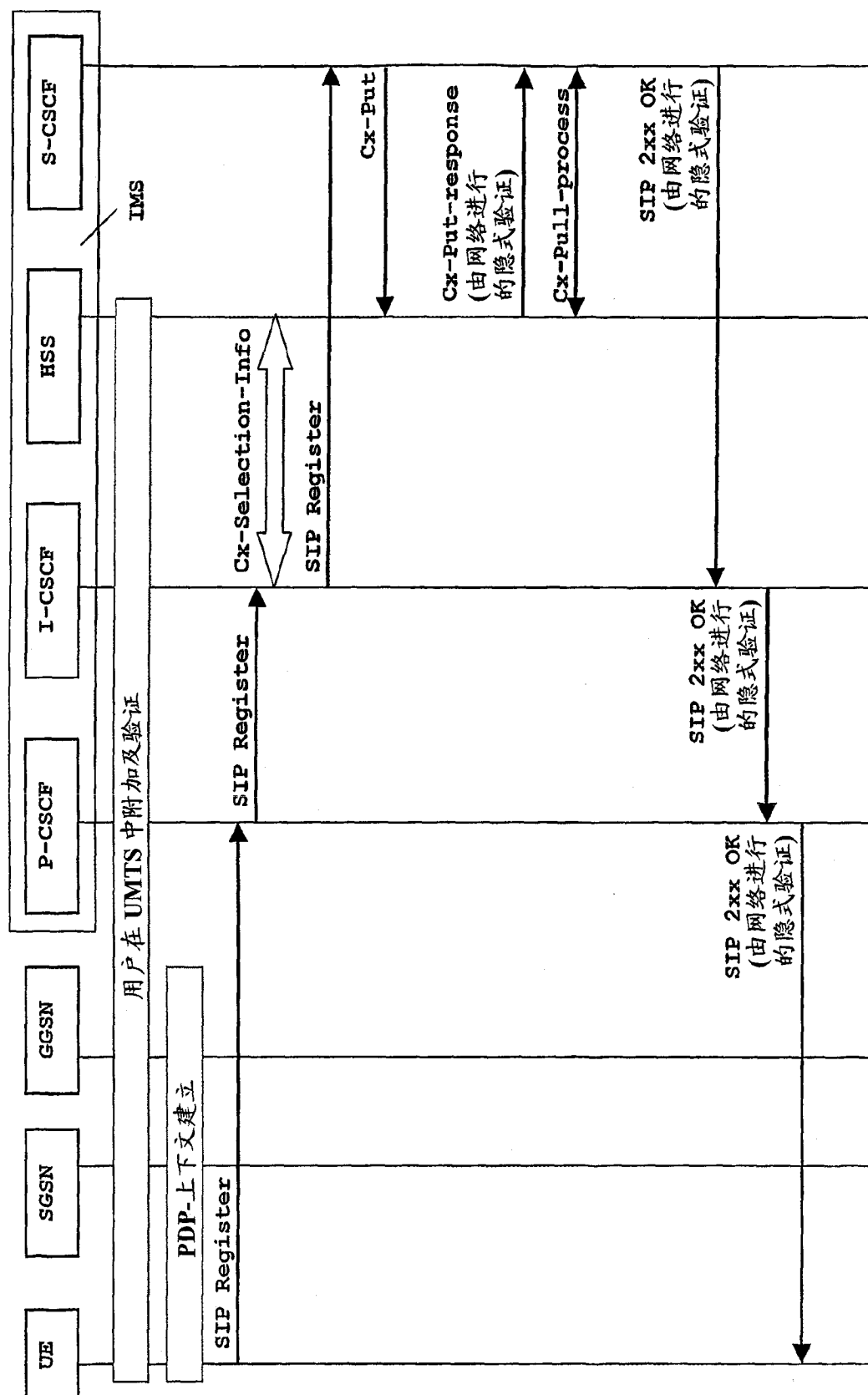


