(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 1795656 B
(45)授权公告日 2011.11.23

(21)申请号 200480014186.0
(22)申请日 2004.05.21
(30)优先权数据
0311921.1 2003.05.23 GB
(85)PCT申请进入国家阶段日
2005.11.23
(86)PCT申请的申请数据
PCT/EP2004/050889 2004.05.21
(87)PCT申请的公布数据
WO2004/105340 EN 2004.12.02
(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 P·尼坎德 J·阿科
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 李亚非 梁永
(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
WO 03015360 A2,2003.02.20, 说明书第7页第24行-30行,第8页第6行-11行,第11页第10行.
EP 0944203 A2,1999.09.22, 说明书第4页第0015段-第5页第0023段.
EP 1244271 A,2002.09.25, 全文.

审查员 李凡

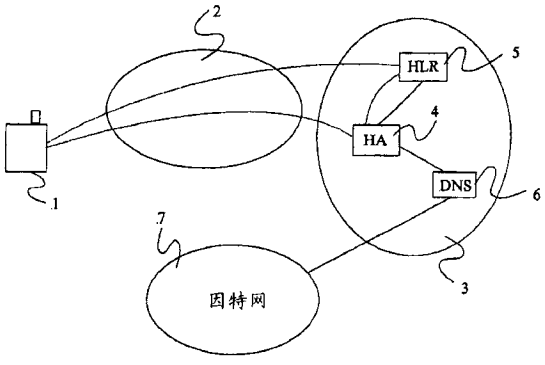
权利要求书 1 页 说明书 5 页 附图 1 页

(54)发明名称

一种安全初始化用户和保密数据的方法

(57)摘要

一种在移动路由系统中当其用户也是无线通信网络的用户时,安全初始化用户和保密数据的方法。该方法包括,在移动路由系统内,使用用于无线通信网络所限定的认证程序对移动路由系统认证用户,收集来自无线网络的相关节点的用户信息,并且商定密钥,通过该密钥可以在用户和移动路由系统之间进行更进一步的通信,并且在对用户移动节点和对应节点提供移动业务过程中使用所述用户信息和密钥。



