



(12)发明专利申请

(10)申请公布号 CN 107070846 A

(43)申请公布日 2017.08.18

(21)申请号 201610873555.6

H04W 12/04(2009.01)

(22)申请日 2007.08.09

H04W 12/06(2009.01)

H04W 80/04(2009.01)

(30)优先权数据

102006038037.1 2006.08.14 DE

(62)分案原申请数据

200780030180.6 2007.08.09

(71)申请人 西门子公司

地址 德国慕尼黑

(72)发明人 R.法尔克 G.霍恩

D.克罗塞尔伯格

(74)专利代理机构 中国专利代理(香港)有限公

司 72001

代理人 胡莉莉 刘春元

(51)Int. Cl.

H04L 29/06(2006.01)

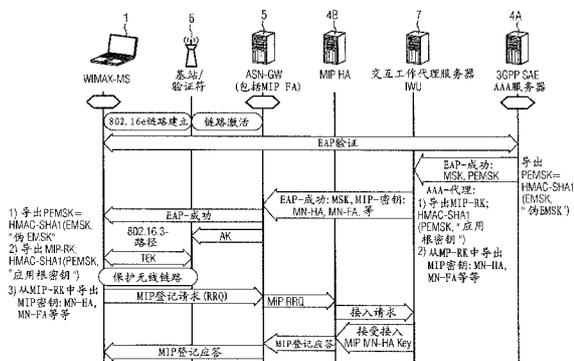
权利要求书2页 说明书10页 附图8页

(54)发明名称

提供接入特定的密钥的方法和系统

(57)摘要

提供用于保护在移动终端设备(1)和接入网络(2)的节点之间数据传输的接入特定的密钥的方法,其中在验证移动终端设备(1)时验证服务器(4A)产生对话密钥,从该对话密钥中推导出基本密钥并传输给交互工作代理服务器(7),其从传输的基本密钥中推导出接入特定的密钥并提供给接入网络(2)的节点。



1. 提供用于保护在移动终端设备 (1) 和接入网络 (2) 的节点之间的数据传输的接入网络密钥的方法, 其中在验证这个移动终端设备 (1) 时本地网络的验证服务器 (4A) 产生对话密钥, 从该对话密钥中推导出基本密钥并传输给接入网络 (2) 中的交互工作代理服务器 (7), 该交互工作代理服务器 (7) 从传输的基本密钥中推导出接入网络密钥并提供给该接入网络 (2) 的节点, 其中移动终端设备 (1) 在验证时同样产生对话密钥并从中推导出接入网络密钥。

2. 按照权利要求1所述的方法, 其中通过MSK (Master SessionKey) 密钥或通过EMSK (ExtendedMaster SessionKey) 密钥形成对话密钥。

3. 按照权利要求1所述的方法, 其中所述验证服务器 (4A) 位于移动终端设备的本地网络中。

4. 按照权利要求1所述的方法, 其中从对话密钥中借助于预先规定的第一推导函数推导出基本密钥。

5. 按照权利要求4所述的方法, 其中通过HMAC-SHA1推导函数、HMAC-SHA256推导函数、HMAC-MD5推导函数、SHA1推导函数、SHA-256推导函数或MD5推导函数形成第一推导函数。

6. 按照权利要求1所述的方法, 其中依赖于对话密钥和符号串 (String) 推导出基本密钥。

7. 按照权利要求1所述的方法, 其中在验证服务器中借助于EAP协议验证移动终端设备。

8. 按照权利要求1所述的方法, 其中在验证服务器中借助于UMTS-AKA协议验证移动终端设备。

9. 按照权利要求1所述的方法, 其中在验证服务器中借助于HTTP-Digest-AKA协议验证移动终端设备。

10. 按照权利要求1所述的方法, 其中借助于Diameter协议或Radius协议实现在验证服务器和交互工作代理服务器之间的数据传输。

11. 按照权利要求1所述的方法, 其中通过WiMax网络形成接入网络。

12. 按照权利要求1所述的方法, 其中通过3GPP网络形成本地网络。

13. 按照权利要求1所述的方法, 其中通过交互工作代理服务器借助于第二推导函数从传输的基本密钥中推导出移动IP根密钥。

14. 按照权利要求13所述的方法, 其中通过HMAC-SHA1推导函数、HMAC-SHA256推导函数、HMAC-MD5推导函数、SHA1推导函数、SHA-256推导函数或MD5推导函数形成第二推导函数。

15. 按照权利要求14所述的方法, 其中借助于第三推导函数从已推导出的移动IP根密钥中推导出用于保护在移动终端设备和接入网络的节点之间数据传输的接入网络密钥。

16. 按照权利要求15所述的方法, 其中通过HMAC-SHA1推导函数、HMAC-SHA256推导函数、HMAC-MD5推导函数、SHA1推导函数、SHA-256推导函数或MD5推导函数形成第三推导函数。

17. 按照权利要求1所述的方法, 其中为在接入网络 (2) 的节点和移动终端设备 (1) 之间的不同数据传输链路分别推导出所属的接入网络密钥。

18. 本地网络的用于提供基本密钥的验证服务器 (4A), 从该基本密钥中能推导出用于

保护在移动终端设备(1)和接入网络(2)的节点之间数据传输链路的接入网络密钥,

其中验证服务器(4A)包括以下装置,该装置用于在验证移动终端设备(1)时产生对话密钥并从中借助于推导函数推导出基本密钥以及将该基本密钥提供给接入网络(2)中的交互工作代理服务器(7),其中移动终端设备(1)在验证时同样产生对话密钥并从中推导出接入网络密钥。

19.按照权利要求18所述的验证服务器,其中所述验证服务器(4A)还包括以下装置,该装置通过HMAC-SHA1推导函数、HMAC-SHA256推导函数、HMAC-MD5推导函数、SHA1推导函数、SHA-256推导函数或MD5推导函数形成推导函数。

20.按照权利要求18所述的验证服务器,其中验证服务器(4A)设置在移动终端设备(1)的本地网络(4)中。

21.提供用于保护在移动终端设备(1)和接入网络(2)的节点之间数据传输的接入网络密钥的交互工作代理服务器(7),其中该交互工作代理服务器(7)位于所述接入网络(2)中并包括以下装置,该装置用于从由本地网络的验证服务器(4A)传输的基本密钥中推导出接入网络密钥并将该接入网络密钥提供给接入网络(2)的节点,其中移动终端设备(1)在验证时同样产生对话密钥并从中推导出接入网络密钥。

22.具有多个接入网络(2)和移动终端设备(1)的至少一个本地网络(4)的数据传输系统,其中

本地网络(4)的验证服务器(4A)包括:用于在验证移动终端设备(1)时产生对话密钥并借助于推导函数从中推导出公共的基本密钥以及将该基本密钥提供给接入网络(2)的装置,该接入网络(2)分别具有交互工作代理服务器(7),

该交互工作代理服务器(7)包括用于从传输的基本密钥中推导出至少一个接入网络密钥的装置,该传输的基本密钥分别被设置用来保护在移动终端设备(1)和各自接入网络(2)的节点之间的数据传输链路,其中移动终端设备(1)在验证时同样产生对话密钥并从中推导出接入网络密钥。

23.按照权利要求22所述的数据传输系统,其中该交互工作代理服务器(7)还包括用于从传输的基本密钥中为接入网络(2)的每个节点推导出所属的接入网络密钥的装置。

提供接入特定的密钥的方法和系统

[0001] 本申请是申请日为2007年8月9日、申请号为200780030180.6 (国际申请号为PCT/EP2007/058284) 以及发明名称为“提供接入特定的密钥的方法和系统”的发明专利申请的分案申请。

技术领域

[0002] 本发明涉及为了保护在移动终端设备和接入网络的节点之间的数据传输而提供接入特定的密钥的方法和系统。

背景技术

[0003] 具有TCP/IP协议的因特网为移动领域提供用于研发更高协议的平台。由于因特网协议的普遍流行,因此以相应的协议扩展可以为移动领域开启更大的应用范围。可是传统的因特网协议最初不是为移动应用而设计的。在传统的分组交换中,在静止的计算机之间交换数据分组,这些计算机并不改变其网络地址而且也不在不同的子网络之间进行转移。在具有移动终端设备或者计算机的无线网络中移动计算机MS (Mobile Station) 经常接入在不同的网络中。DHCP (Dynamic Host Configuration Protocol) 能够借助于相应的服务器把IP地址和另外的配置参数动态分配给网络中的计算机。接入到网络中的计算机通过DHCP协议自动分配空余IP地址。如果移动计算机初始化DHCP,则其必须仅仅在支持关于DHCP协议配置的本地网络的传输范围内。在DHCP协议中动态地址分配是可能的,也就是说在确定的时间内自动分配空余IP地址。在运行该段时间之后必须通过移动计算机MS重新提出请求或者另外分配IP地址。

