发明名称
支持接入网络(AN)验证的方法和设备

摘要
本发明提供用于允许无密钥接入终端(AT)经由一服务网络流访问一分组服务数据节点(PSDN)而不使验证网络流的验证功能无效的方法和设备。
1. 一种用于在一服务网络流上为一无线通信装置建立一定对点会话而不使一验证网络流的验证函数无效的方法，其包含：

在所述验证网络流上将一消息从所述无线通信装置传输到一接入网络实体;

将一访问请求消息从所述接入网络实体传输到一服务器，其中所述访问请求消息是关于允许所述无线通信装置访问所述服务网络流;

判定所述无线通信装置是否应参与一密钥供应过程;

如果所述无线通信装置需要密钥供应，那么将一访问信息从所述服务器传输到所述接入网络实体;

一接收到所述访问消息就在所述服务网络流上提供对所述无线通信装置的访问；和

经由所述服务网络流向所述无线通信装置供应一密钥。

2. 根据权利要求1所述的方法，其中判定所述无线通信装置是否需要密钥供应包含判定所述无线通信装置是否是近被激活的。

3. 根据权利要求2所述的方法，其中判定所述无线通信装置是否需要密钥供应包含识别所述访问请求消息的始发者。

4. 根据权利要求3所述的方法，其中从所述服务器到所述接入网络实体的所述访问消息是一访问接受（AA）消息。

5. 根据权利要求1所述的方法，其中从所述服务器到所述接入网络实体的所述访问消息是一携带一移动IP密钥更新（MKU）属性的访问拒绝（AR）消息。

6. 一种用于支持对试图访问一分组数据服务网络的接入终端的验证的系统，所述系统包含：

一接入网络（AN）;

一分组数据服务节点（PDSN），其以通信方式耦接到所述AN和所述
分组数据服务网络；和

一服务器，其以通信方式耦接到所述 AN 和所述 PDSN，并经配置以判定是否验证一与所述 AN 通信的接入终端 (AT) 以与所述 PDSN 通信，其中判定是否验证与所述 AN 通信的所述 AT 包含：

判定与所述 AT 相关联的一访问请求消息是否指示所述 AN 处的始发；和

判定所述 AT 是新近被激活还是需要一个新密钥。

7. 一种用于支持对试图访问一分组数据服务网络的接入终端的验证的系统，所述系统包含：

一服务器，其经配置具有使用者属性和验证密钥；

一分组数据服务节点（PDSN），其以通信方式耦接到所述服务器和所述分组数据服务网络；和

一接入网络（AN），其以通信方式耦接到所述 PDSN 和所述服务器，且经配置以判定是否验证一无密钥接入终端（AT）以访问所述 PDSN，其中如果所述 AN 从所述服务器接收到一包括一移动 IP 密钥更新(MKU)属性的访问拒绝消息，那么所述 AN 验证所述无密钥接入终端。

8. 一种用于支持对试图访问一分组数据服务网络的接入终端的验证的设备，所述设备包含：

至少一个存储元件；和

至少一个处理元件，其经配置以执行一存储在所述至少一个存储元件上的指令集，所述指令集用于：

判定一与一接入终端（AT）相关联的访问请求消息是否指示一接入网络（AN）处的始发；和

判定所述 AT 是否为无密钥的；且

如果所述访问请求消息指示一 AN 处的始发且所述 AT 是无密钥的，那么允许所述 AN 验证所述 AT。
9. 一种在一接入网络（AN）处用于支持对试图访问一分组数据服务网络的接入终端的验证的设备，所述设备包含：