CN 1795656 B

1. 一种在移动路由系统中当其用户也是无线通信网络的用户时，安全初始化用户和保密数据的方法，该方法包括：

在无线通信网络的移动节点和认证服务器之间重新运行为无线通信网络所限定的认证和密钥协定程序；

把重新运行认证和密钥协定程序所得的共享秘密提供给移动路由系统的稳定的前传代理，而且，利用共享秘密向稳定的前传代理认证移动节点；

商定密钥，通过该密钥可保护在移动节点和稳定的前传代理之间进一步的通信；

在向稳定的前传代理认证移动节点后，在稳定的前传代理处收集来自所述认证服务器的用户信息，并且

在向用户移动节点和对应节点提供移动业务过程中使用所述用户信息和密钥。

2. 如权利要求 1 所述的方法，包括在移动节点和所述认证服务器之间经由稳定的前传代理传送消息，以便重新运行认证。

3. 如权利要求 1 所述的方法，包括将在重新运行认证程序期间商定的会话密钥从认证服务器发送到稳定的前传代理。

4. 如权利要求 2 所述的方法，其中移动路由系统是基于移动 IP 的系统，而稳定的前传代理是归属代理。

5. 如权利要求 2 所述的方法，其中移动路由系统是基于 HIP 的系统。

6. 如权利要求 1 所述的方法，其中所述认证和密钥协定程序是由 3GPP 规定的程序。

7. 如权利要求 1 所述的方法，其中所收集的用户信息包括下列信息的一个或多个：

用户的名称和邮递地址；

和用户相关的电话号码；

用于用户的现用的完全限制域名；和

早期对用户建立的任何移动业务的状态。

8. 一种对移动路由系统的稳定的前传代理进行操作的方法，该方法包括：

在无线通信网络的移动节点和认证节点之间转送与重新运行认证和密钥协定程序相关的消息；

在所述程序完成之后接收来自认证服务器的共享秘密，用于利用共享秘密认证移动节点，并且用于收集来自认证服务器的用户信息；

商定密钥，通过该密钥可保护在移动节点和稳定的前传代理之间进一步的通信；和

在对用户移动节点提供移动业务过程中使用所述用户信息和密钥。

一种安全初始化用户和保密数据的方法

发明领域

[0001] 本发明涉及移动通信系统中的安全通信改向，尤其是用于使移动节点能安全执行与归属网络之间的和通信改向相关的业务处理的方法和装置。

[0002] 发明背景

[0003] 在传统蜂窝电话网络中，移动节点能在小区之间漫游而不需要停止正在进行的电话呼叫。随着移动 IP 业务的引入，已经在找到解决方案来允许移动 IP 节点在不同的访问网络内以及甚至在不同的访问网络（比如 UMTS 或 WLAN）之间漫游而对业务仅有最小程度的破坏。该优选的解决方案是基于允许业务流将被改向到移动节点的当前位置的观点。

[0004] 在一个解决方案中，公知的如移动 IPv6，通信流通过稳定的 IPv6 地址被标识并在前传到移动节点的当前“关心地址”之前被路由到移动节点的归属网络。当移动节点在访问节点之间漫游时，一个包含新的关心地址的更新消息被发送到归属网络。在另一个解决方案中，公知的如主机标识协议 (HIP)，一个公共密钥（或公共密钥的散列）用来标识通信流。在这两种情况下，稳定的前传代理在网络中某些地方被需要以便其它节点不需预先获知移动节点的当前位置而能联系到移动节点。

[0005] 在移动 IPv6 中，该稳定的前传代理被称为归属代理，在该归属代理和移动节点之间必须存在一个安全关联以便防止在其上发生未授权的位置更新。在 HIP 中，不需要这样一个安全关联，因为公共密钥可以被直接用于以安全方式来标识一个特定节点。然而，为了使其它节点得以获知基于 HIP 的移动节点的公共密钥，该公共密钥必须以安全方式被存储在域名系统 (DNS) 服务器中。因此，在这两种情况下，为了与其归属代理通话的目的或者为了在配置阶段更新 DNS 服务器以存储其公共密钥，移动节点必须能够安全执行与其“归属网络”的业务处理。

[0006] 典型地，用于归属代理的安全关联 (SA) 的建立或 DNS 服务器的更新可以被人工执行。虽然这些操作的一些部分已经自动化，例如通过公共密钥基础 结构的使用，但授权步骤必须标注日期还需人工操作。在移动 IPv6 中，该步骤包括判定特定移动节点（即使具有来自于可靠第三方的证明）是否被允许使用一个特定 IPv6 地址。该步骤在给定公共密钥基础结构一般不能告知在网络中进行哪些 IP 地址分配的情况下，不易通过该公共密钥基础结构自动化。在 HIP 中，该步骤较容易但是需要现有的公共密钥基础结构并且需要已经做出关于是否移动节点被允许控制给定域名的判定。现有的这样一个公共密钥基础结构，在给定 DNS 系统的目的是作为公共密钥基础结构起作用的情况下，可被看作是多余的和不必要的 - 需要另一个公共密钥基础结构输入数据到 DNS 服务器中，这将是不可思议的。

[0007] 上述技术问题可能导致未来网络中的业务调度问题。为了设置每个和各个移动节点（超过几百万）用于移动业务而需要人工操作从商务前景上是不可接受的。

发明内容

[0008] 本发明的一个目的是使用现有安全机制来引导可能被移动业务和机制可能需要的任何安全性。

[0009] 根据本发明的第一方面，提供一种在移动路由系统中当其用户也是无线通信网络的用户时，安全初始化用户和保密数据的方法，该方法包括：

[0010] 在移动路由系统内，使用用于无线通信网络所限定的认证程序对移动路由系统认证用户，收集来自无线网络的相关节点的用户信息，并且商定密钥，通过该密钥可以在用户和移动路由系统之间进行更进一步的通信；和

[0011] 在对用户移动节点和对应节点提供移动业务过程中使用所述用户信息和密钥。

[0012] 优选地，与对移动路由系统认证用户的所述步骤相关的消息在由用户使用的移动节点和该用户的归属网络的认证服务器之间经由移动服务器被传送。该移动服务器收集来自蜂窝无线网络的相关节点（用户数据库）的用户信息，并且在重新运行认证程序完成之后，接收来自认证服务器的共享秘密。