图 2 现有技术



三

四



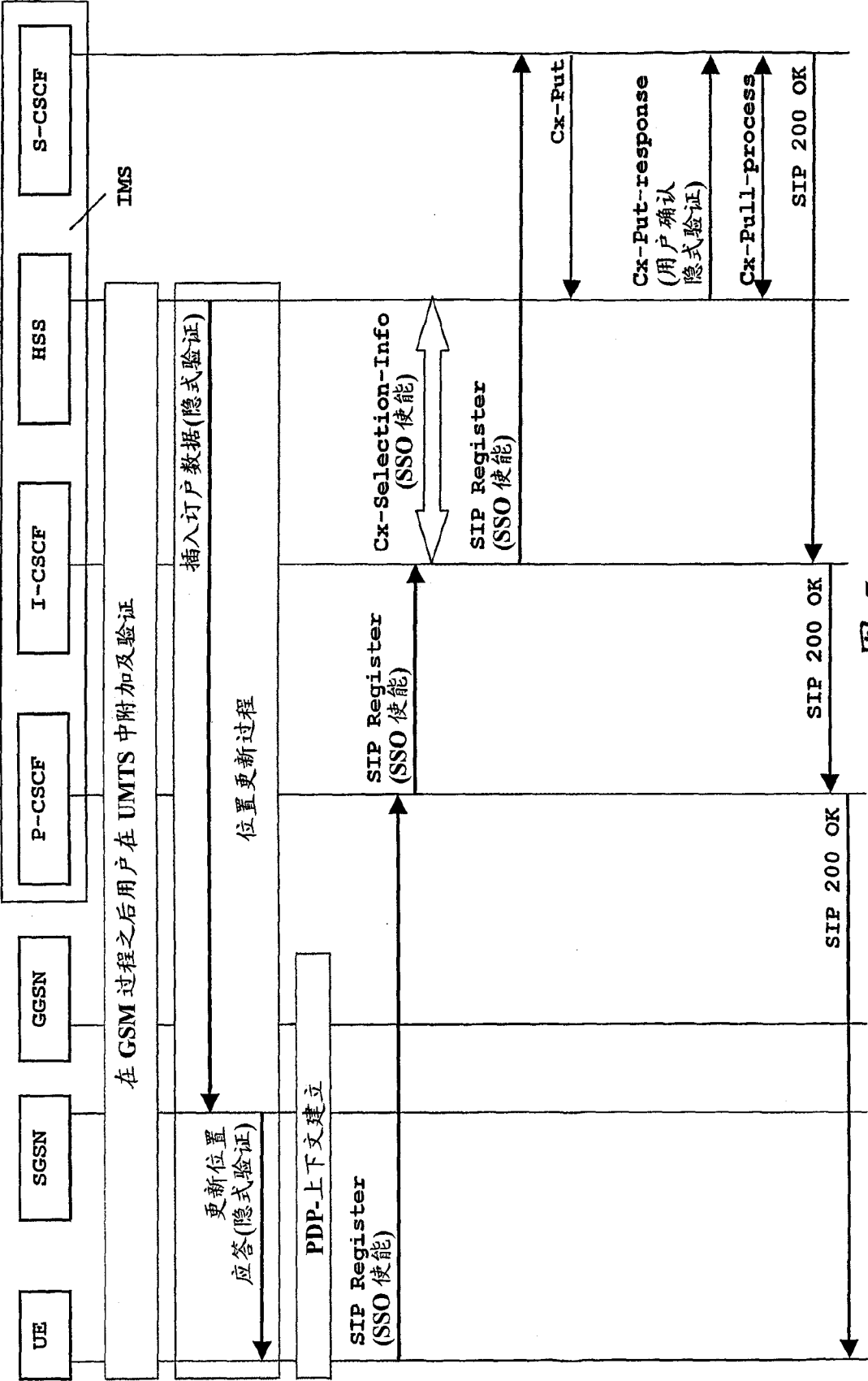