[0004] 移动计算机MS可以利用DHCP接入网络而不必进行手动配置。作为前提条件必须仅仅提供一个DHCP服务器。移动计算机MS可以利用本地网络的这种业务并且例如可以利用中央存储的文件。可是如果一个移动计算机自身提供了这样的业务,则移动计算机不可能发现可能的业务用户,因为在每一个移动计算机接入的网络中改变其IP地址。如果在当前的TCP连接中改变IP地址,则可能发生同样的事情。这导致连接中断。因此在移动IP的情况下,给移动计算机MS分配一个IP地址,该移动计算机也把该IP地址保留在另外的网络中。在传统的IP网络变换的情况下必须相应地对IP地址进行适配调整。在IP地址变换的情况下,IP配置机理与传统的自动配置机理的持续的适配调整会中断当前连接。MIP协议 (RFC2002、RFC2977、RFC3344、RFC3846、RFC3957、RFC3775、RFC3776、RFC4285) 支持移动终端设备MS的流动性。在传统的IP协议中如果移动终端设备变换其IP子网络,则移动终端设备MS每一次必须对其IP地址进行适配调整,因此对移动终端设备MS寻址的数据分组必须选择正确的路径。为了保持当前的TCP连接,移动终端设备MS必须保持其IP地址,因为地址变换必然会导致连接中断。MIP协议能够在两个地址、也就是一个永久的本地地址和一个第二个临时的管理地址之间的透明连接。管理地址 (Care-Of-Adresse) 是以下这样一种地址:通过该地址当前可以联系到移动终端设备MS。

[0005] 只要移动终端设备MS不停留在最初的本地网络中,本地代理 (Home Agent) HA是移

动终端设备MS的一个代理。经常告知本地代理移动计算机MS的当前停留位置。本地代理HA通常是在移动终端设备的本地网络中的路由器的元件。如果移动终端设备MS位于其本地网络的外部,则本地代理HA提供一种功能,因此可以通知移动终端设备MS。然后本地代理HA把向移动终端设备MS寻址的数据分组传递到移动终端设备MS的当前子网络中。

[0006] 外部代理 (Foreign Agent) FA位于移动终端设备MS所移动到的子网络中。外部代理FA把到达的数据分组传递给移动终端设备MS或移动计算机MS。外部代理FA位于一种所谓的外部网络 (Visited Network)。外部代理FA同样通常是路由器的元件。外部代理FA在移动终端设备MS和其本地代理HA之间为所有管理的移动数据分组选择路由。外部代理FA打开由本地代理HA发送的隧道IP数据分组并且把其数据传递给移动终端设备MS。

[0007] 移动终端设备MS的本地地址是一个这样的地址:利用该地址可以永久地联系到移动终端设备MS。本地地址有同本地代理HA一样的地址前缀。管理地址是这样的IP地址:移动终端设备MS在外部网络中应用该地址。

[0008] 本地代理HA管理所谓的移动连接表 (MBT: Mobility Binding Table)。在该表中的条目用于移动终端设备MS的两个地址 (亦即:本地地址和管理地址)彼此相互对应并相应地对数据分组重新进行路由。

[0009] MBT表包含关于本地地址、管理地址和关于这个时间间隔说明的条目,在该时间间隔内对应关系是有效的 (lifetime)。

[0010] 图1示出了按照现有技术的移动连接表MBT的实例。

[0011] 外部代理FA包含一个访问者列表 (VL: Visitor List),其包含关于移动终端设备MS的信息,该移动终端设备刚好位于外部代理FA的IP网络中。

[0012] 图2示出了按照现有技术的这种访问者列表。

[0013] 因此移动计算机MS可以接入一个网络,其首先必须询问:其是位于其本地网络还是外部网络中。移动终端设备MS附加必须询问:哪一个计算机位于本地代理或者外部代理的子网络中。通过所谓的代理发现确定这些信息。

[0014] 通过后面的登记移动终端设备MS可以把其当前所在位置告知其本地代理HA。为此移动计算机或者移动终端设备MS给本地代理发送当前的管理地址。为了进行登记,移动计算机MS把登记需求或者登记请求发送给本地代理。本地代理HA在其表中记录管理地址并以登记应答答复。为此当然存在安全问题。因为原则上每个计算机都可以给本地代理HA发送登记请求,可以简单地欺骗本地代理,计算机移动到另外的网络中。这样,外部计算机就可能接收移动计算机或者移动终端设备MS的所有数据分组,而发送者对此一无所知。为了避免上述情况,移动计算机MS和本地代理HA拥有一个公共的密钥。如果移动计算MS返回到其本地网络中,则其在其本地代理HA中取消登记,因为移动计算机MS从现在起自己就可以接收所有数据分组。移动无线网络此外必须具有如下安全特性。信息仅仅对于所希望的通信伙伴开放,也就是说不允许不希望的窃听者对所传输的数据进行存取。移动无线网络因此必须具有机密性 (Confidentiality)。此外必须具有真实性 (Authenticity)。真实性允许一个通信伙伴毫无疑问地确定:是否真的要建立到所希望的通信伙伴的通信或者是否一个外人冒充了通信伙伴。可以对每个消息或每个连接进行验证。如果在连接的基础上进行验证,则仅仅在通信伙伴的对话 (Session) 开始时一次验明。当然对于另外的对话过程以此为出发点,即后面消息此外来自相应的发送者。即使如果确定通信伙伴的一致性,也就是说验证

了通信伙伴,也可能出现这样的情况,即该通信伙伴不允许访问所有资源或者不允许使用该网络的所有业务。在这种情况下相应的授权是以前面的通信伙伴验证为前提条件的。

[0015] 在移动数据网络中消息必须跨越空中接口上的较长距离并因此对于可能的攻击者来说容易实现。因此在移动和无线数据网络中安全方面问题特别重要。在数据网络中提高安全性的主要方法是加密技术。通过加密能够通过非安全的通信路径、例如通过空中接口传输数据,无授权的第三方不能存取数据。为了加密数据、也就是所谓借助于加密算法把明文转变为密码文本。已加密的文本可以经过非安全的数据传输信道传输,接下来译码或者解密。

[0016] 作为许多令人期待的无线接入技术,WiMax (Worldwide Interoperability for Microwave Access) 建议作为新的标准,其用于IEEE 802.16的无线传输。以WiMax能够以每秒超过100Mbit的数据传输率管理直到50km的发射台。

[0017] 图3示出了用于WiMax无线网络的参照模式。一个移动终端设备MS位于接入网络(ASN: Access Serving Network)的范围内。该接入网络ASN通过至少一个访问网络(Visited Connectivity Service Network VCSN)或者中间网络与本地网络HCSN (Home Connectivity Service Network) 连接。不同网络通过接口或者参考点R彼此连接。移动站MS的本地代理HA位于本地网络(HCSN)中或位于访问网络(VCSN)之一中。

[0018] WiMax支持移动IP的两个实现变体,即:一个所谓的客户MIP (CMIP) (在这种情况下移动站MS自己实现MIP客户功能)和代理MIP (PMIP) (在这种情况下通过WiMax接入网络ASN实现MIP客户功能)。为此在ASN中预先规定的功能性称作代理移动节点(PMN)或PMIP客户。由此MIP也可以与本身不支持MIP的移动站MS一起使用。

[0019] 图4示出了如果本地代理HA位于访问网络VCSN中按照现有技术代理MIP (PMIP)的情况下的连接建立。

[0020] 当在移动终端设备MS和一个基站BS之间建立无线连接之后首先实现接入验证。借助于所谓的AAA服务器(AAA: Authentication, Authorization, Accounting)实现验证、授权和结账功能。在移动终端设备MS和本地网络(HAAA)的AAA服务器之间交换验证消息,借助于该验证消息获得本地代理HA的地址和验证密钥。在本地网络中的验证服务器包含用户的特征数据。AAA服务器包含一个验证询问消息,其包含移动终端设备的用户身份。AAA服务器在成功的接入验证之后产生一个MSK密钥(MSK: Master Session Key)用于保护在移动终端设备MS和接入网络ASN的基站BS之间的通信链路。该MSK密钥由本地网络的AAA服务器经过中间网络CSN传输给接入网络ASN。