　　至少一个存储元件；和

　　至少一个处理元件，其经配置以执行一存储在所述至少一个存储元件上的指令集，所述指令集用于：

　　将与一存储终端（AT）相关的一访问请求消息传输到一服务器；

　　判定从所述服务器接收到的一访问拒绝消息是否包括一移动 IP 密钥更新（MKU）属性；和

　　如果接收到的所述访问拒绝消息包括一 MKU 属性，那么验证所述 AT 以访问一分组数据服务节点（PDSN）。
支持接入网络（AN）验证的方法和设备

技术领域

本发明大体上涉及无线通信网络和分组交换数据网，且更具体的说，本发明涉及支持访问分组交换数据网的服务的无线通信装置的验证。

背景技术

无线通信领域具有许多应用，其包括（例如）无线电波、寻呼机、无线本地环路、个人数字助理（PDA）、网络电话和卫星通信系统。特别重要的应用是用于远程用户的蜂窝式电话系统。本文所使用的术语“蜂窝式”系统包含使用蜂窝式或个人通信服务（PCS）频率的系统。已为所述蜂窝式电话系统开发了多种无线电接口，包括（例如）频分多址（FDMA），时分多址（TDMA）和码分多址（CDMA）。在此方面，已建立多种国内和国际标准，包括（例如）高级移动电话服务（AMPS）、全球移动系统（GSM）和中期标准95（IS-95）。电信工业协会（TIA）和制定其它著名标准的团体发布了IS-95和其派生物IS-95A, IS-95B, ANSI J-STD-008（本文常常统称为IS-95）和建议的高数据率系统。

三代合作伙伴计划 “3GPP”，文献第 3G TS 25.211 号、第 3G TS 25.212 号、
第 3G TS 25.213 号和第 3G TS 25.214 号中。W-CDMA 标准处于并入称为通
用移动电信系统 (UMTS) 的基于 GSM 的系统中的过程中。

以上所引用的电信标准仅仅是可实施的多种通信系统中的一些的实例。
一种通用标准分类称为 “第三代” 或 “3G”，cdma2000 和 W-CDMA 都是它
的成员。这些 3G 标准针对增加的数据率，所述增加的数据率将支持增加的
使用者数目和数据密集应用。

考虑到对无线数据应用的增长需求，对非常有效的无线数据通信系统的
需要已变得愈加重要。一种所述无线数据应用是在分组交换数据网络起始或
终止的数据包的传输。存在多种协议以经由分组交换数据网传输分组通信
量，而使得信息到达其预定目的地。一种所述协议为 “网际协议”，RFC 791
(1981 年 9 月)。网际协议 (IP) 将消息分成分组包，将数据包从发送者发送
到目的地，且在目的地将数据包重组为原始消息。IP 协议要求每一数据包
以含有起始地址和目的地地址字段的 IP 标头开始，所述标头唯一识别主机
和目的地计算机。

从 IP 网络经由无线通信网络或从无线通信网络经由 IP 网络的数据包的
传输可通过遵守一个协议集合来完成，所述协议集合称为协议栈。一般地，
无线通信装置通过一个接口与基站 (BS) 和/或分组数据服务节点 (PDSN)
通信。无线通信装置可为 IP 数据包的起源或目的地，或为无线通信装置
可为到一电子装置的透明链路。在任一状况下，将有效负载信息分到各个数
据包中，其中标头信息被添加到每一数据包。IP 标头位于 PPP 层的顶部，
PPP 层位于 RLP 层的顶部，而 RLP 层位于物理层的顶部。RLP 层是无线链
路协议层，它负责当发生传输错误时重新传输数据包。PPP 层是点对点协议
层，它是用于经由点对点链路传送 IP 通信量的封装协议。经由无线电将数
据包传送到 BS/PDSN，于是，随后经由 IP 网络发送数据包。

当试图无线传输在有线环境中起始或终止的数据时存在许多困难。其中
之一是试图访问所述分组数据服务的无线终端的验证。

发明内容

本发明提供用于解决以上所述困难的方法和设备。一方面，提供一种用于在服务网络流上为无线通信装置建立点对点会话而不会使验证网络流的验证功能无效的方法，所述方法包含：在验证网络流上将一消息从无线通信装置传输到接入网络实体；将一访问请求消息从接入网络实体传输到服务器，其中所述访问请求消息允许无线通信装置访问服务网络流；判定无线通信装置是否应参与密钥供应处理；如果无线通信装置需要密钥供应，那么将访问消息从服务器传输到接入网络实体；一接收到访问消息就在服务网络流上提供对无线通信装置的访问；和经由服务网络流向无线通信装置供应密钥。