图 5

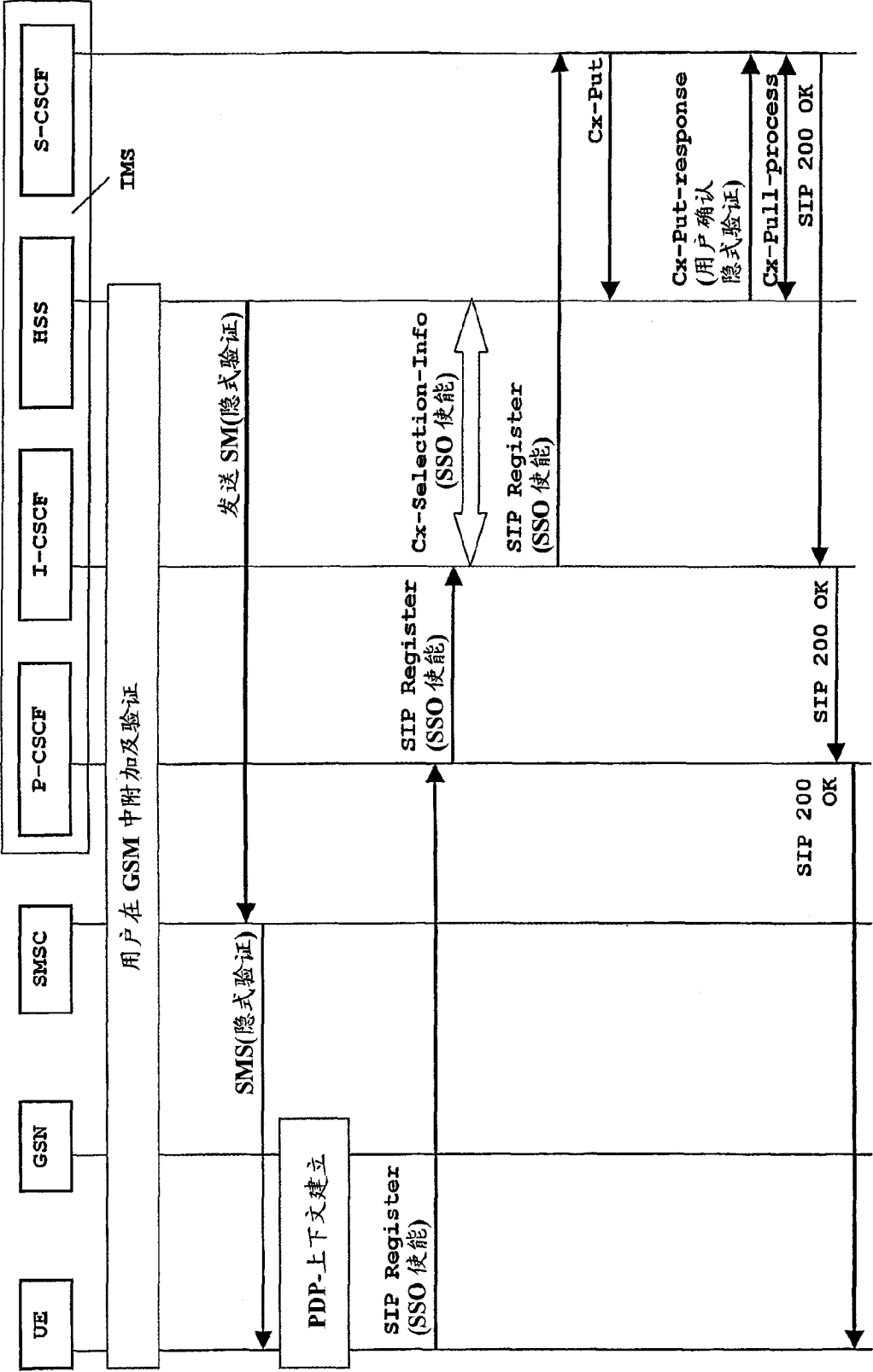
