



(12) 发明专利

(10) 授权公告号 CN 101965739 B

(45) 授权公告日 2013. 12. 25

(21) 申请号 200880126748. 9

(22) 申请日 2008. 02. 15

(85) PCT申请进入国家阶段日
2010. 08. 13

(86) PCT申请的申请数据

PCT/SE2008/050184 2008. 02. 15

(87) PCT申请的公布数据

W02009/102248 EN 2009. 08. 20

(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

(72) 发明人 路易斯·巴里加

戴维·卡斯特利亚诺斯萨莫拉

(74) 专利代理机构 中科专利商标代理有限责任
公司 11021

代理人 赵伟

(51) Int. Cl.

H04L 9/32(2006. 01)

H04W 12/06(2009. 01)

(56) 对比文件

US 2005/0143065 A1, 2005. 06. 30,

US 2005/0143065 A1, 2005. 06. 30,

WO 2007/085779 A1, 2007. 08. 02,

审查员 张卉

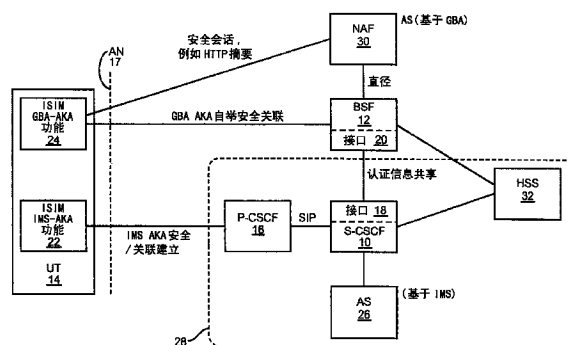
权利要求书3页 说明书8页 附图10页

(54) 发明名称

无线通信网络中的用户认证系统和方法

(57) 摘要

此处教导的方法和系统提供了用于对用户终端进行认证的、要在支持对用户终端的 IMS-AKA 认证的网络实体与支持对用户终端的 GBA-AKA 认证的网络实体之间共享的认证信息。在这些实体之间共享认证信息允许针对对用户终端的 IMS-AKA 认证而产生的认证信息的全部或部分随后用于对用户终端的 GBA-AKA 认证,反之亦然。



1. 一种减少对用户终端的冗余认证操作的方法,所述方法包括:

由对用户终端的 IMS-AKA 认证中使用的呼叫会话控制功能元件 CSCF 和对用户终端的 GBA-AKA 认证中使用的自举服务器功能元件 BSF 之一从归属订户服务器 HSS 获得用于对用户终端的 IMS-AKA 认证的 AKA 矢量;

由所述 CSCF 和所述 BSF 之一使用所述 AKA 矢量对用户终端进行认证;

在所述 CSCF 和所述 BSF 之间,共享用户终端的、至少包括所述 AKA 矢量在内的用户认证信息;以及

由所述 CSCF 和所述 BSF 中的另一个使用相同的 AKA 矢量对用户终端进行认证。

2. 根据权利要求 1 所述的方法,其中,在 CSCF 与 BSF 之间共享用户认证信息的步骤包括:所述 CSCF 从归属订户服务器 HSS 获得用于对用户终端的 IMS-AKA 认证的 AKA 矢量,并将所述 AKA 矢量传送至 BSF,以用于对用户终端的 GBA-AKA 认证。

3. 根据权利要求 2 所述的方法,其中,在 CSCF 与 BSF 之间共享用户认证信息的步骤还包括:所述 CSCF 从 HSS 获得通用自举架构用户安全设置 GUSS;以及将所述 GUSS 与所述 AKA 矢量一起传送至 BSF。

4. 根据权利要求 2 所述的方法,其中,将所述 AKA 矢量从 CSCF 传送至 BSF 的步骤包括:所述 CSCF 将所述 AKA 矢量自动推送至 BSF。

5. 根据权利要求 2 所述的方法,其中,将所述 AKA 矢量从 CSCF 传送至 BSF 的步骤包括:所述 CSCF 响应于从 BSF 接收到请求,将所述 AKA 矢量发送至 BSF。

6. 根据权利要求 1 所述的方法,其中,在 CSCF 与 BSF 之间共享用户认证信息的步骤包括: CSCF 从归属订户服务器 HSS 获得用于对用户终端的 IMS-AKA 认证的 AKA 矢量,根据所述 AKA 矢量来产生导出的 AKA 矢量,并将导出的 AKA 矢量传送至 BSF 以用于对用户终端的 GBA-AKA 认证。

7. 根据权利要求 1 所述的方法,其中,在 CSCF 与 BSF 之间共享用户认证信息的步骤包括:所述 BSF 从归属订户服务器 HSS 获得用于对用户终端的 GBA-AKA 认证的 AKA 矢量;以及并将所述 AKA 矢量从 BSF 传送至 CSCF 以用于对用户终端的 IMS-AKA 认证。

8. 根据权利要求 1 所述的方法,其中,在 CSCF 与 BSF 之间共享用户认证信息的步骤包括:所述 BSF 从归属订户服务器 HSS 获得用于对用户终端的 GBA-AKA 认证的 AKA 矢量;根据所述 AKA 矢量来产生导出的 AKA 矢量;以及将导出的 AKA 矢量从 BSF 传送至 CSCF 以用于对用户终端的 IMS-AKA 认证。

9. 根据权利要求 1 所述的方法,其中,在 CSCF 与 BSF 之间共享用户认证信息的步骤包括:所述 CSCF 联系作为归属订户服务器 HSS 的代理的 BSF;以及经由 BSF 从 HSS 间接接收用于对用户终端的 IMS-AKA 认证的 AKA 矢量。

10. 根据权利要求 9 所述的方法,还包括:所述 BSF 保持 BSF 从 HSS 获得的、针对 CSCF 的 AKA 矢量;以及在 BSF 处使用所述 AKA 矢量以用于对用户终端的 GBA-AKA 认证。

11. 根据权利要求 1 所述的方法,其中,在 CSCF 与 BSF 之间共享用户认证信息的步骤包括:如果在对用户终端的 GBA-AKA 认证之前进行对用户终端的 IMS-AKA 认证,则 CSCF 传送由 CSCF 从归属订户服务器 HSS 获得的认证信息的至少一部分;以及如果在对用户终端的 IMS-AKA 认证之前进行对用户终端的 GBA-AKA 认证,则 BSF 传送由 BSF 从 HSS 获得的认证信息的至少一部分。

12. 一种支持对用户终端的 IMS-AKA 认证的呼叫会话控制功能元件 CSCF(10), 所述 CSCF 执行对用户终端的 IMS-AKA 认证, 并且包括: 自举服务器功能元件接口 BSF 接口 (18), 用于在 CSCF 与用于对用户终端的 GBA-AKA 认证的自举服务器功能元件 BSF 之间, 共享用户终端的、至少包括认证和密钥协商 AKA 矢量在内的用户认证信息, 其中, 所述 AKA 矢量是由所述 CSCF 和 BSF 之一从归属订户服务器 HSS 获得的。

13. 根据权利要求 12 所述的 CSCF, 其中, CSCF 保持由 CSCF 获得的、用于对用户终端的 IMS-AKA 认证的 AKA 矢量, 并且, CSCF 经由 BSF 接口将所述 AKA 矢量或导出的 AKA 矢量传送至 BSF, 以由 BSF 随后用来支持对用户终端的 GBA-AKA 认证, 从而减少用于对用户终端的 GBA-AKA 认证的冗余认证信息的产生。

14. 根据权利要求 13 所述的 CSCF, 其中, CSCF 充当服务 CSCFS-CSCF, 并用于访问归属订户服务器 HSS 以对用户终端进行 IMS-AKA 认证, 并用于从 HSS 获得 AKA 矢量以及保持所述 AKA 矢量作为传送至 BSF 的用户认证信息的至少一部分。

15. 根据权利要求 14 所述的 CSCF, 其中, 作为对用户终端的 IMS-AKA 认证的一部分, CSCF 从 HSS 获得用户终端的通用认证架构用户安全设置 GUSS, 并且, CSCF 保持所述 GUSS 作为传送至 BSF 的用户认证信息的至少一部分。

16. 根据权利要求 12 所述的 CSCF, 其中, 所述 CSCF 经由 BSF 接口与作为归属订户服务器 HSS 的代理的 BSF 进行通信, 以获得用于支持对用户终端的 IMS-AKA 认证的用户认证信息。

17. 根据权利要求 12 所述的 CSCF, 其中, 所述 CSCF 响应于对用户终端的 IMS-AKA 认证, 经由 BSF 接口将认证信息推送至 BSF。

18. 根据权利要求 12 所述的 CSCF, 其中, 所述 CSCF 响应于 BSF 从 CSCF 请求认证信息, 经由 BSF 接口将认证信息发送至 BSF。

19. 根据权利要求 12 所述的 CSCF, 其中, 所述 CSCF 基于经由 BSF 接口从 BSF 接收 AKA 矢量和使用接收到的 AKA 矢量对用户终端进行 IMS-AKA 认证, 在 CSCF 与 BSF 之间共享用户终端的用户认证信息。

20. 一种支持对用户终端的 GBA-AKA 认证的自举服务器功能元件 BSF(42), 所述 BSF 执行对用户终端的 GBA-AKA 的认证, 并且包括: 呼叫会话控制功能元件接口 CSCF 接口 (20), 用于在 BSF 与用于对用户终端的 IMS-AKA 认证的呼叫会话控制功能元件 CSCF 之间共享至少包括认证和密钥协商 AKA 矢量在内的用户认证信息, 其中, 所述 AKA 矢量是由所述 BSF 和 CSCF 之一从归属订户服务器 HSS 获得的。

21. 根据权利要求 20 所述的 BSF, 其中, 所述 BSF 保持由 BSF 获得的、用于对用户终端的 GBA-AKA 认证的 AKA 矢量, 并且, 所述 BSF 经由 CSCF 接口将所述 AKA 矢量或导出的 AKA 矢量传送至 CSCF, 以由 CSCF 随后用来支持对用户终端的 IMS-AKA 认证, 从而减少用于对用户终端的 IMS-AKA 认证的冗余认证信息的产生。

