

[19] 中华人民共和国国家知识产权局

[51] Int. Cl<sup>7</sup>

H04L 29/06

H04Q 7/38



# [12] 发明专利申请公开说明书

[21] 申请号 03811657.X

[43] 公开日 2005年8月17日

[11] 公开号 CN 1656771A

[22] 申请日 2003.4.4 [21] 申请号 03811657.X

[30] 优先权

[32] 2002. 4. 5 [33] US [31] 60/370,442

[32] 2002. 8. 29 [33] US [31] 60/407,469

[86] 国际申请 PCT/US2003/010512 2003.4.4

[87] 国际公布 WO2003/088617 英 2003.10.23

[85] 进入国家阶段日期 2004.11.22

[71] 申请人 高通股份有限公司

地址 美国加利福尼亚州

[72] 发明人 R·F·小奎克 J·戴克

M·里奥 J·曼达亚姆

[74] 专利代理机构 上海专利商标事务所有限公司

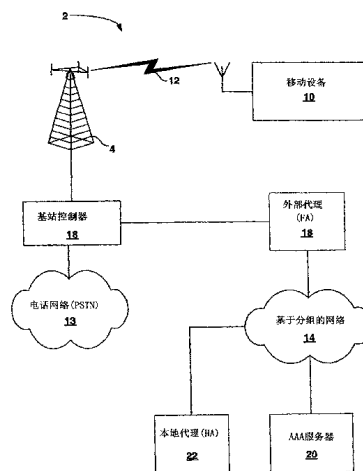
代理人 李家麟

权利要求书7页 说明书16页 附图6页

[54] 发明名称 移动无线系统中的密钥更新

[57] 摘要

所公开的内容描述了移动 IP 网络中使用的安全密钥更新方案。实施更新方案以便于移动设备和认证该移动设备的服务器计算机间的安全密钥更新。这里描述的技术能以如下方式便于安全密钥更新：考虑到了更新例程期间的潜在消息丢失、更新例程期间的移动设备故障或者移动网络设置中一般遇到的其它问题。这样，所述技术能为安全密钥更新提供稳健的方案并且能改进网络安全。



ISSN 1008-4274

1. 一种方法，包括：

接收对接入网络的第一注册请求，所述第一注册请求是用密钥形成的；

响应于所述第一注册请求发送第一应答，表明密钥更新对于接入所述网络是必要的；

接收包括新密钥的第二注册请求；

响应于所述第二注册请求发送第二应答，表明所述新密钥已被接收；

在授权接入网络前接收到另一个第二注册请求时，重发另一个第二应答，表明新密钥已被接收；

接收第三注册请求，所述第三注册请求是用所述新密钥形成的；以及

在所述第三注册请求后授权接入所述网络。

2. 如权利要求1所述的方法，其特征在于，所述第二注册请求包括所述新密钥和一令牌，所述第二应答包括所述令牌。

3. 如权利要求1所述的方法，其特征在于还包括，在授权接入所述网络前接收到另一个第一注册请求时，重发另一个第一应答。

4. 如权利要求1所述的方法，其特征在于还包括，在发送所述第二应答后，在接收到不是用所述新密钥形成的注册请求时重发另一个第一应答。

5. 如权利要求1所述的方法，其特征在于还包括：

在接收到所述第二注册请求时存储所述新密钥；以及

在接收第三注册请求后提交所述新密钥用于认证。

6. 一种方法，包括：

发送使用密钥形成的第一注册请求以请求接入网络；

接收第一应答，表明密钥更新对于接入所述网络是必要的；

响应于所述第一应答发送包括新密钥的第二注册请求；

接收另一个第一应答，表明密钥更新对于接入所述网络是必要的；  
响应于接收另一个第一应答，发送包括所述新密钥的另一个第二注册请求；  
响应于所述第二注册请求，接收一第二应答，表明所述新密钥已被接收；  
发送使用所述新密钥形成的第三注册请求；以及  
在所述第三注册请求后接入所述网络。

7. 如权利要求 6 所述的方法，其特征在于还包括，当在所定义的时间量内未接收到所述第二应答时重发所述第二请求。

8. 一种设备，包括：

接收机，其接收用数据调制的信号；

发射机，其发送用数据调制的信号；以及

密钥更新逻辑，用于更新所述设备的安全密钥，所述设备这样配置，使得：

发射机发送一个用密钥形成的第一注册请求，以请求接入网络；

接收机响应于所述第一注册请求接收第一应答，表明密钥更新对于接入所述网络是必要的；

密钥更新逻辑响应于所述第一应答生成一个新密钥；

发射机发送一个包括所述新密钥的第二注册请求；

接收机接收另一个第一应答，表明密钥更新对于接入所述网络是必要的；

发射机响应于另一个第一应答的接收，发送包括所述新密钥的另一个第二注册请求；

接收机响应于所述第二注册请求接收第二应答，所述第二应答表明所述新密钥已被接收；

发射机发送一个用所述新密钥形成的第三注册请求；以及

设备在所述第三注册请求后获得对所述网络的接入。

9. 如权利要求 8 所述的设备，其特征在于还包括将数据调制到发射机发送的信号上的调制单元、以及从接收机接收到的信号解调数据的解调单元。

10. 如权利要求 8 所述的设备，其特征在于，所述发射机和接收机组成一集

成收发机，其中所述调制单元和解调单元组成一集成的调制解调器。

11. 如权利要求 8 所述的设备，其特征在于，所述设备是从由以下组成的组中选择的：移动电话、膝上型电脑、桌上型电脑、个人数字助理(PDA)、数据终端和数据采集设备。

12. 一种服务器，包括：

接收数据分组的接收机；

发送数据分组的发射机；

认证、授权和核算(AAA)单元，用于为移动网际协议(移动 IP)网络内的移动设备提供认证、授权和核算；以及

用于控制密钥更新例程的密钥更新逻辑，所述服务器这样配置，使得：

接收机接收用密钥形成的第一注册请求，所述第一注册请求请求接入所述移动 IP 网络；

发射机响应于所述第一注册请求发送第一应答，表明密钥更新对接入所述网络是必要的；

在服务器授权接入网络以前，发射机响应于接收机接收另一个第一注册请求而重发另一个第一应答；

接收机接收包括新密钥的第二注册请求；

发射机响应于所述第二注册请求发送第二应答，所述第二应答表明所述新密钥已被接收；

接收机接收用所述新密钥形成的第三注册请求；以及

服务器响应于所述第三注册请求为所述移动设备授权接入所述网络。

13. 如权利要求 12 所述的服务器，其特征在于，所述服务器这样配置，使得：在所述服务器授权接入所述网络以前，所述发射机响应于接收机接收另一个第二注册请求而重发另一个第二应答。

14. 如权利要求 12 所述的服务器，其特征在于，所述服务器还这样配置，使得：发射机在发送所述第二应答后，响应于所述接收机接收到不包括所述新密钥的

注册请求而重发另一个第一应答。

15. 一种包括数字电路的装置，使移动设备：

发送用密钥形成的第一注册请求，以请求接入网络；

在响应于所述第一注册请求接收到第一应答时发送第二注册请求，所述第一应答表明密钥更新对于接入所述网络是必要的，所述第二注册请求包括新密钥；

在接收到另一个第一应答时重发另一个第二注册请求；以及

在响应于所述第二注册请求接收到第二应答时，发送使用所述新密钥形成的第三注册请求，所述第二应答表明所述新密钥已被接收；

16. 如权利要求 15 所述的装置，其特征在于，所述数字电路还使所述移动设备响应于未在所定义的时间量内接收到所述第二应答而重发所述第二请求。

17. 如权利要求 15 所述的装置，其特征在于，所述装置包括在所述移动设备内执行的状态机，其中所述第二注册请求包括所述新密钥和一令牌，所述第二应答包括所述令牌。

18. 一种包括数字电路的装置，使服务器：

响应于第一注册请求发送第一应答，所述第一注册请求是用密钥形成的，所述第一应答表明密钥更新对于接入所述网络是必要的；

响应于第二注册请求发送第二应答，所述第二注册请求包括一新密钥，所述第二应答表明所述新密钥已被接收；

在授权网络接入前，响应于另一个第二注册请求发送另一个第二应答；以及

响应于第三注册请求授权接入所述网络，所述第三注册请求是用所述新密钥形成的。

19. 如权利要求 18 所述的装置，其特征在于，所述数字电路还使服务器：在授权接入所述网络以前，在接收到另一个第一注册请求时重发另一个第一应答。

20. 如权利要求 18 所述的装置，其特征在于，所述数字电路还使服务器：在

接收到不包括所述新密钥的注册请求时，在发送所述第二应答后重发另一个第一应答。

21. 如权利要求 18 所述的装置，其特征在于，所述装置包括在所述服务器内执行的状态机，所述第二注册请求包括所述新密钥和一令牌，所述第二应答包括所述令牌。

22. 一种包括程序代码的计算机可读媒质，所述程序代码在移动设备内执行时使所述移动设备：

发送用密钥形成的第一注册请求以请求接入网络；

在响应于所述第一注册请求接收到第一应答时发送第二注册请求，所述第一应答表明密钥更新对于接入所述网络是必要的，所述第二注册请求包括新一密钥；

在接收到另一个第一应答时重发另一个第二注册请求；以及

在响应于所述第二注册请求接收到第二应答时，发送使用所述新密钥形成的第三注册请求，所述第二应答表明所述新密钥已被接收。

23. 如权利要求 22 所述的计算机可读媒质，其特征在于还包括这样的程序代码：所述程序代码在移动设备内执行时使所述移动设备响应于未在所定义的时间量内接收到所述第二应答而重发所述第二请求。

