[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04K 1/00

[12]发明专利申请公开说明书

[21]申请号 00803128.2

[43]公开日 2002年5月1日

[11]公开号 CN 1347605A

[22]申请日 2000.1.28 [21]申请号 00803128.2
[30]优先权
[32]1999.1.29 [33]US [31]60/117,788
[32]1999.4.9 [33]US [31]60/128,772
[86]国际申请 PCT/US00/02174 2000.1.28
[87]国际公布 WO00/45539 英 2000.8.3
[85]进入国家阶段日期 2001.7.26
[71]申请人 通用仪器公司
地址 美国宾夕法尼亚
[72]发明人 萨莎·梅德万斯凯 史蒂文·E·安德森
保罗·莫罗尼 埃里克·斯普龙克
乔纳森·A·费洛斯

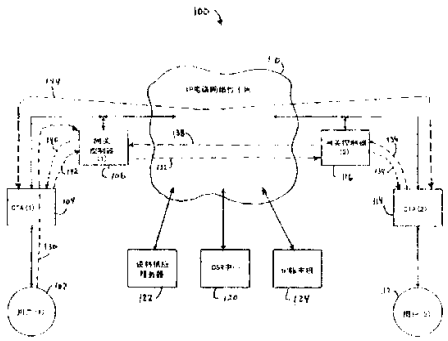
[74]专利代理机构 永新专利商标代理有限公司
代理人 蹇 炜

权利要求书3页 说明书9页 附图页数5页

[54]发明名称 保护CTA之间信号传递和呼叫分组的电话呼叫用密钥管理

[57]摘要

一种在IP电话网络上第一用户(102)和第二用户(112)之间 建立安全通信信道的系统。第一用户和第二用户连接到第一(104) 和第二(116)电话适配器,该适配器随后分别连接到第一(106)和 第二(116)网关控制器,其中网关控制器控制用户对IP电话网络的 接入。电话适配器用于对IP电话网络上交换的用户信息进行加密和 解密。该系统包括一个方法,当在第一网关控制器上接收一个请求建 立第一用户和第二用户之间安全通信信道时,开始该方法。接着,在 第一网关控制器处产生安全密钥(408)。该安全密钥的副本在以前建 立的安全连接上发布给第一和第二电话适配器。最后,通过利用安全 密钥对信息进行加密和解密在第一用户和第二用户之间建立(422) 安全通信信道。



ISSN1008-4274

01.07.26

权 利 要 求 书

1. 一种在 IP 电话网络中建立第一和第二用户之间安全通信信道的方法，其中第一用户和第二用户连接到第一和第二电话适配器，该适配器随后分别连接到第一和第二网关控制器，其中网关控制器控制用户对 IP 电话网络的接入，和其中电话适配器对 IP 电话网络上交换的用户信息加密和解密，该方法包括：

在第一网关控制器处接收一个请求，以在第一用户和第二用户之间建立安全通信信道；

在第一网关控制器处产生一个安全密钥；

在以前建立的安全连接上将该安全密钥发布给第一和第二电话适配器；和

通过利用该安全密钥对信息加密和解密在第一用户和第二用户之间建立安全通信信道。

2. 如权利要求 1 的方法，其中所述产生安全密钥步骤包括在第一网关控制器处产生用作安全密钥的随机数的步骤。

3. 如权利要求 1 的方法，其中所述产生安全密钥步骤包括在第一网关控制器处派生出安全密钥的步骤，其中安全密钥由在第一电话适配器和第一网关控制器之间共享的信号传输密钥中派生出来。

4. 如权利要求 1 的方法，其中所述发布步骤包括：

从第一网关控制器向第二网关控制器发送安全密钥；

从第二网关控制器向第二电话适配器发送安全密钥；

从第一网关控制器向第一电话适配器发送安全密钥。

5. 如权利要求 1 的方法进一步包括步骤：

在第一网关控制器处接收一个请求，以提供安全密钥给执法服务器；和

提供安全密钥给执法服务器。

6. 一种在第一用户和第二用户之间建立安全通信信道的 IP 电话网络，其中第一用户和第二用户连接到第一和第二电话适配器，电话适配器随后分别连接到第一和第二网关控制器，其中网关控制器控制用户对 IP 电话网络的接入，和其中电话适配器对 IP 电话网络上交换的用户信息加密和解密，该 IP 电话网络包括：

