[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
H04Q 7/22
H04L 29/06

[12]发明专利申请公开说明书

[21]申请号 98803340.2

[43]公开日 2000年4月12日

[11]公开号 CN 1250578A

[22]申请日 1998.1.9 [21]申请号 98803340.2
[30]优先权
[32]1997.1.17 [33]US [31]08/784,152
[86]国际申请 PCT/SE98/00022 1998.1.9
[87]国际公布 WO98/32301 英 1998.7.23
[85]进入国家阶段日期 1999.9.14
[71]申请人 艾利森电话股份有限公司
地址 瑞典斯德哥尔摩
[72]发明人 M·诺尔德曼

[74]专利代理机构 中国专利代理(香港)有限公司
代理人 王 岳 李亚非

权利要求书4页 说明书12页 附图页数2页

[54]发明名称 用于接入专用数据通信网的安全接入方法及相关设备

[57]摘要

用于通过无线接入网(52)利用无线主机(32)接入专用IP网(14)的方法(152)及相关设备(10)。一旦验证并允许接入专用IP网(14),无线主机(32)变成专用IP网(14)的虚拟主机。无线主机识别符(WHI)用于识别无线主机(32)。利用验证程序(162)来确认允许利用无线接入网(52)的通信。此后,将WHI提供给专用IP网(14)。如果此WHI是所选的值,同意允许接入专用IP网(14)。一旦同意接入专用IP网(14),用于寻址数据的IP地址由专用IP网(14)分配给无线主机(32)。

ISSN1008-4274

权　利　要　求　书

1. 在专用数据通信网与远程通信站之间传送数据的方法中，专用数据通信网耦合到远程通信站形成其中一部分的无线通信系统的网络基础结构，由远程通信站接入专用数据通信网的一种改善的安全接入方法，所述方法包括以下步骤：

在存储位置上存储识别此远程通信站的远程通信站识别；

由远程通信站生成接入网络基础结构的请求，以允许通过此基础结构的数据通信；

在网络基础结构检测在所述生成步骤期间生成的请求；

验证此远程通信站，以确认此远程通信站利用网络基础结构通信的授权；

如果在所述验证步骤期间验证此远程通信站，将网络接入请求传送给专用数据通信网，利用在所述存储步骤期间存储的远程通信站识别来识别此远程通信站；

为响应在所述传送步骤期间传送的网络接入请求，确定是否允许此远程通信站接入专用数据通信网；和

如果在所述确定步骤期间确定允许此远程通信站接入专用数据通信网，允许此远程通信站接入此专用数据通信网。

2、在专用 IP（互联网协议）网与远程通信站之间传送数据的方法中，专用 IP 网耦合到远程通信站形成其中一部分的无线通信系统的网络基础结构，由远程通信站接入专用 IP 网的一种改善的安全接入方法，所述方法包括以下步骤：

在存储位置上存储识别此远程通信站的远程通信站识别；

由此远程通信站生成接入网络基础结构的请求，以允许通过此基础结构的数据通信；

在此网络基础结构检测在所述生成步骤期间生成的请求；

验证此远程通信站，以确认此远程通信站利用网络基础结构通信的授权；

如果在所述验证步骤期间验证此远程通信站，将 IP 网接入请求传送给专用 IP 网，利用在所述存储步骤期间存储的远程通信站识别来识别此远程通信站；

为响应在所述传送步骤期间传送的 IP 网接入请求，确定是否允

许此远程通信站接入专用 IP 网；和

如果在所述确定步骤期间确定允许此远程通信站接入专用 IP 网，则允许此远程通信站接入专用 IP 网。

3. 根据权利要求 2 的方法，其中在所述存储步骤期间存储远程通信站识别的存储位置位于无线通信系统的网络基础结构上，此远程通信站识别和与此远程通信站有关的验证数据一起存储。

4. 根据权利要求 2 的方法，其中此远程通信站包括耦合到无线收发信机的无线主机，此无线收发信机用于与网络基础结构通信，并且其中所述存储步骤包括存储无线主机识别，此无线主机识别与此无线主机有关。

5. 根据权利要求 4 的方法，其中在所述存储步骤期间存储无线主机识别的存储位置位于无线主机上。

6. 根据权利要求 4 的方法，其中无线主机识别存储在无线收发信机上。

7. 根据权利要求 6 的方法，其中无线收发信机包括可操作在蜂窝通信系统中的蜂窝移动终端，此蜂窝移动终端具有存储器卡，并且其中此无线主机识别存储在此存储器卡上。

8. 根据权利要求 2 的方法，其中此无线通信系统包括蜂窝通信系统，并且其中所述生成请求的步骤包括生成连接请求，此连接请求用于利用无线链路请求无线收发信机与蜂窝通信系统的网络基础结构通过在其之间形成的空中接口的连接。

9. 根据权利要求 2 的方法，其中此无线通信系统包括蜂窝通信系统，其中在远程通信站与专用 IP 网之间传送的数据包括分组数据，和其中在所述生成步骤期间生成的请求提供给为分组数据选择路由的路由器。

10. 根据权利要求 9 的方法，其中蜂窝通信系统包括 GSM 通信系统，和其中提供请求给它的路由器包括 SGSN（业务 GPRS 支持节点）。

11. 根据权利要求 2 的方法，其中此无线通信系统包括蜂窝通信系统，其中在此远程通信站与专用 IP 网之间传送的数据包括分组交换数据，并且其中在所述生成步骤期间生成的请求利用电路交换的电路连接提供给路由器。

12. 根据权利要求 11 的方法，其中此蜂窝通信系统包括 GSM 通

信系统，和其中提供请求给它的路由器包括 MSC/VLR（移动交换中心/被访位置寄存器）。

13. 根据权利要求 2 的方法，其中所述存储步骤还包括存储识别专用 IP 网的专用 IP 网识别的步骤，在此专用 IP 网与远程通信站之间传送数据。

14. 根据权利要求 13 的方法，其中在所述传送步骤传送的 IP 网接入请求传送给利用在存储专用 IP 网识别的所述步骤期间存储的 IP 网识别进行识别的 IP 网。

