



(12) 发明专利

(10) 授权公告号 CN 101496387 B

(45) 授权公告日 2012.09.05

(21) 申请号 200680053705.3

(51) Int. Cl.

(22) 申请日 2006.12.06

H04M 1/66 (2006.01)

(30) 优先权数据

60/780,176 2006.03.06 US

(56) 对比文件

11/419,382 2006.05.19 US

CN 1688124 A, 2005.10.26, 全文.

(85) PCT申请进入国家阶段日

US 2004/0114553 A1, 2004.06.17, 全文.

2008.09.04

US 6769000 B1, 2004.07.27, 全文.

(86) PCT申请的申请数据

US 2005/0130659 A1, 2005.06.16, 全文.

PCT/US2006/046800 2006.12.06

审查员 杨颖

(87) PCT申请的公布数据

WO2007/102867 EN 2007.09.13

(73) 专利权人 思技术公司

地址 美国加利福尼亚州

(72) 发明人 帕维茨·耶格纳

约瑟夫·A·萨洛韦

贾亚拉曼·R·耶尔

阿南德·K·奥斯瓦尔

(74) 专利代理机构 北京东方亿思知识产权代理

有限责任公司 11258

代理人 宋鹤 南霆

权利要求书 2 页 说明书 4 页 附图 3 页

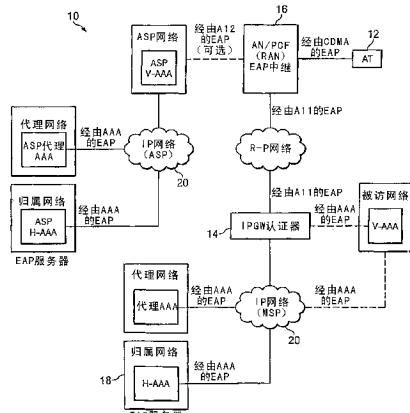
(54) 发明名称

用于移动无线网络中的接入认证的系统和方

法

(57) 摘要

提供了一种用于在移动无线网络中对接入进行认证的系统和方法。该系统和方法包括：通过无线电接入网络，经由高速率分组数据无线电链路和信令接口，与接入终端交换可扩展认证协议（EAP）分组；将 EAP 分组封装在认证授权和计费（AAA）分组中；以及将 AAA 分组发送到认证服务器以便认证。



1. 一种用于在移动无线网络中对接入进行认证的方法,该方法包括:

通过无线电接入网络,经由高速率分组数据无线电链路和信令接口,与接入终端交换可扩展认证协议 EAP 分组;

将所述 EAP 分组封装在认证授权和计费 AAA 分组中;

将所述 AAA 分组发送到认证服务器;以及

基于所述 EAP 分组对接入进行认证。

2. 如权利要求 1 所述的方法,其中所述信令接口是具有用于承载所述 EAP 分组的厂商特定扩展的 A11 信令接口。

3. 如权利要求 1 所述的方法,还包括经由所述高速率分组数据无线电链路和所述信令接口与所述接入终端交换另外的 EAP 分组以建立会话密钥。

4. 如权利要求 1 所述的方法,还包括经由所述高速率分组数据无线电链路和所述信令接口与所述接入终端交换另外的 EAP 分组以建立会话密钥,其中所述信令接口是具有用于承载所述 EAP 分组的厂商特定扩展的 A11 信令接口。

5. 如权利要求 1 所述的方法,还包括经由所述高速率分组数据无线电链路和所述信令接口与所述接入终端交换另外的 EAP 分组以建立会话密钥,

其中,对接入进行认证是利用质询 - 响应协议进行的。

6. 如权利要求 1 所述的方法,还包括经由所述高速率分组数据无线电链路和所述信令接口与所述接入终端交换另外的 EAP 分组以建立会话密钥,

其中,对接入进行认证是利用具有共享密钥的质询 - 响应协议进行的。

7. 如权利要求 1 所述的方法,还包括经由所述高速率分组数据无线电链路和所述信令接口与所述接入终端交换另外的 EAP 分组以建立会话密钥,

其中,对接入进行认证是利用基于证书的协议进行的。

8. 一种用于辅助移动无线网络中的接入认证的网关系统,该网关系统包括:

无线电接入网络接口,用于通过无线电接入网络,经由高速率分组数据无线电链路和信令接口,与接入终端交换可扩展认证协议 EAP 分组;

认证器,用于将所述 EAP 分组封装在认证授权和计费 AAA 分组中;以及

IP 网络接口,用于将所述 AAA 分组发送到认证服务器,其中所述认证服务器用于基于所述 EAP 分组对接入进行认证。

9. 如权利要求 8 所述的网关系统,其中所述信令接口是具有用于承载所述 EAP 分组的厂商特定扩展的 A11 信令接口。

10. 如权利要求 8 所述的网关系统,其中所述 IP 网络接口还操作以用于从所述认证服务器接收会话密钥,并且所述无线电接入网络接口还操作以用于经由所述高速率分组数据无线电链路和所述信令接口向所述接入终端发送认证成功信号。

11. 如权利要求 8 所述的网关系统,其中所述信令接口是具有用于承载所述 EAP 分组的厂商特定扩展的 A11 信令接口。

12. 一种用于在移动无线网络中对接入进行认证的系统,该系统包括:

无线电网络控制器;

认证服务器;以及

耦合到所述无线电网络控制器和所述认证服务器的 IP 网关;

其中,所述 IP 网关操作以用于经由高速率分组数据无线电链路和信令接口通过所述无线电网络控制器与接入终端交换可扩展认证协议 EAP 分组,将所述 EAP 分组封装在认证授权和计费 AAA 分组中,并且将所述 AAA 分组发送到所述认证服务器,其中所述认证服务器用于基于所述 EAP 分组对接入进行认证。

13. 如权利要求 12 所述的系统,其中所述信令接口是具有用于承载所述 EAP 分组的厂商特定扩展的 A11 信令接口。

14. 如权利要求 12 所述的系统,其中所述认证服务器操作以用于经由所述高速率分组数据无线电链路和所述信令接口通过所述 IP 网关和所述无线电网络控制器与所述接入终端交换另外的 EAP 分组以建立会话密钥。

15. 如权利要求 12 所述的系统,其中所述认证服务器操作以用于经由所述高速率分组数据无线电链路和所述信令接口通过所述 IP 网关和所述无线电网络控制器与所述接入终端交换另外的 EAP 分组以建立会话密钥;其中所述信令接口是具有用于承载所述 EAP 分组的厂商特定扩展的 A11 信令接口。

16. 如权利要求 12 所述的系统,其中所述认证服务器操作以用于利用质询 - 响应协议来对接入进行认证,并且经由所述高速率分组数据无线电链路和所述信令接口通过所述 IP 网关和所述无线电网络控制器与所述接入终端交换另外的 EAP 分组以建立会话密钥。

17. 如权利要求 12 所述的系统,其中所述认证服务器操作以用于利用具有共享密钥的质询 - 响应协议来对接入进行认证,并且经由所述高速率分组数据无线电链路和所述信令接口通过所述 IP 网关和所述无线电网络控制器与所述接入终端交换另外的 EAP 分组以建立会话密钥。

18. 如权利要求 12 所述的系统,其中所述认证服务器操作以用于利用基于证书的协议来对接入进行认证,并且经由所述高速率分组数据无线电链路和所述信令接口通过所述 IP 网关和所述无线电网络控制器与所述接入终端交换另外的 EAP 分组以建立会话密钥。

19. 如权利要求 12 所述的系统,其中所述认证服务器操作以用于利用质询 - 响应协议来对接入进行认证,并且经由所述高速率分组数据无线电链路和所述信令接口通过所述 IP 网关和所述无线电网络控制器与所述接入终端交换另外的 EAP 分组以建立会话密钥;其中所述另外的 EAP 分组被封装在 AAA 分组中以便在所述 IP 网关和所述认证服务器之间传输;并且其中所述信令接口是具有用于承载所述 EAP 分组的厂商特定扩展的 A11 信令接口。

20. 一种用于在移动无线网络中对接入进行认证的系统,该系统包括:

用于与接入终端交换可扩展认证协议 EAP 分组的装置;以及

用于在认证授权和计费 AAA 分组中将所述 EAP 分组发送到认证服务器的装置;以及
用于基于所述 EAP 分组对接入进行认证的装置。

21. 如权利要求 20 所述的系统,还包括用于认证所述 EAP 分组的装置,以及用于在认证成功的情况下与所述接入终端建立会话密钥的装置。

用于移动无线网络中的接入认证的系统和方法

技术领域

[0001] 本发明一般地涉及移动通信,更具体而言涉及用于移动无线网络中的接入认证的系统和方法。

背景技术

[0002] 信息技术和因特网的显著增长,以及一般人对及时信息服务的需求,引起了对高性能无线因特网技术的需要。

[0003] 然而,当前的 CDMA2000 数据网络依赖于点对点协议 (PPP) 来建立无线联网会话。这种对 PPP 的依赖导致了严重的性能瓶颈。PPP 信令并没有针对无线环境而被优化,尤其对于移交场景 (handoff scenarios) 来说更是如此。PPP 认证和呼叫建立时间可能为几秒的量级,这对于大多数实时电话应用来说都是不可接受的。另外,单个 PPP 会话就需要相当多的存储器资源,并且 PPP 状态机在处理和存储器方面是颇为密集的。

[0004] 因此,需要减少呼叫建立时间的用于移动无线网络中的接入认证的改进系统和方法。

发明内容

[0005] 根据本发明,基本上减少或消除了与移动无线网络中的认证和呼叫建立相关联的缺点和问题。具体地,本发明通过减少或消除与当前系统相关联的 PPP 建立等待时间而提高了认证和呼叫建立的速度,并且避免了在移动无线网络中的某些组件之间交换的不必要的信令。

[0006] 根据本发明的一个实施例,提供了一种用于在移动无线网络中对接入进行认证的方法。在这种实施例中,该方法包括:通过无线电接入网络,经由高速率分组数据无线电链路和信令接口,与接入终端交换可扩展认证协议 (extensible authentication protocol, EAP) 分组;将 EAP 分组封装在认证授权和计费 (AAA) 分组中;以及将 AAA 分组发送到认证服务器以便认证。

[0007] 根据本发明的另一个实施例,提供了一种用于辅助移动无线网络中的接入认证的网关系统。根据这种实施例,该网关系统包括无线电接入网络接口、认证器和 IP 网络接口。无线电接入网络接口用于通过无线电接入网络,经由高速率分组数据无线电链路和信令接口,与接入终端交换可扩展认证协议 (EAP) 分组。认证器用于将 EAP 分组封装在认证授权和计费 (AAA) 分组中,并且 IP 网络接口用于将 AAA 分组发送到认证服务器。

[0008] 本发明的某些实施例的重要技术优点包括相邻无线电网络控制器和 IP 网关之间的快速移交。

[0009] 本发明的某些实施例的其他重要技术优点可包括低等待时间技术间移交,例如 CDMA 和 WLAN 网络之间的移交。另外,某些实施例可简化用于网络认证的密钥的生成和分发,并且可以消除网络组件之间的一个或多个接口。

[0010] 本领域的技术人员从以下附图、描述和权利要求中可以很清楚看到本发明的其他

技术优点。另外,虽然以上列举了特定的优点,但是各种实施例可以包括所列举的优点中的全部或一些,或者不包括所列举的优点。

附图说明

[0011] 为了更完整地理解本发明及其特征和优点,现在参考结合附图理解的以下描述,附图中:

[0012] 图 1 是根据本发明某些教导用于交换数据的示例性移动无线通信系统的简化组件图;

[0013] 图 2 是示出在本发明某些实施例中用于接入认证的协议操作中涉及的各种层的序列图;

[0014] 图 3 是示出在本发明某些实施例中用于交换 EAP 消息的 AAA 协议栈的简化图;以及

[0015] 图 4 是示出根据本发明一个实施例使用 EAP 和 AKA 协议的 HRPD 认证的序列图。

具体实施方式

[0016] 图 1 是根据本发明某些教导用于交换数据的示例性移动无线通信系统 10 的简化组件图。如图 1 所示,本发明的一个实施例包括高速率分组数据 (High Rate Packet Data, HRPD) 网络,该网络使用基于可扩展认证协议 (EAP) 的认证机制。这种实施例可实现接入终端 (AT) 12、IP 网关 (IPGW) 14 (经由无线电接入网络 (RAN) 16 中的无线电网络控制器 (RNC)) 和认证服务器 18 之间的三方握手。

