



[12] 发明专利申请公开说明书

[21] 申请号 01823415.1

[43] 公开日 2004 年 8 月 18 日

[11] 公开号 CN 1522525A

[22] 申请日 2001.6.27 [21] 申请号 01823415.1

[86] 国际申请 PCT/EP2001/007345 2001.6.27

[87] 国际公布 WO2003/003690 英 2003.1.9

[85] 进入国家阶段日期 2003.12.26

[71] 申请人 诺基亚有限公司

地址 芬兰埃斯波

[72] 发明人 T·胡尔塔

[74] 专利代理机构 中国专利代理(香港)有限公司

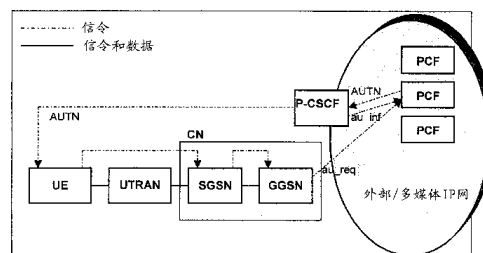
代理人 栾本生 罗 朋

权利要求书 3 页 说明书 6 页 附图 1 页

[54] 发明名称 用于无线通信网中承载授权的方法和系统

[57] 摘要

本发明涉及用于在无线通信网中的承载授权的方法和系统,包括在所述无线通信网的应用层的控制功能(PCF)中产生一个授权绑定信息,分配一个代表控制功能在所述无线通信网中的实际地址的控制功能标识符并且把所述标识符包括到所述授权绑定信息中,传输所产生的授权绑定信息到具有到所述无线通信网的接入的一个终端设备(UE),以及通过基于包括在所述授权绑定信息中的控制功能标识符而导出所述控制功能的实际地址来完成通过所述无线通信网的传送层对所述终端设备的所述承载授权,其中授权绑定信息已经在所述无线通信网中从所述控制功能中产生。这样,在发送实际控制功能地址到终端设备或用户设备中涉及的固有安全风险被消除,并且授权绑定信息的规模被减小。



1. 一种用于在包括应用层和传送层的无线通信网中的承载授权的方法，该方法包括步骤：
 - a) 在所述应用层的控制功能中产生一个授权绑定信息；
 - 5 b) 分配代表所述控制功能在所述无线通信网中的实际地址的控制功能标识符并且把所述标识符包括到所述授权绑定信息中；
 - c) 传输所产生的授权绑定信息到一个具有到所述无线通信网的接入的终端设备；以及
 - d) 通过基于包括在所述授权绑定信息中的控制功能标识符而导出
10 所述控制功能的实际地址来完成通过所述无线通信网的所述传送层对所述终端设备的所述承载授权，其中授权绑定信息已经在所述无线通信网中从所述控制功能中产生。
2. 根据权利要求1的方法，其中所述标识符被安排采用一个选自预定数值范围内的数字整数值。
- 15 3. 根据权利要求1或2的方法，其中所述授权绑定信息包括一个授权令牌，其产生是通过从无线通信网中的代理呼叫状态控制功能（P-CSCF）传输授权信息到所述无线通信网中的多个策略控制功能之一而被启动的。
4. 根据权利要求3的方法，其中产生的授权令牌被发送到所述
20 代理呼叫状态控制功能并且通过所述代理呼叫状态控制功能被转发到所述终端设备。
5. 根据任何一个前述的权利要求的方法，其中所述授权绑定信息从所述终端设备被发送到所述传送层中的一个节点。
6. 根据权利要求5的方法，其中所述节点是服务 GPRS 支持节点，而且授权绑定信息还被从所述服务 GPRS 支持节点传送到所述传送层中的网关 GPRS 支持节点。
- 25 7. 根据权利要求5的方法，其中所述节点适合从包括在所述授权绑定信息中的控制功能标识符来导出在所述无线通信网中的实际控制功能地址。
8. 根据权利要求7的方法，其中所述节点适合从具有所述导出的实际地址的控制功能中请求授权。
- 30 9. 根据权利要求7的方法，其中由所述节点通过使用控制功能

标识符和相应的地址的一个接入点特定列表来执行所述地址导出。

10. 根据权利要求6的方法,其中所述网关 GPRS 支持节点适合从包括在所述授权令牌中的策略控制功能标识符导出在所述无线通信网中的所述实际策略控制功能地址并且从具有导出的实际地址的策略控制功能中请求授权。