22. 根据权利要求 21 所述的 BSF, 其中, 所述 BSF 用于在用户终端向服务层网络的认证期间访问归属订户服务器 HSS, 并用于从 HSS 获得 AKA 矢量以及保持所述 AKA 矢量作为传送至 CSCF 的用户认证信息的至少一部分。

23. 根据权利要求 21 所述的 BSF, 其中, 所述 BSF 通过经由 CSCF 接口从 CSCF 接收认证请求, 从 HSS 代表 CSCF 获得 AKA 矢量以及获得通用认证架构用户安全设置 GUSS, 并经由

CSCF 接口将所述 AKA 矢量传送至 CSCF, 来对于 CSCF 充当归属订户服务器 HSS 的代理。

24. 根据权利要求 23 所述的 BSF, 其中, 所述 BSF 保持从 HSS 获得的 AKA 矢量和 GUSS, 以由 BSF 在对用户终端的 GBA-AKA 认证中使用。

25. 根据权利要求 21 所述的 BSF, 其中, 所述 BSF 基于经由 CSCF 接口从 CSCF 接收 AKA 矢量和使用接收到的 AKA 矢量对用户终端进行 GBA-AKA 认证, 在 BSF 与 CSCF 之间共享用户终端的用户认证信息。

无线通信网络中的用户认证系统和方法

技术领域

[0001] 本发明总体涉及对无线通信网络的用户进行认证,具体涉及在基于 IMS 和 GBA 的用户认证之间共享用户认证信息。

背景技术

[0002] 现有的和正在开发的无线通信网络针对用户提供越来越大范围和越来越多类型的通信服务。在几乎所有实例中,必须在准予访问服务之前认证或验证用户。所需的具体认证常常依赖于所访问的服务的类型。例如,通过因特网协议多媒体核心网子系统(称作“IMS”或“IMS 网络”)可用的服务一般要求对尝试访问这种服务的用户终端的 IMS 注册。该注册包括认证和密钥协商(AKA)安全过程,这涉及用户终端与 IMS 网络之间的会话发起协议(SIP)信令。

[0003] 更具体地,IMS 网络使用给定用户终端的两个标识(identity)。第一标识是 IP 多媒体公开密钥标识(IMPU),第二标识是 IP 多媒体私有标识(IMPI)。IMPI 可以例如是从用户终端的国际移动订户标识(IMSI)导出的。第三代合作伙伴计划(3GPP)标准规定该密钥导出方法是强制的,其中,IMPI 是使用来自在用户终端中实现的通用订户标识模块(USIM)的标识信息来形成的。

[0004] 一般地,用户终端具有一个 IMPI,但其可以具有多个 IMPU。然而,IMPU 与 IMPI 相关。例如,归属订户服务器(HSS)针对每个 IMPI 存储 IMPU 列表。对于包括 IMS-AKA 认证在内的 IMS 注册,呼叫会话控制功能元件(CSCF)与 HSS 进行通信以获得认证矢量。用户终端使用基于 SIP 的 AKA 认证协议来与 CSCF 进行通信。

[0005] IMS 网络服务之外可用的其他应用可能需要其他认证处理。例如,多种应用需要基于通用自举架构(GBA)的认证,这还使用了基于 AKA 的认证(基于 HTTP 信令)。自举服务器功能元件(BSF)联系终端的 HSS,以获得 AKA 矢量,并获得针对用户终端的 GBA-AKA 认证的一般用户安全设置(GUSS)。

[0006] 更具体地,基于 GBA 的认证首先通过运行自举过程在网络与用户终端之间建立共享秘密。然后,在网络应用功能(NAF)与用户终端之间使用共享秘密用于认证目的,其中,用户终端和 BSF 使用 AKA 协议来相互认证,并就之后在用户终端与 NAF 之间应用的会话密钥达成共识。一般地,BSF 通过使用密钥导出过程来限制密钥材料对特定 NAF 的可应用性。密钥导出过程可以用于在密钥材料的生存期期间向多个 NAF 进行认证。密钥生存期是例如根据在 BSF 处实现的本地策略来设置的。

[0007] 尽管 IMS-AKA 认证过程和 GBA-AKA 认证过程均依赖于基于 AKA 的认证,但传统地,它们是分离且独立地完成的。例如,对于相同的用户终端,CSCF 联系 HSS,以获得用于在 IMS 安全域中对用户终端进行认证的 AKA 矢量。类似地,对于相同的终端,BSF 同样联系相同的 HSS,以获得用于在 GBA 安全域中对终端进行认证的 AKA 矢量。因此,对于相同的用户终端,产生和维持重复的认证信息。

发明内容

[0008] 根据此处提出的教导,在支持对用户终端的 IMS-AKA 认证的网络实体与支持对用户终端的 GBA-AKA 认证的网络实体之间共享用于对用户终端进行认证的用户认证信息。在这些实体之间共享认证信息允许针对对用户终端的 IMS-AKA 认证而产生的认证信息的全部或部分随后被用于对用户终端的 GBA-AKA 认证,反之亦然。

[0009] 作为参考,示例情况中的“IMS-AKA”是指第三代合作伙伴计划 (3GPP) 发布的、针对因特网协议多媒体核心网子系统 (IMS) 的认证和密钥协商 (AKA) 安全规范。类似地,示例情况中的“GBA-AKA”是指 3GPP 发布的、针对通用认证架构 (GAA) 的上下文中的通用自举架构 (GBA) 的 AKA 安全规范。当然,此处的教导扩展至用于基于类似标准的网络以及用于基于相关现有 3GPP 标准的演进的网络的、以类似方式工作的实体和过程。

[0010] 在至少一实施例中,一种减少对用户终端的冗余认证操作的方法,包括:在对用户终端的 IMS-AKA 认证中使用的呼叫会话控制功能元件 (CSCF) 与对用户终端的 GBA-AKA 认证中使用的自举服务器功能元件 (BSF) 之间,共享用户认证信息。在至少一个这种实施例中,共享认证信息包括:例如 CSCF 在对用户终端的 IMS-AKA 认证期间从归属订户服务器 (HSS) 获得 AKA 矢量;以及将所述 AKA 矢量或所导出的 AKA 矢量从 CSCF 传送至 BSF。该传送允许 BSF 在对用户终端的随后 GBA-AKA 认证中使用所传送的 AKA 矢量,而不是例如,BSF 访问 HSS 以产生新 AKA 矢量信息,从而支持 GBA-AKA 认证。

[0011] 在一个或多个其他实施例中,在对用户终端的 IMS-AKA 认证中使用的 CSCF 包括:BSF 接口,用于在 CSCF 与 BSF 之间共享用户认证信息,以由 BSF 在对用户终端的 GBA-AKA 认证中使用。在 CSCF 与 BSF 之间共享的认证信息包括例如 CSCF 在对用户终端的 IMS-AKA 认证期间从 HSS 获得的 AKA 矢量。BSF 使用从 CSCF 传送至所述 BSF 的 AKA 矢量,而不是与 HSS 协调以产生用于对用户终端的 GBA-AKA 认证的另一 AKA 矢量,从而消除或至少减少了 IMS-AKA 和 GBA-AKA 认证操作之间的冗余。

[0012] 在其他实施例中,在对用户终端的 GBA-AKA 认证中使用的 BSF 包括:CSCF 接口,用于在 BSF 与 CSCF 之间共享用于对用户终端的 IMS-AKA 认证的用户认证信息。所共享的认证信息可以包括 AKA 矢量。例如,BSF 可以在对用户终端的 GBA-AKA 认证期间从 HSS 获得 AKA 矢量,然后将所述 AKA 矢量传送至 CSCF,以由 CSCF 在对用户终端的 IMS-AKA 认证中使用。因此,该传送排除了 CSCF 从 HSS 获得用于 IMS-AKA 认证的新 AKA 矢量的需要。

[0013] 在至少一个这种实施例中,BSF 对于 CSCF 充当 HSS 的代理。因此,CSCF 联系 BSF 而不是 HSS,以获得用于对用户终端的 IMS-AKA 认证的 AKA 矢量。BSF 用于从 HSS 获得 AKA 矢量并将所述 AKA 矢量或所导出的 AKA 矢量传送至 CSCF,以供 CSCF 在对用户终端的 IMS-AKA 认证中使用。此外,BSF 用于保留所述 AKA 矢量的副本,以供 BSF 在对用户终端的 GBA-AKA 认证中使用。该保留使 BSF 免于从 HSS 获得用于 GBA-AKA 认证的单独 AKA 矢量。作为获得所述 AKA 矢量的一部分,BSF 可以获得用户终端的一般用户安全设置 (GUSS),并使用所述 AKA 矢量和 GUSS 来自举对用户终端的 GBA-AKA 认证。

[0014] 当然,本发明不限于上述特征和优点。事实上,本领域技术人员将在阅读以下详细描述以及在阅览附图时认识到附加的特征和优点。

附图说明

[0015] 图 1 是无线接入网和一个或多个核心网的一实施例的图,包括作为 IMS 域网络实体的呼叫会话控制功能元件 (CSCF) 和作为 GBA 域网络实体的自举服务器功能元件 (BSF)。

[0016] 图 2 是从 CSCF 的角度来看,在 CSCF 与 BSF 之间共享给定用户终端的用户认证信息的方法的一实施例的逻辑流程图。

[0017] 图 3 是从 BSF 的角度来看,在 CSCF 与 BSF 之间共享给定用户终端的用户认证信息的方法的一实施例的逻辑流程图。

[0018] 图 4 是用户终端、CSCF 和 BSF 的示例电路实现的框图,并包括用于共享用户认证信息的、CSCF 与 BSF 之间的接口的示例细节。

[0019] 图 5 是传统 IMS-AKA 认证过程的呼叫流程图。

[0020] 图 6 是传统 GBA-AKA 认证过程的呼叫流程图。

[0021] 图 7 是 IMS-AKA 认证过程和 GBA-AKA 认证过程的呼叫流程图,其中,根据此处教导的方法的一实施例在两个认证过程之间共享用户认证信息。