15. 根据权利要求 2 的方法，其中所述生成步骤还包括生成无线主机提供的 IP 网识别，此无线主机提供的 IP 网识别识别专用 IP 网，将在此专用 IP 网与远程通信站之间传送数据。

16. 根据权利要求 15 的方法，其中在所述传送步骤期间传送的 IP 网接入请求传送给利用在所述生成步骤期间生成的无线主机提供的 IP 网识别所识别的专用 IP 网。

17. 根据权利要求 2 的方法，其中此远程通信站具有与之有关的默认 IP 网识别，和其中在所述传送步骤期间传送的 IP 网接入请求传送给利用此默认 IP 网识别所识别的专用 IP 网。

18. 根据权利要求 2 的方法，还包括验证接入专用 IP 网的请求的步骤。

19. 根据权利要求 2 的方法，其中所述确定步骤包括以下步骤：

在专用 IP 网上存储识别允许接入专用 IP 网的远程通信站的远程通信站识别表；和

比较与在所述传送步骤期间传送的 IP 网接入请求有关的远程通信站识别与存储在此表上的远程通信站识别。

20、根据权利要求 19 的方法，包括另一步骤，如果允许远程通信站接入专用 IP 网，就在此专用 IP 网上分配一个地址给此远程通信站，分配给此远程通信站的地址用于寻址由此专用 IP 网传送给此远程通信站的数据。

21、根据权利要求 20 的方法，其中在所述分配步骤期间分配的地址包括临时地址，此临时地址在所选时间识别此远程通信站。

22、在具有无线接入网、耦合到此无线接入网的专用数据通信网和可选择地利用此无线接入网与专用数据通信网传送数据的远程通

信站的无线通信系统中，用于有选择地允许由远程通信站接入专用数据通信网的一种改善设备，所述设备包括：

存储部件，用于存储识别此远程通信站的远程通信站识别；

检测器，耦合到无线接入网基础结构，所述检测器用于检测请求远程通信站接入无线接入网以便允许通过无线接入网的数据通信的请求；

验证器，耦合到此无线接入网，所述验证器用于确认远程通信站利用无线接入网通信的授权；

网络接入请求器，耦合到所述验证器，所述网络接入请求器用于响应所述验证器的验证，所述网络接入请求器用于生成由远程通信站请求接入专用数据通信网的请求，利用存储在所述存储部件中的远程通信站识别符识别请求中的远程通信站；和

确定器，位于专用 IP 网上，所述确定器用于响应所述网络接入请求器所请求的请求来确定是否允许远程通信站接入专用数据通信网。

23、根据权利要求 22 的设备，还包括位于专用 IP 网上的地址分配器，所述地址分配器用于给远程通信站分配一个地址，所述地址分配器分配的地址用于寻址由专用 IP 网传送给此远程通信站的数据。

24、根据权利要求 23 的设备，其中所述地址分配器包括用于动态分配临时 IP 地址的动态分配器，此临时 IP 地址用于在所选时间寻址传送给此远程通信站的数据。

25、根据权利要求 22 的设备，其中所述存储部件还存储识别专用数据通信网的专用数据通信地址。

说　明　书

用于接入专用数据通信网的安全接入方法及相关设备

本发明一般涉及无线主机与位于网络的设备之间的通信。更具体地，本发明涉及用于允许无线主机接入诸如专用 IP 网的专用数据通信网的方法和相关设备。

在专用数据通信网由专用 IP 网形成的实施例中，专用 IP 网耦合到由诸如蜂窝通信系统的无线通信系统的网络基础结构形成的无线接入网。一旦允许无线主机接入专用 IP 网，则由专用 IP 网给无线主机分配 IP 地址。在专用 IP 网络上接入的信息利用由专用 IP 网分配的 IP 地址寻址到此无线主机。

由无线主机发出的由无线主机接入专用 IP 网的请求首先发送到无线接入网。执行验证程序以确认允许无线主机利用无线接入网通信。如果此无线主机被验证，就将识别无线主机的无线主机识别（WHI）传送给专用 IP 网。如果 WHI 识别允许接入专用 IP 网的无线主机，则允许此无线主机接入此专用 IP 网，此专用 IP 网随后给此无线主机分配一个 IP 地址，此 IP 地址用于寻址数据给此无线主机。

提供一种用于接入专用 IP 或其他数据通信网的简单和有效的方法。WHI 用于在无线接入网和专用 IP 网中识别无线主机。当 WHI 存储在无线接入网时，则不必通过空中接口发送给无线接入网基础结构。并且，如果允许此无线主机接入专用 IP 网，则由专用 IP 网给此无线主机分配一个 IP 地址，此 IP 地址能动态地分配给无线主机，而且不必永久地给此无线主机分配单独的 IP 地址。

发明背景

通信技术的发展已允许显著改善能用于在发送与接收站之间传送数据的方法。

例如，在无线电通信中，数字通信技术的发展已允许引入和推广新类型的通信系统。例如，利用数字通信技术的蜂窝通信系统已在许多地区安装并被广泛使用。

通信技术的发展也已促进计算机系统的分散化。处理装置能分布在单独的位置并通过网络连接连接在一起。分布式处理装置之间的网

络连接及其之间的通信例如已加速诸如互联网的 IP 网的出现和广泛利用。已同样形成了其他的专用数据通信网。

通信技术中的发展也允许无线与网络连接的通信系统的合并。例如，诸如便携式计算机的终端设备有可能通过无线链路耦合到无线通信系统的网络基础结构，并且又利用网络连接耦合到互联网(Internet)连接的网络设备。所以终端设备形成至互联网连接的网络设备的无线主机，由于不能与终端设备形成诸如硬连接的物理链路。

专用 IP 网由一组利用网络连接连接在一起的网络设备组成，但限制这些设备对网络的接入。专用 IP 网的数量正在增加，并且利用无线主机接入这些专用 IP 网的需求日益增加。其他数据通信网的数量增加，并且利用无线主机接入这些通信网的需求日益增加。

由于专用网的限制接入特性，需要保证此无线主机被授权接入此专用网。而且，如果此无线主机被授权接入此专用网，相应需要保证无线主机正确接收接入专用网的可接受电平。也就是说，此无线主机应看作虚拟主机，给定与实际耦合到这样的网络的主机所给定的电平相同的接入专用网的电平。