[0021] 在接入验证之后,正如在图4中看到的,配置在接入网络ASN中的DHCP代理服务器。如果IP地址和主机配置已经包含在AAA应答消息中,则在DHCP代理服务器中下载全部信息。

[0022] 在成功验证和授权之后移动站或者移动终端设备MS发送一个DHCP发现消息并且进行IP地址分配。

[0023] 如果一个移动终端设备MS接入网络中,则该移动终端设备MS必须询问:其是位于本地网络中还是位于外部网络中。此外移动终端设备MS必须询问:哪一个计算机位于本地代理或外部代理的各自网络中。通过所谓的代理发现来确定这些信息。存在两种形式的代理发现,即:所谓的代理广告(Agent Advertisement)和代理请求(Agent Solicitation)。

[0024] 在代理广告的情况下,代理(也就是说本地或外部代理)周期性地给予网络的所有

计算机或者移动终端设备发送广播消息。每个在确定时间间隔监听广播消息的计算机如此可以识别在各自子网络内的代理。

[0025] 如果重新激活移动终端设备MS,则其实际上一般不等待下一个代理广告。移动终端设备MS必须立即了解,其刚好位于哪一个子网络中。在所谓的代理请求的情况下,移动终端设备MS因此给各自网络的所有计算机发送一个请求,执行代理广告。通过代理请求可以迫使移动终端设备MS自身立刻识别代理,如此显著缩短等待时间。如果没有代理广告,例如在包丢失或网络变换的情况下,则当然也执行代理请求。借助于所述代理发现移动终端设备MS还可以确定:其是位于其本地网络中还是位于外部网络中。根据在代理广告消息内部的分组信息移动终端设备MS识别其本地代理。如果移动终端设备MS从一个外部网络得到消息包,则其可以附加确定:其是否从最后的广告起改变其位置。如果移动终端设备MS没有接收到广告消息,则移动终端设备MS首先以此为出发点,即:其位于本地网络中并且本地代理HA被干扰。移动终端设备然后尝试与网络的路由器进行联系,以便确认这种猜测。如果移动终端设备MS并不处于其本地网络中,则其接下来尝试,联系DHCP服务器并且获得子网络的地址。如果成功,则移动终端设备MS把这个地址用作所谓的并置管理地址(Colocated Care-Of-Adresse)并且与本地代理HA进行联系。并置管理地址是在外部网络中分配移动终端设备MS的地址,该地址也被传送给本地代理HA。

[0026] 应该区分基于网络的移动管理(PMIP)和基于终端设备的移动管理(CMIP)。在基于终端设备的移动管理CMIP中终端设备支持移动IP(MIP)。

[0027] 图4示出了在传统的基于网络的移动管理(PMIP)的情况下的连接建立,而图5示出了在传统的基于终端设备的移动管理(CMIP)的情况下的连接建立。

[0028] 当在移动终端设备MS和网络之间建立连接时本地网络的验证服务器(H-AAA)在成功验证用户之后发送一个验证确认消息(SUCCESS)。该验证确认消息告知验证客户,成功结束用户验证。

[0029] 在代理MIP或者基于网络的移动管理(PMIP)的情况下移动终端设备不支持移动IP或者在移动终端设备MS中没有激活相应的MIP软件。

[0030] 与此相对照,在客户MIP(CMIP)的情况下或者在基于终端设备的移动管理的情况下支持各自的终端设备或者移动站MS的移动IP。

[0031] 在代理MIP中移动终端设备MS仅仅识别一个由DHCP分配的IP地址。移动终端设备不知道移动终端设备MS的管理地址,而是PMIP客户、外部代理FA和本地代理HA知晓该移动终端设备MS的管理地址。与此相对照,在客户MIP中移动终端设备MS识别其两个IP地址,也就是说不仅识别本地地址而且也识别管理地址。

[0032] 正如在图4、5中可以看出的,在IP地址分配之后进行MIP登记。在MIP登记时本地代理HA发送关于移动终端设备MS的当前位置的信息。为了进行登记,移动终端设备MS或者相应的PMIP客户给本地代理HA发送一个包含当前的管理地址的登记请求。本地代理HA在由其管理的表中记录管理地址并且以登记应答(Registration Reply)进行答复。因为原则上每个计算机都可以给本地代理HA发送登记请求,一个计算机或移动终端设备MS移动到另外的网络中,可能很简单地欺骗本地代理HA。为了避免欺骗,不仅移动终端设备MS而且本地代理HA拥有一个公共的密钥,也就是一个所谓的移动IP密钥(MIP-KEY)。

[0033] 在代理MIP(PMIP)中,由PMIP客户在接入网络ASN内部通过外部代理FA给本地代理

HA传输登记请求(MIPRRQ)。本地代理HA能够从所属的验证服务器H-AAA为用户分配一个密钥并且与MIP登记应答(MIP Registration Reply)一起传输这个密钥,正如在图4中示出的。

[0034] 在基于终端设备的移动管理(CMIP)的情况下,登记询问消息(MIPRRQ)直接从移动终端设备MS经过外部代理FA指向本地代理HA,正如在图5中示出的。

[0035] 在WiMax接入网络中,除了移动IP(CMIP)外还使用代理移动IP(PMIP),以便能够进行针对客户的移动管理,该客户本身不具有移动IP客户功能。对于PMIP,在接入网络中设置一个代理移动IP客户,其代表客户发送MIP信令。该移动协议在WiMax中用于在两个接入网络ASN或者在两个网络供应商NAP之间切换。对此所属的WiMax本地代理有选择地位于一个WiMax本地网络HCSN中或位于访问的WiMax网络(VCSN)中。在WiMax的情况下,以此为出发点,即:本地AAA服务器位于本地网络HCSN中,其识别与用户共享的长期加密密钥以及另外的用户参数。

[0036] 在进行登记时,WiMax本地代理在WiMax本地AAA服务器中询问安全参数,例如临时的加密密钥。这是必须的,因此仅仅被授权的客户在本地代理中可以进行登记并且为了保护MIP信令。作为验证和密钥说明协议(Schlüsselvereinbarungsprotokoll)的一部分、移动终端设备以验证服务器执行该协议、移动终端设备也可以推导这些安全参数。对此在WiMax接入网络中从所谓的EMSK密钥(Extended Master Session Key)中推导并提供AMSK或者移动IP根密钥(MIP-RK)。接下来从这个移动IP根密钥中推导出另外密钥用于保护在移动节点或者外部代理FA和本地代理HA之间的不同通信链路。对此分别通过用于客户移动IP情况和代理移动IP情况的自身密钥推导不同的移动IP变体、比如移动IP V6和移动IP V4。

[0037] 在传统的WiMax接入网络中不支持交互工作或者与其他形式网络的合作。

[0038] 图6示出了按照现有技术的在WiMax接入网络和3GPP本地网络之间的合作。正如从图6中可以看出的,在WiMax接入网络中设置一个验证代理服务器(AAA-转接),其具有一个交互工作单元IWU作为到3GPP本地网络的接口。验证服务器在与3GPP网络交互工作的情况下承担密钥产生和密钥推导的任务,这在网络申请的范围内是必需的,以便为用户或者移动终端设备激活代理移动IP。在代理移动IP的情况下一个代理移动IP客户位于WiMax本地网络WiMax-CSN的ASN网关或者验证代理服务器中。该WiMax本地网络WiMax-CSN与3GPP网络连接,正如在图6中可以看出的。在代理移动IP的情况下,交互工作单元IWU因此能够在网络申请时为了保护在代理移动IP客户和本地网络之间的链路而产生一个移动IP密钥(MIP-Key)。对此代理移动IP客户最好位于ASN网关中并因此形成接入网络结构的一部分。因此在代理移动IP的情况下不必改变3GPP验证服务器或者3GPP服务器不必满足WiMax接入网络的技术条件。