24. 一种包括程序代码的计算机可读媒质，所述程序代码在网络服务器内执行时使所述服务器：

响应于第一注册请求发送第一应答，所述第一注册请求是用密钥形成的，所述第一应答表明密钥更新对于接入所述网络是必要的；

响应于第二注册请求发送第二应答，所述第二注册请求包括新密钥，所述第二应答表明所述新密钥已被接收；

在授权网络接入前响应于另一个第二注册请求发送另一个第二应答；以及

响应于第三注册请求授权接入所述网络，所述第三注册请求是用所述新密钥形成的。

25. 如权利要求 24 所述的计算机可读介质，其特征在于还包括这样的程序代码：所述程序代码在服务器内执行时，在授权接入所述网络以前接收到另一个第一注册请求时，使所述服务器重发另一个第一应答。

26. 如权利要求 24 所述的计算机可读介质，其特征在于还包括这样的程序代码：所述程序代码在服务器内执行时，在接收到不包括所述新密钥的注册请求时，使所述服务器在发送所述第二应答后重发另一个第一应答。

27. 一种系统，包括：

移动设备；以及

网络服务器，

所述移动设备被配置成向网络服务器发送用密钥形成的第一注册请求，以请求接入网络，

所述网络服务器被配置成在被置于密钥更新状态下时，响应于所述第一注册请求发送第一应答，所述第一应答表明密钥更新对于接入所述网络是必要的，

所述移动设备还被配置成在接收到所述第一应答时转变为更新密钥状态，并且响应于所述第一应答发送第二注册请求，所述第二注册请求包括一新密钥，

所述网络服务器还被配置成在接收到所述第二注册请求时转变为更新确认状态，并且响应于所述第二注册请求发送第二应答，所述第二应答表明所述新密钥已被接收，

所述移动设备还被配置成在接收到所述第二应答时转变为密钥有效状态，并且响应于所述第二应答发送第三注册请求，所述第三注册请求是用所述新密钥形成的，以及

所述网络服务器还被配置成在接收到所述第三注册请求时转变为密钥 OK 状态，并且响应于所述第三注册请求为所述移动设备授权接入所述网络。

28. 如权利要求 27 所述的系统，其特征在于还包括一代理，其转换来自移动设备的请求并将其转发到网络服务器，以及转换来自网络服务器的应答并将其转发到移动设备。

29. 一种装置，包括：

发送用密钥形成的第一注册请求以请求接入网络的装置；

响应于所述第一注册请求接收第一应答的装置，所述第一应答表明密钥更新对于接入所述网络是必要的；

发送第二注册请求的装置，所述第二注册请求包括一新密钥；

响应于接收另一个第一应答而重发另一个第二注册请求的装置；

响应于所述第二注册请求接收第二应答的装置，所述第二应答表明所述新密钥已被接收；

发送第三注册请求的装置，所述第三注册请求是用所述新密钥形成的；以及在所述第三注册请求后接入所述网络的装置。

30. 一种装置，包括：

接收请求接入网络的第一注册请求的装置，所述第一注册请求是用密钥形成的；

响应于所述第一注册请求而发送第一应答的装置，所述第一应答表明密钥更新对于接入所述网络是必要的；

接收第二注册请求的装置，所述第二注册请求包括新一密钥；

响应于所述第二注册请求发送第二应答的装置，所述第二应答表明所述新密钥已被接收；

响应于接收另一个第二注册请求而发送另一个第二应答的装置；

接收第三注册请求的装置，所述第三注册请求是用所述新密钥形成的；以及响应于所述第三注册请求授权接入所述网络的装置。



---

## 移动无线系统中的密钥更新

### 领域

所公开的内容涉及被配置成支持移动无线网络协议的移动设备、以及被配置成用于移动网络环境中移动设备的认证、授权和核算(AAA)的服务器。

### 背景

在通信网络中，网络节点使用网络通信协议交换数据。网际协议(IP)是便于网络节点间分组化的数据通信的网络通信协议。移动 IP 是便于在基于分组的网络中使用移动计算设备的协议。换言之，移动 IP 协议允许网络中的节点移动性。能运行移动 IP 协议的移动计算设备的示例包括：诸如蜂窝电话和卫星电话这样的移动电话、膝上型电脑、个人数字助理(PDA)、数据终端、数据采集设备以及其它计算设备。

移动 IP 使移动设备能发送和接收与基于分组的通信应用相关的分组，所述应用诸如 web 浏览、电子邮件、消息传递等等。基于分组的网络一般利用网络地址来标识网络中的设备，比如在因特网的情况下利用 IP 地址。根据这些 IP 地址将数据路由到设备或自设备路由数据。然而，移动设备会移到网络中不同的位置。为此，移动 IP 使分组能经由隧道过程被重新路由到移动设备的当前附着点。

在移动 IP 中，移动设备被分配到一个本地代理(HA)，本地代理一般是路由器或是移动设备的本地子网上的另一实体。当移动设备远离本地时，它会被分配到一个外部代理(FA)。外部代理一般是移动设备访问的子网上的一个路由器，它在附着到所访问的子网时向移动设备提供路由服务。

被发送到移动设备的本地地址的信息可以通过外部代理、经由称为隧道传送给的过程被重新路由到移动设备。特别是，一旦移动设备通过外部代理注册，本地代理(HA)就把分组经隧道传送到外部代理。然后，FA 能把分组传送到移动设备。特别是，当 FA 从移动设备接收到一注册应答(RRP)时，它就通过读取 RRP 分组的本地地址字段来更新其路由表。这样，从 HA 被隧道传送到 FA 的分组能被正确地传送到移动设备。此外，外部代理会充当用于把分组从移动设备发送到附着到网络的其它

设备的缺省路由器。

AAA 服务器是指执行认证(authentication)、授权(authorization)和核算(accounting)功能的服务器计算机。AAA 服务器一般由因特网服务提供商(ISP)进行维护。在移动 IP 中, AAA 服务器能认证和授权一移动设备来接入网络, 并且能为了记账目的而提供核算信息。

在 IS-835 网络中, 为了接入网络, 移动设备向外部代理(FA)发送一注册请求(RRQ), 所述 RRQ 是用安全密钥形成的。特别是, 安全密钥可用于认证移动设备的用户。例如, 移动设备可以按照一密码认证协议(PAP)来发送密钥, 或者在不安全的系统中产生使用该密钥形成的认证符值。例如, 移动设备能使用安全密钥对询问握手认证协议(CHAP)产生响应。

在任一情况下, 在移动设备发送了使用安全密钥形成的 RRQ 之后, FA 就把 RRQ 转换成接入请求(ARQ), 并将所述 ARQ 发送到 AAA 服务器。然后, 如果 AAA 授权接入, FA 就把注册请求转发到 HA。然后可以使用分组隧道传送来把分组从 HA 传送到 FA, FA 能把分组传送到移动设备。

在特定的情况下, 可能期望改变移动设备的安全密钥。例如, 如果一不正当的设备获得对密钥的接入, 则该不正当设备就能作为未经授权的用户接入基于分组的网络。在本公开内容中, “不正当设备”是指使用另一设备的安全密钥来接入或者试图接入一网络的设备。如果成功, 不正当设备就能扮演所述移动设备。更坏的是, 不正当设备会使用安全密钥伪装成另一用户接入因特网, 并且执行网络犯罪、网络恐怖主义等等。因此, 通常期望改变移动设备的安全密钥, 比如响应于已知的不正当设备威胁、或者周期性地改变以便预见和阻碍可能的不正当设备威胁。

## 概述

所公开的内容涉及移动 IP 网络中使用的安全密钥更新方案。实施更新方案以便于在移动设备和认证该移动设备的服务器计算机之间的安全密钥更新。这里描述的技术能以如下方式便于安全密钥更新: 考虑到了更新例程期间的潜在消息丢失、更新例程期间的移动设备故障或者移动网络环境中一般遇到的其它问题。特别是, 能实现状态机, 响应于更新方案中消息的接收或非接收而引起一个或多个消息的重发。这样, 所述技术能为安全密钥更新提供稳健的方案并且能改进网络安全。

在一实施例中, 所公开的内容提供了一种方法, 所述方法包括接收对接入网

网的第一注册请求，所述第一注册请求是用密钥形成的。所述方法还包括响应于第一注册请求而发送第一应答，表明密钥更新是接入网络所必要的，并且接收包括新密钥的第二注册请求。所述方法还包括响应于第二注册请求发送一个表明新密钥被接收的第二应答，并且在授权接入网络前、在接收到另一第二注册请求时重发一个表明新密钥被接收到的另一个第二应答。所述方法还包括接收第三注册请求，所述第三注册请求是用新密钥形成的，并且响应于所述第三注册请求授权接入网络。

在另一实施例中，所公开的内容提供了一种方法，所述方法包括发送一个用密钥形成的第一注册请求以请求接入网络、以及接收第一应答，所述第一应答表明密钥更新是接入网络所必要的。所述方法还包括响应于第一应答而发送包括新密钥的第二注册请求，以及接收另一个表明密钥更新是接入网络所必要的第一应答。所述方法还包括响应于另一第一应答的接收而发送包括所述新密钥的另一个第二注册请求，以及响应于所述第二注册请求接收第二应答，所述第二应答表明新密钥被接收到。所述方法还包括发送用新密钥形成的第三注册请求，以及在第三注册请求后接入网络。

这些技术及这里描述的其它技术可以分别由移动设备或服务器执行，所述服务器向移动设备提供了网络接入。在任一情况下，技术都可以用硬件、软件、固件或者它们的任意组合来实现。为了执行这里所述的技术之一，可以对移动设备、服务器、或者形成这一设备或服务器的一部分的电路实施各个实施例。对于某些软件实施例而言，所述技术可以体现在包括程序代码的计算机可读介质上，所述程序代码在被执行时执行所述技术中的一种或多种。