[0013] 优选地，在重新运行认证程序期间商定的会话密钥通过认证服务器被发送到移动服务器。

[0014] 在本发明的第一实施例中，移动路由系统是基于移动 IP 的系统，在这种情况下移动服务器是归属代理。在本发明的一个替换的实施例中，移动路由系统 是基于 HIP 的系统，移动服务器是前传代理。

[0015] 举例来说，所述认证程序可以是认证和密钥协定 (AKA) 程序。当然可以使用其它程序。

[0016] 根据本发明的第二方面，提供了一种操作用于移动无线通信系统中的移动节点的方法，该方法包括：

[0017] 为了对移动路由系统认证移动节点的目的，初始化用于无线通信网络所限定的认证程序，并且经由移动路由系统的移动服务器采用认证服务器运行所述程序。

[0018] 根据本发明的第三方面，提供一种操作移动路由系统的移动服务器的方法，该方法包括：

[0019] 在移动节点和认证节点之间转送与认证程序相关的消息；

[0020] 在所述程序完成之后，接收来自认证服务器的共享秘密，并且收集来自认证服务器和 / 或其它网络节点的用户信息；和

[0021] 在对用户移动节点提供移动业务过程中使用所述用户信息和密钥。

[0022] 根据本发明的第四方面，提供一种操作移动无线通信网络的认证服务器的方法，该方法包括：

[0023] 经由移动服务器采用移动节点运行认证程序；和

[0024] 发送由所述程序产生的共享秘密到所述移动服务器。

[0025] 附图简述

[0026] 图 1 示意地示出包括移动路由系统的移动无线通信系统。

[0027] 某些实施例的详细描述

[0028] 程序已被定义和指定用于使移动节点能在蜂窝通信系统中由归属网络安全地认证。例如，被称为认证和密钥协定 (AKA) 的 3GPP 认证程序，采用存储在蜂窝装置的用户识别模块 (SIM) 卡中的密钥，和用户的归属网络的 HSS 节点中的密钥对蜂窝装置（或者更确切是对于 SIM 卡）进行网络级认证。在漫游蜂窝装置的情况下，AKA 程序通过访问的网络来执行，同时归属网络告知访问网络该认证决定。但也存在有 AKA 的替换程序并落在本发

明的范围内，该讨论将限于以 AKA 为例。

[0029] 用于网络级认证的 AKA 程序的使用将典型地允许用户进行电话呼叫但是不必认证用于特定业务的移动节点。就 IP 移动业务，比如移动 IP 和 HIP 而言， 需要独立的认证程序。如已经讨论的，这些独立的程序之前已经被人工执行。

[0030] 在此建议为了对移动路由系统认证移动节点的目的，重复使用 AKA 程序以及在移动节点 (SIM 卡) 和归属网络之间共享的相关秘密。首先讨论移动 IP 的情况，图 1 以简化的形式示出了一个通用的系统结构。移动节点 1 当前被连接到被访问网络 2。假定 AKA 程序已经预先运行以便对归属网络 3 认证该移动节点并且从而对被访问网络 2 认证该移动节点。移动节点 1 因此已在网络级访问外网。该程序可包括下列步骤 :

[0031] 步骤 1. 移动节点 1 通过例如经由 GPRS 建立连接来建立 (IP) 网络连接。如已经描述的，该步骤假定 AKA 程序已被执行以提供网络访问认证。但是，该步骤被认为独立于 IP 移动认证程序，即使这两个程序使用相同的 SIM 卡。

[0032] 步骤 2. 该移动节点对移动路由系统的归属代理 4 启动认证程序。

[0033] 步骤 3. 归属代理 4 在移动节点 1 和归属网络 3 的认证服务器 (HLR)5 之间转送消息，以便在归属代理和移动节点之间执行 (即重新运行，(re-run))AKA(USIM) 认证。这包括下列步骤 :