[0039] 但是在客户代理移动IP的情况下不支持在WiMax接入网络和3GPP本地网络之间的交互工作。目前不存在适合的协议,以便把安全参数传递给客户或者移动终端设备。其原因在于:移动终端设备在传统的优选措施下从验证协议和密钥说明协议中推导出安全参数。

发明内容

[0040] 因此本发明的技术问题是:建立为了保护在移动终端设备和接入网络的节点之间的数据传输而提供接入特定的密钥的方法和系统,如果本地网络的验证服务器不支持移动

管理,则也使客户IP (CMIP)成为可能。

[0041] 本发明建立了为保护在移动终端设备和接入网络的节点之间的数据传输而提供接入特定的密钥的方法,其中在验证移动终端设备时验证服务器产生一个对话密钥,从中推导出基本密钥并传输给交互工作代理服务器,其从传输的基本密钥中推导出接入特定的密钥并且提供给接入网络的节点。

[0042] 在本发明方的一个优选实施形式中通过MSK (Master Session Key) 密钥或通过EMSK (Extended Master Session Key) 密钥形成对话密钥。

[0043] 在本发明的方法中因此考虑本地主机对话密钥 (MSK或者EMSK),其出于安全原因不允许抛弃本地网络的验证服务器 (AAA),以便从中推导出伪密钥或者基本密钥,其接下来传输给交互工作代理服务器,其中交互工作代理服务器从接收的基本密钥中根据预先规定的密钥体系推导出所需的接入特定的密钥并且为接入网络的每个节点提供这种接入特定的密钥。

[0044] 在本发明方法的一个实施形式中验证服务器位于移动终端设备的本地网络中。

[0045] 在本发明方法的一个实施形式中借助于预先规定的第一推导函数从对话密钥中推导出基本密钥。

[0046] 主要通过HMAC-SHA1推导函数、HMAC-SHA256推导函数、HMAC-MD5推导函数、SHA1推导函数、SHA-256推导函数或MD5推导函数形成第一推导函数。

[0047] 在本发明方法的一个优选实施形式中依赖于对话密钥和字符串 (String) 实现基本密钥的推导。

[0048] 在本发明方法的一个实施形式中借助于EAP协议实现在验证服务器中验证移动终端设备。

[0049] 在本发明方法的另一个实施形式中借助于UMTS-AKA协议实现在验证服务器中验证移动终端设备。

[0050] 在本发明方法的一个替代实施形式中借助于HTTP-Digest-AKA协议实现在验证服务器中验证移动终端设备。

[0051] 在本发明方法的另一个实施形式中借助于Diameter协议或Radius协议实现在验证服务器和交互工作代理服务器之间的数据传输。

[0052] 在本发明方法的一个优选实施形式中通过WiMax网络形成接入网络。

[0053] 在本发明方法的一个优选实施形式中通过3GPP网络形成本地网络。

[0054] 在本发明方法的一个优选实施形式中通过交互工作代理服务器借助于第二推导函数从传输的基本密钥中推导出移动IP根密钥。

[0055] 对此主要通过HMAC-SHA1推导函数、HMAC-SHA256推导函数、HMAC-MD5推导函数、SHA1推导函数、SHA-256推导函数或MD5推导函数形成第二推导函数。

[0056] 在本发明方法的一个优选实施形式中借助于第三推导函数从已推导出的移动IP根密钥中推导出用于保护在移动终端设备和接入网络的节点之间数据传输的接入特定的密钥。

[0057] 第三推导函数主要涉及HMAC-SHA1推导函数、HMAC-SHA256推导函数、HMAC-MD5推导函数、SHA1推导函数、SHA-256推导函数或MD5推导函数。

[0058] 在本发明方法的一个实施形式中对于在接入网络的节点和移动终端设备之间的

不同传输链路分别推导出一个所属的接入特定的密钥。

[0059] 在本发明方法的一个实施形式中移动终端设备在验证时同样产生对话密钥并且从中推导出该接入特定的密钥。

[0060] 此外本发明建立用于提供基本密钥的验证服务器,从基本密钥中可以推导出用于保护在移动终端设备和接入网络的节点之间数据传输链路的接入特定的密钥,其中验证服务器在验证移动终端设备时产生一个对话密钥,从中借助于推导函数推导出基本密钥并且提供给交互工作代理服务器。

[0061] 此外本发明建立一个用于提供接入特定的密钥的交互工作代理服务器,该接入特定的密钥用于保护在移动终端设备和接入网络的节点之间进行的数据传输,其中交互工作代理服务器从由验证服务器传输的基本密钥中推导出接入特定的密钥并提供给接入网络的节点。

[0062] 此外本发明建立具有多个接入网络和移动终端设备的至少一个本地网络的数据传输系统,其中本地网络的验证服务器在验证移动终端设备时产生对话密钥并从中推导出公共基本密钥,其被传输给接入网络,接入网络分别具有交互工作代理服务器,其从传输的基本密钥中推导出至少一个接入特定的密钥,该接入特定的密钥分别预先规定用于保护在移动终端设备和各自接入网络的节点之间的数据传输链路。

[0063] 此外参考用于阐述本发明特征的附图描述为了保护在移动终端设备和接入网络的节点之间数据传输而提供接入特定的密钥的本发明方法和本发明系统的优选实施例。

附图说明

[0064] 图1:按照现有技术的移动申请表(**Mobilitätsanmeldungstabelle**) ;

[0065] 图2:按照现有技术的访问者列表;

[0066] 图3:用于WiMax无线网络的参考模型;

[0067] 图4:按照现有技术的在代理移动IP (PMIP) 情况下的连接建立;

[0068] 图5:按照现有技术的在客户MIP (CMIP) 情况下的连接建立;

[0069] 图6:用于描述按照现有技术、在WiMax接入网络和3GPP网络之间合作的方框图;

[0070] 图7:具有提供接入特定的密钥的本发明系统的可能实施形式的方框图;

[0071] 图8:描述提供接入特定的密钥的本发明方法的可能实施形式的信号示意图;

[0072] 图9:描述提供接入特定的密钥的本发明方法的可能实施形式的另外信号示意图。

具体实施方式

[0073] 图7示出了一个网络结构,其中可以采用本发明提供接入特定的密钥的方法。移动终端设备1 (MS=Mobile Station) 经过接口R1连接在接入网络2 (ASN=Access Service Network) 上。接入网络2经过接口R3连接在访问网络3 (VCSN=Visited Connectivity Service Network) 上。这个访问网络3在其一侧经过接口R5与本地网络4 (HCSN=Home Connectivity Service Network) 进行连接。

[0074] 如果移动终端设备1从第一个接入网络2移动到第二接入网络2',则在第一和第二接入网络之间实现切换 (Handover)。这种切换 (Handover) 在WiMax技术规范中称作“宏移动管理”或也称作“R3移动”或者“互相ASN移动”。该访问网络3和本地网络4分别连接在接入业

务供应商 (ASP) 的网络或连接在因特网上。

[0075] 每个接入网络2包含多个基站6,其自身方面经过接口R6连接在ASN网关节点上。在图6中示出的ASN网关节点5包含一个验证服务器5A、一个MIP外部代理5B和可选的一个PMIP客户5C以及可选的一个交互工作代理单元7。在每个访问网络3中存在一个AAA服务器3A,正如在图6中示出的。在本地网络4中同样存在一个验证服务器4A以及一个本地代理4B。在一个可能的替换实施形式中在本地网络4中存在交互工作单元7。

[0076] 在移动终端设备1一侧区分两种情况。移动终端设备1本身支持移动IP并且具有一个自己的CMIP客户或移动终端设备1不支持移动IP并且需要在接入网络2的网关节点5中的PMIP客户5C。