11. 根据权利要求10的方法,其中由所述网关 GPRS 支持节点通过使用策略控制功能标识符和相应的地址的一个接入点特定列表来执行所述地址导出。

12. 一种用于在无线通信网中的承载授权的系统,包括:

- 10 a) 用于在所述无线通信网的一个应用层中提供的控制功能(PCF)中产生授权绑定信息的装置;

b) 用于分配代表所述控制功能在所述无线通信网中的实际地址的控制功能标识符并且用于把所述标识符包括到所述授权绑定信息中的装置;

- 15 c) 用于传输所产生的授权绑定信息到具有到所述无线通信网的接入的终端设备(UE)的装置;以及

- d) 用于通过基于包括在所述授权绑定信息中的控制功能标识符而导出所述控制功能的实际地址来完成通过所述无线通信网的传送层对所述终端设备的所述承载授权的装置,其中授权绑定信息已经在所述无线通信网中从所述控制功能中产生。

- 20 13. 根据权利要求12的系统,其中所述标识符是一个选自预定数值范围的数字整数值。

14. 根据权利要求12或13的系统,其中所述授权绑定信息包括一个授权令牌,其产生是通过在一个核心网中的代理呼叫状态控制功能(P-CSCF)传输授权信息到所述无线通信网中的多个策略控制功能之一而被启动的。

15. 根据权利要求14的系统,其中所述策略控制功能被安排把产生的授权令牌发送回所述代理呼叫状态控制功能,所述代理呼叫状态控制功能被安排把该令牌转发到所述终端设备,所述终端设备被安排把该令牌传送到所述核心网内的服务 GPRS 支持节点(SGSN),并且所述服务 GPRS 支持节点被安排把该令牌发送到所述核心网内的网关 GPRS 支持节点(GGSN)。

16. 根据权利要求 15 的系统，其中所述网关 GPRS 支持节点被安排从包括在所述授权令牌中的策略控制功能标识符导出在所述无线通信网中的所述实际策略控制功能地址并且从具有导出的实际地址的策略控制功能中请求授权 (au-req)。

- 5 17. 根据权利要求 16 的系统，其中所述网关 GPRS 支持节点被安排使用策略控制功能标识符和相应的地址的一个接入点特定列表来执行所述地址导出。

用于无线通信网中承载授权的方法和系统

技术领域

- 5 本发明涉及为在无线通信网如通用移动通信系统（UMTS）网中承载授权提供改进的安全性的一种方法和系统。

背景技术

- 全球移动通信系统（GSM）的数据业务已经开始了移动通信的新时代。早期的模拟蜂窝调制解调器由于它是缓慢和不可靠的，已经对市场没有吸引力了。现在，数据市场正在向前（更多的突发）和向上（更多的通信量）发展，并且标准化协会正在为更高的数据率，而且更重要的还为分组数据业务工作。因为数据通过网络被更有效地发送并且因此降低了费用，而且还减少了接入时间，所以这必将扩展对终端用户
- 10 的吸引力。

- 15 因为在数据应用中一般倾向是产生日益增加的突发数据流，这导致低效率使用电路交换连接。此外，固定网已经看到不仅仅因为互联网接入要求的增长而带来的数据通信量的巨大增长，这样以致假定移动网将因为技术和用户预期的前进而扩展。现在的 GSM 交换网是基于窄带 ISDN（综合业务数字网）电路，所以速率限制原因从接入网移动到核心网。
- 20

- 新的通用分组无线电业务（GPRS）网将为话务员提供使用分组计费的能力，并且支持数据传送以高达八倍时隙无线电接口容量通过高速网。GPRS 在 GSM 网中引进两个新节点，一个服务 GPRS 支持节点（SGSN）和一个网关 GPRS 支持节点（GGSN）。SGSN 记录在它的服务
- 25 区内的移动终端的位置并且向/从移动终端发送和接收分组，把它们传送到 RNC（无线网络控制器）或者 GGSN。GGSN 从外部网络接收分组，把它们传送到 SGSN，或者从 SGSN 接收分组，把它们传送到外部网络。