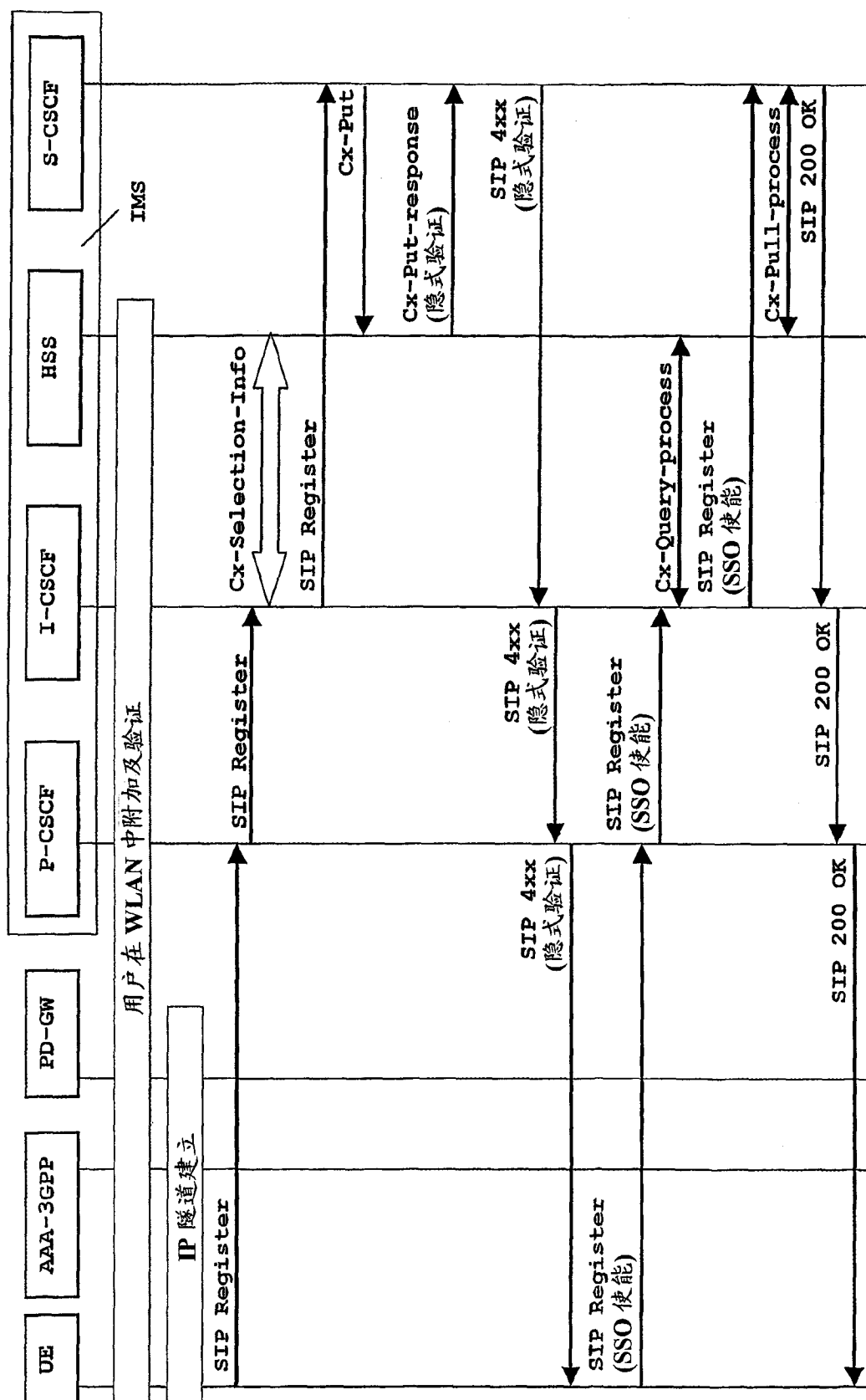