在附图和下列描述中提出了各个实施例的其它细节。从以下描述、附图以及权利要求书中，其它的特征、目的和优点将变得更为明显。

#### 附图简述

图 1 是一框图，说明了为支持移动联网协议而配置的系统，其中安全密钥更新例程可由移动设备和 AAA 服务器执行。

图 2 是一消息流程图，说明了为按照一实施例执行安全密钥更新而通过外部代理在移动设备和 AAA 服务器间进行的通信。

图 3 是为实现这里所述的安全密钥更新例程而配置的移动设备的示例性框图。

图 4 是为实现这里所述的安全密钥更新例程而配置的 AAA 服务器的示例性框

图。

图 5 是说明从移动设备的角度所见的安全密钥更新例程的流程图。

图 6 是说明从 AAA 服务器的角度所见的安全密钥更新例程的流程图。

#### 详细描述

通常，所公开的内容涉及移动 IP 网络中所使用的安全密钥更新方案。实施更新方案以便于在移动设备和认证该移动设备的服务器计算机之间的安全密钥更新。安全密钥类似于密码，并且可由移动设备使用，用于在移动设备尝试接入基于分组的网络时进行认证。然而，在各种情况下，可能期望改变安全密钥，比如响应于已知的密钥误用威胁、或者周期性地改变以便预见和阻碍可能的威胁。在任一情况下，这里所述的技术都能以如下方式便于安全密钥更新：考虑到了更新例程期间的潜在消息丢失、更新例程期间的移动设备故障、或者移动网络设置中一般遇到的其它问题。这样，所述技术能为安全密钥更新提供一种稳健的方案，并且能改进网络安全。

图 1 是一框图，说明了为支持诸如移动 IP 等移动联网协议而配置的系统 2。特别是，系统 2 包括一移动设备 10，其通过移动网络协议获得对基于分组的网络 14 的接入。移动设备 10 可以是能被移到不同的地理位置的任一设备。例如，移动设备 10 可包括工作组 Windows™、Unix 或 Linux 环境中的桌上型、膝上型或便携式的计算机、或者是基于用于小便携式设备的 Palm™、Windows CE 或类似操作系统环境的个人数字助理(PDA)、或者是诸如移动电话、交互电视、无线数据终端、无线数据采集设备等等的其它无线设备。

例如，在移动设备 10 的环境中以移动电话的形式略述了本发明的许多细节。在该情况下，移动设备 10 可被配置成传送语音通信信号和数据分组，所述语音通信信号和数据分组都能通过基于分组的网络 14 被传送。移动设备 10 与基站 4 交换无线信号 12。无线信号 12 可包括按照多种调制技术的任一种调制的信号，包括例如：码分多址(CDMA)调制的信号、时分多址(TDMA)调制的信号、频分多址(FDMA)调制的信号或者两种或多种调制技术的各种组合。

移动设备 10 可被设计成支持例如一个或多个 CDMA 标准，比如 (1) “TIA/EIA-95-B Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System” (IS-95 标准)，(2) “TIA/EIA-98-C Recommended Minimum Standard for Dual-Mode Wideband Spread

Spectrum Cellular Mobile Station” (IS-98 标准), (3) 由名为“第三代合伙人计划”(3GPP)的协会提出的标准,其包含在一组文献中,包括文献号 3G TS 25.211、3G TS 25.212、3G TS 25.213 和 3G TS 25.214(W-CDMA 标准), (4) 由名为“第三代合伙人计划 2”(3GPP2)的协会提出的标准,其包含在一组文献中,包括“TR-45.5 Physical Layer Standard for cdma2000 Spread Spectrum Systems”、“C.S0005-A Upper Layer(Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems”和“C.S0024 CDMA2000 High Rate Packet Data Air Interface Specification”(CDMA2000 标准), (5) 在 TIA/EIA-IS-856 中阐述的 HDR 系统,“CDMA2000 High Rate Packet Data Air Interface Specification”, 以及(6) 某些其它标准。或者或另外, 移动设备 10 可被设计成支持其它标准, 比如 GSM 标准或相关标准, 例如 DCS1800 和 PCS1900 标准。GSM 系统采用 FDMA 和 TDMA 调制技术的组合。移动 10 还支持其它的 FDMA 和 TDMA 标准。

或者, 信号 12 可以按照用于无线联网的调制方案来调制, 比如一般由符合 IEEE 802.11b 无线联网标准的设备实现的二进制相移键控(BPSK)或正交移键控(QPSK)调制方案, 或者一般由符合 IEEE 802.11g 或 IEEE 802.11a 无线联网标准的设备所实现的 OFDM 调制方案。同样, 信号 12 也可以按照由蓝牙专门业务组定义的调制方案来调制。然而, 在那些情况下, 会使用一接入点(而不是基站 4)来从移动设备 10 接收并转发信号。

在图 1 所示的示例中, 基站 14 从移动设备 10 接收无线信号 12, 基站控制器 18, 有时称为基收发机系统(BTS), 对所述信号进行解调。基站控制器 18 能在基站 4 和公共交换电话网(PSTN)13 间提供接口, 使得电话呼叫可以被路由到移动设备 10 或从移动设备 10 被路由。此外, 基站控制器 18 会在基站 4 以及连到基于分组的网络 14 的代理 18 之间提供接口, 使得分组能被路由到移动设备 10 以及从移动设备 10 被路由。基站控制器 18 可以标识哪些已解调信号对应于语音数据、以及哪些已解调信号对应于分组, 并且相应地转发数据。例如, 如果无线信号对应于一数据呼叫, 基站控制器 18 就能把数据转发到基于分组的网络 14 的代理。

在移动设备 10 不是移动电话的其它实施例中, 移动设备 10 与连到基于分组的网络 14 的代理的接入点通信。然而, 在该情况下, 移动设备 10 一般不会接入 PSTN 13。移动 IP 网络的这些及其它配置也能实现下面描述的技术。在某些实施例中, 移动设备 10 甚至能通过物理的传输线连到代理, 例如通过临时的有线连接。

在该情况下，下面描述的稳健的更新方案可用于避免可能由传输线上的数据冲突所引起的问题。在还有其它实施例中，无须使用外部代理，移动设备 10 可直接连到网络。

在任一情况下，为了获得对基于分组的网络 14 的接入，移动设备 10 会要求来自 AAA 服务器 20 的授权。例如，因特网服务提供商 (ISP) 会维护 AAA 服务器 20 以执行认证、授权和核算功能。换言之，在移动 IP 环境中，AAA 服务器 20 能认证并授权移动设备 10 以接入网络 14，并且能对移动设备 10 的开通时间进行核算，使得移动设备 10 的用户能被 ISP 相应地记账。

在支持移动 IP 协议的系统 2 中，移动设备 10 会在本地子网上有一 IP 地址。该本地 IP 地址可以以被分配给静态主机的 IP 地址的相同方式被管理。本地 IP 地址用于将分组路由到本地代理 (HA) 22，HA 一般是移动设备 10 的本地子网上的路由器。此外，本地代理 22 可以隧道传送分组，用于在其远离本地时传送到移动设备 10，并且为移动设备 10 维持当前的位置信息。

当远离其本地子网时，移动设备 10 可被分配到一外部代理 (FA) 18。在 IS-835-A 网络中，外部代理 18 是指分组数据服务节点 (PDSN)，并且一般是所访问的子网上的路由器，它向移动设备 10 提供路由服务。在 IS-835-A 网络中，除了充当外部代理以外，PDSN 也能有其它功能。在任一情况下，外部代理 18 都能把分组传送到移动设备 10，所述分组是由本地代理 22 通过网络 14 经隧道传送的。对于移动设备 18 所发送的分组，外部代理 18 能充当将分组发送到附着到网络 14 的其它设备的缺省路由器。

如上所述，为了获得对基于分组的网络 14 的接入，移动设备 14 会向服务提供商要求授权。例如，授权可使用安全密钥 (下文称为密钥) 来获得。例如，移动设备 10 能按照密钥认证协议 (PAP) 发送带有注册请求的密钥，或者在不安全的系统中会产生使用该密钥形成的认证符值。例如，移动设备能使用安全密钥对询问握手认证协议 (CHAP) 产生响应。然后，AAA 服务器 20 验证该响应以便验证移动设备 10 的用户。以这些或其它可能的方式，移动设备 10 能使用其安全密钥请求授权。该密钥类似于密码，该密码认证移动设备 10 的用户是与 AAA 服务器 20 相关联的服务提供商的授权用户。

在从移动设备 10 接收到用授权密钥形成的注册请求后，AAA 服务器 20 使移动设备 10 能接入基于分组的网络 14 内各台计算机上保存的资源 and 信息。为核算起见，

AAA 服务器 20 也能记录开通时间使用率,在此期间移动设备 10 能接入基于分组的网络 14。例如,基于分组的网络 14 能包括诸如因特网这样的全局网络,或可包括较小的公共或专用网络。

在特定的情况下,可能期望改变移动设备 10 的安全密钥。例如,如果不正当设备获得对密钥的接入,不正当设备就能作为未经授权的用户接入基于分组的网络 14。同样,术语“不正当设备”是指使用另一设备的密钥接入或试图接入网络 14 的设备。如果成功,不正当设备就能从移动设备 10 盗取开通时间,或者从服务提供商盗取开通时间。此外,不正当设备可以使用该密钥伪装成另一用户来接入网络 14,并且会执行网络犯罪或网络恐怖主义。为了这些及其它原因,可能期望改变移动设备 10 的密钥,比如响应于已知的不正当威胁、或者周期性地改变以便预见和阻碍不正当的威胁。