[0022] 图 8 是 IMS-AKA 认证过程和 GBA-AKA 认证过程的呼叫流程图,其中,根据此处教导的方法的另一实施例在两个认证过程之间共享用户认证信息。

[0023] 图 9 是 IMS-AKA 认证过程和 GBA-AKA 认证过程的呼叫流程图,其中,根据此处教导的方法的又一实施例在两个认证过程之间共享用户认证信息。

[0024] 图 10 是 IMS-AKA 认证过程和 GBA-AKA 认证过程的呼叫流程图,其中,根据此处教导的方法的另一实施例在两个认证过程之间共享用户认证信息。

[0025] 图 11 是 IMS-AKA 认证过程和 GBA-AKA 认证过程的呼叫流程图,其中,根据此处教导的方法的另一实施例在两个认证过程之间共享用户认证信息。

具体实施方式

[0026] 图 1 是可操作共享用于对用户终端 (UT) 14 进行 IMS-AKA 认证和对相同用户终端 14 进行 GBA-AKA 认证的用户认证信息的呼叫会话控制功能元件 (CSCF) 10 和自举服务器功能元件 (BSF) 12 的一实施例的框图。在这些网络实体之间共享认证信息允许针对对用户终端 14 的 IMS-AKA 认证而产生的认证信息的全部或部分随后被用于对相同用户终端 14 的 GBA-AKA 认证,反之亦然。除其他优点以外,这种共享减少或消除了否则对用户终端 14 进行独立的 IMS-AKA 和 GBA-AKA 认证而执行的冗余认证操作。

[0027] 此处,“IMS-AKA”表示由适用的第三代合作伙伴计划 (3GPP) 标准定义的认证和密钥协商 (AKA) 过程以及对因特网协议多媒体核心网子系统 (IMS) 的用户终端认证的规范,并进行了此处教导的、用于认证信息共享的修改。3GPP AKA 达到了两个目的:a) 用户与网络之间的相互认证(使用特定密钥);以及 b) 密钥协商,其中导出附加密钥以进一步用于完整性和机密性保护。此处考虑的用于共享的“认证信息”可以包括相互认证和密钥协商信息。类似地,“GBA-AKA”表示针对通用自举架构 (GBA) 中的用户终端认证而定义的 AKA 过程,并进行了此处教导的、用于认证信息共享的修改。

[0028] 在示意中,CSCF 10 被示意为“S-CSCF 10”,表示其对于用户终端 14 的“服务”作用。更具体地,作为非限制性示例,用户终端 14 通过在示意中被表示为“P-CSCF 16”的“代理”CSCF 来以通信方式耦合至 S-CSCF 10。(用户终端 14 可以通过实质上任何类型的无线接入/核心网 17 来进行无线通信接入。)S-CSCF 10 包括“自举服务器功能元件接口”,此

处其被称作“BSF 接口 18”。相应地,BSF 12 包括“呼叫会话控制功能元件接口”,此处其被称作“CSCF 接口 20”。

[0029] 相应的接口 18 和 20 用于将 S-CSCF 10 以通信方式耦合(直接或间接地)至 BSF 12,以在 S-CSCF 10 与 BSF 12 之间共享用户认证信息。除其他优点以外,在这两个实体之间共享用户认证信息减少(并可能消除)了否则对用户终端 14 进行 IMS-AKA 认证和对相同用户终端 14 进行 GBA-AKA 认证而执行的冗余认证操作。

[0030] 为了更好地理解所公开的示例配置的该优点和其他优点,可能有帮助的是,注意到用户终端 14 包括 IMS-AKA 认证功能 22 和 GBA-AKA 认证功能 24,这两种认证功能均可以经由在通用集成电路卡(UICC)等上承载的安全处理电路(硬件和/或软件)来实现。用户终端 14 使用例如其 IMS-AKA 认证功能 22,对其自身认证,以安全地访问从被表示为 AS 26 的基于 IMS 的应用服务器(可被包括在 IMS 网络 28 中或可通过 IMS 网络 28 访问)可得的一个或多个 IMS 应用。作为非限制性示例,这种应用包括存在感测以及多媒体广播。

[0031] 一个或多个其他应用可以在 IMS 网络的服务之外或与 IMS 网络的服务分开可用,但对于用户终端 14 来说可经由网络应用功能(NAF)30 来访问。用户终端 14 使用其 GBA-AKA 认证功能 24,针对访问对其自身进行认证,以访问通过 NAF 30 而可用的应用。该 GBA-AKA 认证由 BSF 12 支持,并在传统情况下需要 BSF 12 访问归属订户服务器(HSS)32,以获得用于对用户终端 14 进行认证的用户认证信息(如 AKA 矢量)。类似地,对用户终端 14 的前述 IMS-AKA 认证在传统情况下需要 S-CSCF 10 访问 HSS 32,以获得例如用于对用户终端 14 进行认证的 AKA 矢量。

[0032] 认识到 IMS-AKA 认证过程和单独的 GBA-AKA 认证过程均依赖于相同的基础 AKA 认证结构,并均依赖于产生对用户终端 14 加密的 AKA 矢量,此处的教导提供了在 S-CSCF 10 与 BSF 12 之间共享用户认证信息,以便减少传统上在对相同用户终端 14 执行单独的、独立的 IMS-AKA 和 GBA-AKA 认证过程时引起的冗余等。

[0033] 作为非限制性示例,图 2 示出了可以例如通过在 S-CSCF 10 处配置基于硬件和/或软件的电路而在 S-CSCF 10 处实现的处理逻辑。处理“起始”于以下假定:已经针对用户终端 14 发起或触发了 IMS-AKA 认证,从而 S-CSCF 10 获得或产生了针对用户终端 14 的用户认证信息(框 100)。例如, S-CSCF 10 从用户终端的 HSS 32 获得 AKA 矢量。

[0034] 处理继续: S-CSCF 10 至少暂时保留用户认证信息(框 102),该用户认证信息可以由 S-CSCF 10 获得的、用于执行对用户终端 14 的 IMS-AKA 认证的信息的全部或所选部分。处理继续: S-CSCF 10 将用户认证信息传送至 BSF 12(框 104)。即, S-CSCF 10 经由其 BSF 接口 18 将针对对用户终端 14 进行 IMS-AKA 认证而产生的认证数据的至少一部分发送至 BSF 12,以由 BSF 12 在对用户终端 14 的 GBA-AKA 认证中使用。这样做允许 BSF 12“重用”所传送的认证信息的全部或一部分,以支持对用户终端 14 的后续 GBA-AKA 认证。

[0035] 图 3 中的框 106、108 和 110 充当共享用户认证信息的对应的非限制性示例,但是从 BSF 12 的角度示出的。即,假定首先触发 GBA-AKA 认证,并且 BSF 12 在获得针对用户终端 14 的认证信息,以支持执行该 GBA-AKA 认证(框 106),至少暂时保留针对用户终端 14 的认证信息(框 108),并将该认证信息传送至 S-CSCF 10(框 110),以供其重用于支持对用户终端 14 的 IMS-AKA 认证。可以通过适当地配置基于硬件和/或软件的电路,在 BSF 12 处实现所示的处理逻辑。

[0036] 在这一点上,图 4 示出了用户终端 14、S-CSCF 10 和 BSF 12 的示例非限制性实现。本领域技术人员应当理解,这些示意被简化为适于理解此处的教导。

[0037] 首先,用户终端 14 的示意实施例包括系统处理电路 40(如一个或多个基于微处理器的电路)、通信电路 42(如蜂窝和 / 或其他无线收发机电路)以及安全性处理电路 44(如具有安全存储器、秘密存储器、终端标识信息等的基于 UICC 的安全域处理环境)。本领域技术人员应当理解,术语“用户终端”此处被赋予了宽泛的构造,并且作为示例而非限制性地包括蜂窝无线电话、无线寻呼机、PDA、调制解调器 / 网卡以及实质上任何其他类型的通信模块或设备。

[0038] 其次, S-CSCF 10 的示意实施例包括一个或多个处理电路 46,该一个或多个处理电路 46 包括 BSF 接口 18 或与 BSF 接口 18 相关联。这些电路可以以硬件或软件或者其任意组合来实现。在一实施例中,使 S-CSCF 10 基于利用由一个或多个所包括的微处理器电路执行的所存储的程序指令供给或配置 S-CSCF 10,来支持此处所描述和要求保护的认证信息共享。

[0039] 类似地, BSF 12 的示意实施例包括一个或多个处理电路 48,该一个或多个处理电路 48 包括 CSCF 接口 20 或与 CSCF 接口 20 相关联。这些电路可以以硬件或软件或者其任意组合来实现。在一实施例中,使 BSF12 基于利用由一个或多个所包括的微处理器电路执行的所存储的程序指令供给或配置 BSF 12,来支持此处所描述和要求保护的认证信息共享。

[0040] 从示例电路细节转移开,图 5 和 6 一起示出了针对给定用户终端的传统的独立(非共享)IMS-AKA 和 GBA-AKA 认证。因此,如此处所描述和要求保护的,在至少一实施例中,术语“IMS-AKA 认证”和“GBA-AKA 认证”可以具有这些示意处理步骤作为其基本框架,并且关于在 S-CSCF 10 与 BSF 12 之间共享认证信息进行了一个或多个修改。此处所描述和要求保护的其他实施例更显著地背离了这些基本认证示意,但所有这些实施例在实现安全的 IMS 域和安全的 GBA 域访问的意义上提供对用户终端 14 的 IMS-AKA 和 GBA-AKA 认证。

[0041] 通过如对于传统 IMS 域和 GBA 域认证所做的那样,对给定用户终端执行独立的、非共享 IMA-AKA 和 GBA-AKA 认证过程,网络运营商在初始时(投资时)和运行时(运营时)产生不必要的费用。例如,运营商针对不同类型的服务部署 IMS 和 GBA/GAA 技术将是越来越常见的,这意味着认证的低效将越来越成问题。