[0077] 图8示出了用于阐述本发明方法的可能实施形式的信号图,其中交互工作单元7在第一实施形式中位于接入网络2中或在一个替换实施形式中位于本地网络4中。在本发明方法中,提供用于保护在移动终端设备1和接入网络2的任意节点之间进行的数据传输的接入特定的密钥,其中在验证移动终端设备1时,位于移动终端设备1的本地网络4中的验证服务器4A产生一个对话密钥并且从这个对话密钥中推导出一个基本密钥,该基本密钥被传输给交互工作代理服务器7,正如在图7中示出的。交互工作代理服务器7从接收的基本密钥中借助于推导函数推导出所需的接入特定的密钥并且提供该接入特定的密钥用于接入网络2的各自节点。从中要推导出传输的基本密钥的对话密钥在一个实施形式中是MSK (Master Session Key) 或EMSK (Extended Master Session Key) 密钥。正如在图8中示出的,验证服务器4A借助于HMAC-SHA1推导函数从扩展主对话密钥EMSK中推导出一个伪EMSK密钥或一个公共的基本密钥。在一个替换实施形式中通过HMAC-SHA256推导函数、HMAC-MD5推导函数、SHA1推导函数、SHA256推导函数或MD5推导函数形成该推导函数。已推导出的基本密钥或者伪密钥在EAP成功消息与主对话密钥ESK一起传输给交互工作单元7,其例如形成为交互工作代理服务器。

[0078] 在本发明方法的一个可能实施形式中依赖于对话密钥MSK和/或EMSK并且附加从符号串、也就是说根据变体之一推导出基本密钥或者伪密钥:

[0079] $PEMSK = H(MSK, EMSK, \text{"String"})$

[0080] $PEMSK = H(MSK, \text{"String"})$

[0081] $PEMSK = H(EMSK, \text{"String"})$ 。

[0082] 在这个在图8中示出的实施形式中借助于EAP数据传输协议验证移动终端设备1。在一个替换实施形式中在验证服务器4A中借助于UMTS-AKA协议或借助于HTTP-Digest-AKA协议验证移动终端设备。最好借助于Diameter协议或Radius协议实现在验证服务器4A和交互工作代理服务器7之间的数据传输。

[0083] 已推导出的基本密钥或者伪密钥在密钥体系中是中间级。该基本密钥可以作为公共基本密钥也转送给不同的、预先规定在不同的接入网络3中的交互工作代理服务器7。接入网络2例如是WiMax网络。验证服务器4A所处的本地网络4例如是3GPP网络。

[0084] 正如在图8中看出的,交互工作代理服务器7一旦获得传输的基本密钥,就借助于第二推导函数形成移动IP根密钥IMP-RK。第二推导函数可能同样涉及HMAC-SHA1推导函数、HMAC-SHA256推导函数、HMAC-MD5推导函数、SHA1推导函数、SHA-256推导函数或MD5推导函数。在另一个实施形式中也可以采用另外的推导函数或者密钥推导函数KDF。从如此推导出

的移动IP根密钥MIP-RK中可以根据密钥体系推导出用于保护在移动终端设备1和接入网络2的节点之间数据传输的另外接入特定的密钥。第三推导函数例如涉及HMAC-SHA1推导函数、HMAC-SHA256推导函数、HMAC-MD5推导函数、SHA1推导函数、SHA-256推导函数或涉及MD5推导函数。

[0085] 应用移动IP根密钥MIP-RK,以便从中产生应用密钥或者接入特定的密钥,例如:

[0086] $MN-HA-MIP4 = H(MIP-RK, "String" | HA-IP)$

[0087] $MN-HA-CMIP6 = H(MIP-RK, "String" | HA-IP)$

[0088] $MN-FA = H(MIP-RK, "String" | FA-IP)$

[0089] $FA-H = H(MIP-RK, "String" | FA-IP | HA-IP | NONCE)$ 。

[0090] 符号“|”代表字符串的级联。

[0091] 对此还可以如下修改密钥推导,即为PMIPv4和CMIPv4推导出独立的密钥。例如:

[0092] $MN-HA-CMIP4 = H(MIP-RK, "CMIP4MNHA" | HA-IP)$

[0093] $MN-HA-PMIP4 = H(MIP-RK, "PMIP4MAHA" | HA-IP)$

[0094] 对于在接入网络2的节点和移动终端设备1之间的每一个不同的数据传输链路以这种方式分别从移动IP根密钥中推导出一个所属的接入特定的密钥,移动IP根密钥自身从传输的基本密钥中推导出。

[0095] 在本发明方法中,在用户的基于EAP的网络申请范围内如此扩展目前的密钥推导,即:交互工作代理服务器7给接入网络提供适合的CMIP密钥,其同样也可以用于PMIP。在本发明方法中借助于适当的密钥推导函数KDF通过验证服务器从MSK和/或EMSK和/或另外的输入、例如字符串中推导出基本密钥或者伪密钥。

[0096] 图9示出了用于阐述基于本发明方法的原理的信号图。在验证移动终端设备1时,借助于验证和密钥说明协议、例如基于Radius或Diameter的EPA在第一网络中的安全服务器或者验证服务器4A在临时的加密密钥TKS、例如主对话密钥MSK或者EMSK的基础上产生基本密钥或者伪密钥PTSK或者临时的伪加密密钥。接下来把利用推导函数推导出的伪密钥传输给例如位于第二网络中的交互工作代理服务器7,其中在其一侧为每个应用服务器或者节点8、9从另外的推导函数中推导出一个接入特定的密钥。接下来每个应用服务器8、9从交互工作代理服务器7获得为其推导的接入特定的密钥。接下来借助于所传输的密钥对在终端设备1和各自应用服务器8、9之间的数据传输链路以加密方式进行保护。

[0097] 利用本发明方法,验证服务器(例如WLAN服务器或3GPP服务器)能够用于WiMax接入网络,其中验证服务器不必提供所期待的WiMax接入网络的CMIP/PMIP功能,而是仅仅为了必须扩展功能,从对话密钥中推导出基本密钥。本发明方法此外提供这样的优点,即:在WiMax接入网络中也支持CMIP并且因此避免了关于宏移动的各种限制。在本发明的方法中,WiMax网络除了设置交互工作代理服务器7之外不需要另外的改变或修改。移动终端设备1、验证服务器以及交互工作代理服务器7知道使用哪个基本密钥或者伪密钥。由此能够在WiMax网络内部支持不同的MIP密钥(Bootstrapping-Varianten)。在本发明方法中把例如来自3GPP网络的密钥材料转变为WiMax网络的密钥材料,其中WiMax网络可以使用已形成的密钥而不必进行适配调整。

[0098] 在本发明的一个实施形式中,在WiMax网络外部(例如在3GPP网络)中建立了根据本发明的验证功能。本发明方法使未来的WiMax-3GPP交互工作成为可能而不必由此受到

WiMax网络的限制。本发明方法的另外优点在于：对于任意应用很容易扩展在不同网络之间以及为移动应用提供密钥的交互工作。在本发明方法中交互工作代理服务器7只需了解：必须提供哪一种应用特定的密钥以及怎样推导出这些密钥。因此在本发明方法中不需要本地验证服务器为所有接入的不同网络分别产生一个所需的密钥。与此相应在本发明方法中不同网络比较简单地灵活接入本地网络。

[0099] 在本发明方法中移动终端设备1在验证时同样产生对话密钥并且以相同的方式推导出接入特定的密钥。

移动连接表

本地地址	管理地址	时间间隔 (ms)
131.192.180.42	129.142.23.42	100
213.123.24.140	172.23.142.49	150
...

图1现有技术

访问者列表

本地地址	本地代理地址	媒体地址	时间间隔
131.192.180.42	129.142.23.42	08-00-46-26-75-6A	100
213.123.24.140	172.23.142.49	00-02-B3-77-43-00	150
...