接收请求装置，用于在第一网关控制器上接收一个请求以在第一用户和第二用户之间建立安全通信信道；

产生安全密钥装置，用于在第一网关控制器上产生一个安全密钥；

发布密钥装置，用于在以前建立的安全连接上将安全密钥发布给第一和第二电话适配器；和

建立安全通信信道的装置，用于通过利用安全密钥对信息加密和解密在第一用户和第二用户之间建立安全通信信道。

7. 一种网关控制器，用于在 IP 电话网络中建立安全通信信道，该网关控制器连接到电话适配器与电话网络骨干网之间，该网关控制器包括：

一个密钥产生模块，具有逻辑电路以产生安全密钥；

一个密钥存储器，连接到密钥产生模块并且具有逻辑电路以存储安全密钥；和

一个消息处理器，连接到密钥产生模块和密钥存储模块，并且具有逻辑电路以处理电话适配器与电话网络骨干网之间交换的消息，其中消息处理器进一步包括：

接收一个请求建立第一用户和第二用户之间的安全通信信道的逻辑电路，该第一用户连接到电话适配器，而第二用户连接到远程电话适配器；

在以前建立的安全连接上发布安全密钥给电话适配器的逻辑电路，由此可以通过利用安全密钥读信息加密和解密建立第一用户和第二用户之间的安全通信信道。

8. 权利要求 7 的网关控制器，其中密钥产生模块具有逻辑电路以产生作为安全密钥的随机数。

9. 权利要求 7 的网关控制器，其中密钥产生模块具有逻辑电路以根据与电话适配器共享的信号传输密钥派生出安全密钥。

10. 权利要求 7 的网关控制器，其中密钥存储模块具有逻辑电路以在存储之前利用属于执法的公共/专用密钥对对安全密钥进行加密。

说 明 书

保护 CTA 之间信号传递和呼叫分组的电话呼叫用密钥管理

有关申请的相互对照

本申请要求1999年1月29日提交的美国临时专利申请60/117788和 1999 年 4 月 9 日提交的美国临时专利申请 60/128772 的优先权，这些申请的内容为参考目的在此引用。

本发明技术领域

本发明涉及电话网络通信领域，更具体地涉及在 IP 电话网络中建立用户之间的安全通信信道。

本发明背景技术

互联网协议（IP）电话网络允许大量用户通过安全信道相互通信。通常，用户通过电话适配器（TA）连接到电话网络。在电缆 IP 网络中，可以使用电缆电话适配器（CTA）。CTA 将用户信息例如话音或数据转换为网络上传输的分组，并且将所接收分组转换为用户使用的数字或模拟信号。

为实现 IP 电话网络中两个用户之间的安全信道，它们有关的 CTA 使用相同加密技术和密钥。可是，这就出现了一个 CTA 与 CTA 通信的问题，可能建立非常大量（成百万）的可能连接。因此，任何单一 CTA

不可能为所有可能连接预先保持安全关系。因此，当第一次建立安全信道（电话呼叫）时，必须在不工作时建立安全关系（例如，加密密钥）。

建立 CTA 到 CTA 通信的标准技术提供保密的密钥交换（已验证的和机密的），并且使用两个技术之一。在第一技术中，在双方之间共享一个已知密钥。如上所述，该技术与成百万用户不成比例，因此不适合于普通 IP 电话网络。第二技术，使用公共密钥技术，例如与数字签名组合的 Diffie-Hellman 交换。这种技术在时间和 CPU 耗时上成本高，并且可能引起呼叫建立的明显延迟或增加 CTA 设备的成本。因此，不希望公共密钥技术用于这种用途。

本发明概述

本发明提供一个在 IP 电话网络用户之间建立安全通信的系统。在 IP 电话网络中，网关控制器用于控制用户与 IP 电话网络设施之间的信息传递。

包括在本发明中的该系统包括提供网关控制器，该控制器产生用于对用户之间消息加密和解密的媒体数据流加密密钥。当第一用户试图建立与第二用户的安全信道时，与第一用户连接的网关控制器（信源）产生媒体数据流加密密钥，在信号传递消息中发送该密钥给服务第二用户的网关控制器（信宿）。两个网关控制器然后发送该密钥给服务第一和第二用户的两个 CTA。这允许两个 CTA 和从而两个用户迅速在 IP 电话网络上建立安全通信信道。

在本发明的实施例中，提供了在 IP 电话网络中第一用户和第二用户之间建立安全通信信道的方法。第一用户和第二于连接到第一和第二电话适配器，随后它们分别连接到第一和第二网关控制器，其中网关控制器控制用户对 IP 电话网络的接入。该电话适配器用于对 IP 电话网络上交换的用户信息加密和解密。该方法通过在第一网关控制器上接收建立第一用户和第二用户之间安全通信信道的请求开始。接着，在第一网关控制器上产生保密密钥。该保密密钥的副本在以前建立的安全连接上发布给第一和第二电话适配器。最后，在第一用户和第二用户之间通过利用该保密密钥对信息加密和解密建立安全通信信道。