[0042] 在基于 TISpan 安全性架构的低效问题的更详细示例中,可以假定用户首先访问基于 GBA 的应用,从而经由支持 BSF 来触发向用户的 HSS 的 GBA-AKA 认证过程。还可以假定相同用户稍后尝试访问基于 IMS 的应用,从而经由支持 P/S-CSCF 来触发向相同 HSS 的 IMS-AKA 认证过程。这两种认证有些重复,并由于 HSS 处的不必要认证矢量(AV)消耗而导致低效的密钥管理,并且由于 S-CSCF 和 BSF 中对相同用户的重复(但不相关)认证会话而可能造成同步风险。

[0043] 特别地,尽管这些会话在某种意义上是重复的,但它们传统上是完全独立的,即使许多会话信息是公共的。在这种独立性下,一个会话的改变不会在另一会话中“被注意”或反映。(这种改变由重新认证、密钥刷新等来触发。)此外,不存在 IMS 与 GBA 域之间的任何安全性信息共享意味着,应用需要是 IMS 感知的和 GBA 感知的,以便通过基于 IMS-AKA 的基础设施和基于 GBA-AKA 的基础设施“可达”。这些需求使得应用(使用 HTTP/传输层安全性)实现两个接口(即,IMS/SIP 接口和 GBA/NAF 接口)成为必要,而这非期望地提高了初

始和运行成本。

[0044] 接着,转至此处提出的、用于联结或修改 IMS-AKA 和 GBA-AKA 认证过程以通过认证信息共享达到更高效率的示例性方法和设备,图 7 示出了 IMS-AKA 认证过程“A”与随后的 GBA-AKA 认证过程“B”之间的认证信息共享。该过程流是参照图 1 中使用的实体标识符来示出的。

[0045] 如图所示,S-CSCF 10 和 BSF 12 以通信方式耦合在一起,以进行认证信息共享,例如通过它们各自的接口 18 和 20。采用该耦合,当用户终端 14 触发了成功的 IMS-AKA 认证(作为 IMS 注册的一部分)时,S-CSCF 10 向 BSF 12 发送通知。该通知包括例如由 S-CSCF 10 从 HSS 32 获得的、用于对用户终端 14 进行 IMS-AKA 认证的 AKA 矢量。

[0046] 在互补配置中,响应于接收到该通知,BSF 12 可以被配置用于触发向 HSS 32 请求用户终端的 GBA 用户安全性设置(GUSS)。然后,BSF12 可以使用来自 S-CSCF 10 的 AKA 矢量和来自 HSS 32 的 GUSS 来创建自举用户终端 14 所需的信息。这样做排除了 HSS 32 产生用于基于 GBA 的自举的新的独立 AKA 矢量的需要。

[0047] 稍后,当用户终端 14 尝试访问基于 GBA 的应用时,其从 BSF 12 请求认证自举。BSF 12 经由来自 S-CSCF 10 的认证信息共享来检测对于用户终端 14 已经发生了自举,从而绕开自举过程并将自举事务标识符(B-TID)直接返回给用户终端 14。进而,用户终端根据 GBA 过程,使用 B-TID 与 NAF 30 建立安全性关联。

[0048] 备选地,BSF 12 不必要分发 B-TID,取而代之,用户终端 14 可以直接联系 NAF 30。在这种情况下,用户终端 14 可以被配置用于 B-TID 产生。在任何情况下,以上方法对面向用户终端 14 的标准化 IMS 接口具有最小影响。

[0049] 图 8 和 9 引入了在 S-CSCF 10 与 BSF 12 之间共享用户认证信息的附加实施例,这避免了用于对相同用户终端 14 进行 IMS-AKA 和 GBA-AKA 认证的“额外”(冗余)访问。更具体地,图 8 示出了 S-CSCF10 被配置用于取得用户终端 14 的 GUSS,作为 IMS 注册的一部分,以及取得用户终端 14 的认证矢量(AKA 矢量)。即,不是简单地从 HSS 32 获得 AKA 矢量以将用户终端 14 注册至 IMS 网络 28,而是 S-CSCF 10 附加地从 HSS 32 获得用户终端 14 的 GUSS。此外,S-CSCF 10 向 BSF 12 传送用户终端 14 的 AKA 矢量和 GUSS,作为共享的用户认证信息。BSF 12 使用共享的用户认证信息来执行用户终端 14 的常规自举过程,只是其不需要访问 HSS 32 以获取 AKA 矢量或 GUSS,这是由于这些项目经由接口 18 和 20 从 S-CSCF 传送到该 BSF 12。

[0050] 在某种意义上,上述操作对 S-CSCF 10 的操作的影响比对 BSF 12 的影响大。在一些情形或实现中,对 BSF 12 处的操作的影响大于对 S-CSCF 10 处的操作的影响是更有利的。图 9 示出了一个这样的实施例,其中,BSF 12 为 HSS 32 充当对于 S-CSCF 10 的代理。更具体地,在该实施例中,如适用的 3GPP 接口标准所定义的,BSF 12 被配置用于在“Cx”接口中作为面向 S-CSCF 10 的透明 HSS 代理来工作。

[0051] 在这种代理实施例中,来自支持用户终端 14 的 IMS 注册的 S-CSCF10 的 AV 请求被 BSF 12 “拦截”,或被导引至充当 HSS 32 的代理的 BSF12。响应于 S-CSCF 的请求,BSF 12 联系 HSS 32,并获得用户终端 14 的 AV 和 GUSS。此外,如上所述,BSF 12 使用这些项目来执行用户终端 14 的常规自举,并通过例如 Cx 接口将 AV 返回给 S-CSCF 10。尽管不限于这种上下文,但代理实施例可以提供 BSF12 与 HSS 32 处于同一位置的特定优点。

[0052] 关于以上用户认证信息的基于 S-CSCF-BSF 接口的共享的多个优点之一对于用户终端 14 的透明性。换言之,IMS-AKA 与 GBA-AKA 安全域之间的认证共享不需要用户终端 14 的意识或用户终端 14 的信令支持。尽管不存在对用户终端 14 的影响可能是有利的,但此处的至少一实施例还考虑基于用户终端信令的认证效率。

[0053] 例如,在至少一实施例中,用户终端 14 向 BSF 12 发信号通知其已经被注册在 IMS 网络 28 中,即,其已经经历 IMS-AKA 认证。具体地,此处给出的至少一实施例提出:用户终端 14 应当被配置为向 BSF 12 发信号通知用户终端 14 已经被注册在 IMS 网络 28 中。在至少一实施例中,这种信令基于 B-TID。

[0054] 在这一点上,在前述任意示例实施例中,BSF 12 可以向 S-CSCF 10 提供用户终端 14 的 B-TID。然后,通过用户(信令)接口将 B-TID 发送至用户终端 14,即,在图 7-9 的呼叫流中所示的 IMS “200 同意”消息中。

[0055] 根据此处考虑的一个或多个实施例,用户终端 14 将该消息的接收解释为已发生自举的指示,从而排除了联系 BSF 12 的需要。因此,用户终端 14 不联系 BSF 12 以进行自举,而是根据 GBA 过程,直接联系 NAF 30。图 10 示出了这种处理的一实施例。

[0056] 该方法不需要用户终端 14 处的改变,但有利地,该方法使得可以将 IMS-AKA 认证与 GBA-AKA 认证联结,这意味着可以响应于 IMS 注册而自动自举(或完成)GBA-AKA 认证,而对 IMS 注册几乎没有影响。

[0057] 例如,用户终端 14 可以被配置为 IMS-GBA “融合”终端,其中,其被配置用于在用户终端 14 经历 IMS 注册之后,向 NAF 30 发信号通知标记或其他指示符。在这些实施例中,所述标记向 NAF 30 指示用户终端 14 已经经历了作为 IMS 注册的一部分的 IMS-AKA 认证,并且用户终端 14 发送 IMPU(IP 多媒体公开密钥标识)而不是尚未可用的 B-TID。进而,NAF 30 使用从用户终端 14 接收到的 IMPU 来联系 BSF 12,以取得对应的自举信息和 B-TID。在 HTTP 摘要之后,NAF 30 将 B-TID 发送至用户终端 14。

[0058] 在另一实施例中,BSF 12 被配置为充当 SIP AS,从而变为使用 IMS 服务标识可达。相应地,用户终端 14 被配置用于向 BSF 12 发出 SIP 消息(例如,SIP “邀请 (INVITE)”消息),以从 BSF 12 获得 B-TID,而无需任何自举。

[0059] 在另一实施例中,NAF 30 被配置为充当 SIP AS,分配了 IMS 服务标识。采用该配置,NAF 30 是用户终端 14 使用 SIP 信令可达的,并且,在一个或多个这样的实施例中,用户终端 14 被配置用于向 NAF 30 发送例如 SIP 邀请。当然,这种操作需要用户终端 14 处的 IMS-AKA/GBA-AKA 融合操作,并需要 NAF 30 能够获得认证密钥分发。

[0060] 尽管图 7-10 示出了在用户终端尝试访问需要 GBA-AKA 认证的服务之前进行 IMS 注册的示例,但是本领域技术人员应当理解,用户认证过程的共享可以由或基于首先进行的 GBA-AKA 认证触发。图 11 给出了针对以下情况的非限制性处理示例:用户终端 14 首先访问基于 GBA 的应用并稍后访问基于 IMS 的应用。

[0061] 在示意中可见,用户终端 14 可以被配置用于呈现其已经通过经历成功的 GBA 自举、作为 IMS 注册信息的一部分而获得的 B-TID。因此,在 S-CSCF 10 的一个或多个实施例中,其将在 IMS 注册过程期间从用户终端 14 接收到 B-TID 信息解释为用户终端已经经历了成功的 GBA-AKA 认证的指示。因此,S-CSCF 10 联系 BSF 12,以核实自举信息并从 BSF 12 获得 AV。该过程排除了 S-CSCF 10 对用户终端 14 进行显示认证的需要,并且 S-CSCF 10 将