- UMTS（通用移动通信系统）将直接给人们传递高级信息并且给他们提供到新的和革新的业务的接入。它将给大量市场提供人格化的移动通信，而与位置、网络或者使用的终端无关。
- 30

如在 3GPP 规范 TS23 060 中定义的，按照 99 年发布的 3GPP（第

三代伙伴关系规划)，在通用分组域结构和传输机制中，提供移动蜂窝业务的电信网络，如一个公用陆地移动通信网（PLMN），具有用于移动接入以及消息始发或者接收的接入点、参考节点和接口。此外，无论何时在业务请求的执行中涉及分组交换 PLMN 和任何其它网络，如

5 基于互联网协议（IP）的网络，都需要网络互通。

在下文中，术语应用层将被用于指定一个 IP 子系统，例如一个 IP 多媒体子系统，其中包括一个 P-CSCF（代理呼叫状态控制功能）和多个 PCF（策略控制功能）。基于移动网络结构的 IP 包括一个应用层和一个传送层。为了特定的接入类型，传送层协议和机制通常被优化，

10 而应用层通常是一般的，这与接入类型无关。在应用层中建立一个会话中，基础传送层必须在无线电接口上和传送网中建立传送承载。

在网络和互通中，这种网络结构中必要的控制功能是完成识别和认证业务请求者以及确认业务请求类型以确保业务请求者被授权使用特定的网络业务的认证和授权功能。

15 因为一个应用所要求的服务质量需要超过“最大努力”业务的特别授权，所以需要承载授权是在这个上下文中一个特定的需要。IP 多媒体是这种应用的一个例子。

在 3GPP 中，正在为 IP 多媒体承载授权而规定有关策略控制，使得相对于一个正在进行的多媒体会话来授权一个分组数据协议（PDP）

20 上下文。同时，为了该目的已经批准了 GGSN 和 PCF 之间的一个接口。

为了映射 PDP 上下文到 IP 多媒体会话，已经提议使用一个授权令牌（AUTN）作为一个绑定信息。现在，这个 AUTN 打算是由互联网工程任务组（IETF）在到 SIP 的授权方案扩展内规定的会话启动协议（SIP）参数。

25 在 3GPP 中，现在考虑在代理呼叫状态控制功能（P-CSCF）中协同定位 PCF，在 3GPP UMTS 版本 5 规范中就是这样。然而，如果在这个规范的将来版本中，PCF 作为一个单独实体来实现，则在一个外部网络中存在多个 PCF 时，正确的 PCF 确定可能是有问题的。

为了解决这个问题，还提议分配 PCF 地址作为发送到用户设备

30 （UE）的 AUTN 的一部分。然而，特别在其中 SIP 应用驻留在一个终端设备（TE）如一台便携式电脑中的情况下，发送 PCF 地址到 UE 可能代表一个安全风险。特别的，随后行为失常的 UE 可以通过不断给它发送

授权请求而堵塞 PCF。

发明内容

因此，本发明的一个目的是提供用于承载授权的方法和系统，它为业务接入授权提供改进的安全性。

- 5 根据本发明，通过根据权利要求 1 的方法以及通过根据权利要求 7 的系统达到这个目的。

本发明更有利的发展是附加的从属权利要求的主题。

- 因此，在包括一个应用层和一个传送层的无线通信网中，承载授权由下述步骤完成：a) 在所述应用层的控制功能中，例如，在出自多个策略控制功能的一个策略控制功能中或者在出自多个应用服务器/代理的一个应用服务器/代理，例如，在所述无线通信网中提供的一个 P-CSCF 中产生一个授权绑定信息，b) 分配一个代表所述控制功能在所述无线通信网中的实际地址的控制功能标识符并且把所述标识符包括到所述授权绑定信息中，c) 传送这样产生的授权绑定信息到一个终端设备，例如，具有到所述无线通信网接入的用户设备，以及 d) 通过基于包括在所述授权绑定信息中的控制功能标识符而导出所述控制功能的实际地址来完成通过所述无线通信网的传送层对所述终端设备的所述承载授权，其中授权绑定信息已经在所述无线通信网中从所述控制功能中产生。
- 10 15