由于无线主机至专用数据通信网的网络设备的耦合包括无线链路，所以必须利用地址来识别无线主机，以便能传送数据给此主机。在其中无线主机能与网络设备通信的一些现有通信系统中，动态分配无线主机的地址。也就是说，例如，在专用数据通信网由专用 IP 网组成的实施例中，不是给无线主机分配永久的 IP 地址，而是在要传送数据给此无线主机时给此主机分配临时 IP 地址。IPv6 动态 IP 地址分配是用于动态分配 IP 地址给无线主机的分配方法的示例。在这种方法中，为了提供无线主机的固定识别，分配 DNS（域名系统）名。DNS 名是提供给无线主机和连到 IP 网的其他设备的符号名。

无线主机能接入专用 IP 网的一种方式是利用从无线主机至专用 IP 网的拨出连接。一旦形成交换连接，利用口令识别此无线主机。

无线主机有时能接入专用 IP 网的另一种方式是利用验证隧道（tunnel）接入专用 IP 网。无线主机利用验证隧道连到专用 IP 网，并且在专用 IP 网上利用识别与口令来验证此无线主机。这样的隧穿方法有时称为“层 2 隧穿”。Micro_Soft 公司开发的 PPTP 系统、Sysco Systems 开发的 L2F 系统以及 IETF 开发的 L2TP 系统涉及隧穿 PPP。

无线主机接入专用 IP 或其他数据通信网的现有方法要求大量的协议开销。如在带宽限制的通信系统中，协议开销是带宽消耗的。

当无线主机利用蜂窝通信系统的网络基础结构接入专用网时，网络基础结构部分起着无线接入网的作用。例如，当专用数据通信网形成专用 IP 网时，需要两个 IP 地址来允许无线主机与专用 IP 网之间的通信。在由网络基础结构部分形成的无线接入网需要第一 IP 地址，并且在专用 IP 网需要第二 IP 地址。从而，要求此无线主机属于两个网络，即接入 IP 网络与专用 IP 网。结果，必须给此无线主机分配两个 IP 地址。如果在这两个网络中使用 DNS，也必需在这两个网络中分配 DNS 名。

层 2 隧穿方法要求形成具有三个附加层的协议栈，这三个附加层是 PPP 层，层 2 隧穿层和基本 IP 层。由于这样的附加协议层而导致的协议开销是带宽消耗的，这样的要求在带宽有限系统中一般是不希望的。

一些无线主机另外能利用电路交换以及分组交换连接传送分组数据。GSM（全球移动通信系统）蜂窝通信系统是允许其中无线主机可操作的利用分组交换并且也利用电路交换连接传送分组数据的蜂窝通信系统的示例。提供一种允许无线主机利用相同的接入程序接入专用 IP 或其他数据通信网而不管要在其间传送的数据类型的方法将是有益的。

在用于提供无线主机接入例如专用 IP 网的常规方法中，直接进行至专用 IP 网的拨号连接。例如，可以进行至专用 IP 网的远程接入服务器的那个连接。与拨号连接相关的电话费用可以是显著的。例如，如果在蜂窝通信系统的网络基础结构与专用 IP 网之间要求 LATA 之间的交换连接等，则可能收取长途电话费来形成拨号连接。当然，希望无线主机能接入尽可能靠近此无线主机所在位置的无线接入网，并随后利用此无线接入网与专用 IP 网之间的 IP 传输。

更好地允许无线主机接入专用数据通信网以便在其间传送分组数据的方法将是有利的。

本发明的显著改进涉及与无线主机接入和专用 IP 网有关的此背景信息。

发明概述

本发明有益地提供一种用于允许无线主机接入诸如专用 IP 网的专用数据通信网的方法和相关设备。本发明还有益地提供一种一旦同意接入专用网就动态分配临时地址给无线主机的方法和相关设备，此动态分配的地址用于寻址要传送给此无线主机的数据。

在本发明的一个方面中，无线主机利用空中接口耦合到诸如 GSM 网络的 PLMN（公用陆地移动网）的网络基础结构。PLMN 又耦合到专用 IP 网。网络基础结构从而形成无线接入网。当无线主机请求接入专用 IP 网时，首先在由 PLMN 的网络基础结构形成的无线接入网上验证通信，执行验证程序以确认允许利用无线接入网的通信。如果验证程序确认允许这样的通信，则先前存储在无线接入网上并识别无线主机的无线主机识别（WHI）传送给专用 IP 网，如果提供给专用 IP 网的无线主机识别对应于允许接入专用 IP 网的无线主机的识别，则专用 IP 网允许接入无线主机。由专用 IP 网给此无线主机分配一个 IP 地址，这样的 IP 地址用于寻址传送给此无线主机的数据，此 IP 地址可以是动态分配的地址，用于在所选的时间临时识别此无线主机。

从而，不要求无线主机具有单独的 IP 识别来接入无线接入网。相反地，存储在由 PLMN 基础结构形成的无线接入网上的无线主机识别用于在专用 IP 网上识别此无线主机。此无线主机识别可以例如作为无线接入网中的鉴约数据来提供。例如，由专用 IP 网的操作员选择无线主机识别，并且此无线主机识别根据专用 IP 网操作员与 PLMN 操作员之间的协议提供给 PLMN 的网络基础结构并存储在此基础结构上。

一旦提供至专用 IP 网的接入，就由专用 IP 网而不是由 PLMN 提供无线主机的 IP 地址。允许此无线主机变成专用 IP 网的虚拟主机，从而保证用户与专用 IP 网的包括安全和防火墙的主机环境应同样适用于此无线主机。在 PLMN 与专用 IP 网之间使用 IP 隧穿。IP 遂道能利用验证过程或通过安排 PLMN 与专用 IP 网操作员之间的安排的安全传输来保证安全。遂道验证密钥可以与 WHI 一起存储在 HLR、SIM 卡或无线主机，以提供无线主机识别以及其他数据的安全传输。然而，遂穿不扩展到空中接口。相反地，特定于空中接口传输协议用于在无线主机与 PLMN 的网络基础结构之间传送数据报。