通过参照说明书其余部分和附带的权利要求书，可以进一步理解本文所公开的本发明特性和优点。

附图简介

图 1 表示按照本发明构成的 IP 电话网络一部分；

图 2 表示按照本发明构成的网关控制器；

图 3 表示按照本发明的图 1 的 IP 电话网络中消息流的消息流图；

图 4 表示在使用图 3 所示消息的图 1 中 IP 电话网络用户之间建立安全通信信道的方法；和

图 5 表示图 1 的 IP 电话网络和包括对普通旧的电话系统（POTS）网关的连接。

优选实施例的说明

本发明包括一个在 IP 电话网络用户之间建立安全通信信道的系统。本发明实施例利用基于密钥的加密技术作为实现 IP 电话网络中安全通信的机理。这样的实施例不限于使用任何一种加密技术，因此有可能使用几个类型的加密技术构成本发明的实施例。由于所选择的加密技术类型对于本发明不是必要的，不提供特定加密技术的详细说明。

为清楚和方便，假设 IP 电话网络是电缆网络，所以电缆电话适配器（CTA）将用于各个实施例中。可是，本发明不限于使用 CTA，实际上可以使用特定网络所需要的任何其它类型电话适配器实现本发明。

图 1 表示按照本发明构成的 IP 电话网络 100 的一部分。网络 100 包括一个连接到信源 CTA104 的第一用户 102。信源 CTA104 进一步连接到信源网关控制器 106 和 IP 电话网络骨干网 110。

该网络 100 也包括一个连接到信宿(destination)CTA114 的第二用户。信宿 CTA114 进一步连接到信宿网关控制器 116 和 IP 电话网络骨干网 110。另外，该网络 100 也包括一个客户服务代表（CSR）中心 120，一个资料供应服务器 122 和一个记帐主机 124。

该网络 100 的每个用户通过初始化程序启动网络服务。例如，当用户 102 和有关 CTA104 连接到该网络时，在 CTA104、网关控制器 106 和 CSR120 之间交换一系列消息。该消息为用户 102 提供电话服务启动，建立帐户信息和产生 CTA 对网络上交换消息加密和解密使用的加

密密钥。记帐主机 124 用于建立每个用户的帐户信息，并且对网络的使用记帐。资料供应服务器 112 用于对特定 IP 电话网络内的 CTA 设备初始化和登记。

图 2 表示按照本发明构成的网关控制器 200 的一个实施例。网关控制器 200 包括一个消息处理器 202、一个密钥产生模块 204 和一个密钥存储器 206。网关控制器 200 连接到 IP 电话网络骨干网与网络适配器例如 CTA 设备之间。例如，网关控制器 200 适合于用作图 1 中的网关控制器 106。

消息处理器 202 处理 CTA 和电话网络其它成员之间交换的消息。例如，在初始 CTA 登记程序中，当在 CTA 与网络其它成员之间交换消息时。

密钥产生模块 204 具有逻辑电路以产生或获得用于对 IP 电话骨干网 110 上 CTA 之间交换消息加密和解密使用的密钥。该密钥可以存储在密钥存储器 206 中。密钥存储器具有逻辑电路以在存储器利用公共/专用密钥对之前对密钥加密。例如，公共/专用密钥对可以由该网络 100 设施提供或由政府执法官员提供。

图 3 表示消息交换图 300，该图表示该网络 100 成员之间交换消息以在用户 102 和用户 112 之间建立安全通信信道。该消息在线 302 代表的信源 CTA、线 304 代表的信源网关控制器 106、线 306 代表的信宿网关控制器 116 和线 308 代表的信宿 CTA114 上发送和接收。

图 4 表示流程图，表示利用图 3 所示消息安徽子本发明建立安全通信信道的程序。

在方框 402，通过消息 301 如图所示建立信源与信宿之间的安全信号传递。在方框 404，通过消息 312 和 314 在信源和信宿 CTA 和它们有关网关控制器之间建立安全信号传递。

在方框 406，用户 102 希望设立对用户 112 的安全呼叫并且因此通知 CTA104，而 CTA104 随后通知网关控制器 106，如同消息 316 和路径 103 所示。在方框 408，信源网关控制器产生用于建立用户 102 所请求的安全通信信道的一个密钥。在实施例中，该密钥是随机数并且可以例如在密钥产生模块 204 中产生。