- 20 优选地，标识符被安排采用选自预定的数值范围一个数字整数值。

- 授权绑定信息可以从终端设备被发送到一个传送层中的节点。该节点可以是一个服务 GPRS 支持节点，其中，授权绑定信息还从服务 GPRS 支持节点被发送到传送层中的网关 GPRS 支持节点。该节点可以适合从包括在授权绑定信息中的控制功能标识符导出在无线通信网中的实际控制功能地址。而且，该节点可以适合从具有导出的实际地址的控制功能中请求授权 (au-req)。
- 25

- 更优选地，该授权绑定信息是一个授权令牌，其产生是通过从无线通信网的应用层中的应用服务器/代理传送授权信息到无线通信网中的多个策略控制功能之一而被启动的。
- 30

在一个有利的结构中，产生的授权令牌被发送回应用服务器/代理，通过该应用服务器/代理被转发到终端设备，通过该终端设备被传

送到无线通信网的传送层，例如到传送层内的服务 GPRS 支持节点 (SGSN)，并且从服务 GPRS 支持节点传送到传送层内的网关 GPRS 支持节点 (GGSN)。

因此，无线通信网的传送层，例如，网关 GPRS 支持节点，适合从
5 包括在授权令牌中的控制功能标识符中导出在无线通信网中的实际控制功能地址并且从具有导出的实际地址的控制功能中请求授权。

特别优选和有利的，网关 GPRS 支持节点通过使用策略控制功能标识符和相应的地址的接入点特定列表来完成地址导出。

根据本发明在无线通信网中的承载授权系统有利地包括相同的组成单元，并且因此提供相同的作用和利益。
10

附图说明

在下文中，根据优选实施方案并且参考附图将更详细地描述本发明，其中：

图 1 用示意图显示其中能够实现本发明的通用分组域结构的部分框图；以及
15

图 2 以简化的方式表示根据本发明的一个实施方案使用授权令牌的 IP 多媒体承载授权的原理。

优选实施方案的描述

图 1 用示意图显示公用陆地移动网 (PLMN) 的通用分组交换域结构的部分框图，其包括例如基于 UMTS 的无线电接入系统，其中作为选择或者附加地为多个无线电技术的用户设备 (UEs) 提供到基于 UMTS 的核心网的接入的无线电接入技术而引进了多个独立的宽带无线接入网。
20

在该优选实施方案中，传送层包括一个 GPRS 系统和由 PDP (分组数据协议) 上下文提供的 IMS 会话承载。因此，该绑定信息 (AUTH) 正绑定传送层承载和 IMS 会话。
25

无论何时在业务请求执行中涉及分组交换域 PLMN 和任何其它网络，如基于互联网协议 (IP) 的一个网络，就需要网络互通。这种互通分别通过一个到固定网参考点 Gi 的 PLMN 和一个在 PLMN 接口之间连接两个独立的 PLMN 的 Gp 接口被建立。
30

一个公用分组交换域核心网 (CN) 提供分组交换 (PS) 业务并且被设计支持不同的服务质量等级以允许有效传送非实时业务，如间歇

性和突发数据传送或者偶尔传输大数据量，以及实时业务如语音或视频。

基本上包括一个终端设备 (TE) 和一个移动终端 (MT) 的一个服务 GPRS 支持节点 (SGSN) 构成个人移动站 (MS) 的附着点，记录它的位置并且执行安全功能和接入控制。SGSN 通过一个 Iu 接口被连接到 UMTS 陆地无线电接入网 (UTRAN) 并且通过一个基于 IP 的 PLMN 内部主干网 (Gn 接口) 被连接到网关 GPRS 支持节点 (GGSN)。在 PDP 上下文激活中，SGSN 用 GGSN 和 UTRAN 建立用于路由选择目的的 PDP 上下文，即在一个用户将使用的 UTRAN 中的无线网络控制器 (RNC)。随后，GGSN 提供与外部分组交换网的互通。GGSN 可以通过 PLMN 内部或者 PLMN 之间的主干网被连接到多个 SGSN。

如上所述，为了接入 PS 业务，也就是发送和接收 PS 数据，MS 必须使 SGSN 激活适当的 PDP 上下文，以使能够启动与外部数据网的互通之前，SGSN 知道 MS。可适用的 PDP 上下文有关操作同样在 3GPP 规范 TS23 060 中被定义。在互通期间，通过给数据分组装备 PS 特定协议信息以及用封装和隧道传送它们，用户数据随后在 MS 和外部数据网，即 GGSN 或 MS 之间被透明传送。