[0017] 根据本发明的某些教导,EAP 消息是利用 HRPD 空中信令协议在 AT12 和 RAN16 之间通过空中传送的。EAP 消息是经由 CDMA 在 AT12 和 RAN16 之间传输的。AT12 可充当 EAP 对等体,而 RAN16 可充当经由信令接口将 EAP 消息转发到 IPGW14 的 EAP 中继代理。本发明的一个方面包括驻留在 IPGW14 内的基于 EAP 的认证器。从 IPGW14,EAP 消息可经由接入认证和计费 (AAA) 协议 (例如 RADIUS 或 DIAMETER) 被传送到认证服务器 18,其中可能经过一个或多个 AAA 代理服务器 (未示出)。根据本发明的某些教导,认证服务器 18 可以是 AAA 服务器或专有的安全性管理器,并且提供 EAP 服务器的功能。在图 1 中,认证服务器 18 被示为归属网络 (home network) 中的专有安全性管理器 (“H-SM”)。

[0018] EAP 既可以用于设备认证也可用于服务认证。因此,EAP 可以被连续地使用,一次用于接入 RAN16(即设备认证),一次用于与 IP 网络 20 建立 IP 连接(即服务认证)。如图 1 所示,两个认证序列都可端接于归属网络中的同一认证服务器中。这种双重 EAP 认证在 AT12 被授权访问 IP 服务之前可能是必要的。取决于部署场景和运营商的认证策略,AT12 有可能执行单个 EAP 认证,例如当 AT12 在设备认证或服务认证中的任一者(而不是两者)期间被认证时。

[0019] 根据本发明的某些教导,AT12(EAP 对等体)和 IPGW14(EAP 认证器)之间使用的协议是基于 EAP 的。EAP 消息被封装在 HRPD 分组中,以便在 AT12 和 RAN16 之间传输。

[0020] 经由 HRPD 的 EAP 可用于结合 HRPD Rev. A 利用增强型多流分组应用来认证设备。根据本发明的教导,EAP 认证器可位于 IPGW 中,并且相应地,HRPD RAN 可经由 A11 接口将 EAP 消息中继到 EAP 认证器。IPGW 中的 AAA 客户端随后可以将 EAP 消息封装在 AAA 分组中,

并且将它们转发到归属网络中的 EAP 服务器以便认证。IPGW14 和认证服务器 18 之间使用的协议可以基于 DIAMETER(支持 EAP)。如果移动性服务和接入服务是由同一运营商提供的，则可以只需要一个 EAP 认证。

[0021] 或者，RAN 可以使用 A12 接口来在接入服务提供商的网络内承载设备认证。设备认证于是可被端接于 EAP 服务器中。在这种配置中，EAP 认证器可以处于 RAN 中，并且可能不需要使用 EAP 中继功能。但是，注意如果接入服务和移动性服务是由同一运营商提供的，则可能不需要为设备认证使用 A12。

[0022] 图 2 是示出了在本发明某些实施例中用于接入认证的协议操作中涉及的各种层的序列图。更具体而言，图 2 示出了在若干个基于 EAP 的实体之间的 EAP 交换中涉及的层，所述实体包括 EAP 对等体、EAP 中继、EAP 认证器和 EAP 服务器。根据本发明的某些教导，EAP 对等体可以实现在接入终端中，EAP 中继可实现在 RNC 中，EAP 认证器可实现在 IPGW 中，EAP 服务器可实现在认证服务器（例如 AAA 服务器或 H-SM）中。图 2 还示出了位于被访网络中的认证服务器（V-SM），其可能参与也可能不参与 EAP 交换。从图 2 可见，EAP 方法一般被封装在 EAP 分组中，以便在接入终端 12（EAP 对等体）和认证服务器 18（EAP 服务器）之间运送。为了在接入终端 12 和 RAN16 之间运送，EAP 分组被进一步封装在更低层的协议中（例如，HRPD/CDMA）。在到达 RAN16 后，EAP 分组被从用于在接入终端 12 和 RAN16 之间运送的更低层分组中去除，并且被重新封装在适合于在 RAN16 和 IPGW14 之间运送的更低层协议中。IPGW14 进而从这些更低层协议分组中去除 EAP 分组，并且重新封装它们以便运送到认证服务器 18。在某些实施例中，IPGW14 将这些 EAP 分组封装在 AAA 分组中，然后将 AAA 分组封装在可能适合于基于 DIAMETER 的认证的 TCP/IP 分组中（如图 2 所示）。或者，IPGW14 可将 AAA 分组封装在其他更低层的分组中，例如 UDP，其可能适合于基于 RADIUS 的认证。