图2现有技术

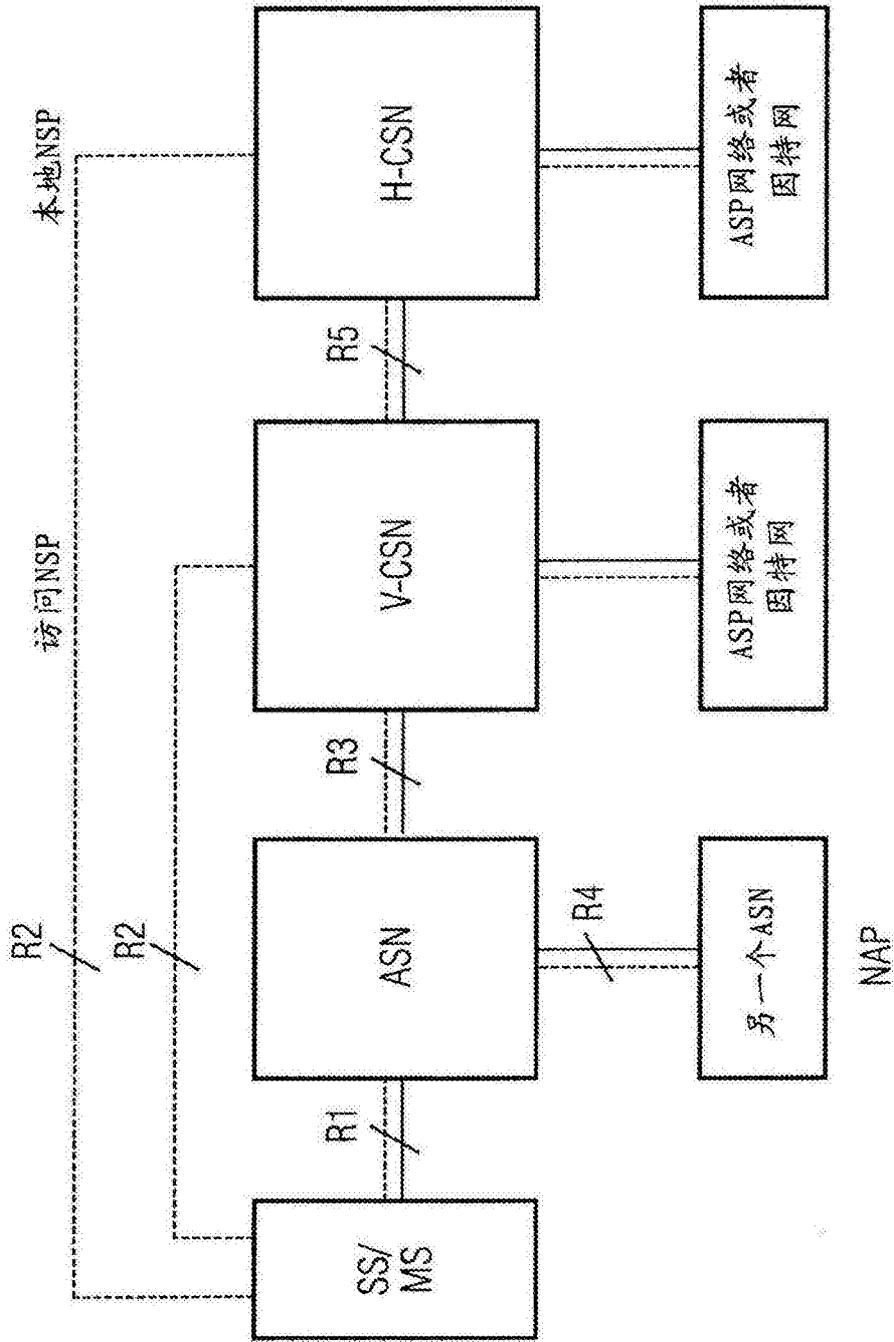


图3现有技术

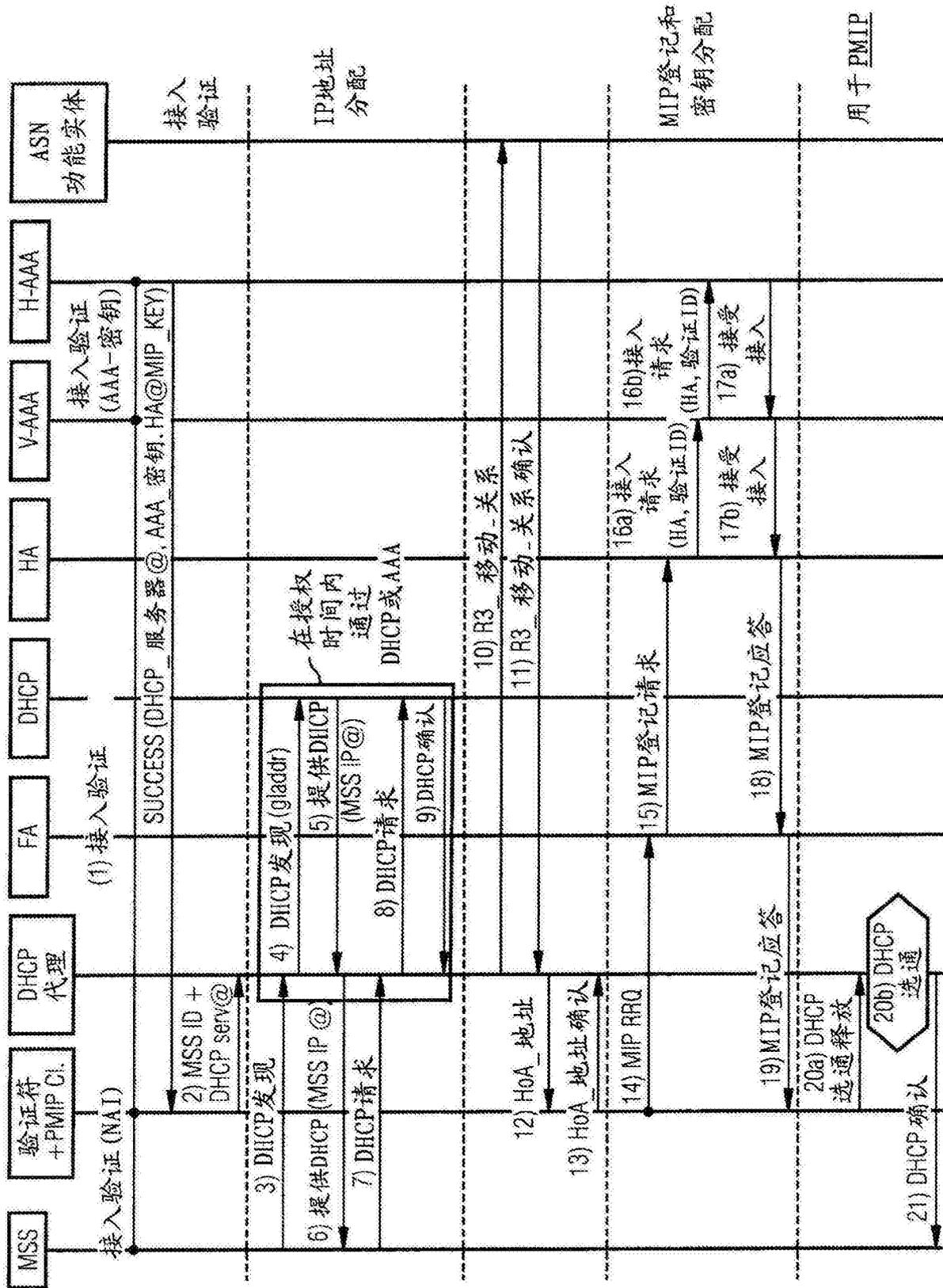


图4现有技术