简单地将“同意 (OK)”消息返回给用户终端 14。

[0062] 无论 IMS-AKA 认证在时间上是最先的、是位于 GBA-AKA 认证之后、还是相反,此处的教导都提供了用于在 IMS 域中的认证实体与 GBA 域中的认证实体之间共享用户认证信息的方法和设备。这种共享减少或消除了用于对相同用户终端 14 进行 IMS-AKA 和 GBA-AKA 认证的冗余认证操作。

[0063] 此外,此处考虑的认证信息共享的一个或多个实施例包括 AKA 矢量导出。例如, S-CSCF 10 可以从 HSS 32 获得用于 IMS-AKA 认证的 AKA 矢量。如先前教导的, S-CSCF 10 可以向 BSF 12 传送 AKA 矢量 (即,发送副本),以由 BSF 12 在 GBA-AKA 认证中使用。然而,在一个或多个其他实施例中, S-CSCF 10 根据从 HSS 32 获得的 AKA 矢量来产生导出的 AKA 矢量,并向 BSF 12 传送导出的 AKA 矢量,以由 BSF 12 在对用户终端 14 的 GBA-AKA 认证中使用。

[0064] 对导出的 AKA 矢量的使用增强了 IMS-GBA 域分离度,但仍消除了 S-CSCF 10 和 BSF 12 从 HSS 32 获得单独 AKA 认证矢量的需要。当然,可以实施对该技术的变型。例如, S-CSCF 10 可以将其从 HSS 32 获得的 AKA 矢量传送至 BSF 12,然后,BSF 12 可以被配置用于产生导出的 AKA 矢量。此外,可以在反方向上应用相同技术。即,BSF 12 可以从 HSS 32 获得 AKA 矢量,然后将该 AKA 矢量传送至 S-CSCF 10,或者,其可以传送导出的 AKA 矢量。如果 S-CSCF 10 接收到 HSS 产生的 AKA 矢量,则其可以使用该 AKA 矢量来直接对用户终端 14 进行 IMS-AKA 认证,或者,其可以被配置用于从所传送的矢量导出 AKA 矢量。

[0065] 在所有情况下,用户终端 14 可以被配置用于互补操作。即,用户终端 14 在某种意义上“知道”S-CSCF 10 与 BSF 12 之间的矢量共享配置,并相应地进行动作。如果 S-CSCF 10 和 BSF 12 分别针对 IMS-AKA 认证和 GBA-AKA 认证使用相同的 AKA 矢量,则用户终端 14 也是这样。相反,如果 S-CSCF 10 和 BSF 12 之一使用 HSS 产生的 AKA 矢量,而另一个使用导出的 AKA 矢量,则用户终端 14 也是这样。在这一点上,可以利用相同矢量导出算法来配置用户终端 14,使得其可以在需要时产生用于认证的适当的导出 AKA 矢量。

[0066] 概括地说,此处的教导提出了一种融合的 IMS 核心和 GBA 基础设施配置,提供了在 IMS 和 GBA 域之间对认证过程、参数和基础设施的重用,从而减少了网络运营商的 CAPEX 和 OPEX。在一个或多个实施例中,这种共享是经由融合的 IMS 核心和 3GPP GBA 基础设施来实现的,其中共享了会话管理、高效认证和密钥管理。该方法重用了 IMS 和 GBA 域之间的公共认证功能和组件。在支持这些功能和特征的情况下,例如 IMS 域 S-CSCF 10 与 GBA 域 BSF 12 之间的新接口提供了对用户认证信息的共享。

[0067] 在了解这些较概括的要点的情况下,应当理解,以上描述和附图表示此处教导的方法、系统和各个设备的非限制性示例。由此,本发明不限于以上描述和附图。本发明仅由权利要求书及其法律等价物所限定。