因此，在这些和其他方面中，安全接入方法及实施此方法的相关

设备利用远程通信站接入专用数据通信网。一旦提供接入，就在专用数据通信网与远程通信站之间传送数据，此专用数据通信网耦合到无线通信系统的网络基础结构。远程通信站识别存储在无线通信系统的网络基础结构上。由远程通信站生成登记请求来请求远程通信站的登记，以便接入网络基础结构来允许利用此基础结构的数据通信。在网络基础结构上检测此登记请求。验证远程通信站以确认授权远程通信站利用网络基础结构通信。如果验证远程通信站，其中由远程通信站识别来识别此远程通信站，就将网络接入请求传送给专用数据通信网。为响应网络接入请求，确定是否允许远程通信站接入专用数据通信网。并且，如果确定允许此远程通信站接入专用网，则允许此远程通信站接入此专用数据通信网。在同意允许接入专用数据通信网之后，可以给此无线主机分配一个地址，诸如临时地址。

从下面简单概括的附图、之后本发明目前优选实施例的具体描述和所附的权利要求书中能更全面理解本发明及其范围。

附图简述

图 1 表示其中本发明一个实施例可操作的通信系统的功能方框图；

图 2 表示在无线主机与专用 IP 网之间传送的数据的路由选择的逻辑功能方框图；

图 3 表示包括本发明一个实施例分配用于寻址传送给无线主机的数据的地址的专用 IP 网的功能方框图；

图 4 表示本发明实施例方法的方法步骤的逻辑流程图。

详细描述

首先参见图 1，一般以 10 表示的通信系统允许远程通信站 12 与专用 IP 网 14 之间的数据通信。专用 IP 网 14 在这里形成允许有选择地接入的专用内联网。在远程通信站 12 允许接入专用 IP 网 14 时，能在其间传送数据。在一个实施例中，在远程通信站 12 与专用 IP 网 14 之间传送分组数据。虽然在图中所示的示例性实施例中示出专用 IP 网，但在其他实施例中，能通过本发明实施例的操作同样接入其他类型的专用数据通信网。因此，虽然下面的描述结合专用 IP 网 14 来说明，但应理解，本发明也可用于允许接入其他数据通信网。

在此图中所示的示例性实施例中，通信系统 10 由 GSM（全球移动

通信系统）蜂窝通信系统组成，此 GSM 通信系统的网络基础结构形成专用 IP 网 14 所耦合的无线接入网。在其他实施例中，通信系统 10 可选择地由其他结构组成。

无线通信站 10 包括无线收发信机，这里为 GSM 移动终端 16。此移动终端 16 包括 SIM（用户识别模块）卡 18，它插入或连到移动终端 16，在这里利用线 22 表示。

SIM 卡 18 包括以常规方式存储验证信息的存储位置 24，此 SIM 卡 18 还包括用于存储专用 IP 网 14 地址的存储位置 26。在本发明的一个实施例中，此 SIM 卡还包括用于存储 WHI（无线主机识别符）的存储位置 28，其他用户数据能另外存储在 SIM 卡 18 的其他存储位置上。

这里移动终端 16 利用线路 34 耦合到无线主机 32。在一个实施例中，无线主机 32 形成便携式计算机，它能利用专用 IP 网 14 的网络设备接收传送给它的数据。无线主机 32 可以选择地利用例如红外耦合器的无触点耦合器耦合到移动终端 16。在本发明的一个实施例中，无线主机 32 包括用于存储类似于存储在存储位置 24、26 与 28 上的数据的存储位置 36、38 和 42。即，在这样的实施例中，验证信息、专用 IP 地址 14 的地址和 WHI 的值分别存储在存储位置 36－42 上。在此图中所示的示例性实施例中，这样的信息冗余地存储在 SIM 卡 18 与无线主机 32 的存储位置上。在其他实施例中，只有验证信息存储在存储位置 24 或 36 之一上。

通信系统 10 的网络基础结构形成利用骨干网 46 耦合到专用 IP 网 14 的无线接入网。由 GSM 系统的网络基础结构形成的无线接入网在这里表示为包括 BTS（基站收发信机）52。BTS52 可用于生成下行链路信号 54 和在由远程通信站与 BTS52 之间的无线链路形成的空中接口上接收上行链路信号 56。

在其中通信系统 10 的部分由 GSM 通信系统结构形成的实施例中，这样的结构以及在远程通信站 12 与 BTS52 之间形成的空中接口由 GSM 系统特定标准来定义。

BTS 组（在此图中示出单个 BTS52）利用线路 58 耦合到 BSC（基站控制器）62。BSC62 特别可用于控制与之耦合的 BTS 的操作，BSC62 在此利用线路 64 还耦合到 MSC/VLR（移动交换中心/被访位置寄存

器）66，MSC/VLR66 可以常规方式来形成适当的连接，以便在 BSC62 与 PSTN（公用交换电话网）68 之间利用线路 72 形成通信路径。

MSC/VLR66 还利用线路 74 耦合到 HLR（归属位置寄存器）76。HLR76 包括验证中心（未单独示出），在此中心上特别存储 IMSI（国际移动用户识别）和伪随机号码值，在用于确认远程通信站的鉴别验证程序期间使用该值。

在本发明一个实施例中，与无线主机 32 有关的 WHI 值也存储在 HLR76 上。并且，在本发明的另一个实施例中，与专用 IP 网 14 有关的地址也存储在 HLR76 上。

BSC62 与 HLR76 还耦合到 SGSN（服务 GPRS 支持节点）82，BSC62 利用线路 84 耦合到 SGSN82。并且，HLR76 利用线路 86 耦合到 SGSN82，SGSN82 还利用线路 88 耦合到骨干网 46。从而，SGSN82 耦合到专用 IP 网 14。

专用 IP 网 14 在此形成 HIPN（归属智能外围网），在此表示为包括 GGSN（网关 GPRS 支持节点）92 和归属 IP 接入控制网络 94。下面将结合图 3 描述形成专用 IP 网 14 的 HIPN 的其他细节。