图 2 是说明移动设备 10 和 AAA 服务器 20 之间通过外部代理(FA)18 进行的通信。通信实际上通过各种其它设备发送,比如基站 18(图 1)或无线网络接入点。在任一情况下,图 2 说明用于更新安全密钥的改进了的方案。

密钥更新过程可包括一系列的事件,其中移动设备 10 和 AAA 服务器 20 响应于所述事件转换到各个状态。如果在传输期间错过或丢失了一事件,即发送的请求或发送的应答,移动设备 10 或 AAA 服务器就能相应地响应以确保所有事件都发生。这样,移动设备 10 和 AAA 服务器 20 能确保它们不会彼此失去同步。换言之,移动设备 10 和 AAA 服务器 20 能避免所保存的安全密钥不匹配的情况发生。

在一实施例中,移动设备 10 能在密钥更新过程期间在两个可能的状态间转变,AAA 服务器 20 能在三个可能的状态间转变。这样,在移动设备 10 和 AAA 服务器 20 都向存储器提交新密钥并且辨认出移动设备 10 接入网络 14 所使用的新密钥之前,可能要求密钥的更新、以及更新的确认。图 2 所述的技术能实现几个优点,包括避免了在更新过程期间丢失一个或多个通信的问题。此外,所述技术可以通过修改移动设备 10、AAA 服务器 20 和 FA 18 来实现。换言之,所述技术对于系统 2 的其它设备来说是透明的。可以修改移动设备 10 和 AAA 服务器 20 以包括相应的状态机,并且修改 FA 18 以确保当它在密钥更新例程期间接收到接入拒绝(AR)时,它不会终止呼叫。

如图 2 所示,移动设备 10 最初可以在“密钥有效”状态(如 25 所指)下。在密钥有效状态下,移动设备 10 有一个安全密钥被保存在存储器中,要在接入网络

14 时使用。移动设备 10 尝试通过发送注册请求(A)而建立移动 IP 会话。注册请求这里简称为“RRQ”。外部代理 18 接收 RRQ(A)并且发送接入请求(1)，比如按照本领域公知的 RADIUS(远程认证拨入用户服务)客户端/服务器协议。接入请求在此简称为“ARQ”。AAA 服务器 20 接收 ARQ(1)以确认移动设备 10。

在正常情况下，AAA 服务器会接受认证信息，如果正确，则用接入接受(AA)消息响应。然而，在图 2 的示意图中，AAA 服务器 20 最初在“更新密钥”状态(如 26 所指)。在该情况下，AAA 服务器 20 用形式为接入拒绝(2)的应答进行响应，表示移动设备 10 必须更新其密钥，而不是确认 ARQ。接入拒绝在此简称为“AR”。外部代理 18 接收 AR(2)并且发送注册应答(B)以指示移动设备 10 更新其密钥。注册应答在此简称为“RRP”。

AAA 服务器 20 可以通过多种刺激或事件的任一种被置于更新密钥状态。例如，服务提供商会响应于移动用户的请求、或者响应于安全的已知破坏而将 AAA 服务器 20 置于更新密钥状态。或者，AAA 服务器 20 会周期性地进入更新密钥状态以阻碍任何潜在的安全破坏。在任一情况下，一旦 AAA 服务器 20 被置于更新密钥状态，它就会在接收到与来自移动设备 10 的 RRQ 相对应的 ARQ 时启动更新密钥例程。

一旦移动设备 10 接收到表明它必须更新其密钥的 RRP(B)，移动设备 10 就进入更新密钥状态(如 27 所指)。在更新密钥状态下，移动设备 10 产生一新密钥和令牌。例如，移动设备 10 会包括随机数发生器，比如基于硬件的能量计算器，其在给定的实例下计算接收到的电磁能量，并且基于给定实例下接收到的电磁能量的随机量而生成一随机数。令牌也以类似方式产生，并且对应于会用于确认 AAA 服务器 20 随后接收到新密钥的另一个数。然而，令牌的生成和交换仅仅是实现这种确认的示例性方法。在某些实施例中，移动设备 10 会生成和/或发送多个密钥，包括移动-AAA 密钥、移动-HA 密钥、CHAP-密钥或者其它认证密钥。

移动设备 10 接着发送 RRQ(C)，其包括所示新密钥(即多个新密钥)和令牌。外部代理 18 接收 RRQ(C)并向 AAA 服务器 20 发送包括新密钥和令牌的 ARQ(3)。外部主机、或者某些其它外部装置保护新密钥和令牌不受到潜在的窃听。例如，最近生成的密钥可以用仅对于移动设备 10 和 AAA 服务器 20 已知的单独加密密钥来加密。

例如，外部代理 18 可包括一查找表以便将移动设备 10 所使用的 RRQ 格式的进入请求转换成 AAA 服务器所使用的 ARQ 格式的外出应答，或者将 AR 格式的进入应答转换成 RRP 格式的外出应答。然而，在外部代理 18 将请求或应答从一个格式



转变为另一个格式时，请求和应答中保护的信息一般不改变。因此，如果 RRQ(C) 包括新密钥和令牌，ARQ(3) 就类似地包括所述新密钥和令牌。

在接收到 ARQ(3) 时，AAA 服务器 20 将新密钥保存在存储器中，并且转变为更新确认状态(如 28 所指)。然后，AAA 服务器 20 解密该消息并且用 AR(4) 响应，将令牌返回到移动设备 10，该令牌向移动设备 10 认证了 AAA 服务器 20。这向移动设备 10 证明它正在与正确的 AAA 服务器通信，并且向移动设备 10 指示被发送到 AAA 服务器 20 的新密钥被接收。外部代理 18 接收 AR(4) 并且发送 RRP(D) 以便将令牌转发回移动设备 10。然而在其它实施例中，令牌的生成和交换可以改为采用于另一技术而被消除，所述技术向移动设备 10 指示被发送到 AAA 服务器 20 的新密钥被接收。

在接收到带有令牌的 RRP(D) 时，如果该令牌与前面在 RRQ(C) 中发送的令牌相匹配，移动设备 10 就转换回密钥有效状态(如 29 所指)。然后，移动设备 10 作出用其新密钥形成的正常注册请求 RRQ(E)。同样，使用新密钥形成的正常注册请求包括发送密钥、发送用密钥生成的授权值、响应于 CHAP 挑战等等。

在任一情况下，外部代理 18 接收 RRQ(E) 并将 AR(5) 发送到 AAA 服务器 20。一旦 AAA 服务器 20 接收到与使用新密钥生成的请求相对应的 AR(5)，AAA 服务器 20 就转变为密钥 OK 状态(如 30 所指)，并把所存储的新密钥提交给永久存储器，并且用接入接受(AA) 向外部代理 18 应答。外部代理 18 接着被授权以便与本地代理 22 通信。

作为移动 IP 协议的一部分，外部代理 18 把 RRQ 转发到本地代理 22。作为移动-HA 认证的一部分，HA 22 把 ARQ 发送到 AAA 服务器 20。AAA 服务器 20 向 HA 22 发送带有移动-HA 密钥的 AA，移动-HA 密钥也能由移动设备 10 生成并被发送到 AAA 服务器 20，新密钥和令牌的传输如上所述。HA 22 使用移动-HA 密钥验证移动-本地认证扩展。然后，本地代理能向外部代理发送 RRP，外部代理接着又能将 RRP 发送到移动设备 10。这样，一旦移动设备 10 的密钥被更新然后被 AAA 服务器 20 验证，数据就可以通过本地代理 22 和外部代理 18 之间的隧道传送被路由到移动设备 10。

图 2 所示的密钥更新例程可以实现几个优点，包括避免了如果在更新过程期间丢失了一个或多个通信而产生的问题。特别是，在 AAA 服务器 20 中使用至少三个分开的状态以及在移动设备 10 中使用至少两个分开的状态能确保系统能处理更

新例程期间的潜在消息损失。在该情况下，如果 AAA 服务器正在预期更新例程的一系列定义的 ARQ 中的下一个 ARQ，但接收到一个不同的 ARQ，AAA 服务器 20 就能通过重发前面发送过的 AR 进行响应，以确保移动设备 10 和 AAA 服务器 20 具有相同的密钥。因而，移动设备 10 上的密钥不会与 AAA 服务器 20 上保存的密钥失去同步。密钥同步的丢失会使移动设备 10 由于认证失败而不能接入局域网。

此外，图 2 所示的技术能避免与密钥更新例程期间移动设备 10 的功率故障相关的问题。同样，如果在更新例程期间发生诸如空中链路丢失、重置、呼叫失败或其它中断这样的事件，也能避免这些问题。在那些情况下，移动设备 10 和 AAA 服务器 20 能避免失去同步，AAA 服务器 20 能避免粘着于暂时的状态。相反，更新密钥例程会通过重发前面发送过但未被接收或确认的一个或多个通信而继续。重要的是，一旦 AAA 服务器 20 接收到新密钥，它就用令牌应答或另一应答进行响应，所述应答足以向移动设备 10 传达新密钥已被接收。接着，在 AAA 服务器 20 接收到与使用新密钥发送的 RRQ 相对应的 ARQ 以前，它不转变为密钥 OK 状态。这样，在更新方案的每一个事件出现以前，密钥更新例程不会终止。

图 2 所述的技术还可便于处理通过以下引起的问题：一旦已接收到通信则进行一个或多个通信的重发、或者更新例程期间其它通信的传输，比如拒绝从 AAA 服务器 20 到移动设备 10 的服务通信。在那些情况下，由于特定的事件不会发生，因此密钥更新例程不会终止。此外，所述技术的另一优点是它们可以如下实现：通过用相应的状态机修改移动设备 10 和 AAA 服务器 20、以及修改 FA 18 以确保当 FA 18 在密钥更新例程期间接收到 AR 时呼叫并不终止。换言之，实现所述技术所要求的修改对于系统 2 的其它设备来说是透明的。