在方框 410，该密钥从信源网关控制器传输给信宿网关控制器，如同消息 318 和路径 132 所示。在方框 412，信宿网关控制器传递该密钥给信宿 CTA，如同消息 320 和路径 134 所示。在方框 414，信宿 CTA 发送确认应答给信宿网关控制器指示已收到该密钥，如同消息 322 和路径 136 所示。

在方框 416，该信宿网关控制器发送确认应答给信源网关控制器，指示已收到该密钥，如同消息 324 在路径 138 所示。在方框 418，信源网关控制器传递该密钥给信源 CTA，如同消息 326 在路径 140 所示。在方框 420，信源 CTA 通过发送确认应答来回答，如同消息 328 和路径 142 所示。

在方框 422，现在可以在信源 CTA 和信宿 CTA 之间建立能够在电话用户 102 和 112 之间交换加密消息的安全信道，如同消息 330 和路径 144 所示。

作为上述操作的结果，信源网关控制器产生一个加密密钥并且将

它发布给信源和信宿 CTA，以快速设立安全通信信道，由此允许用户 102 和用户 112 在 IP 电话网络 100 上通信。在实施例中，发布密钥的消息是用于操作该网络 100 的另外消息。在另一个实施例中，该密钥可以被结合到现有呼叫信号传递消息中，以便保持总消息开销较低并且改善网络效率。

图 5 表示图 1 的 IP 电话网络 100，并且包括一个与普通旧电话系统（POTS）网关 504 的连接。POTS 网关 504 连接到该网络 100 的第三用户 502。

为建立用户 102 与用户 502 之间的安全通信信道，可以使用图 4 的方法，可是，由于没有信宿 CTA，不使用与信宿 CTA 有关的操作。例如，POTS 网关可以提供专用和验证后连接。因此，下文描述当利用 POTS 网关时呼叫建立中的差别。

在方框 410，信源网关控制器发送密钥给 POTS 网关 504，如同路径 506 所示。方框 412 和 414 被跳过。在方框 416，POTS 网关发送确认信号给信源网关控制器，如同路径 508 所示。方框 418 到 422 保持相同。

利用上述图 4 的方法，可以在 CTA104 和 POTS 网关 504 之间建立专用和验证的安全信道，如同路径 520 所示，以便用户 102 和 504 可以交换消息。

在本发明呼叫开始方相反的另一个实施例中，可以从信宿网关请求加密密钥。例如，用户 502 请求与用户 102 进行呼叫。POTS 网关 504 从网关控制器 106 请求加密密钥，该网关控制器服务用户 102。网关

控制器 106 然后产生加密密钥并且将它提供给 POTS 网关，以允许在 POTS 网关与 CTA104 之间产生安全通信信道。

在本发明的另一个实施例中，可以在信源网关控制器通过对信源网关控制器和信源 CTA 之间已经共享的机密派生而产生加密密钥。因此，信源网关控制器和信源 CTA 两者可以根据共享的机密派生出密钥。在实施例中，在已经发布给信宿 CTA 之后，信源网关控制器不必发送该密钥给信源 CTA。这些导致交换较少消息而在用户之间建立安全信道。

在本发明的另一个实施例中，在信源网关控制器产生的密钥可以与执法机构共享。执法行为通信协助（CALEA）要求电话系统允许政府为窃听目的接入它们网络中的谈话业务流。为帮助此目的，CALEA 服务器 510 可以包含在该网络 100 中，如图 5 所示。CALEA 服务器可以由执法部分访问，直接访问如同 512 所示，或从该网络 100 中的某些其它位置访问。

信源网关控制器可以用几个方式工作，以满足 CALEA 要求。在第一操作方法中，信源网关控制器从 CALEA 服务器接收请求 514，以传递特定用户使用的任何密钥。例如，当用户 102 请求进行呼叫并且产生密钥时，该密钥发送给 CALEA 服务器，如同 516 所示。在第二操作方法中，信源网关控制器接收请求 514，传递特定用户正在使用的任何密钥。例如，如果用户 102 已经具有利用特定密钥建立的呼叫，该密钥被传输给 CALEA 服务器，如同 516 所示。在第三操作方法中，信源网关控制器接收请求 514，传递特定用户以前使用的任何密钥。例

如，如果用户 102 以前已经利用特定密钥进行呼叫，该密钥被存储在网关控制器的密钥存储器 206。该密钥从密钥存储器中提取并且发送给 CALEA 服务器，如同 516 所示。

在实施例中，该密钥在存储前被加密。利用属于执法部分的公共/专用密钥进行加密。因此，一旦提取，任何这样加密的密钥对只能由执法人员利用已知专用密钥进行解密。

一旦该密钥在 CALEA 服务器上，消息由网络改地址到该服务器，以便由执法部分人员利用该密钥解码和监视。因此，本发明的网关控制器实施例包括对 CALEA 要求的支持。