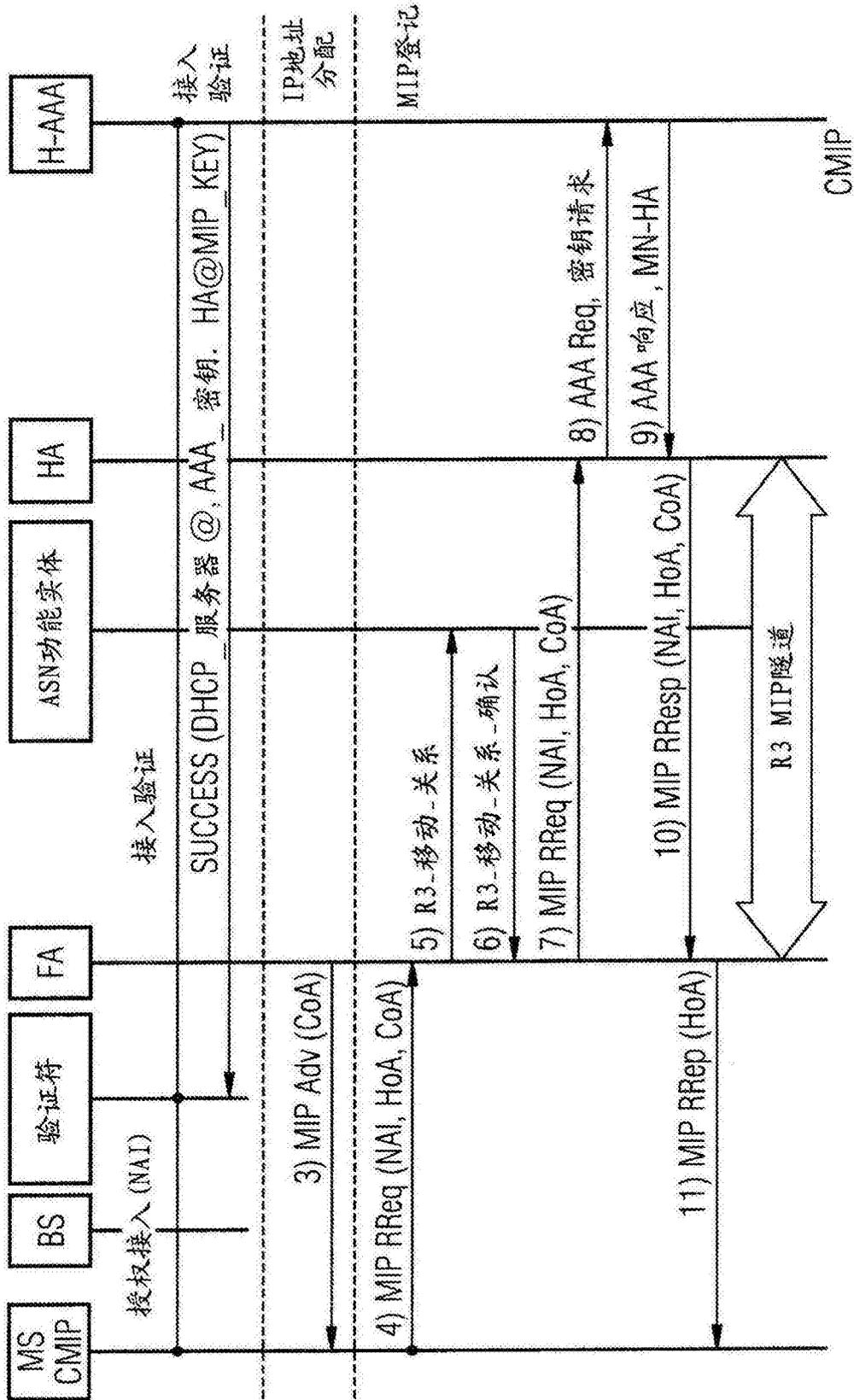


图5现有技术

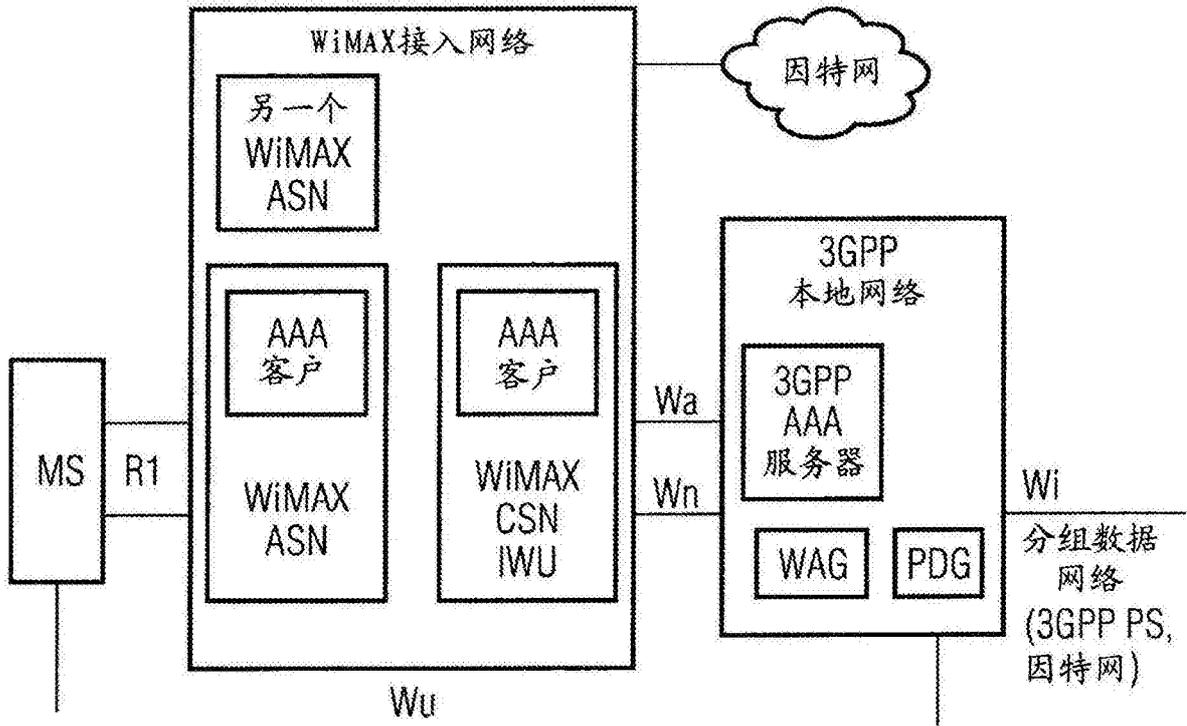


图6现有技术

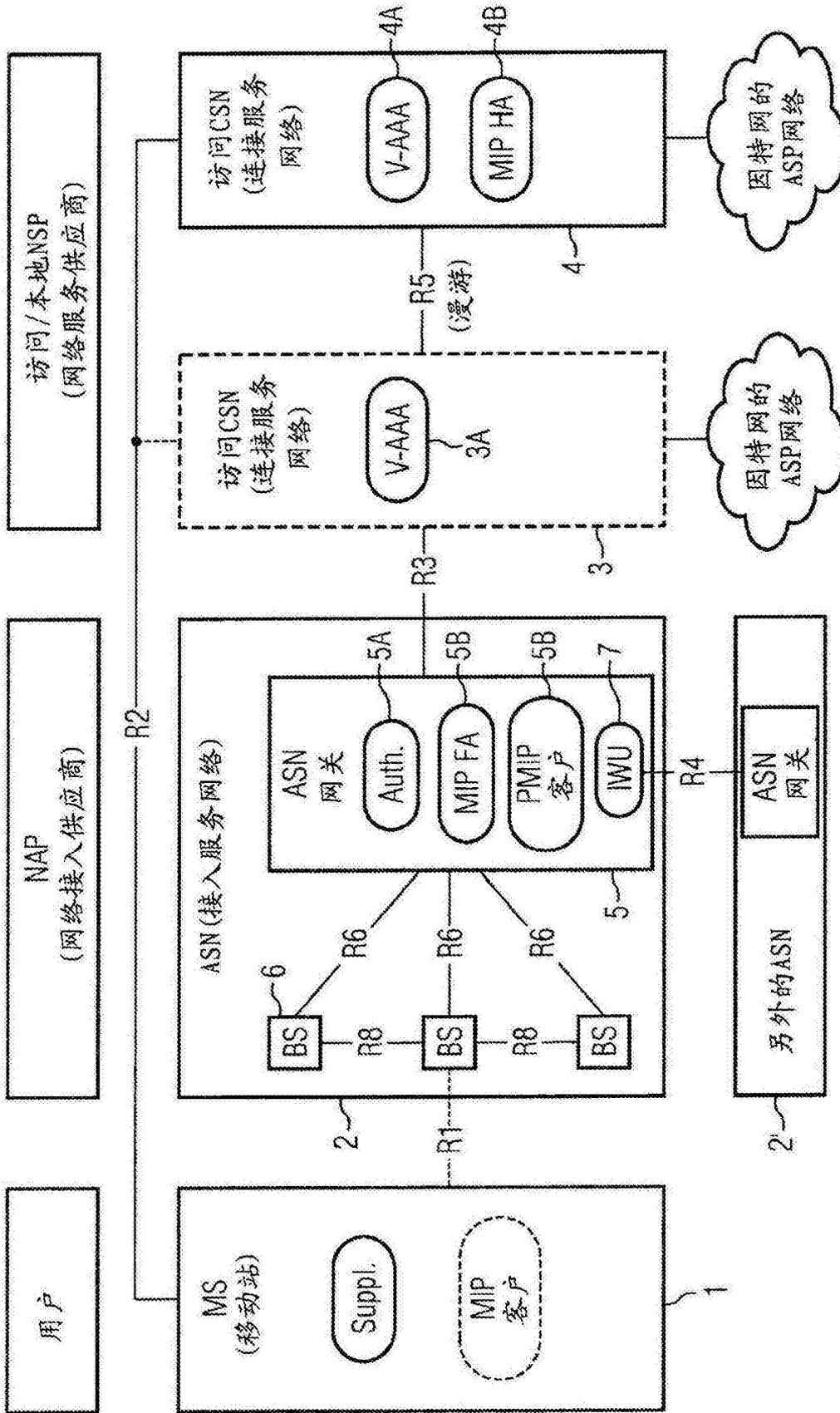