骨干网 46 还耦合到另外的 IP 网络，诸如 IP 网 96。

骨干网 46 还表示为利用 GGSN98 耦合到利用互联网连接 104 形成另一 HIPN（这里为 HIPN102）的另一 IP 网。并且，骨干网 46 也耦合到另一专用 IP 网，利用互联网连接 108 形成另一 HIPN106。这样的附加 HIPN96、102 与 106 是示例性的并且表示为说明专用 IP 网能用于耦合到诸如此图中所示的 GSM 系统的网络基础结构的无线接入网的方式。

在操作期间，在无线主机 32 的操作员希望接入专用 IP 网 14 时，在无线主机上生成合适的命令来发出接入专用 IP 网 14 的请求。表示如此请求的信号提供给移动终端 16，并且移动终端 16 生成一个请求，作为上行链路信号 56 通过空中接口传送给 BTS52。在 GSM 通信系统中，开始连接程序，BTS52 通过 BSC62 传送此请求给 MSC/VLR66。

从 HLR76 中恢复 IMSI 和伪随机号码值，并执行验证程序。虽然能在 GSM 系统的特定标准中找到在 GSM 通信系统中完成的验证程序的具体细节，但一般地，验证程序验证，即确认，允许移动终端 16 利用形成无线接入网的网络基础结构通信。一旦成功完成验证程序，

即，确认移动终端 16 为允许利用由网络基础结构形成的无线接入网通信的验证终端，就将与此无线主机有关的 WHI 值传送给专用 IP 网 14。

在一个实施例中，当 WHI 存储在 HLR76 上时，所存储的值利用线路 86 提供给 SGSN82 并通过骨干网 46 提供给专用 IP 网 14。如果验证程序确认移动终端 16 的验证性，存储在 HLR 上的 WHI 传送给 SGSN82。从而，利用无线接入网执行的验证程序来验证 WHI 的值。WHI 在 HLR76 或在无线接入网的另一部分上的存储要求专用 IP 网 14 操作员与无线接入网操作员之间用于在无线接入网上 WHI 值安全存储的协议。仅在专用 IP 网 14 上提供单独 IP 地址或 DNS（域名业务）名，而不在任何其他地方提供。从而，由于在专用 IP 网上提供 IP 地址与 DNS 名，所以无线主机 32 在允许接入专用 IP 网时变成网络 14 的虚拟主机。包括网络安全性和网络防火墙的网络 14 的用户与主机环境也适用于无线主机 32。

无线主机 32 同样能接入其他网络，诸如 HIPN96、102 与 106。

在一个实施例中，也在 SGSN82 与 GGSN92 之间通过骨干网 46 执行验证的 IP 遂穿，以保证专用 IP 网 14 与由网络基础结构形成的无线接入网之间的 WHI 与其他数据的安全传输。执行这样的验证的隧穿，是因为骨干网 46 可能由许多不同操作员共享并且不能保证骨干网的安全性。例如，如果要接入 HIPN106，利用公用互联网 108 为数据选择路由。执行验证的 IP 隧穿以验证 SGSN82 与 GGSN92 之间的业务，即数据通信。验证通过骨干网进行路由选择的业务保证在 GGSN92 上收到 WHI 值时此 WHI 值的有效性。当例如要接入 HIPN102 时，同样利用验证程序来验证通过互联网 104 的传输。

在一个实施例中，GGSN92 包括接入控制机构，以保证只允许所要的 WHI 值接入专用 IP 网。所要的 WHI 的表存储在 GGSN92 的接入控制机构上。并且，还可以执行 WHI 验证程序来进一步增加安全等级和使响应 WHI 管理错误而错误接入专用 IP 网的可能性最小。虽然未在图 1 中单独示出，但利用位于骨干网 46 的防火墙来保护 SGSN82 与 GGSN92。

在专用 IP 网 14 中，使用标准的 HIPN 安全性程序，诸如防火墙和口令。从而，一旦允许无线主机 32 接入专用 IP 网，则给无线主机

32 提供与直接连到网络 14 的其他主机相同的环境和安全等级。

图 2 表示图 1 所示的通信系统 10 部分的逻辑安排。而且，在本发明实施例操作期间，这里为无线主机 32 的无线主机有选择地允许接入专用 IP 网，这里再次表示为形成 HIPN14。

在无线主机 32 将接入专用 IP 网 14 时，移动终端 16 生成连到由 GSM 系统的网络基础结构形成的无线接入网的连接请求。在利用分组交换电路连接时，根据 SGSN82 执行连接程序。并且，在使用电路交换电路连接时，根据 MSC/VLR66 执行连接程序。

在连接程序期间，IMSI、WHI 值和其他相关用户数据从 HLR76 下载到 MSC/VLR66 与 SGSN82 中合适的一个。其他合适的用户数据包括专用 IP 网 14 的地址。诸如 HIPN96、102 与 106（图 1 所示的）的其他专用 IP 网的地址也可以下载，以允许接入可选择的或第二选择的可选 IP 网。识别专用 IP 网 14 的 HIPN 地址在一个实施例中是诸如专用 IP 网 14 的 GGSN92 的 GGSN 的地址。

此后，移动终端 16 在合适时生成“PDP 路由选择上下文激活请求”给 SGSN82 或接入 MSC/VLR66。例如，通过设置在移动终端始发的呼叫来执行至 MSC/VLR66 的接入。可选择地，能进行通过空中接口明确表示应接入 MSC/VLR 的附加协议的标准化。

根据至 SGSN82 的激活请求或至 MSC/VLR66 的接入，将接入哪个 HIPN 的指示在合适时还提供给 SGSN 或 MSC/VLR。例如，移动终端 16 表示，利用存储在 HLR 上的 HIPN 地址识别的专用 IP 网是要接入的专用 IP 网地址。可选择地，移动终端 16 自己能提供将接入的专用 IP 网的地址，或能利用默认的地址来识别将接入的专用 IP 网。