[0023] 图 3 是示出在本发明某些实施例中用于交换 EAP 消息的 AAA 协议栈的简化图。图 3 示出了可能存在于 RAN 和认证服务器之间的多种网络接口。与图 2 中一样，图 3 表明了 EAP 分组如何被封装在各种更低层的协议分组中，以便传输到通信系统 10 的各种网络组件。例如，在 RAN16 中，EAP 分组被封装在信令协议分组（例如 A11 分组）和其他更低层分组中，以便传输到 IPGW16。IPGW16 接收更低层分组并提取 EAP 分组。IPGW16 随后将 EAP 分组重新封装在认证协议分组（例如 AAA 分组）和其他更低层分组中，以便通过 IP 网络 20 传输。这些分组经过若干个可选的中间组件，但最终到达认证服务器 18。认证服务器 18 随后从更低层分组中提取 EAP 分组，如图 3 所示。

[0024] 在本发明的某些实施例中，通信系统 10 中的设备认证可能要求 AT12 和 IPGW14 之间的 EAP 消息交换。在一个实施例中，EAP 消息是利用现有消息经由 A11 接口在移动 IP 厂商特定扩展（Vendor-Specific Extension, VSE）中承载的。新的 VSE 可被定义和使用来经由 A11 接口传输 EAP 数据。EAP 数据可包括 EAP 消息，以及从 EAP 交换推导出的打算用于 RAN16 的密钥。经由 A11 接口发送的 EAP 消息还可能需要被保护，尤其如果移动性服务和接入服务是由不同实体操作的话更是如此。

[0025] EAP 认证可产生由 AT 和认证服务器推导出的主会话密钥（MSK）。根据本发明的某些教导，认证服务器将密钥安全地发送到驻留在 IPGW 中的 EAP 认证器。认证器随后可使用该密钥来推导出用于流量保护和其他目的的其他密钥。在某些实施例中，可以为 RAN 推导出密钥材料，并安装密钥材料以用于空中保护。AT 可使用类似的密钥推导来推导出与网络

推导出的密钥相匹配的密钥。如果双重或单个认证被使用，则密钥推导一般是相同的。驻留在认证服务器中的 EAP 服务器可从扩展的 MSK 推导出移动性密钥。服务器可使用根密钥来生成所有其他密钥。这种密钥可在认证期间被自举 (bootstrap) 并被缓存在 IPGW 中。在 AT 和 EAP 服务器中都生成 EAP 密钥。

[0026] 图 4 是示出根据本发明一个实施例使用 EAP 以及认证和密钥协定 (Authentication & Key Agreement, AKA) 协议的 HRPD 认证的序列图。根据本发明的教导，IPGW14 和接入终端 12 通过 RAN16，经由高速率分组数据 (HRPD) 无线电链路和信令接口来交换 EAP 分组。IPGW14 随后将 EAP 分组封装在认证协议分组（例如 AAA 分组）中，并且将 AAA 分组发送到认证服务器 18 以便进一步处理。认证服务器 18 进而可以基于 EAP 分组来对接入进行认证。在图 4 所示的实施例中，例如，认证服务器 18 可运行 AKA 算法以生成某些认证质询和响应，这些认证质询和响应通过 IPGW14 和 RAN16 被返回到接入终端 12。接入终端 12 随后可验证质询和响应并生成其自己的认证质询和响应，其自己的认证质询和响应被发送回认证服务器 18。作为此交换的一部分，认证服务器 18 和接入终端 12 可相互推导会话密钥。认证服务器 18 随后可将此会话密钥发送到 IPGW14，以便用于与接入终端 12 建立链路层安全性。

[0027] AKA 是基于质询 - 响应机制和对称加密的。与传统的认证方法相比，AKA 一般提供更强的安全性，其具有更长的密钥长度和对客户端和服务器两者认证。

[0028] 虽然已经利用若干实施例描述了本发明，但是可以向本领域的技术人员建议许多改变、变化、变更、变换和修改，并且希望本发明包括落在所附权利要求的范围之内的这种改变、变化、变更、变换和修改。