因此，在 GGSN 和 P-CSCF 之间执行为互通的初始授权协商准备。

现在参考图 2 将描述本发明的一个优选实施方案。

图 2 用示意图显示图 1 的通用分组交换域结构方案，在 P-CSCF 中，策略控制功能 (PCF) 被增加或者协同定位。用虚线内相应的箭头指示信令流方向。

根据图 2，在至少一个外部网络中提供了多个 PCF 并且被安排和分组交换核心网中的 P-CSCF 及 GGSN 通信。另外，在 P-CSCF 和 UE 之间、UE 和 SGSN 之间以及 SGSN 和 GGSN 之间信令通信被建立。

在和外部网络中已有的多个 PCF 的操作中，P-CSCF 发送授权信息 (au-inf) 到那些 PCF 之一。在对其的应答中，通过编址的 PCF 在应用层中产生一个授权令牌 (AUTN)，授权请求已经基于由 P-CSCF 转发的授权信息被发送到所述编址的 PCF，并且被发送回 P-CSCF 以作为授权信息而向 UE 被发送。

现在，如果和在常规方案中一样 PCF 地址被分配作为 AUTN 的一部分，并且因此其中包括，发送 AUTN 到 UE 涉及还发送 PCF 地址到 UE，

则导致上面提及的固有安全风险。

根据该优选实施方案，PCF 标识符被分配给外部网络中的每个 PCF。PCF 标识符是一个数字整数值如 1、2、3 等。当 PCF 随后产生一个 AUTN 时，PCF 分配这个 PCF 标识符作为 AUTN 的一部分来替代 PCF 地址并且发送 AUTN 到 P-CSCF，后者进而又把它转发到 UE。

有利地，使用 PCF 标识符替代全部 PCF 地址（或者 IP 地址）也减少令牌规模，并且因此通过减少传输负荷而提供提高的操作效率或者允许将另外的信息包括到相同规模的令牌中。

由于给予 UE 的信息只包括 PCF 标识符值，所以 UE 不能从接收的 AUTN 中确定当前的 PCF 地址，因此，消除在发送 PCF 地址到 UE 中固有地涉及的安全风险。

按照下文完成恢复正确的 PCF 地址。在已接收到 AUTN 后，当建立用于一个 IP 多媒体会话的所述承载或多个承载时，UE 通过用于数据传送的传送层的传送信道把 AUTN 发送到 SGSN。SGSN 随后把 AUTN 转发到和外部网络通信的 GGSN。

根据本发明，GGSN 包括一个有效的 PCF 标识符和相应的 PCF 地址的接入点特定列表。一旦接收包括 PCF 标识符的 AUTN，GGSN 就能够从 PCF 标识符导出正确的 PCF 地址，并且因此发送一个授权请求（au_req）到正确的 PCF，也就是较早发布 AUTN 的一个。

应当理解，本发明不要求使用 SIP，而是适用于应用层的任何信令协议，其被用于在其中在信令消息中可能携带各自的消息内容的外部（IP）网络上建立应用会话。

还应当指出，本发明不限于上述优选实施方案，而是也能在呼叫处理网络单元和其中授权绑定信息给一个应用会话提供用于绑定一个承载以建立授权连接的机制的任何网络中实现。因此，优选实施方案可以在附加的权利要求的范围内改变。