另一方面，提供一种支持试图访问分组数据服务网络的接入终端的验证的系统，所述系统包含：一接入网络 (AN)；一分组数据服务节点 (PDSN)，其通信地端接到 AN 和分组数据服务网络；和一服务器，其通信地端接到 AN 和 PDSN 并配置来判定是否验证一与 AN 通信的接入终端 (AT) 以与 PDSN 通信，其中判定是否验证与 AN 通信的接入终端 (AT) 包含：判定与 AT 相关联的访问请求消息是否指示 AN 处的起始；和判定 AT 是新近被激活还是需要一个新的密钥。

另一方面，提供一种用于支持试图访问分组数据服务网络的接入终端的验证的系统，所述系统包含：一服务器，其以使用者属性和验证密钥配置；一分组数据服务节点 (PDSN)，其通信地端接到服务器和分组数据服务网络；和一接入网络 (AN)，其通信地端接到 PDSN 和服务器，且经配置来判定是否验证无密钥接入终端 (AT) 以访问 PDSN，其中如果 AN 从服务器接收到一包括移动 IP 密钥更新 (MKU) 属性的访问拒绝消息，那么 AN 会验证无密钥接入终端。

另一方面，提供一种用于支持试图访问分组数据服务网络的接入终端的
验证的设备，所述设备包含：至少一个存储元件；和至少一个处理元件，其
经配置以执行存储在所述至少一个存储元件上的指令集，所述指令集用于：
判定与接入终端（AT）相关联的访问请求消息是否指示接入网络（AN）处
的起始；判定 AT 是否为无密钥的；和如果访问请求消息指示 AN 处的起始
且 AT 是为无密钥的，那么允许 AN 验证 AT。

另一方面，提供一种在一接入网络（AN）处的用于支持试图访问分组
data 服务网络的接入终端的验证的设备，所述设备包含：至少一个存储元件；
和至少一个处理元件，其经配置以执行存储在所述至少一个存储元件上的指
令集，所述指令集用于：将与存储终端（AT）相关联的访问请求消息传输
到服务器；判定从服务器接收到的访问拒绝消息是否包括移动 IP 密钥更新
（MKU）属性；和如果接收到的访问拒绝消息包括 MKU 属性，那么验证
AT 以访问分组数据服务节点（PDSN）。

附图说明

图 1 是无线通信网络的示意图。

图 2 是接入终端（AT）、接入网络（AN）、AN-验证、授权和记账（AN-AAA）
服务器和 PDSN 之间的数据连通性的示意图。

图 3 是说明用于经由验证网络流验证的通信流的示意图。

图 4 是说明用于经由验证网络流验证的另一通信流的示意图。

具体实施方式

如图 1 所说明，无线通信网络 10 一般包括数个接入终端（也称为远
端站、移动站、用户单元或使用者设备）12a-12d、数个基站（也称为基
站收发器（BTS）或节点 B）14a-14c、基站控制器（BSC）（也称为无线
网络控制器或数据包控制功能）16、一移动交换中心（MSC）或交换器 18、
一分组数据服务节点（PDSN）或网络互联功能（IWF）20、一公共交换电
话网络（PSTN）22（一般为电话公司）和一分组交换数据网 24（一般为网
际协议（IP）网络）。为了简化的目的，展示四个接入终端 12a-12d、三个基
站 14a-14c，一个 BSC 16、一个 MSC 18 和一个 PDSN 20。所属领域技术人员应了解，可存在任何数量的接入终端 12、基站 14、BSC 16、MSC 18 和 PDSN 20。

在一个实施例中，无线通信网络 10 为分组数据服务网络。接入终端 12a-12d 可为许多不同类型的无线通信装置中的任何一种，诸如：移动式电话、连接到运行基于 IP 的网站浏览器应用的便携式计算机的蜂窝式电话、车载免提套件相关联的蜂窝式电话、运行基于 IP 的网站浏览器应用的个人数据助理 (PDA)、合并便携式计算机的无线通信模块或诸如可在无线本地环路或读数系统中发现的固定位置通信模块。在最通用的实施例中，接入终端可为任何类型的通信单元。

接入终端 12a-12d 可有利地经配置成执行一或一个以上无线分组数据协议，例如，在 EIA/TIA/IS-707 标准中所述的协议。在一个特定实施例中，接入终端 12a-12d 生成指定给 IP 网络 24 的 IP 数据包，且使用点对点协议 (PPP) 将 IP 数据包压缩成帧。