图 3 是为实现这里所述的密钥更新例程而配置的移动设备 10 的示例性框图。在该例中，移动设备 10 包括各个组件，包括天线 32、RF 接收机/发射机 33、调制解调器(调制—解调单元)34、移动 IP 控制单元 35、存储器 36、密钥更新逻辑 38 和新密钥发生器 39。

RF 接收机/发射机 33 经由天线 32 发送和接收按照所使用的调制方案进行调制的电磁信号。RF 接收机/发射机 33 还能执行进入信号的模数转换以及外出信号的数模转换。RF 接收机/发射机 33 可包括分开的接收机和发射机组件，或者能包括集成电路，即收发机。调制解调器 34 能包括一数字处理器，其执行外出信号的调制和进入信号的解调。

移动 IP 控制单元 35 控制移动 IP 协议下通信的发送和接收。例如，在注册例程期间，移动 IP 控制单元 35 能产生外出的 RRQ，或者能解释进入的 RRP。此外，移动 IP 控制单元 35 可使用安全密钥以便产生一认证符，以验证移动设备 10 的身份。移动 IP 控制单元 35 可接入存储器 36 以获得在注册过程期间使用的安全密钥。此外，移动 IP 控制单元 35 能访问密钥更新逻辑 38 以标识移动设备 10 是否已进入密钥更新状态。

密钥更新逻辑 38 可包括用于在安全密钥更新例程期间转变移动设备 10 的状态的状态逻辑。特别是，如果移动 IP 控制单元 35 将进入的 RRP 解释为来自 AAA 服务器的更新密钥消息，密钥更新逻辑 38 就把移动设备 10 转变为更新密钥状态。在更新密钥状态下，移动 IP 控制单元 35 会调用新密钥发生器 39 来产生要被发送到 AAA 服务器 20 的新密钥。在一例中，新密钥发生器 39 会产生至少两个新数字：1) 新密钥和 2) 令牌。然后，移动设备 10 能转变带有新密钥和令牌的 RRQ，并且在它接收到形式为包含该令牌的 RRP 的确认前保持在密钥更新状态。在某些实施例中，移动设备可能生成和/或发送多个密钥，诸如移动-AAA 密钥、移动-HA 密钥、CHAP-密钥等等。某些或全部所述密钥都可以是最新生成的密钥，或者某些前面被存储的，以及其它最新生成的密钥。在其它情况下，可以改为使用某些其它确认技术而避免令牌的生成和交换。

新密钥发生器 39 会包括能产生随机或伪随机数的任何电路。在一例中，如前所述，新密钥发生器 39 包括基于硬件的能量计算器，它计算天线 32 在给定的实例下接收到的电磁能量，并且基于在给定实例下的接收到的电磁能量的随机量而生成一个随机数。令牌可以以类似方式生成。根据需要，移动 IP 控制单元 35 也在传输前对所述安全密钥和令牌进行加密，比如通过使用仅对于移动设备 10 和 AAA 服务器 20 是已知的加密密钥。在任一情况下，最新生成的密钥和令牌都可以被保存在存储器 36 中以便以后使用。

在进入更新密钥状态后，移动设备 10 会保持在更新密钥状态下，直到它接收到令牌应答为止。这样，在转变为更新密钥状态后，如果移动设备 10 不在分配的时间量内接收令牌应答，它就重发相同的密钥以及令牌，如果移动设备 10 接收到更新密钥，它就重发最新生成的密钥和令牌，并且忽略其它通信。在任一情况下，图 3 的配置都允许移动设备 10 处理通信被丢失或未接收到的情况。在那些情况下，在移动设备 10 试图使用新密钥来获得对网络 14(图 1)的接入前，移动设备 10 会简

单地重复密钥更新例程的一个或多个步骤，以便确保发生正确的事件使移动设备 10 和 AAA 服务器 20 保持同步。

图 4 是为实现这里所述的密钥更新例程而配置的 AAA 服务器 20 的示例性框图。在该例中，AAA 服务器 20 包括各个组件，包括接收机/发射机 42、AAA 控制单元 44、存储器 46 以及密钥更新逻辑 48。

接收机/发射机 42 按照网际协议 (IP) 和移动网际协议 (移动 IP) 发送和接收信号 45。特别是，接收机/发射机 42 可以是接收形式为接入请求 (ARQ) 的信号并且发送形式为接入拒绝 (AR) 或接入接受 (AA) 的信号的电路。接收机/发射机 42 可以包括单独的接收机和发射机组件，或者可包括一集成单元，即收发机。接收机/发射机 42 可工作在数字领域，尽管本发明不必限于该领域。

AAA 控制单元 44 可包括处理器所执行的硬件或软件模块。在任一情况下，AAA 控制单元 44 可被配置成执行认证、授权和核算服务。存储器 46 可以保存一个安全密钥列表以及相关的用户或设备，AAA 服务器 20 能对所述用户或设备许可网络接入。当 AAA 服务器 20 所支持的网络设备请求网络接入时，比如通过发送使用相应的安全密钥形成的注册请求，AAA 服务器 20 就根据存储器 46 中保存的相应用户密钥来认证或拒绝对正在请求设备的接入。同样，认证过程可包括用注册请求发送密钥、或者用注册请求发送使用密钥生成的认证值。例如，AAA 服务器 10 可调用一询问握手认证协议 (CHAP)，移动设备 10 必须使用密钥对该协议进行响应以便被认证。在任一情况下，如果正在请求的设备发送一个用正确密钥形成的注册请求，AAA 服务器 20 就能对正在请求的设备许可网络接入。

密钥更新逻辑 48 可包括一状态机，它被配置成使 AAA 服务器 20 执行这里所述的密钥更新例程。密钥更新逻辑 48 可以为 AAA 服务器 20 定义与密钥更新有关的至少三个可能状态：1) 密钥 OK，2) 更新密钥，以及 3) 更新确认。在正常操作期间，密钥更新逻辑能标识密钥 OK 状态，该情况下，AAA 服务器从请求接入网络的设备接受请求，并且执行认证以验证请求设备的用户。

在特定的情况下，密钥更新逻辑 48 可被置于更新密钥状态，比如响应于外部输入，或者周期性地 (定时的) 进行。更新密钥状态对于要被 AAA 服务器 20 认证的一个特定设备是特定的，或者可能更普遍，使得要被 AAA 服务器 20 所认证的某些或全部设备必须更新它们的密钥。在任一情况下，当 AAA 服务器 20 相对于可能请求网络接入的任何给定设备被置于更新密钥状态中时，它会如这里所述为该设备起

动密钥更新例程。

特别是，当 AAA 服务器 20 被置于更新密钥状态中时，它会响应于来自给定设备的注册请求发送一个 AR(更新密钥)应答。例如，如果 AAA 服务器 20 在 ARQ 为移动设备 10 请求网络接入时进行接收，AAA 服务器就返回一个 AR(更新密钥)应答，表明移动设备 10 必须更新其密钥。接着，AAA 服务器 20 期望从移动设备 10 接收包括新密钥和令牌的 ARQ。如果 AAA 服务器 20 接收到所述 ARQ(新密钥、令牌)请求，AAA 控制单元 44 就把新密钥保存在存储器 46 中，密钥更新逻辑将 AAA 服务器 20 转变为更新确认状态。然后，AAA 服务器 20 发送一 AR(令牌)应答，以便将该令牌返回到移动设备 10，从而向移动设备 10 表明 AAA 服务器 20 已接收到所述新密钥。然而同样，按照本发明的原理，可以使用其它技术(除了交换令牌以外)来向移动设备 10 表明 AAA 服务器 20 已接收到所述新密钥。

AAA 服务器 20 在接收到另一 ARQ 以前不返回到密钥 OK 状态，所述另一 ARQ 与移动设备 10 发送并且用新密钥形成的 RRQ 相对应。在这一点上，已知 AAA 服务器 20 和移动设备 10 相对于新密钥是同步的，且更新密钥例程中未丢失任何通信。这样，AAA 服务器 20 把与移动设备 10 使用新密钥发送的 RRQ 相对应的随后的 ARQ 视为从接收到 AAA 服务器的令牌应答的移动设备 10 而来的确认、并且也视为对接入网络的请求。因而，当 AAA 服务器 20 接收到与移动设备 10 使用新密钥发送的 RRQ 相对应的 ARQ 时，密钥更新逻辑 48 转变为密钥 OK 状态，AAA 控制单元执行移动设备 10 的认证。

图 5 是说明从移动设备 10 的角度所见的安全密钥更新例程的实施例的流程图。如图 5 所示，发射机/接收机 33 发送一注册请求(RRQ)(51)。例如，移动 IP 控制单元 35 会使用其当前的密钥产生所示 RRQ，而调制解调器 34 会调制该 RRQ 并将已调的数字信号转换成要由发射机/接收机 33 经由天线 32 发送的模拟 RF 信号。在正常的操作期间，移动设备 10 不会接收更新密钥应答(52 的“否”支路)。相反，在正常的操作期间，移动设备 10 会接收一个或接受该请求或拒绝该请求的应答。如果移动设备 10 从 AAA 服务器 20 接收到授权(53 的“是”支路)，移动设备 10 就会获得对基于分组的网络 14(图 1)的接入，使移动设备 10 能通过基于分组的网络 14 进行通信(54)。另一方面，如果移动设备 10 从 AAA 服务器接收到拒绝(53 的“否”支路)，移动设备 10 就会通过发送另一注册请求而尝试注册(51)。