[0034] - 移动节点 1 发送其标识到 HLR。

[0035] -HLR5 发送一个应答到移动节点 1。

[0036] - 移动节点 1 可选择地验证该 HLR 的应答的可靠性。

[0037] - 移动节点发送一个应答到 HLR。

[0038] -HLR 验证该移动节点的应答的可靠性。

[0039] -HLR 可选择地发送一个确认返回给移动节点。

[0040] - 移动节点和 HLR 均建立一个 (或多个) 共享会话密钥，比如 USIM CK 和 IK。

[0041] 步骤 4.HLR5 将重新运行 AKA 程序的结果 (包括会话密钥) 前传到归属代理 4。

[0042] 步骤 5. 移动节点 1 生成一公共密钥对。

[0043] 步骤 6. 移动节点 1 发送一个消息到归属代理 4，这通过使用在步骤 3 中建立的一个 (或多个) 共享会话密钥被保护。该消息包含下列信息 :

[0044] - 移动节点的公共密钥。

[0045] - 移动节点的可选标记，该可选标记通过采用与公共密钥相关的私有密钥获得。

[0046] - 可选的期望参数，比如期望的完全限制域名 (fully qualified domain name, FQDN)。

[0047] - 可选的共享秘密 (如果提供的话，这部分必须被加密)。

[0048] 步骤 7. 归属代理 4 通过使用一个 (或多个) 共享会话密钥和可选地使用所述标记验证移动节点的消息的可靠性。

[0049] 步骤 8. 归属代理 4 从 HLR5 和可能的其它用户数据库收集某些预定信息，以及本地 DNS 服务器 6(区域) 的现有内容。该信息可包括例如 :

[0050] - 与该 SIM 卡相关的用户的名称和邮递地址。

[0051] - 与该 SIM 卡相关的电话号码。

[0052] -DNS 中 (用于该特定用户或者用于其他用户) 现有的多个 FQDN。

[0053] - 早期对该特定用户或 SIM 卡建立的任何移动业务的状态。

[0054] 步骤 9. 归属代理 4 判定关于一个合适的 FQDN 和 / 或 IP 地址中哪一个能被分配给该装置作出判定。例如，归属代理可检查期望的与操作者的域名（例如 sonera.net）结合的 FQDN，用户的电话号码或名称（例如 matti-virtanen.sonera.net），以及具有相同 FQDN 的可能的先前实体的存在。归属代理还在下列实体中进行必要的配置：

[0055] - 本地 DNS 服务器 6（使用例如动态 DNS 协议），其中被选择的 FQDN 和相关的公共密钥被存储。

[0056] - 一个或多个用户数据库（可能包括帐单信息中的更改）。

[0057] 步骤 10. 归属代理 4 将该配置传送回移动节点，包括：

[0058] - 所选择的 FQDN 和可选地，IP 地址。

[0059] - 可选地，由该装置（比如归属代理）使用的某个网络节点的公共密钥。

[0060] 步骤 11. 移动节点 1 存储所接收的信息。应注意如果在装置和用户的凭证之间存在分离，比如通常在电话和插入其中的 SIM 卡之间存在分离，则该信息必须以一种特定方式被处理。在由任何用户 (SIM 卡）使用的装置中保存该信息，将允许其它用户使用该信息。这个风险可通过在 SIM 中保存所接收的信息，或以另一个 SIM 卡被插入后不可访问的方式在该装置中保存该信息而降低。

[0061] 作为 AKA 重新运行以及通过归属代理进行数据收集和分配的结果，移动节点现在能以安全方式使用移动业务。通过使用公共密钥和 / 或共享秘密，在归属代理和移动节点之间的通信是安全的。

[0062] 就 HIP 的情况而言，归属代理由前传代理（或定位点）代替。前传代理在 AKA 重新运行期间在移动节点和 HLR 之间起到媒介的作用。除了上述的步骤之外，在步骤 9 中前传代理的地址被存储在 DNS 服务器中。然后移动节点的公共密钥和前传代理的地址可从 DNS 服务器经由因特网 7 由第三方重新得到，并且无论移动节点的当前位置和 IP 地址如何，通信均能通向该移动节点。

[0063] 存在几种在其它环境下（例如 RFC 3310）采用小区电话认证的建议，因此 SIM 认证的重复使用，其本身不是新的。但是在这里认证步骤以特定方式用于特定应用，同时具有其它步骤用于在移动服务器（即归属或前传代理）收集来自一个用户数据库或多个用户数据库的信息。

[0064] 存在几种甚至在例如移动 Ipv6 的环境下也采用小区电话认证的建议。但是在每次在移动节点和移动服务器之间执行业务处理时这些建议采用这样的认证，并且缺少判定 IP 地址和 FQDN 的机制。