在一个实施例中，IP 网络 24 转接到 PDSN 20，PDSN 20 转接到 MSC 18，MSC 转接到 BSC 16 和 PSTN 22，且 BSC 16 经由配置来根据若干已知协议中的任何一种而传输语音和/或数据包的有线线路转接到基站 14a-14c，所述协议包括 (例如) E1、T1、异步传输模式 (ATM)、网际协议 (IP)、点对点协议 (PPP)、帧中继、高低速率数字用户线 (HDSL)、非对称数字用户线 (ADSL) 或其他普通的数字用户线设备和服务 (xDSL)。在另一个实施例中，BSC 16 直接转接到 PDSN 20，且 MSC 18 不转接到 PDSN 20。

在无线通信网络 10 的典型操作中，基站 14a-14c 接收并解调来自符合在电话呼叫、网站浏览或其它数据通信中的多种接入终端 12a-12d 的反向链路信号集。每一由给定基站 14a-14c 接收到的反向链路信号在所述基站 14a-14c 内加以处理。每一基站 14a-14c 可通过调制反向链路信号集将其传输到接入终端 12a-12d 来与复数个接入终端 12a-12d 通信。例如，如图 1
所示，基站 14a 同时与第一和第二接入终端 12a、12b 通信，且基站 14c 同时与第三和第四接入终端12c、12d通信。所得的数据包转发到 BSC 16，BSC 16 提供呼叫资源分配和移动管理功能性，包括针对一特定接入终端 12a-12d 的从一个基站 14a-14c 到另一个基站 14a-14c 的呼叫软切换协调。例如，接入终端 12c 正同时与两个基站 14b、14c 通信。最后，当接入终端 12c 移动到离基站 14c 中的一个足够远时，呼叫将切换到另一个基站 14b。

如果传输为常规的电话呼叫，那么 BSC 16 会将接收到的数据发送到 MSC 18，MSC 18 为其与 PSTN 22 的接口提供额外的路由服务。如果传输是基于数据包的传输，例如指定向 IP 网络 24 的数据呼叫，那么 MSC 18 会将数据包发送到 PDSN 20，而 PDSN 20 将把数据包发送到 IP 网络 24。或者，BSC 16 直接将数据包发送到 PDSN 20，而 PDSN 20 将数据包发送到 IP 网络 24。

在 WCDMA 系统中，虽然无线通信系统组件的术语各异，但是功能是相同的。例如，基站也可称为在 UMTS 陆地无线接入网络（U-TRAN）中操作的无线网络控制器（RNC）。

在基站范围内操作的从基站到接入终端的前向链路可包含复数个信道。从接入终端到基站的反向链路也包含复数个信道。

每一信道运载不同类型的信息到目标目的地。例如，在 cdma2000 1xEV-DV 系统中，在基础信道上运载语音通信量，且在补充信道或分组数据信道上运载数据通信量。补充信道一般被启动大约几秒持续时间且很少改变调制和编码格式，而分组数据信道会动态地从 20 ms 间隔变成另一间隔。

在典型的通信系统中，“源”生成表示（例如）语音通信量或数据通信量的信息位流。对此位流进行再分并分组，附加多个控制位，且将结果压缩成适当的格式以进行传输。在前向或反向链路上传输前，一般根据一个或一个以上格式编码、调制并扩展语音通信量和数据通信量。在 CDMA 系统中，传输信道格式最终取决于正在传输的语音通信量和数据通信量的信道类型。
和信道条件，此可根据噪声和干扰来描述。

在多种现有的通信系统中，可传输语音和数据通信量的各种格式存在不同名称，例如，帧、数据包和子数据包。本文所描述的实施例的范畴延伸到使用多种传输格式中的任一种的所有无线通信系统。然而，为了易于说明的目的，本文将使用术语“数据包”来描述运载通信量的传输信道格式和通信量的结构。

此外，请注意，CDMA 系统的“数据包”在结构上不同于分组交换数据网的“数据包”。两者都是描述传输数据的格式的单元，但是其中一者是无线网络优选的且另一者是分组交换数据网优选的。例如，来自 IP 源的数据包将含有标头部分和数据部分。然而用于经由无线电传输的数据包运载经编码和调制且有能够在压缩成数据包之前受到符号重复的数据。因此，来自分组交换数据网的数据包将必须重新格式化以在无线网络上使用。在本文和现有技术中所述的实施例中，词语“数据包”的意义需由这个词语的用途推断。