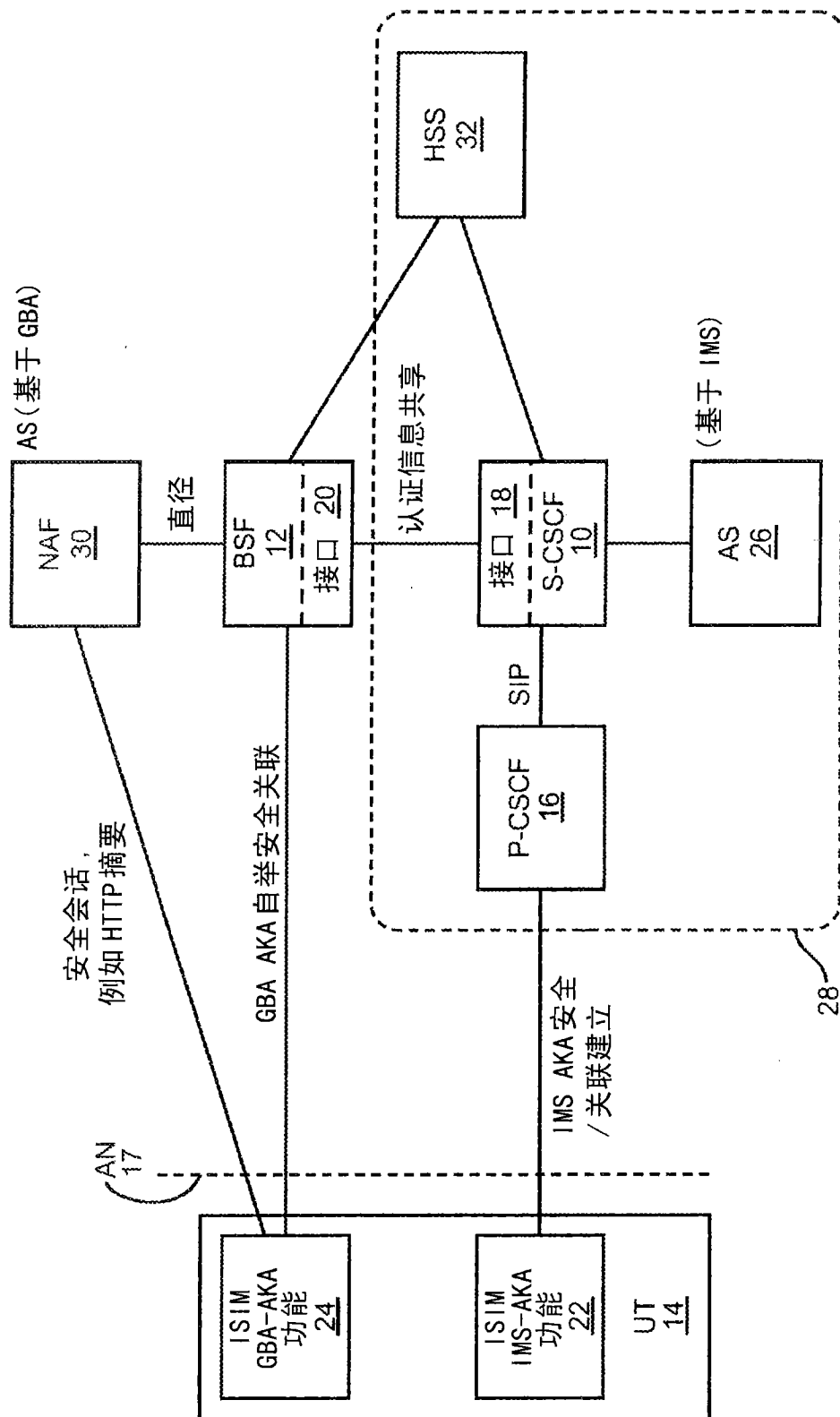


图 1

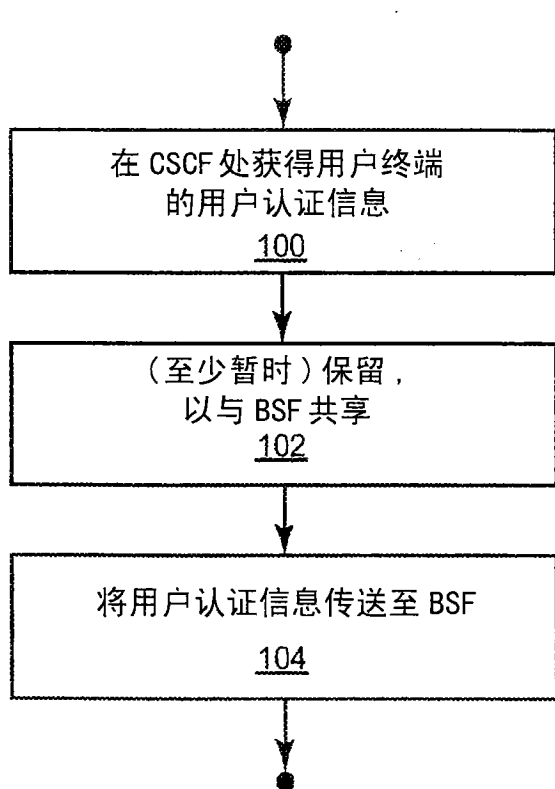


图 2

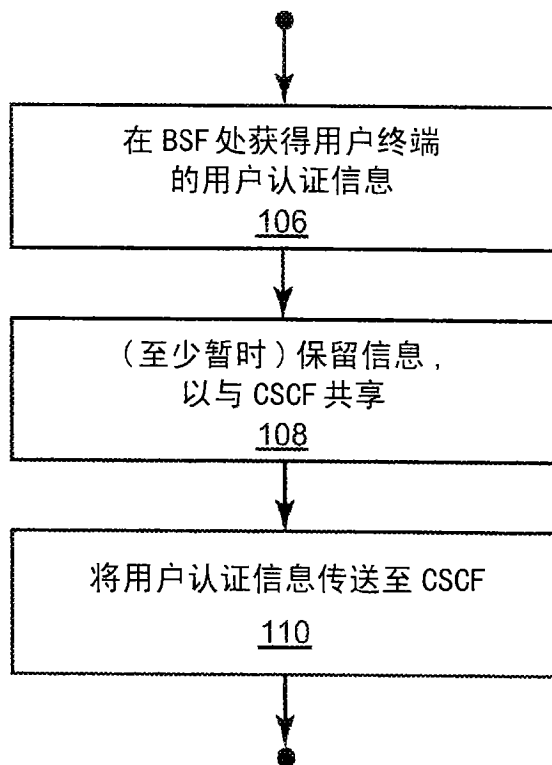


图 3

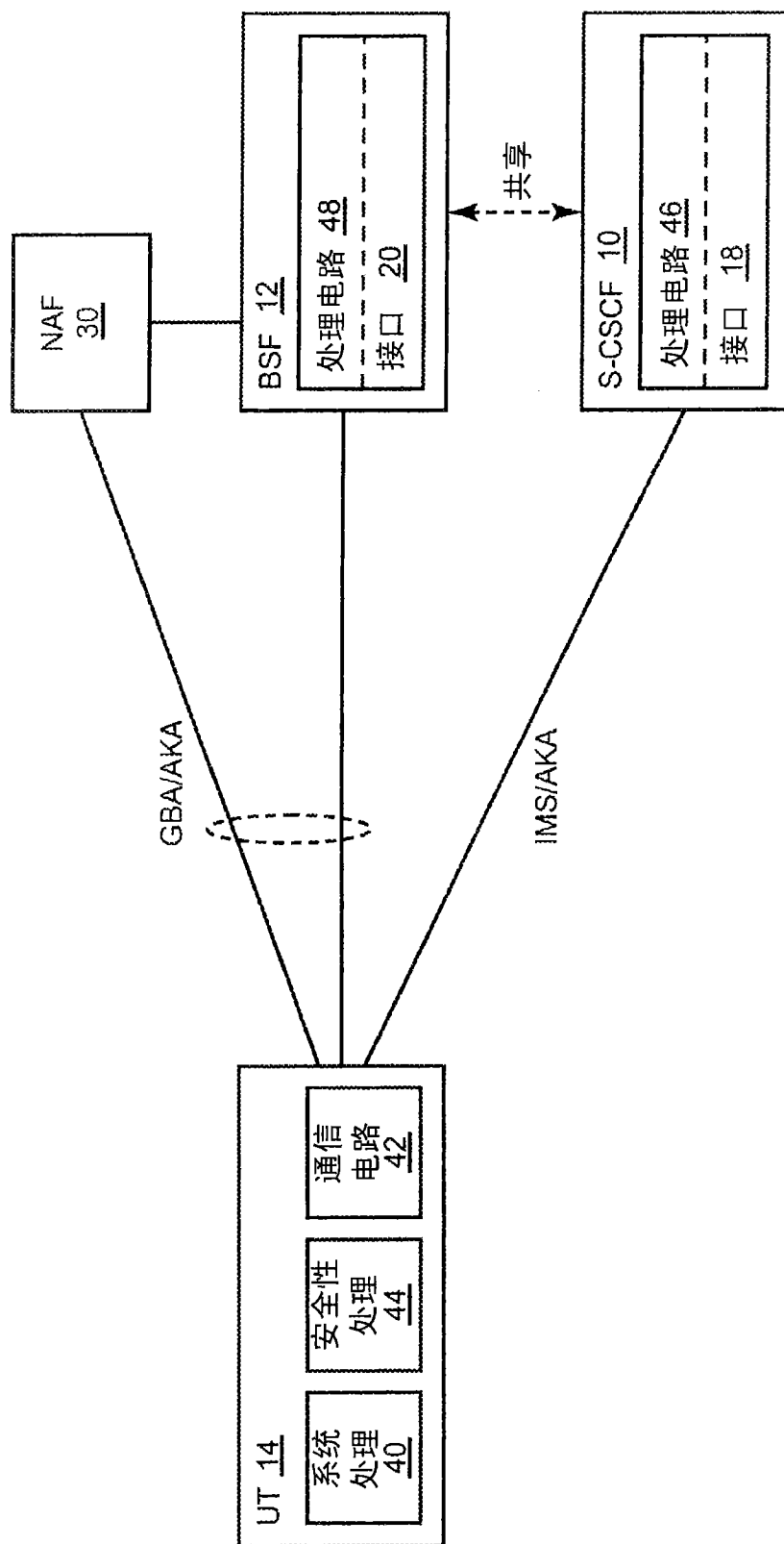