然而，如果 AAA 服务器 20 处于更新密钥状态，移动设备 10 就会响应于其注

册请求而接收一更新密钥应答(52的“是”支路)。在该情况下,密钥更新逻辑38就将移动设备10转换到更新密钥状态,新密钥发生器39产生一新密钥和一令牌(55)。然后,移动设备发送带有所述新密钥和令牌的注册请求(56)。例如,移动IP控制单元35可以使用最新生成的密钥和最新生成的令牌来产生RRQ(新密钥、令牌),调制解调器34会调制所述RRQ(新密钥、令牌),并且将已调的数字信号转换为由发射机/接收机33经由天线32发送的模拟RF信号。如果移动设备10在转换为更新密钥状态55后被重置,它还能在这一重置后发送所述RRQ(新密钥、令牌)(56)。

响应于所述RRQ(新密钥、令牌),如果移动设备10接收到一令牌应答RRP(令牌)(是支路57),移动设备10就知道AAA服务器20接收到所述新密钥。在该情况下,密钥更新逻辑38把移动设备10转变回密钥有效状态(58),移动设备10发送使用当前密钥形成的正常注册请求(51),所述当前密钥对应于所述新密钥。如果移动设备10从AAA服务器20接收到授权(53的“是”支路),移动设备10就会获得对基于分组的网络14(图1)的接入,使移动设备10能通过基于分组的网络14进行通信(54)。根据需要,如果在定时间隔内未接收到预期的响应,移动设备10也能实现定时器以引起任何给定注册请求的重发。

图6是从AAA服务器20的角度所见的安全密钥更新例程的实施例的流程图。如图所示,当接收机/发射机42接收到使用旧密钥形成的接入请求时(61),AAA控制单元44就调用密钥更新逻辑48以确定AAA服务器20的状态。如果AAA服务器不处于更新密钥状态(62的“否”支路)或者更新确认状态(63的“否”支路),则AAA服务器20就处于密钥OK状态(64)。在该情况下,AAA控制单元44认证该接入请求并且相应地响应移动设备10(65)。特别是,AAA控制单元44可以检验所发送的安全密钥并且将其与存储器46中保存的安全密钥进行比较。或者,AAA控制单元可以检验使用安全密钥生成的所发送的授权值,并且从授权值提取安全密钥,以便与存储器中保存的安全密钥进行比较。在另一例中,AAA控制单元44可以检验移动设备对注册请求所调用的CHAP询问的响应。

在任一情况下,如果移动设备10发送了一个用正确密钥形成的注册请求,AAA服务器20就通过发送一接入应答进行响应,授权移动设备10接入网络14(图1)。如果不是,AAA服务器20就可以通过发送一接入拒绝进行响应,拒绝移动设备10接入网络14。

然而，如果 AAA 服务器 20 处于更新密钥状态下(62 的“是”支路)，则 AAA 服务器 20 会与移动设备 10 启动一更新密钥例程。同样，如果为了某些原因，AAA 服务器 20 最初处于更新确认状态(63 的“是”支路)，AAA 服务器 20 就能转变为更新密钥状态(66)。在任一情况下，一旦 AAA 服务器 20 处于更新密钥状态下，AAA 控制单元 44 就可以产生一更新密钥应答，以用于接收机/发射机 42 进行传输(67)。然后，在发送更新密钥应答之后，如果 AAA 服务器 20 接收了一个包括新密钥和令牌的接入请求(68)(69 的“是”支路)，密钥更新逻辑 48 就将 AAA 服务器 20 转变为更新确认状态(71)，AAA 服务器 20 发送一个包括所述令牌的接入应答(72)。特别是，AAA 控制单元 44 可以产生令牌应答，接收机/发射机 42 发送所述令牌应答，向移动设备 10 表明它正在与正确的 AAA 服务器通信。而且，移动设备 10 对令牌应答的接收提供了一指示，表明新密钥被 AAA 服务器 20 接收到。

接着，在发送令牌应答后(72)，如果 AAA 服务器 20 接收到一接入请求(73)，该接入请求与移动设备 10 发送的并且用新密钥形成的 RRQ 相对应(74 的“是”支路)，密钥更新逻辑 48 就把 AAA 服务器 20 转变为密钥 OK 状态(75)。在这一点上，AAA 服务器 20 可以把新密钥提交给永久存储器，AAA 控制单元 44 会认证该接入请求并且相应地响应移动设备 10(65)。特别是，通过确定移动设备 10 是否使用与前面被 AAA 服务器 20 接收到的新密钥相对应的新密钥作为密钥更新例程的一部分，AAA 控制单元 44 可以认证移动设备 10。

这里描述的密钥更新技术能实现几个优点，包括避免了如果在更新过程期间丢失一个或多个通信所引起的问题。例如，如果在 AAA 服务器 20 发送令牌应答后(72)，它接收包括所述新密钥和所述令牌的另一个接入请求(73, 74 的“否”支路, 69 的“是”支路)，AAA 服务器 20 就能保持在更新确认状态(71)，并且重发令牌应答(72)。在该情况下，AAA 服务器 20 会假定前面的令牌应答已丢失，或者未被移动设备 10 接收到。

同样，如果 AAA 服务器 20 预期具有新密钥和令牌的接入请求，但不接收这样的请求(69 的“否”支路)，AAA 服务器 20 就会重启更新密钥例程。因而，在该情况下，AAA 服务器会转变为更新密钥状态(70)并且重发另一个更新密钥应答(67)。这样，就能确保更新例程的正确执行，即更新密钥例程的全部事件的正确执行。特别是，一旦 AAA 服务器 20 被置于更新密钥状态(62, 66 或 70)，它就不转变为密钥 OK 状态，直到它接收到具有所述新密钥和所述令牌的接入应答为止(69 的“是”支

路), 然后接收一接入请求, 该接入请求对应于移动设备 10 所发送的并且用所述新密钥形成的 RRQ(77 的“是”支路)。

这里所述的技术能便于处理由于以下引起的问题: 一旦已接收到一个或多个通信时所述通信的重发、或者在更新例程期间其它通信的传输, 比如拒绝从 AAA 服务器 20 到移动设备 10 的服务通信。在那些情况下, 密钥更新例程不会终止, 因为更新密钥例程的全部事件不会已发生。此外, 所述技术的其它优点在于, 它们可以通过仅修改移动设备 10 和 AAA 服务器 20 各自的状态机并且修改 FA 18 来实现, 以确保当它在密钥更新例程期间接收到接入拒绝(AR)时呼叫不结束。换言之, 实现所述技术所需的修改对于系统 2 的其它设备来说是透明的。同样, 通过要求在 AAA 服务器 20 转变到密钥 OK 状态前执行更新例程的全部事件, 这里描述的更新例程改进了对不正当攻击的安全性。

这里描述的技术分别能由移动设备和服务器实现, 所述服务器认证移动设备的用户。在任一情况下, 所述技术都能以硬件、软件、固件或者它们的任意组合来实现。如果以软件实现, 所述技术就是指包括程序代码的计算机可读媒质, 所述程序代码在执行时, 实施这里所述的一个或多个技术。例如, 所述计算机可读媒质能保存计算机可读指令, 所述指令在诸如数字信号处理器(DSP)这样的处理器内执行时, 使相应的移动设备或服务器实现这里所述的一个或多个技术。许多细节都在 IS-835-A 网络环境中提供。类似的技术也能应用于各种其它无线网络。