如以上针对无线通信网络所论述，对位进行卷积或涡轮编码、重复及刺穿以生成二进制码符号序列。使所得的码符号隔行交错以获得调制符号。然后，对调制符号进行沃尔什（Walsh）覆盖并在正交相分支上与导频序列组合、以伪随机噪声（PN）序列扩展、基频滤波且调制到传输载波信号上。

在一些 CDMA 系统中，源可生成“逻辑”信道以经由上述物理信道传输。逻辑信道是与特定应用相关联的位流，它可与其它逻辑信道形成多路复用，每一信道包含与其它应用相关联的位流。然后，经多路复用的逻辑信道准备以上述方式经由物理信道传输。在前述 IS-856 中发布的 cdma2000 1xEV-DO 系统中，逻辑信道称为“流”且由流协议定义。

因为实施例的主题是针对移动 IP 电话，所以也将立刻使用 RFC 2002（1996 年 10 月）的术语。在此文献中发布的协议使移动通信装置能够将接触点改变到因特网，而不必改变装置的 IP 地址。即，RFC 2002 描述了一种
注册方案，其向家乡代理（home agent）通知移动通信装置的位置，使得家乡代理可经由外地代理（foreign agent）发送数据包。“家乡代理”是在接入终端的家乡系统处理 IP数据包的基础结构元件。“外地代理”是在被访问的系统处服务接入终端的基础结构元件。参看图1，外地代理和/或家乡代理的功能可由被访问的网络中的 BSC16或家乡网络中的 BSC16来完成。验证、授权和记帐功能通常由服务器执行，所述服务器称为验证、授权和记帐（AAA）服务器。AAA服务器通常地与到PDSN或BSC中。

在cdma2000 1xEV-DO（下文称为EV-DO）中，图1的无线通信系统实体在概念上简化成接入终端和接入网络。接入终端（AT）是允许使用者经由EV-DO无线接入网络访问分组交换数据网的任何装置。接入网络（AN）包含提供分组交换数据网与接入终端之间的数据连通性的任何网络设备/实体。

图2是AT200、AN210、AN-AAA服务器220和PDSN230之间的数据连通性的示意图。当AT200需要访问PDSN230时，AT200与AN210之间就建立通信会话。所述会话根据PPP协议执行且称为验证网络流。AN210与AN-AAA服务器220通信以判定是否允许AT200访问PDSN230。

基于在验证网络流内传送的验证信息，AN210在AT200与PDSN230之间透明地传递服务网络流。PDSN230进一步与AN-AAA服务器220通信以判定是否允许AT200访问分组交换数据网（未图示）。基于服务网络流内传送的验证信息，PDSN230允许分组交换数据网（未图示）与AT200之间的IP通信量。

在验证网络流上，使用例如CHAP（竞争握手验证协议）来执行验证。在所述实施例中无需过分的实验即可使用其它的验证协议，但是为了易于说明，本文将说明CHAP。在服务网络流上，可使用CHAP、移动IP验证或PAP（口令验证协议）执行验证。

注意，在EV-DO系统中，验证网络流和服务网络流为可经由物理、无
无线电、传输信道一起多路复用的逻辑信道。

由于需要在 AN 验证 AT 在 EV-DO 网络上的初始注册，因此引发了一个问题。使用服务网络注在 AAA 处供应验证口令/密钥。为了参与密钥更新程序，AT 将必须由 AN 来传递，AN 充当在 AT 与 PDSN 之间中继消息的“受门人”（gatekeeper）。然而，新激活的 AT 并不具有验证密钥。在初始注册期间，不存在与位于 AN-AAA 服务器处的新激活的 AT 相关联的密钥。AN-AAA 服务器不向 AN 提供对所述 AT 的许可，因此 AN 将不验证 AT。换言之，AT 需要一密钥以被供应一密钥。当服务提供者希望为已激活的 AT 供应新密钥时，也会引起此问题。为了利用密钥更新程序，已激活的 AT 将需要访问验证网络流。然而，验证网络流已“键入”了新密钥而不是由已激活的 AT 持有的旧密钥。