图7

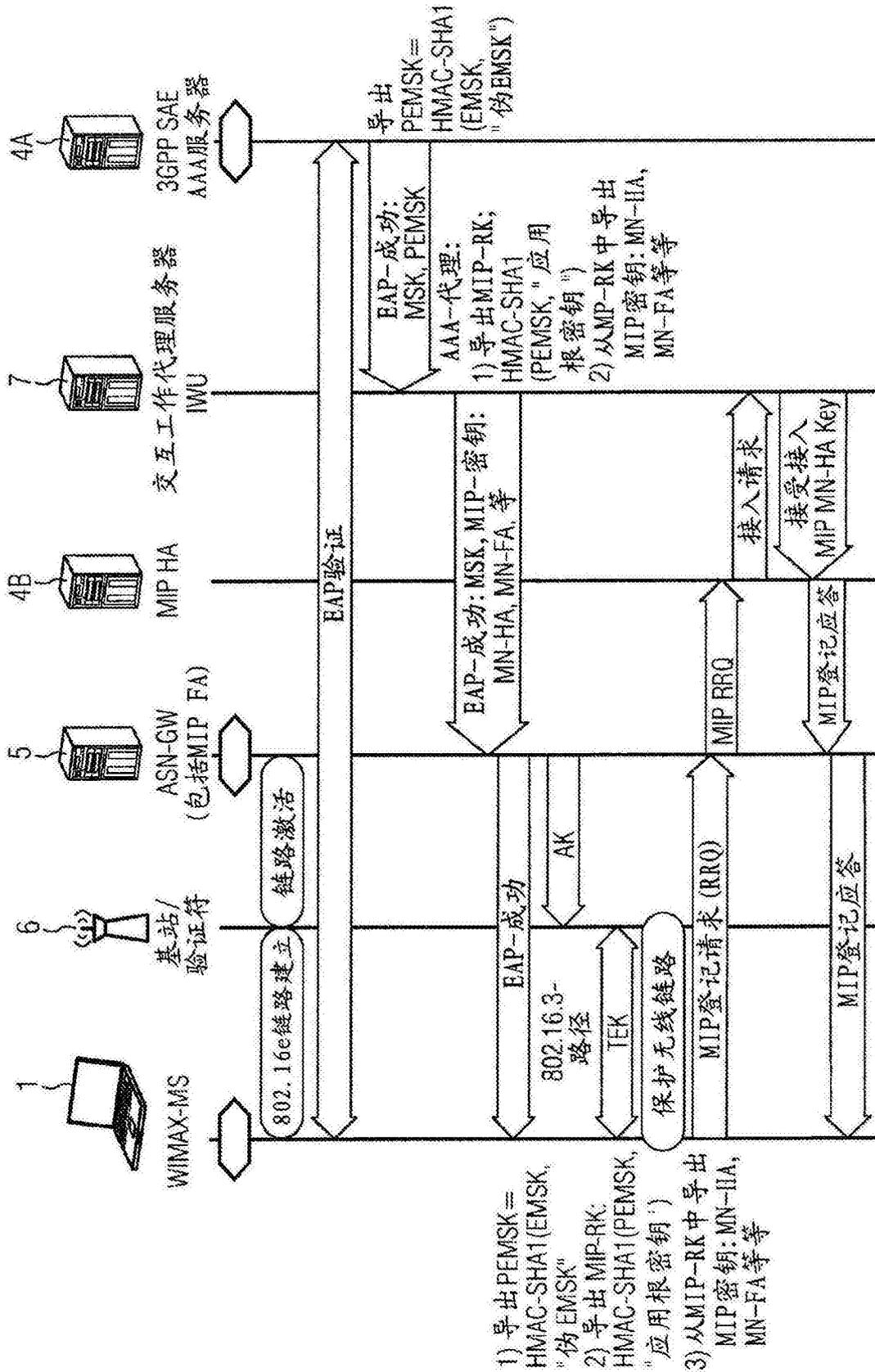


图8

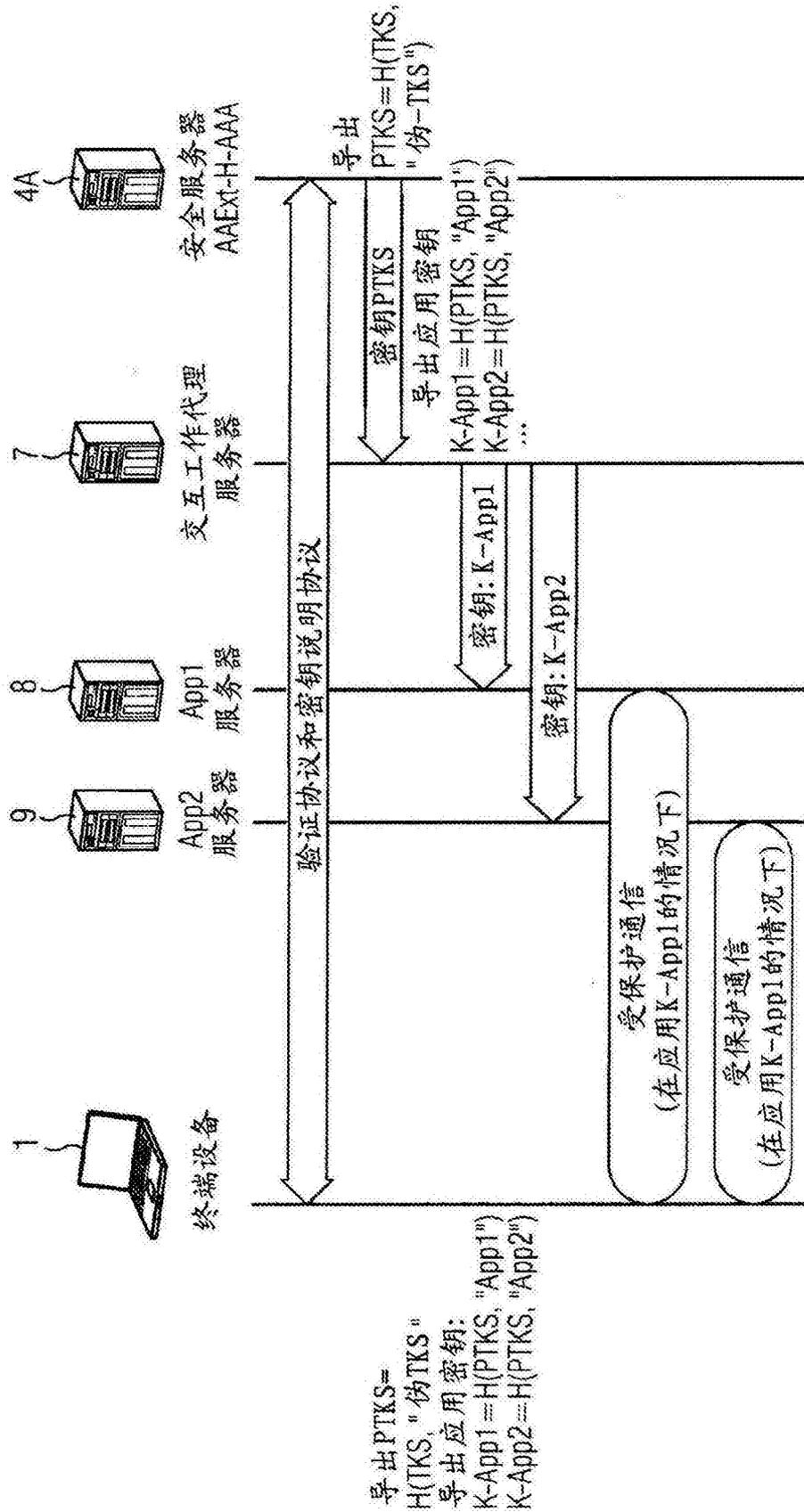


图9