这些及其它实施例都在权利要求的范围内。



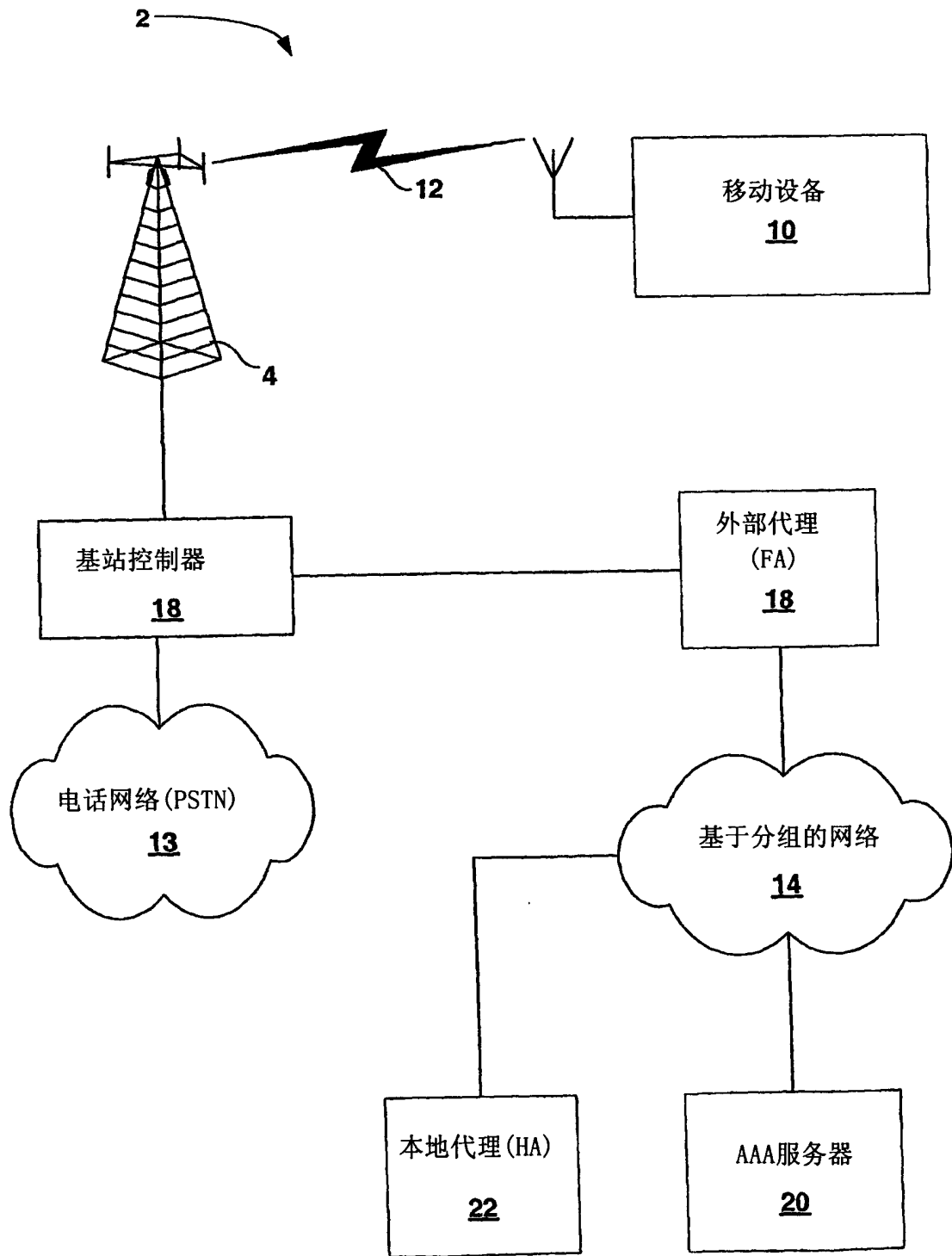
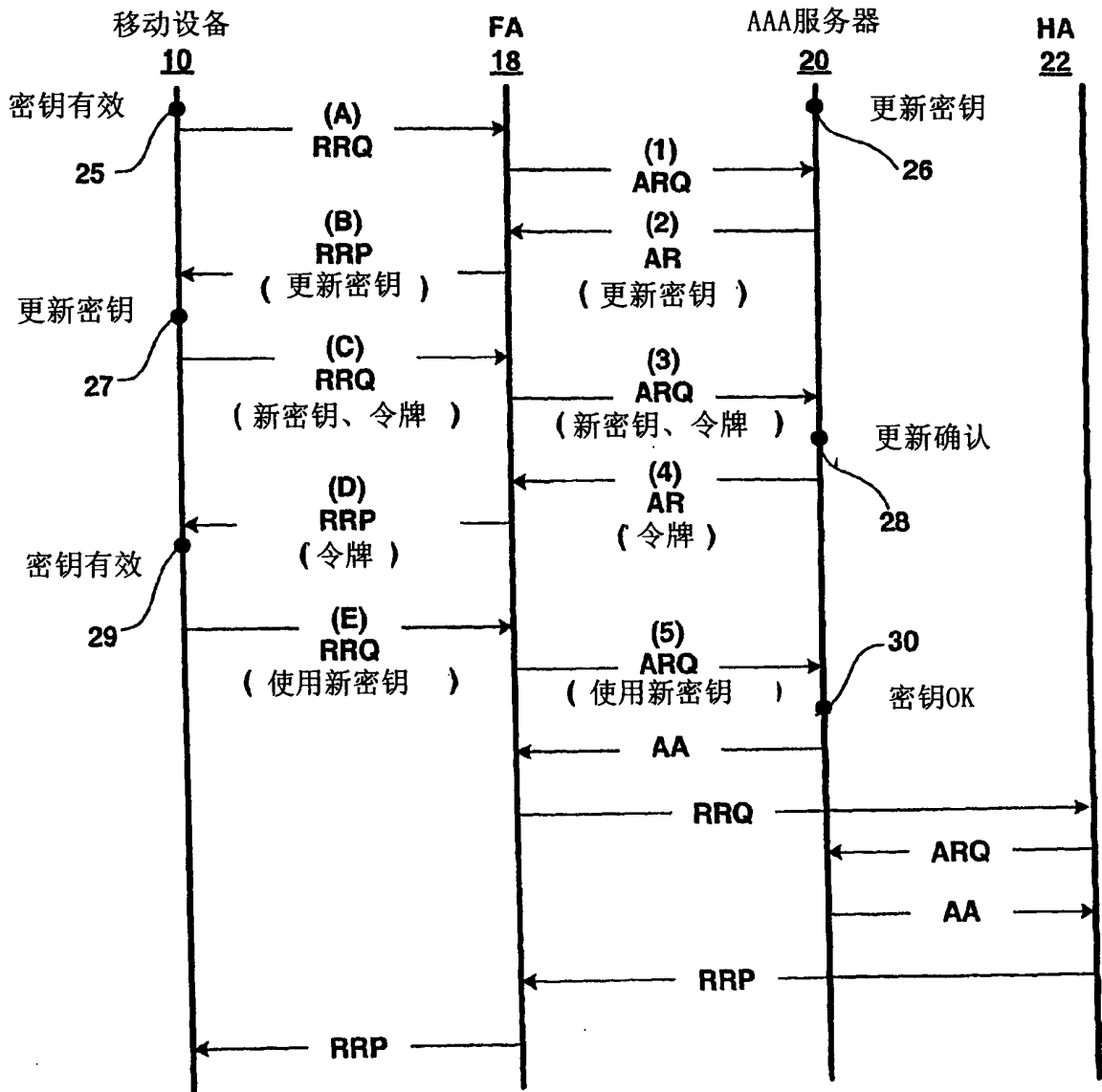