SGSN82 与 MSC/VLR66 中合适的一个，分析提供给它的 IMSI 值，并在未提供地址给它时确定默认的专用 IP 网的地址。

SGSN82 和 MSC/VLR66 中合适的一个生成“产生 PDP 上下文”命令，它在要接入专用 IP 网 14 时，利用骨干网 46 传送给 GGSN92，或在要接入另一网络时，传送给另一 GGSN。“产生 PDP 上下文”命令包括无线主机的 WHI，并且此值在形成专用 IP 网 14 的 HIPN 上用作主机识别。

图 2 还表示可利用无线链路连到另一 WAR（无线接入路由器）114 的无线主机 112。并且 WAR114 耦合到骨干网 46。无线主机 112 是可

能允许其接入 IP 网 14 的另一示例性设备。

图 3 表示前面图 1 与 2 所示的 HIPN 形成的专用 IP 网 14 的逻辑模型。由网络 14 形成的 HIPN 提供包括以下的业务和用户环境：DHCP（动态主机配置分布）业务、DNS（域名业务）业务、新闻业务、邮件业务、登录业务、NTP 业务、WWW（万维网）业务、其他应用服务器、至互联网的连接、至内联网的连接、至骨干网的连接和在连到另一网络的每个接口上的防火墙。

无线主机 32 至专用 IP 网的接入提供纵向业务和至移动终端归属组织的接入。在这样的情况中，专用 IP 网是业务提供者的专用网的一部分。公用 IP 网提供公用互联网业务。相反地，如果接入公用 IP 网，公用 IP 网位于互联网业务提供者的由其操作员或专用互联网业务提供者提供的归属或被访 PLMN（公用陆地移动网）上。

然后，参见图 3，再次示出耦合到骨干网 46 的形成专用 IP 网 14 的 HIPN。也起着防火墙作用的 WHR（无线主机路由器）124 耦合到骨干网 46。WHR124 由特别支持有选择地允许诸如无线主机 32 的无线主机变为网络的虚拟主机的路由器形成。网络 14 包括分别连到互联网 132 与内联网 134 的其他路由器，这里为路由器 126 与 128。路由器 124－128 利用也耦合 DHCP（动态主机配置分布）设备 142 与 DNS（域名业务）设备 144 的局域网（LAN）138 相连。在此图中也示出也连到 LAN138 的其他可选的应用服务器，其中服务器 146 是代表性的。并且，直接耦合到专用 IP 网 14 的无线主机 148 在此图中还表示为与 LAN138 相连接。

DHCP142 可分配地址给无线主机，诸如无线主机 32。WHI 值在 DHCP142 上用作无线主机地址。DNS144 用于存储诸如无线主机 32 的无线主机的名。WHI 值用作 DNS144 上的主名，并且也能与 WHI 一起存储其他附属名。示例性地，例如，DNS 名包括 WHI2444501234567890@org. country；MSISDN467051234567@org. country；和 my host @org. country。

由于 WHI 值是无线网络提供的明确识别在无线主机上使用的无线预约的识别，所以能有益地使用此 WHI 值。通过在 HLR76（图 1 所示）上存储作为用户数据的 WHI 值，利用合适的安全等级存储 WHI 值。由于接入 GSM 网络的无线主机在接收允许使用所存储的 WHI 之前进行验

证，所以不需要单独的登录来接入专用 IP 网 14。

必须保证专用 IP 网 14 与无线接入路由器 124 之间传输的安全。为保证此传输的安全性，无线主机路由器 124 与形成 GSM 一部分的无线接入路由器，无线接入网存储有关允许其间进行通信的各个路由器的地址与验证信息。这样的测量保证到达无线主机路由器 124 的 WHI 是安全和正确的。如果需要，可以加密路由器之间的传输来提供数据机密性与可靠性更大的保证。可选地，WHR124 上的验证程序可以与 WHI 有关，从而在 WHI 管理中保护 IP 网不出差错。

也可以从无线主机 32 接收 WHI 和验证密钥，并且能在同意无线主机 32 接入专用 IP 网之前，在专用 IP 网上另外执行验证程序。

GGSN 拒绝没有有效 WHI 的接入尝试。而且，必须在 WHR124 以及 DHCP142 与 DNS144 中预先配置有效的 WHI。DHCP142 利用所分配的用于寻址要传送给无线主机的数据的 IP 地址来更新 DNS144。

虽然图 3 所示的专用 IP 网 14 仅表示单个 LAN138，但能在几个物理 LAN 实现此网络或在没有物理 LAN 的单个平台上实现此网络。当在几个物理位置上出现与 WHR124 相同的 WHR 时，每个 WHR 认为是形成专用 IP 网的 HIPN 的子网络(SHIPN)。在这样的安排中，每个 SHIPN 能利用骨干网与另一 SHIPN 通信。

图 4 表示本发明实施例的方法，一般以 152 表示。方法 152 提供一种由远程通信站接入专用 IP 网的安全接入方法。

首先，并如方框 154 所示，远程通信站识别存储在形成无线通信系统的无线接入网的网络基础结构上，远程通信站识别和与远程通信站有关的验证数据一起存储。

然后，并如方框 156 所示，由远程通信站生成请求接入网络基础结构的请求，以允许通过此基础结构进行数据通信。

如方框 158 所示，在网络基础结构上检测此请求。如方框 162 所示，验证远程通信站，以确认远程通信站授权利用网络基础结构通信。

此后，如方框 164 所示，将 IP 网络接入请求传送给专用 IP 网。然后，如方框 166 所示，确定是否允许远程通信站接入此专用 IP 网。

并且，如果确定允许此远程通信站接入此网络，允许此远程通信站接入专用 IP 网。

在本发明实施例操作过程中允许无线主机变成专用 IP 网的虚拟主机，无线主机识别（WHI）在专用 IP 网中用作主机识别符。无线主机只需在无线接入网与专用 IP 网操作员之间不存在有关例如识别信息安全性的安全存储条约时在专用 IP 网上验证它自己。验证程序确认发送接入请求的结构的验证性。在通过空中接口传送 IP 分组时，也有益地减少通过空中接口生成接入专用 IP 网请求所需的带宽，这是因为只利用特定于空中接口的协议来通过空中接口传送 IP 分组。