[0029] 例如，以上已经描述了其中 EAP 被用于提供灵活的认证机制的本发明示例性实施例，但是其他协议可以取代 EAP 或者与 EAP 一起被使用。具体地，支持多个认证机制和认证机制的动态协商的任何认证协议都可适用于实现本发明的原理。另外，这里描述的认证机制想要是示例性的而不是穷尽性的。在不脱离本发明精神的情况下，可以使用其他认证机制，包括其他共享秘密协议和基于证书的机制，例如传输层安全性。

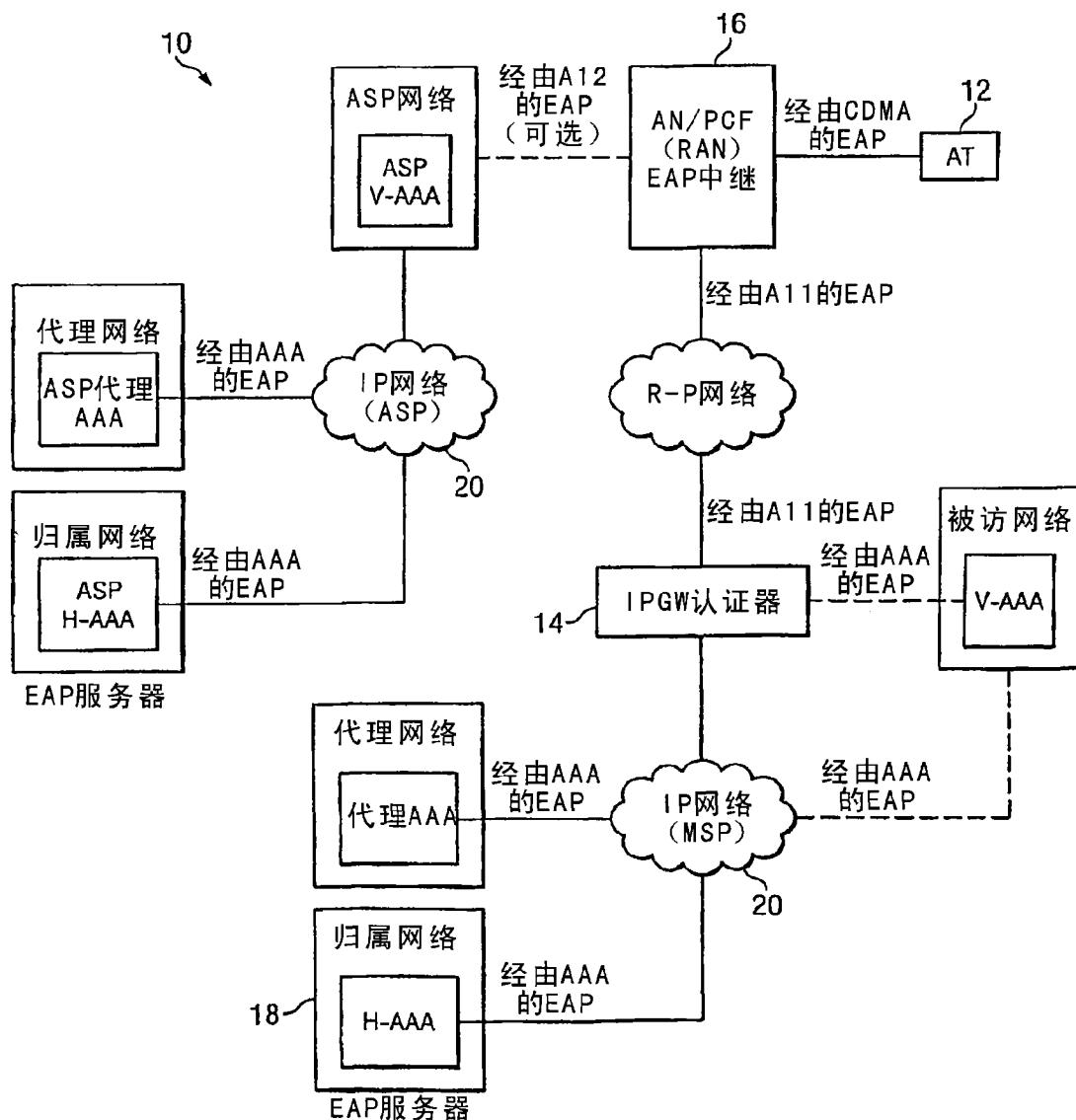


图 1