[0065] 还存在采用小区电话和其它传统认证机制来以通常方式生成适用于任何应用的所谓用户凭证。但是这里所描述的解决方案避免了该步骤，并且除了最终所得到的 DNS 系统作为 PKI 的“不稳定”形式之外，避免了任何 PKI 的使用。此外，当前的解决方案明显能够做出关于 FQDN 和 IP 地址的必要认证判定而不同于现有建议。

[0066] 现有的标准协议用于对 DNS 进行动态更新。但是，目前这些方案由于具有预先提供的共享秘密 (DNS TSIG)，或者能提供共享秘密，比如 kerberos(GSSTSIG) 的其他机制，或者安全 DNS，是安全的。现在所有这些机制作出安全判定而不考虑做出请求的特定实体。这是不足够的，因为对一个特定节点控制其本身的 IP 地址和 DNS 名而不是其它节点的地址和

名称是必需的。这里提出的该建议通过将用户数据库和认证程序相结合来处理这个问题。

[0067] 本发明的实施例将能实现移动业务在不均匀网络中的轻松调度。

[0068] 上述讨论已考虑到的情况是：当初始化的网络级认证程序和重新运行程序都被执行时访问网络是相同的。要指出的一个问题是如果移动节点在可能采用不同认证程序的不同访问网络之间移动将发生什么。例如考虑其中移动节点在 UMTS 访问网络和 WLAN 访问网络之间漫游的情况。虽然 UMTS 网络将使用 AKA 在网络级认证用户，但是 WLAN 网络可能在该级使用某个其它程序。本发明包括一个可能性，即在 WLAN 网络级访问程序已经被执行之后，AKA 程 序被再次使用对关于移动业务的用户授权。

[0069] 本领域技术人员应该理解的是，在不脱离本发明范围的情况下可以对上述实施例进行多种修改。

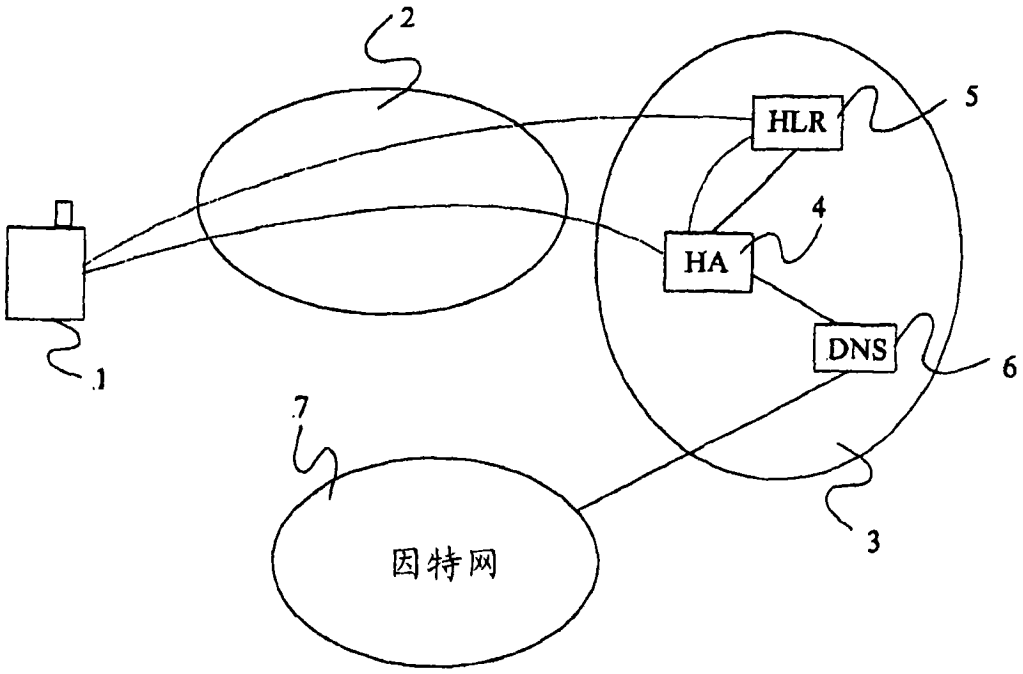


图 1