前面的描述是实施本发明的优选示例，而本发明范围不必受此描述限制。本发明的范围由下面的权利要求书来定义。

说 明 书 附 图

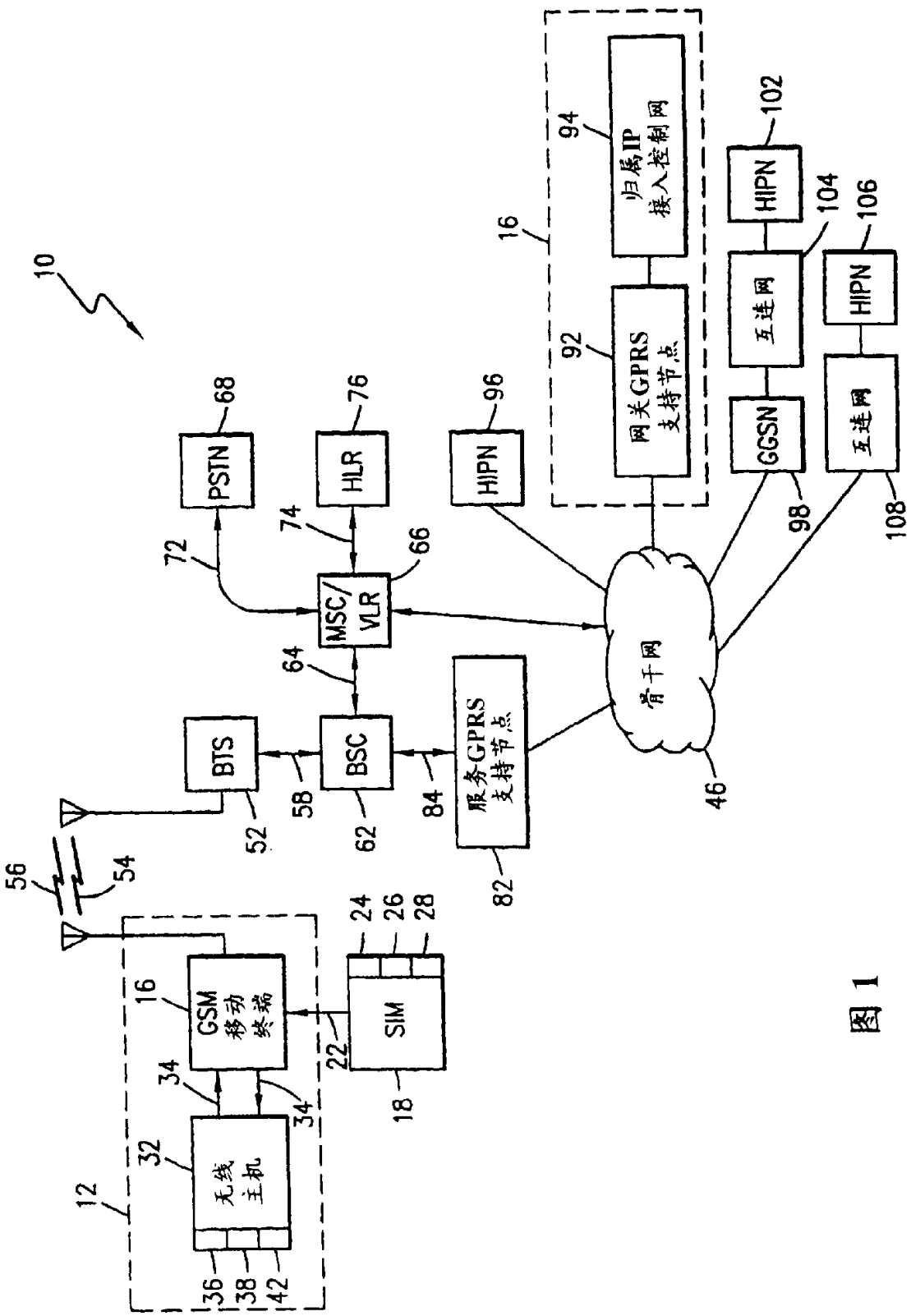
10
12
16
GSM 移动终端
无线主机
32
34
34
36
38
42
SIM
18
22
24
26
28
56
54
BTS
52
58
BSC
62
64
MSC/VLR
66
72
PSTN
68
74
HLR
76
84
服务GPRS支持节点
82
HIPN
96
骨干网
46
16
网关GPRS支持节点
92
归属IP接入控制网
94
GGSN
98
互连网
104
HIPN
102
互连网
108
HIPN
106

图 1

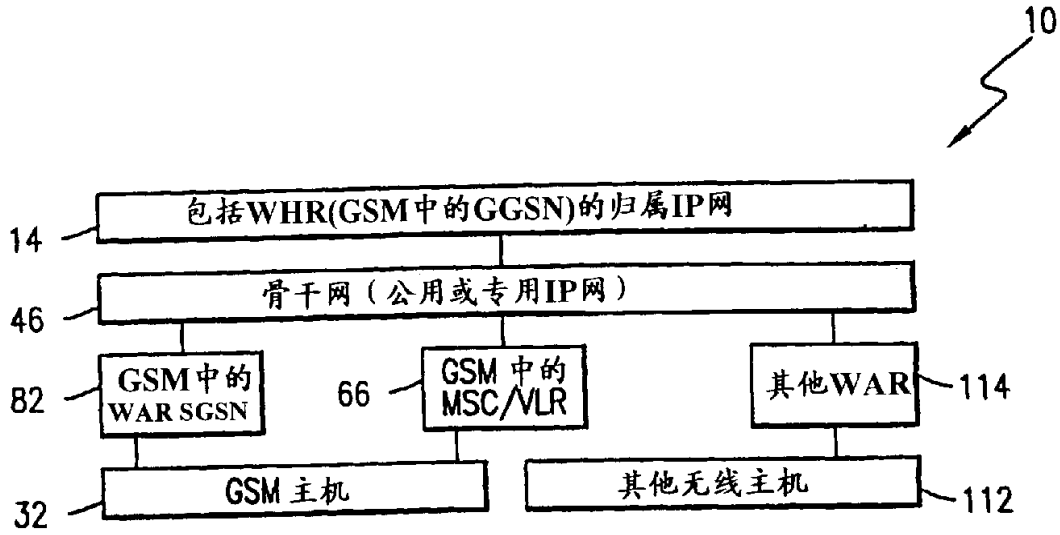
10
包括WHR(GSM中的GGSN)的归属IP网
14
骨干网（公用或专用IP网）
46
GSM中的 WAR SGSN
82
GSM 中的 MSC/VLR
66
其他WAR
114
GSM 主机
32
其他无线主机
112