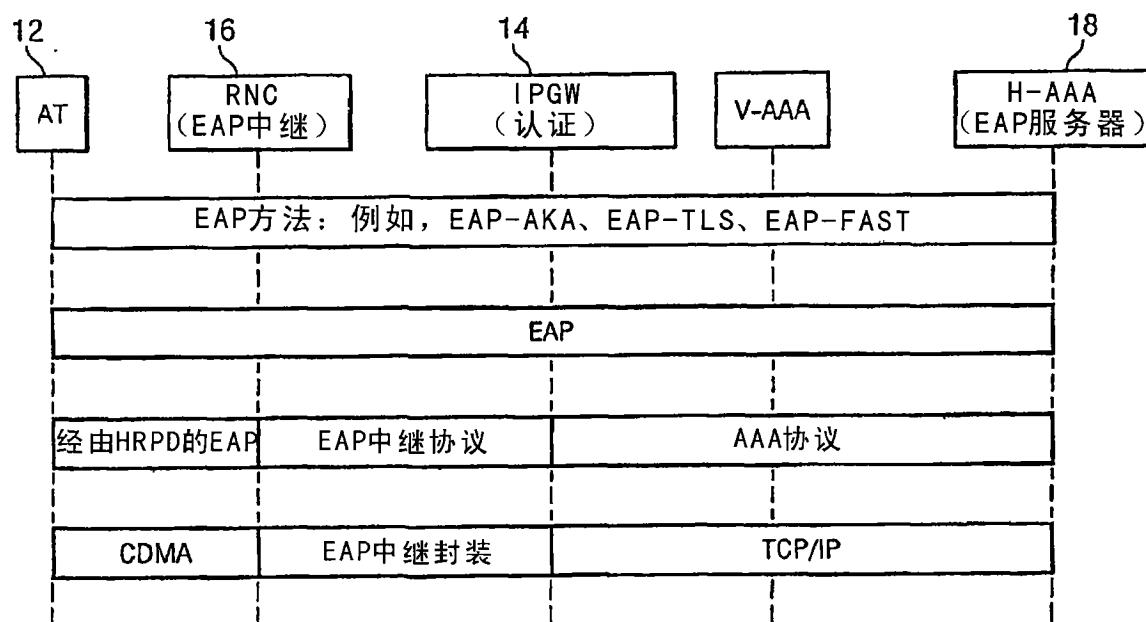


图 2

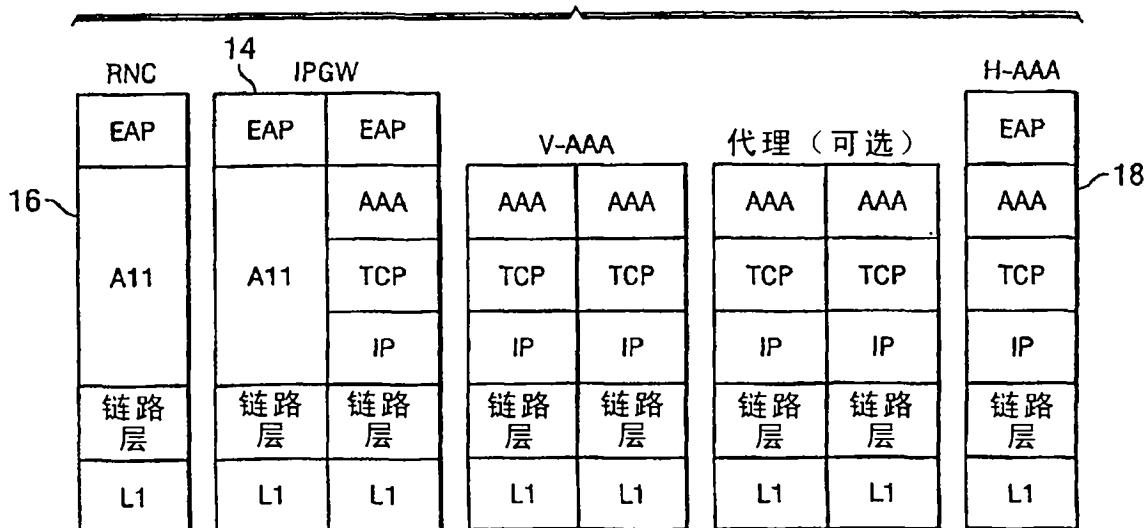


图 3

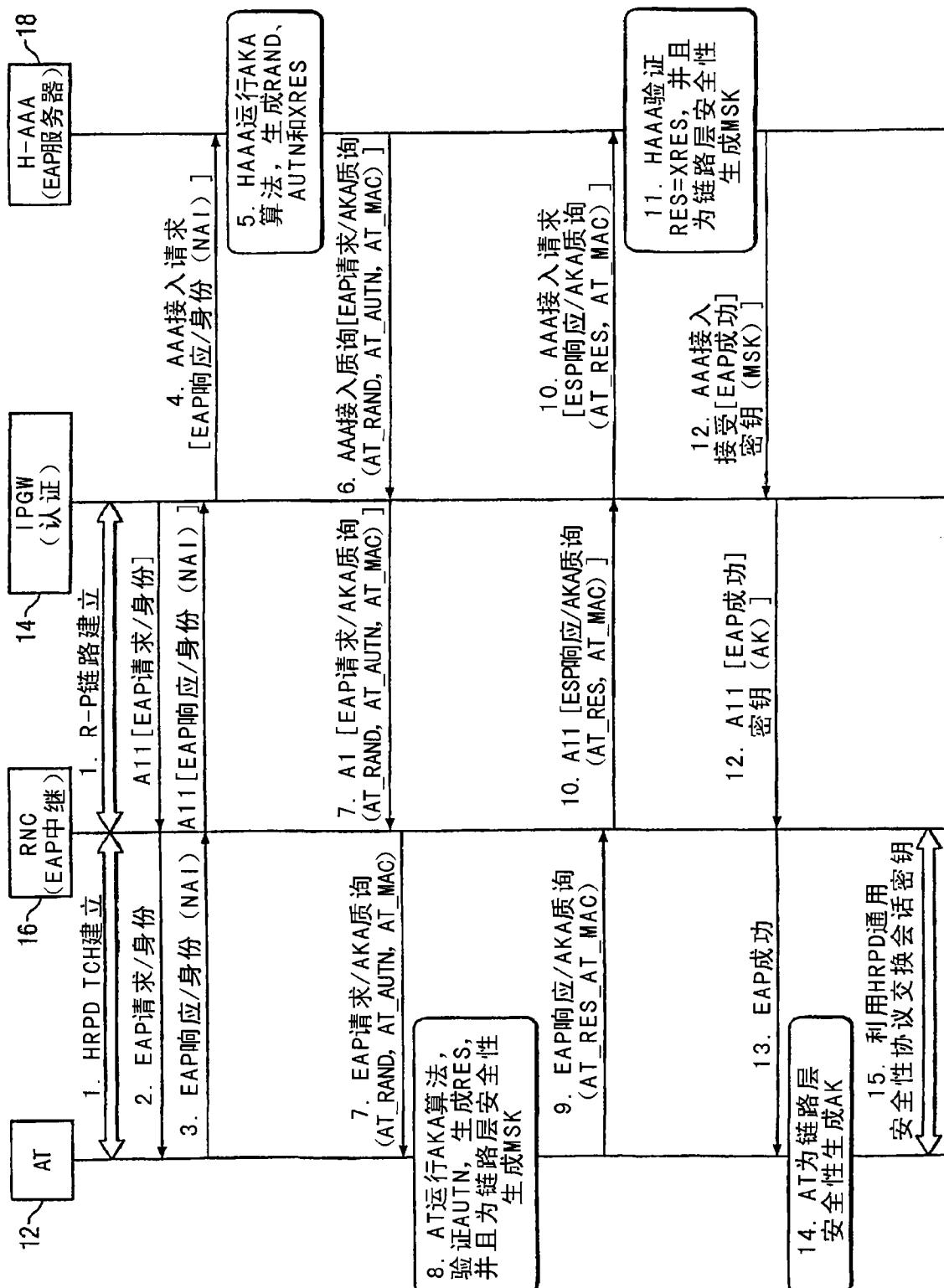


图4