图 4

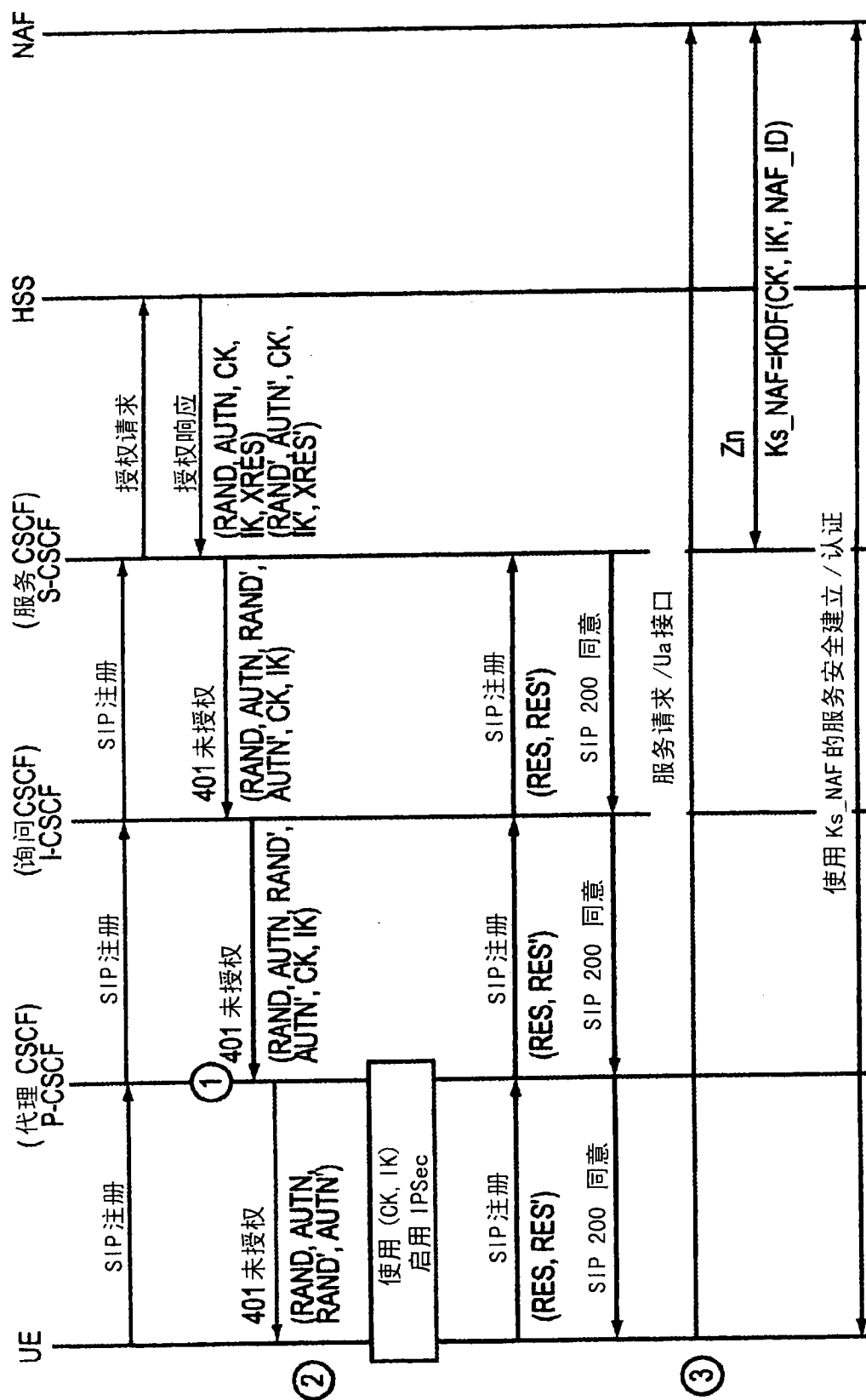


图 5 现有技术

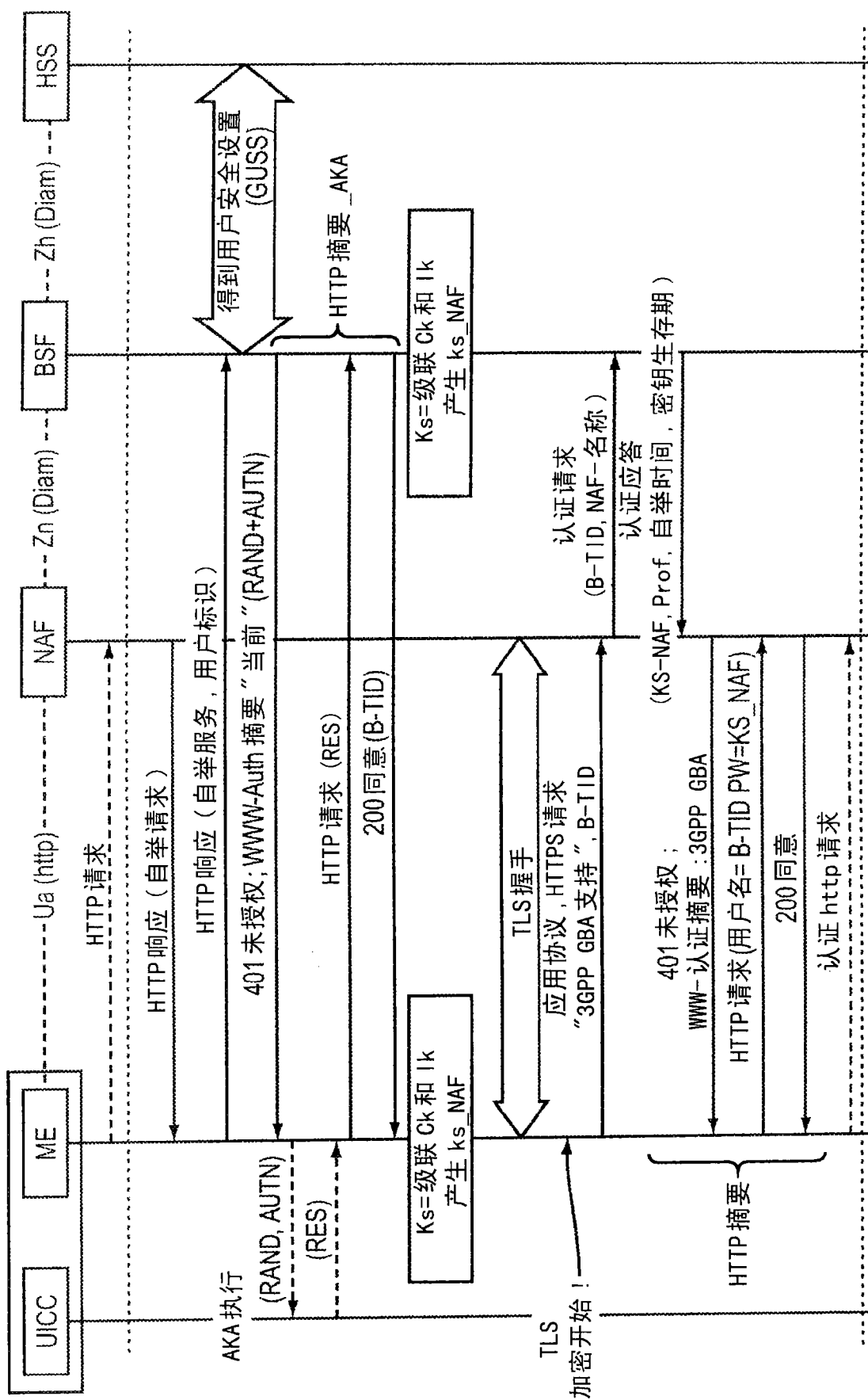


图 6 现有技术

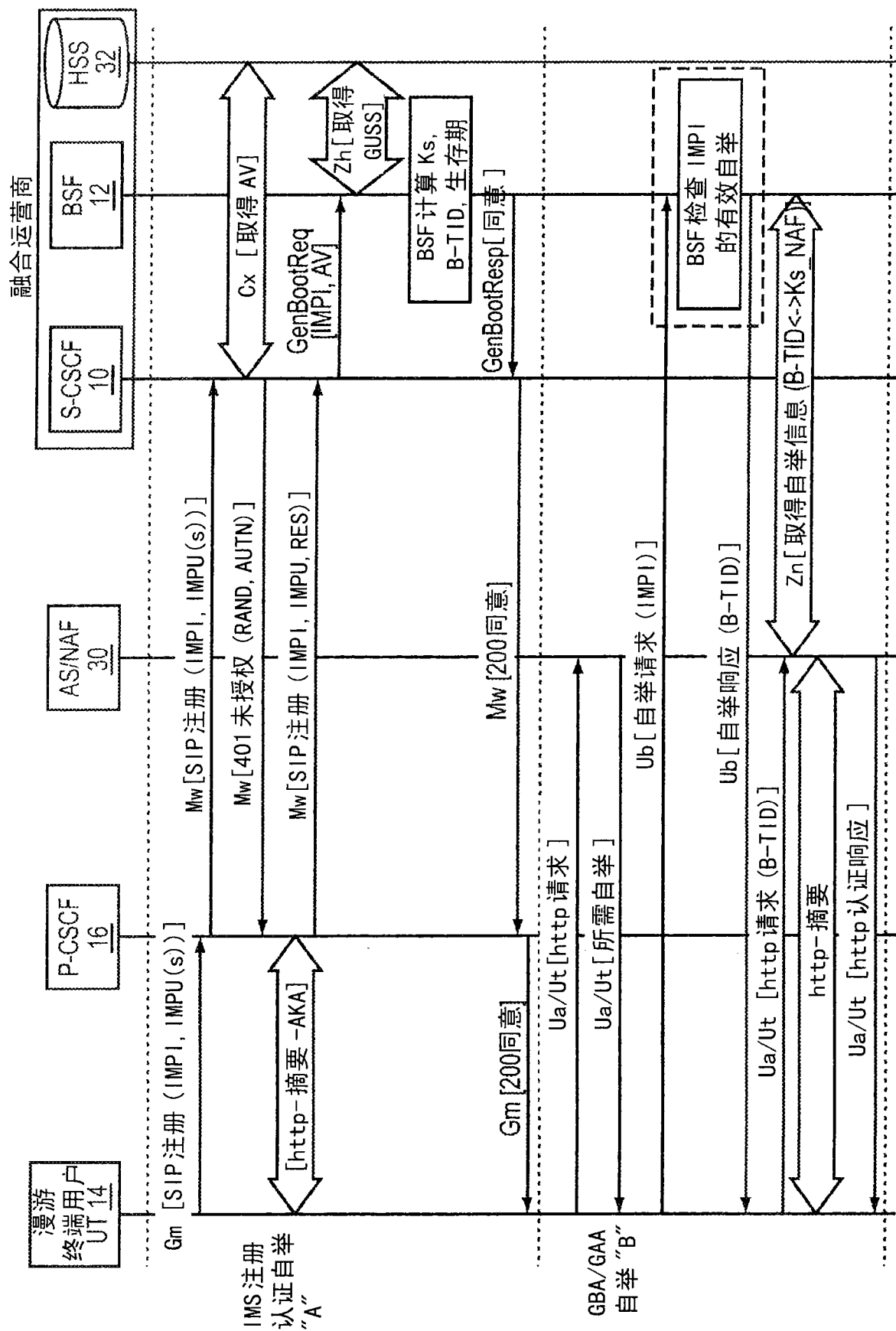


图 7