图 2

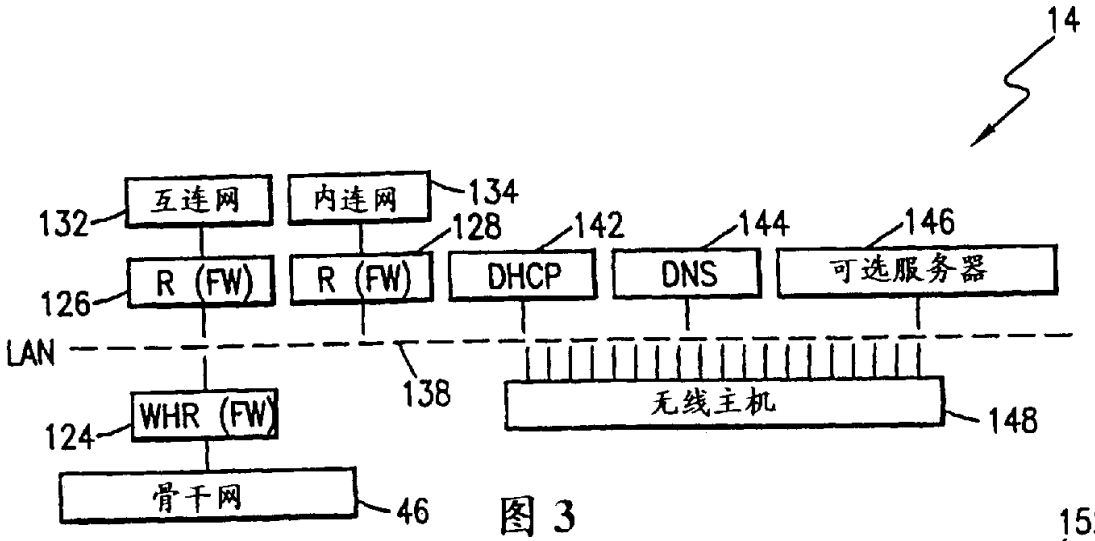
14
互连网
132
内连网
134
R (FW)
126
R (FW)
128
DHCP
142
DNS
144
可选服务器
146
LAN
138
WHR (FW)
124
无线主机
148
骨干网
46

图 3

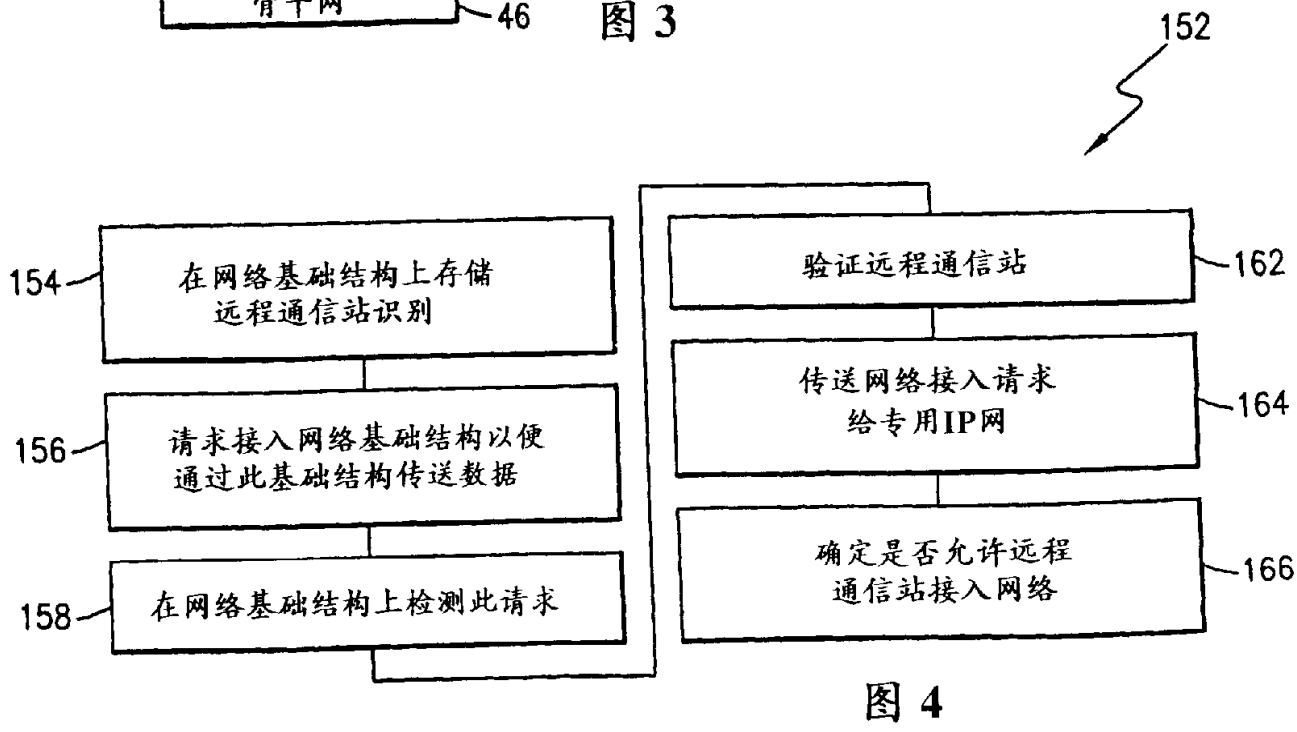
152
在网络基础结构上存储 远程通信站识别
154
请求接入网络基础结构以便 通过此基础结构传送数据
156
在网络基础结构上检测此请求
158
验证远程通信站
162
传送网络接入请求 给专用IP网
164
确定是否允许远程 通信站接入网络
166

图 4