图 1



● 表明当前状态

图 2

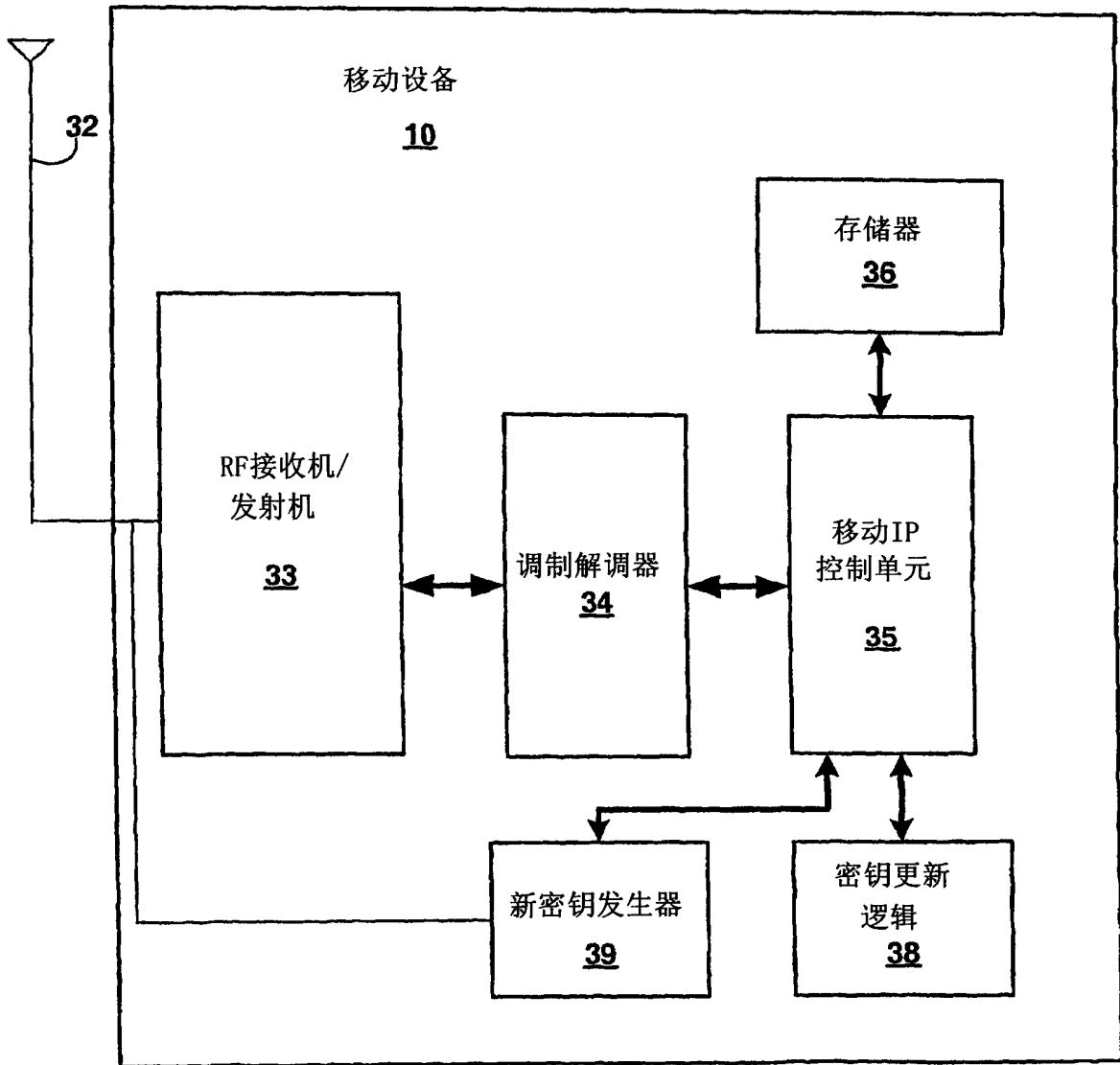


图 3

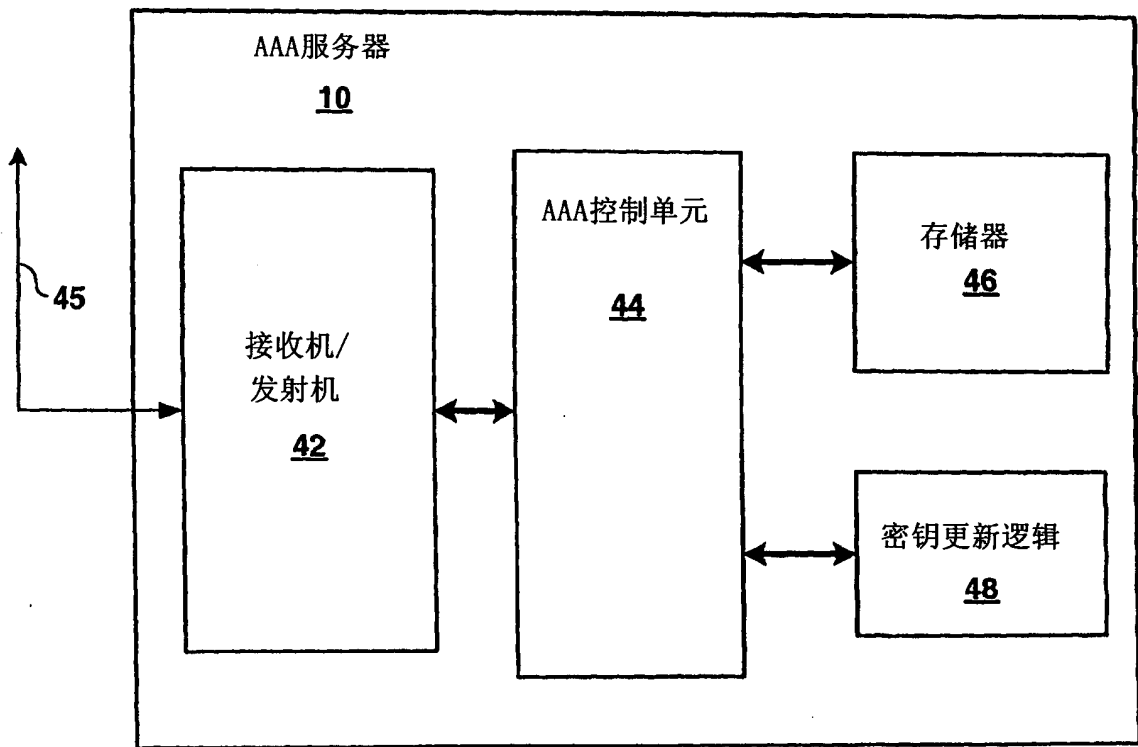


图 4

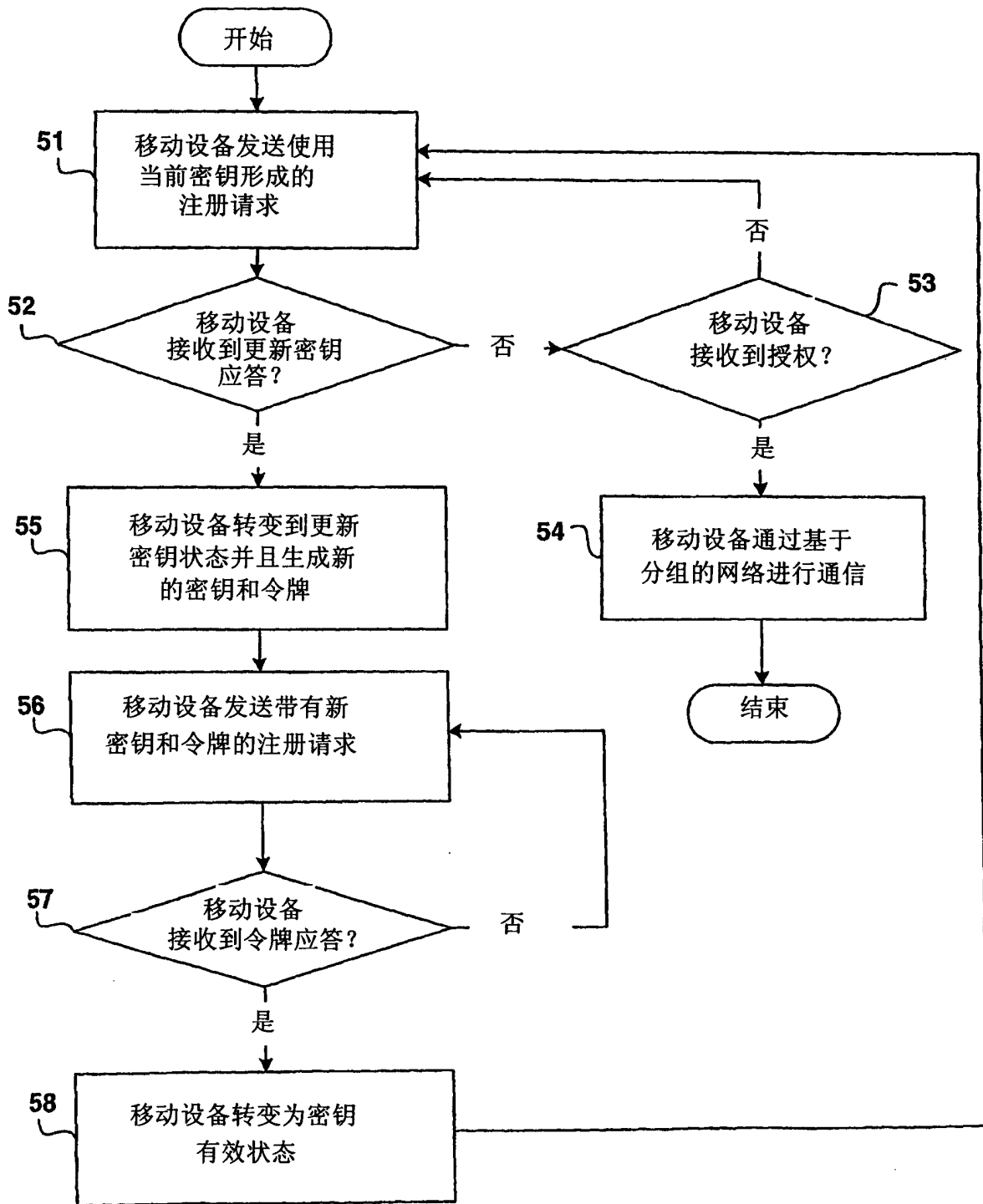


图 5

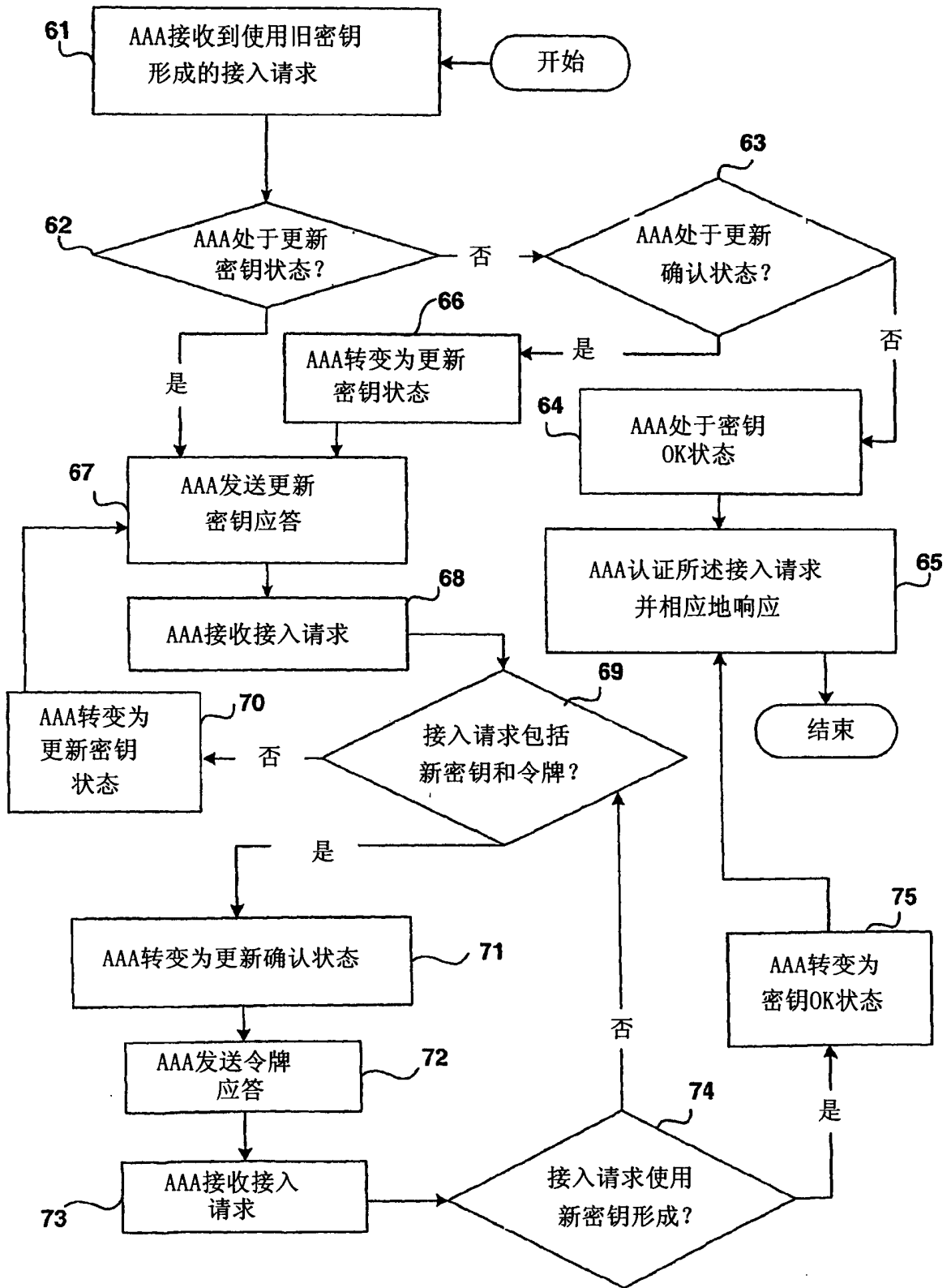


图 6