图 6



七

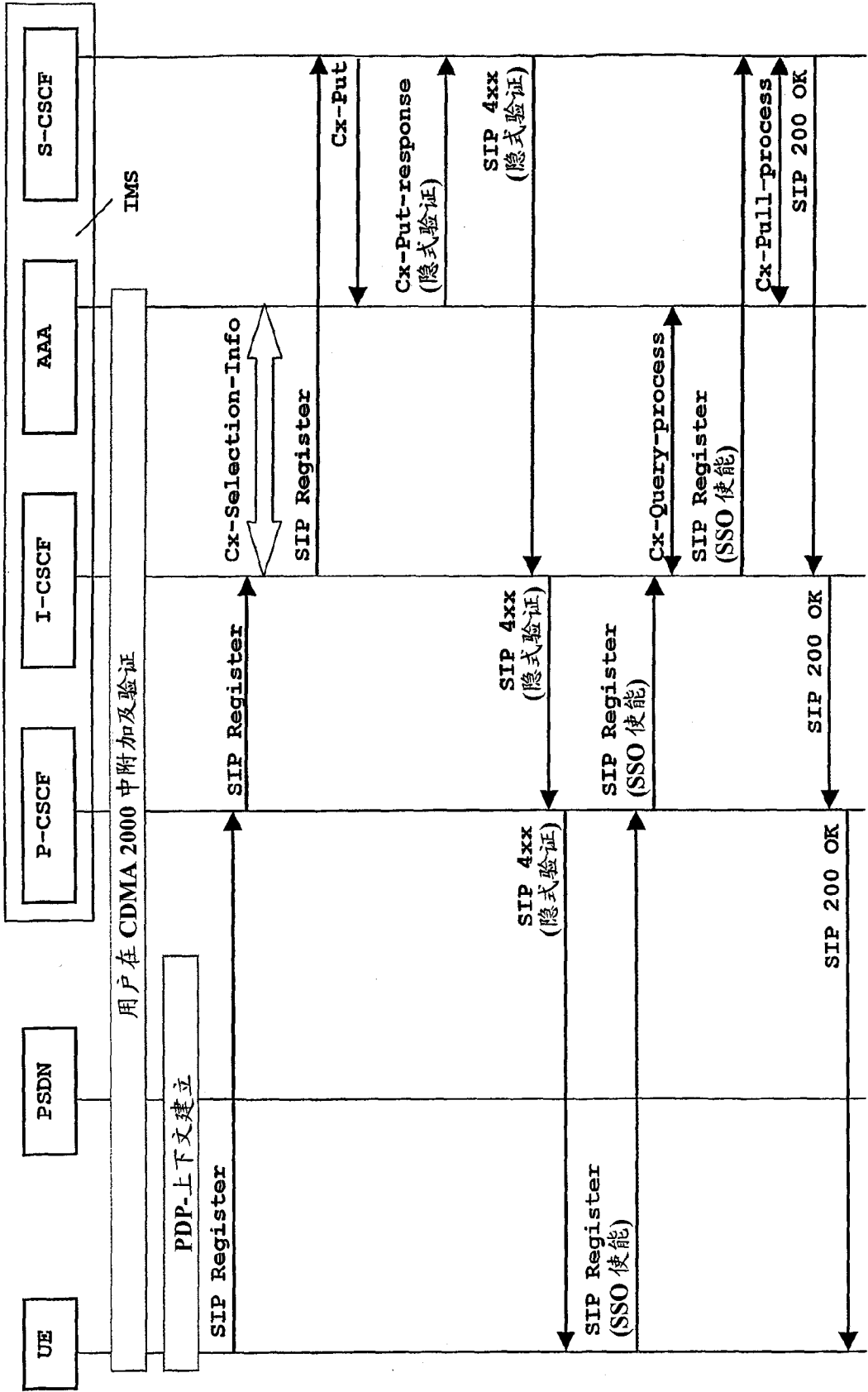