当前对这个问题的解决方案是使验证网络流的验证功能无效，但这是有问题的。使验证网络流的验证功能无效将使网络易受到“否定服务”的攻击，其中任何伪劣的 AT 都能够建立 PPP 会话且使其开放一不确定的时间段，而不会被验证。本文所提供的实施例用于在服务网络流上建立 PPP 会话而不使验证网络流的验证功能无效。

在下述实施例中，提供用于经由服务网络流触发移动 IP 密钥更新（MKU）程序而不会使验证网络流无效的方法和设备。在一个实施例中，由 AN-AAA 服务器所执行的行为触发 MKU 程序。在另一个实施例中，由 AN 所执行的行为触发 MKU 程序。

图 3 是说明 AN-AAA 服务器触发 MKU 程序的实施例的流程图。在这个实施例中，用 AT 新近被激活或 AT 是需要一个新密钥的已被激活的单元的信息来对 AN-AAA 服务器进行编程。（在移动 IP 的说法中，AT 也称为移动节点（MN）。）在步骤 300 中，AN 试图使用例如 CHAP 之类的验证协议建立一与 AT 的验证网络流。

在步骤 310 中，AT 发送一个使用者识别符作为对来自 AN 的询问的回
应的一部分，所述使用者识别符可包括（但不限于）移动节点识别符 MN ID 或网络访问识别符 NAI。所述回复通常包含使用者识别符和从所述询问取得的随机值，其中通常使用散列函数隐瞒所述回复。RFC 1994（1996 年 8 月）发布了 CHAP 验证程序中的称为 MD5 的单向散列函数的使用。

在步骤 320 中，AN 将“访问请求”（ARQ）消息传输到 AN-AAA 服务器。在这个实施例中，ARQ 消息应传达关于 ARQ 消息的起始者的特征信息。换言之，ARQ 消息的起始者是一 AN（与 PDSN 和另一 AAA 服务器相对）的信息应包括 ARQ 消息。在 TIA-878 中，“高速分组数据（HRPD）网络访问接口的互通规范（IOS）”是可选的，它是否是访问验证的内容的 HRPD 访问验证字段。在当前实施例中，此可选字段用于决定是否允许访问服务网络流。

在步骤 330 中，AN-AAA 服务器接收 AN 识别符和含有来自 AT 的 CHAP 回应的 ARQ 消息，且基于两个条件做出一决定。所述条件为使用者属性与新近激活状态相关联（或需要密钥供应）和 ARQ 消息是由 AN 始发的。

在步骤 340 中，如果满足这两个标准，那么 AN-AAA 服务器将“访问接受”（AA）消息传输到 AN。否则，将“访问拒绝”（AR）消息传输到 AN。

在步骤 350 中，如果从 AN-AAA 服务器接收到一 AA 消息，那么 AN 返回一验证成功的指示，否则，如果从 AN-AAA 服务器接收到一 AR 消息，那么 AN 返回一验证失败的指示。如果接收到 AA 消息，那么程序流程进行到步骤 360，否则，程序流程以 AT 的验证失败而结束。

在步骤 360 中，AN 中继 AT 与 PDSN 之间消息的，于是，与 PDSN 通信的 AN-AAA 服务器触发一 MKU 程序。在一成功的 MKU 过程结束时，AN-AAA 与 AT 将具有一共同的共享密密集合。

以上的程序流程允许 AT 访问服务网络流以被供应有验证信息。为了让程序流程达成此目的，AN-AAA 服务器应具有指示 AT 是新近激活的单元或需要密钥供应的信息。此外，AN-AAA 服务器应具有关于 ARQ 消息的始发
者的信。AN-AAA 服务器的处理和存储元件应配置以使用以上两个标准来判定是否将 AA 消息发送到 AN，而不管是否缺乏针对验证网络流上的验证程序的口令/密钥。