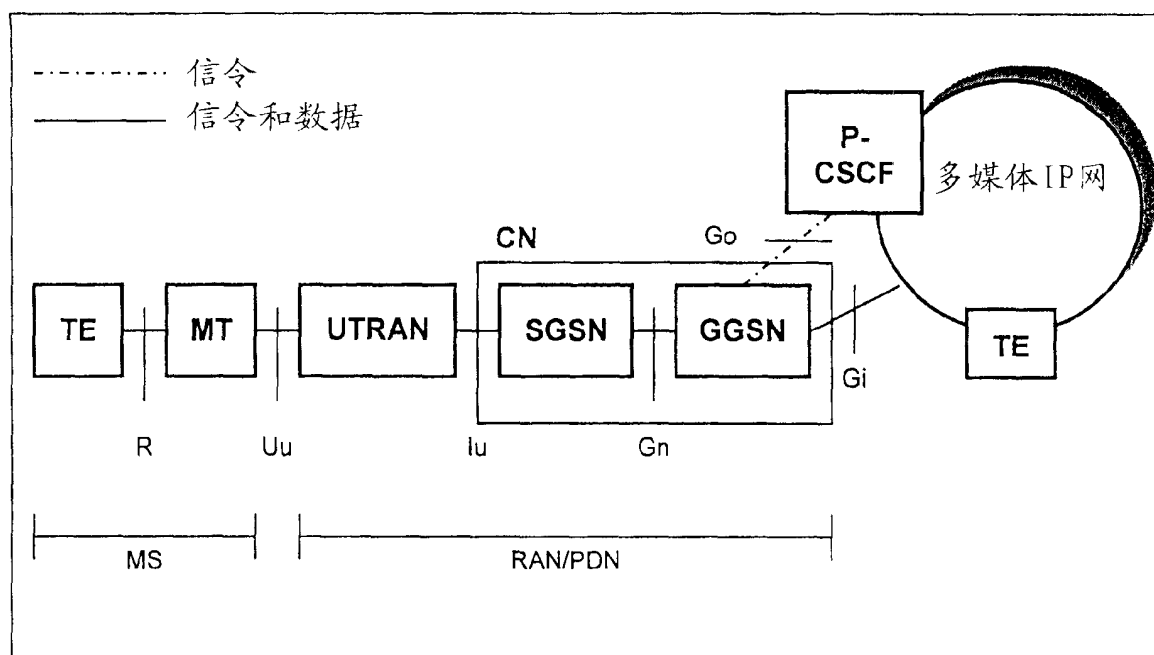


图 1

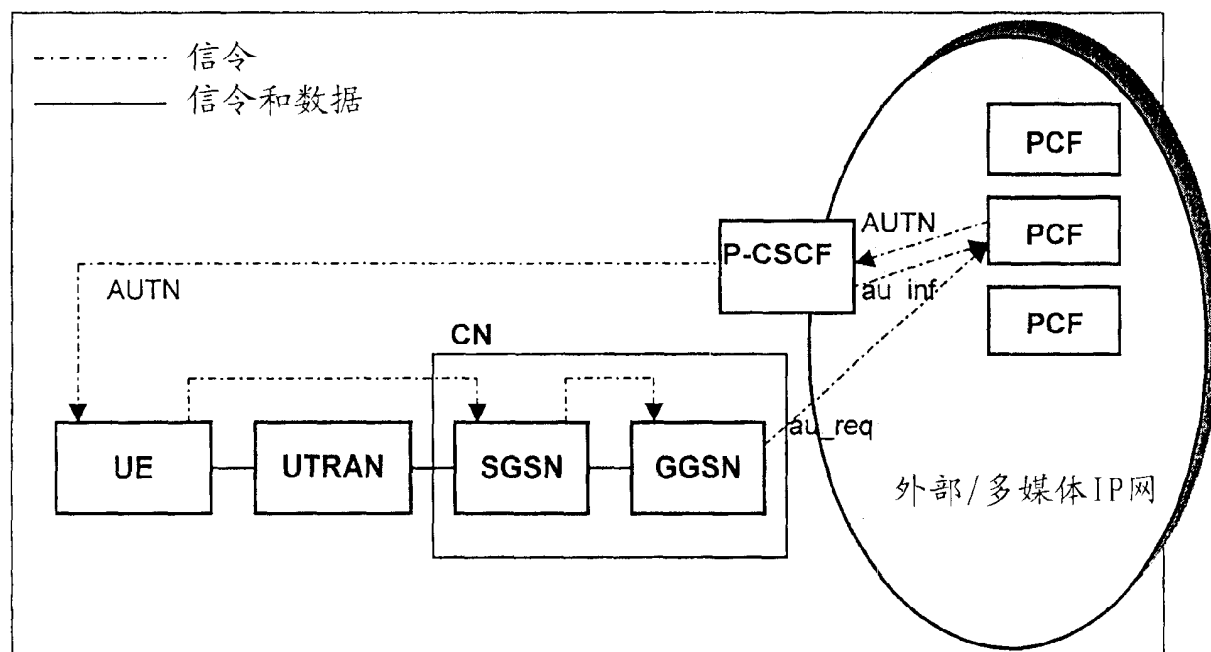


图 2