图 8

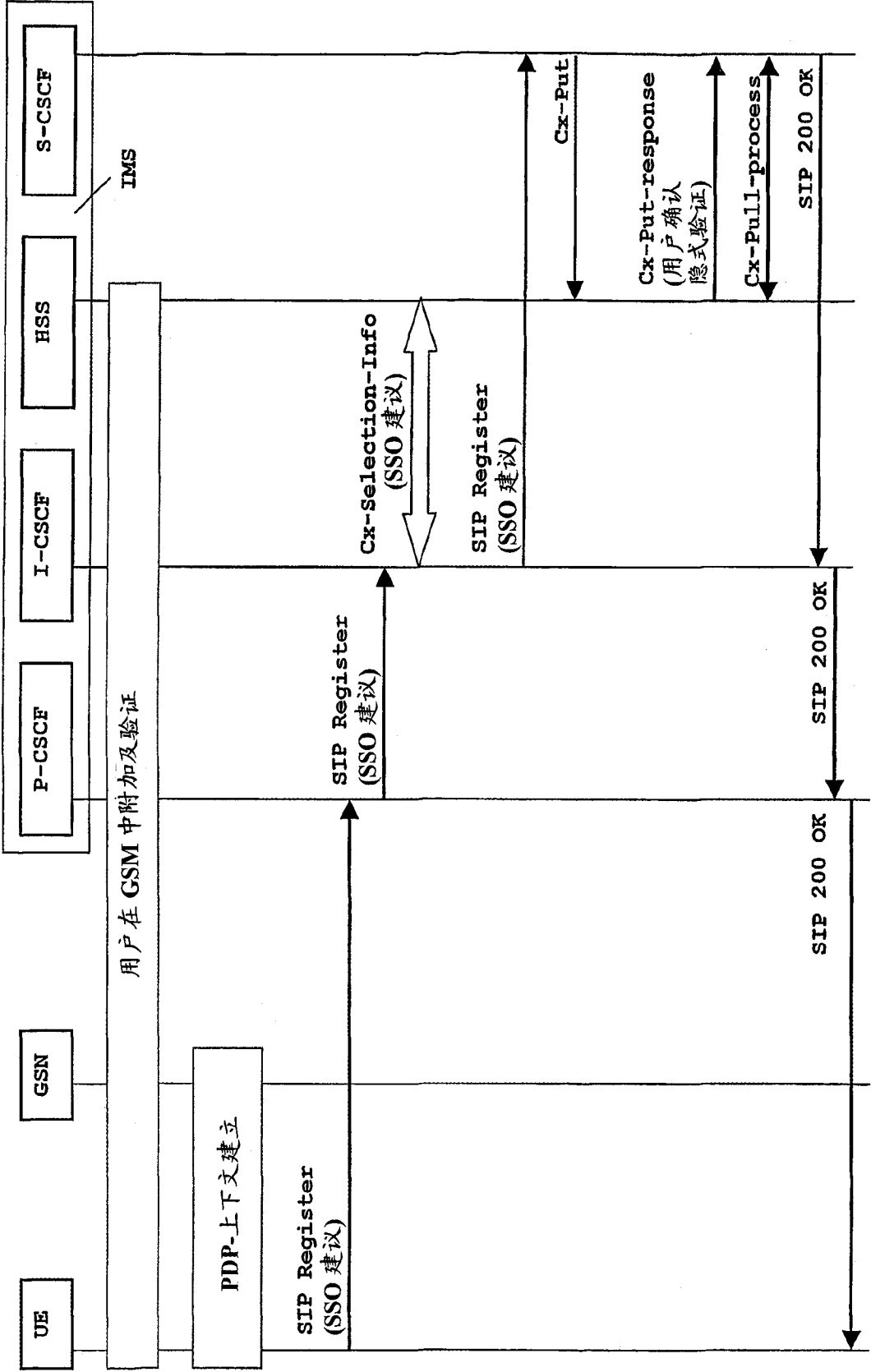


图 9