图 4 是说明 AN 触发 MKU 程序的实施例的流程图。在步骤 400 中，AN 尝试使用例如 CHAP 之类的验证协议建立与 AT 的验证网络流。

在步骤 410 中，AT 发送一个使用者识别符作为对来自 AN 的询问的回应。

在步骤 420 中，AN 将“访问请求”（ARQ）消息传输到 AN-AAA 服务器。

在步骤 430 中，AN-AAA 服务器接收 ARQ 消息并判定 AT 是新近激活的单元还是需要密钥供应。然后，程序流程继续进行到步骤 440。

在步骤 440 中，AN-AAA 服务器将包括“所需的 MKU 更新”属性的“访问拒绝”（AR）消息传输到 AN。注意，先前实施例需要 AN-AAA 服务器来基于所述的两个标准来改变其行为，而这个实施例不需要 AN-AAA 服务器配置进行任何改变。

在步骤 450 中，AN 接收具有 MKU 属性的 AR 消息，此二者的到达为一个新的标准集合允许 AT 访问 PDSN，而不需要具有适当的验证信息。AN 中的存储和处理元件配置以将包括 MKU 属性的 AR 消息的到达解释为 AT 是新近激活还是需要密钥供应的指示。本文将此任一状态称为“无密钥”。因此，在步骤 460 中，AN 判定 MKU 更新为无密钥 AT 所需且将验证成功的指示返回到 AT。

在步骤 470 中，AN 中继 AT 与 PDSN 之间的消息，于是，由与 PDSN 通信的 AN-AAA 服务器触发 MKU 程序。注意，只要 AN-AAA 服务器判定 AT 新近被激活或只要系统提供者判定应将新的口令/密钥供应给一些或所有接入终端，就可在 AR 消息中设置 MKU 属性。因此，这个实施例在选择性地将密钥供应提供给已激活的接入终端上具有增加的灵活性。
所属领域技术人员应了解，可使用任何各种不同技术和工艺来表示信息和信号。例如，遍及以上描述所引用的数据、指令、命令、信息、信号位、符号和芯片可由电压、电流、电磁波、磁场或磁性粒子、光场或光学粒子和其任何组合表示。

所属领域技术人员应进一步了解，连同本文所揭示的实施例描述的各种说明性逻辑块、模块、电路和算法步骤可实施为电子硬件、计算机软件和二者的组合。为了清楚地说明硬件和软件的可交换性，多种说明性组件、区块、模块、电路和步骤已大体根据其功能加以描述。所示功能实施为硬件还是软件取决于强加于整个系统的特定应用和设计限制。熟练的技术人员可针对每一特定应用以变化的方式实施所述的功能，但是不应将这些实施决定解释为偏离本发明的范畴。

连同本文所揭示的实施例描述的各种说明性逻辑块、模块和电路可以各物来实施或执行：通用处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、场可编程门阵列（FPGA）和其它可编程逻辑装置、离散门和晶体管逻辑、离散硬件组件或设计成执行本文所述的功能的其任何组合。通用处理器可为微处理器，但或者，所述处理器可为任何常规的处理器、控制器、微控制器或状态机。处理器也可实行为计算装置的组合（例如，DSP 和微处理器的组合）、复数个微处理器、与 DSP 核心协作的一或一个以上微处理器，或任何其它所述配置。

连同本文所述的实施例描述的方法或算法的步骤可直接以硬件、由处理器执行的软件模块或两者的组合实施。软件模块可位于 RAM 存储器（随机存取存储器）、闪存、ROM 存储器（只读存储器）、EPROM 存储器（可擦可编程只读存储器）、EEPROM 存储器（电可擦可编程只读存储器）、寄存器、硬盘、可移动磁盘、CD-ROM（光盘只读存储器）或现有技术已知的任何其它形式的存储媒体中。示例性的存储媒体耦接到处理器，所述处理器可从存储媒体读取信息且可将信息写入到存储媒体。或者，可将存储媒体整合到处
理器中。处理器和存储媒体可位于 ASIC 中。ASIC 可位于使用者终端中。或者，处理器和存储媒体可作为离散组件位于使用者终端中。

提供所揭示的实施例的先前描述以使所属领域任何技术人员能够制造或使用本发明。所属领域技术人员将易了解这些实施例的多种修改，且在不偏离本发明的精神或范畴的情况下，本文所界定的通用原理可应用于其它实施例。因此，并不希望本发明限于本文所展示的实施例，而应符合与本文所揭示的原理和新颖特征一致的最广泛的范畴。
图 3