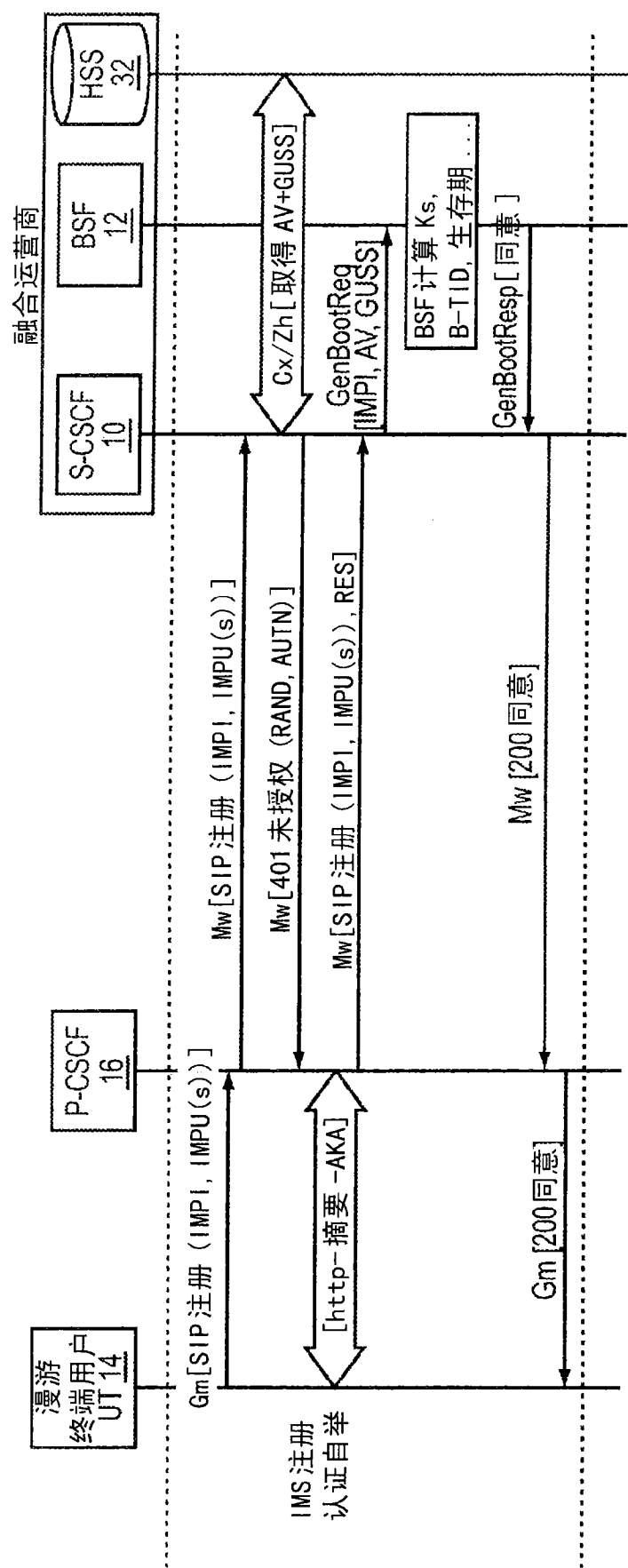


图 8

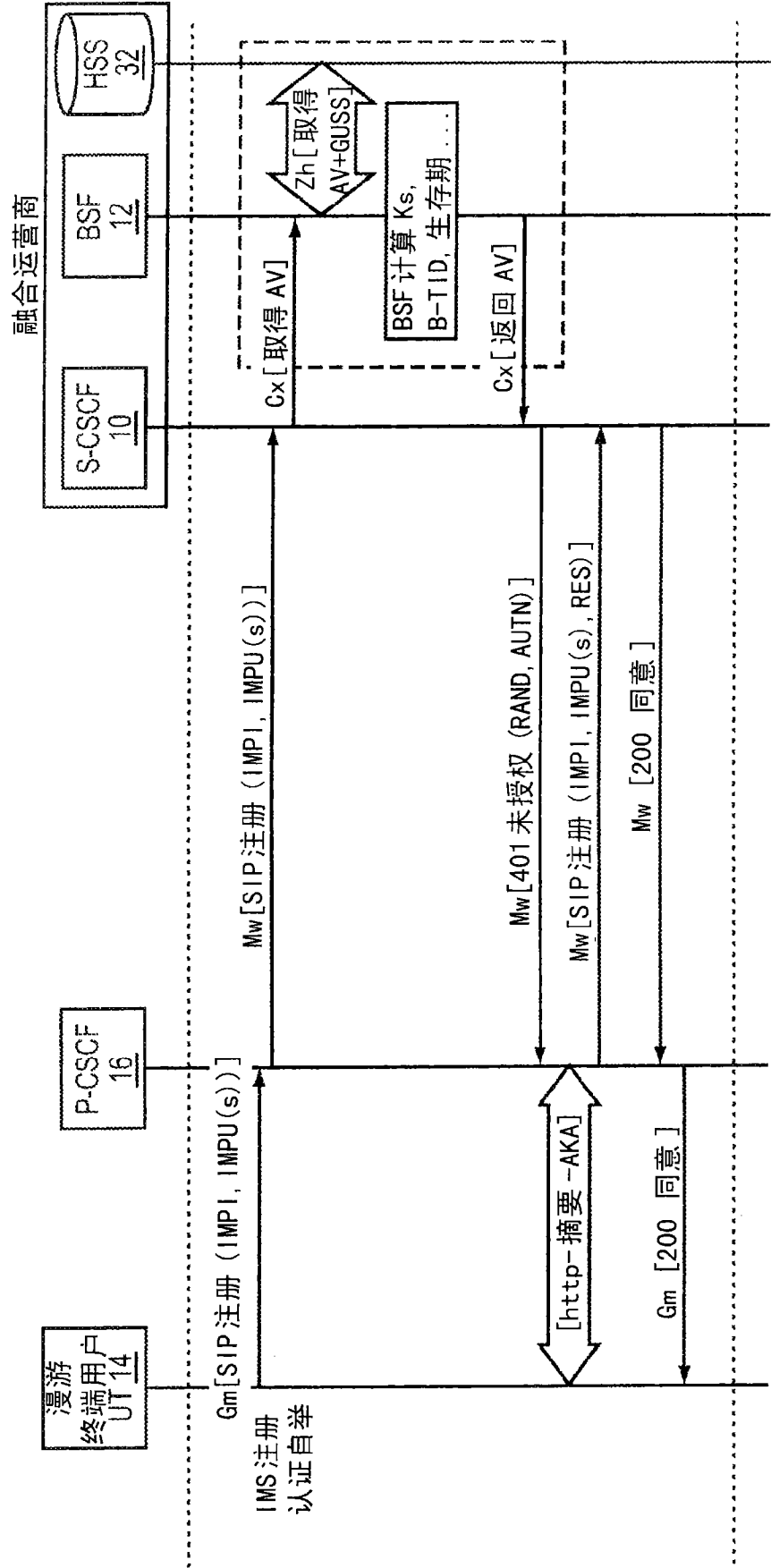


图 9

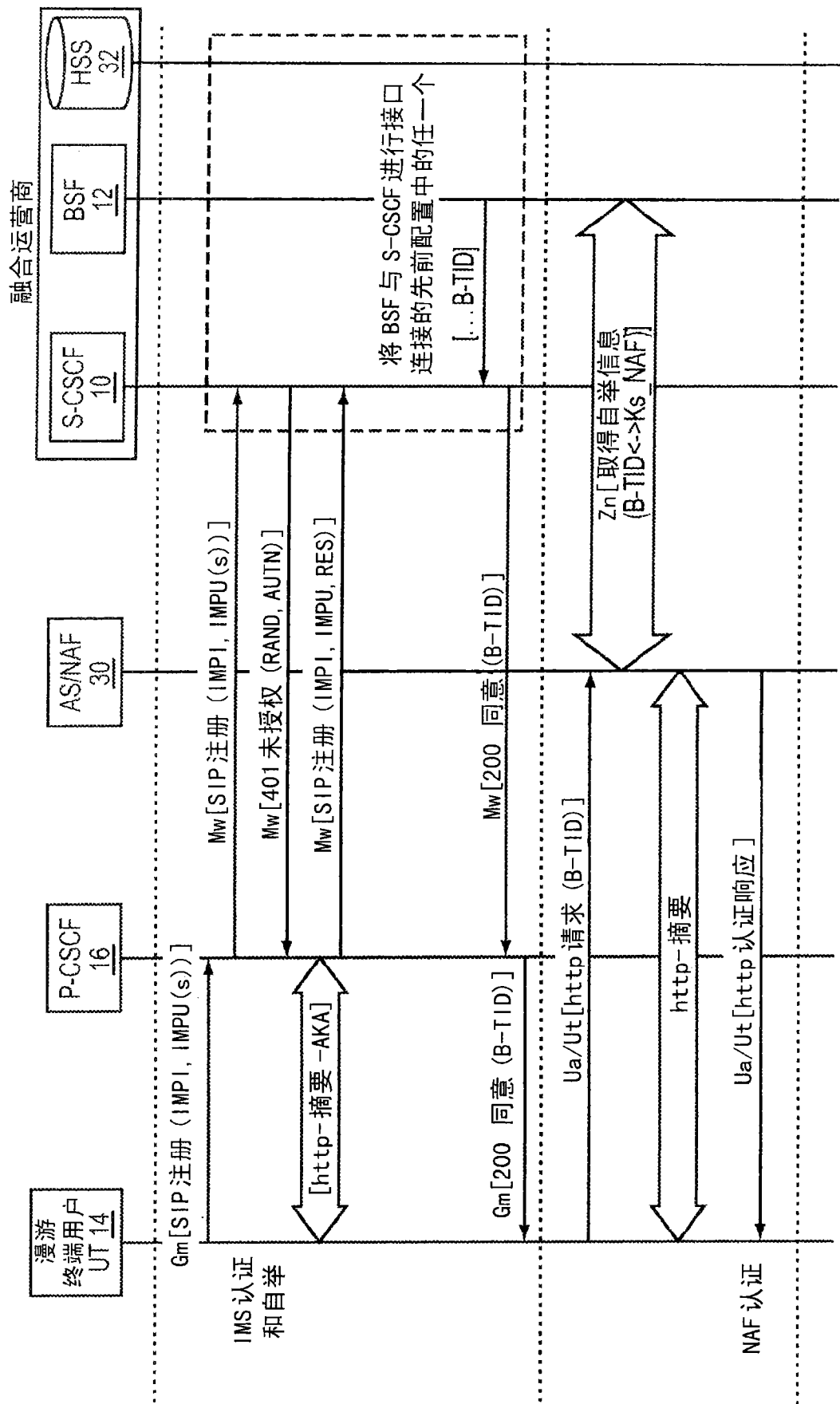


图 10

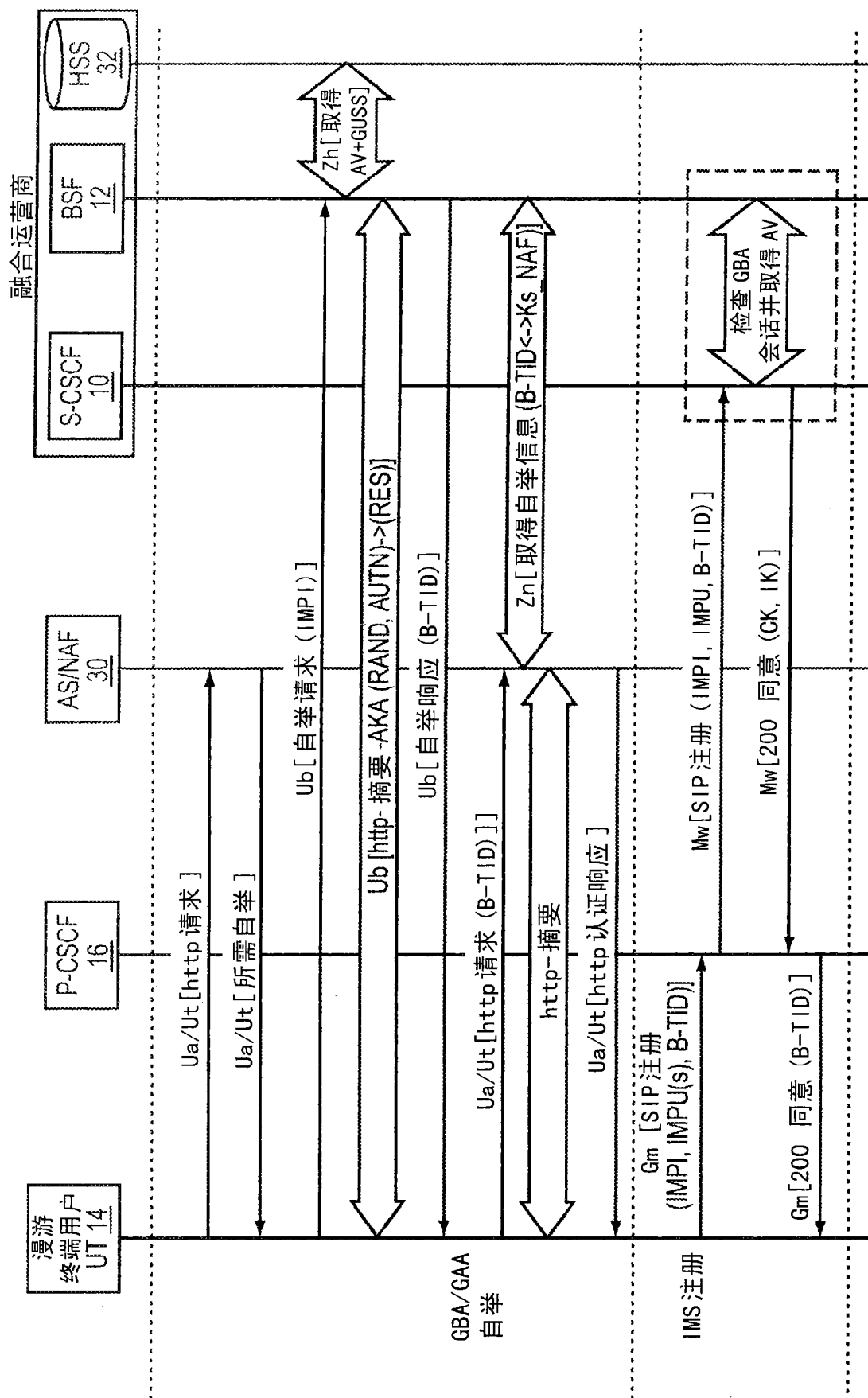


图 11