本发明提供了在电话网络两个用户之间建立安全通信信道的一个方法和设备。本领域技术人员明白，可以对上述方法和实施例进行修改而不脱离本发明的范围。因此，所公开内容和说明书在此用于说明性目的，而不是限制，本发明的范围由下列权利要求书阐述。

说 明 书 附 图

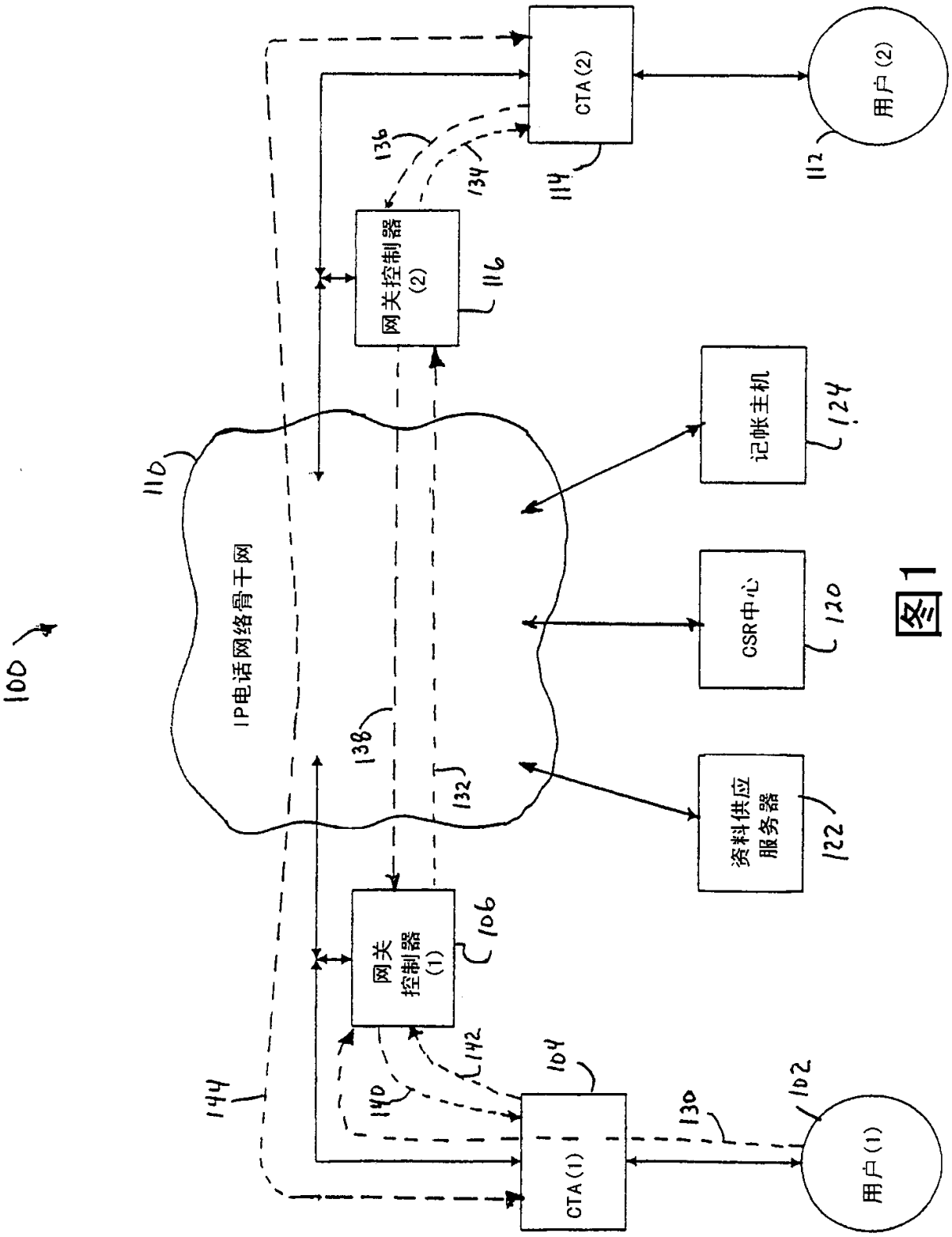

100
IP电话网络骨干网
110
网关控制器(1)
106
网关控制器(2)
116
CTA(1)
104
CTA(2)
114
用户(1)
102
用户(2)
112
资料供应服务器
122
CSR中心
120
记帐主机
124
130
132
134
136
138
140
142
144

图1

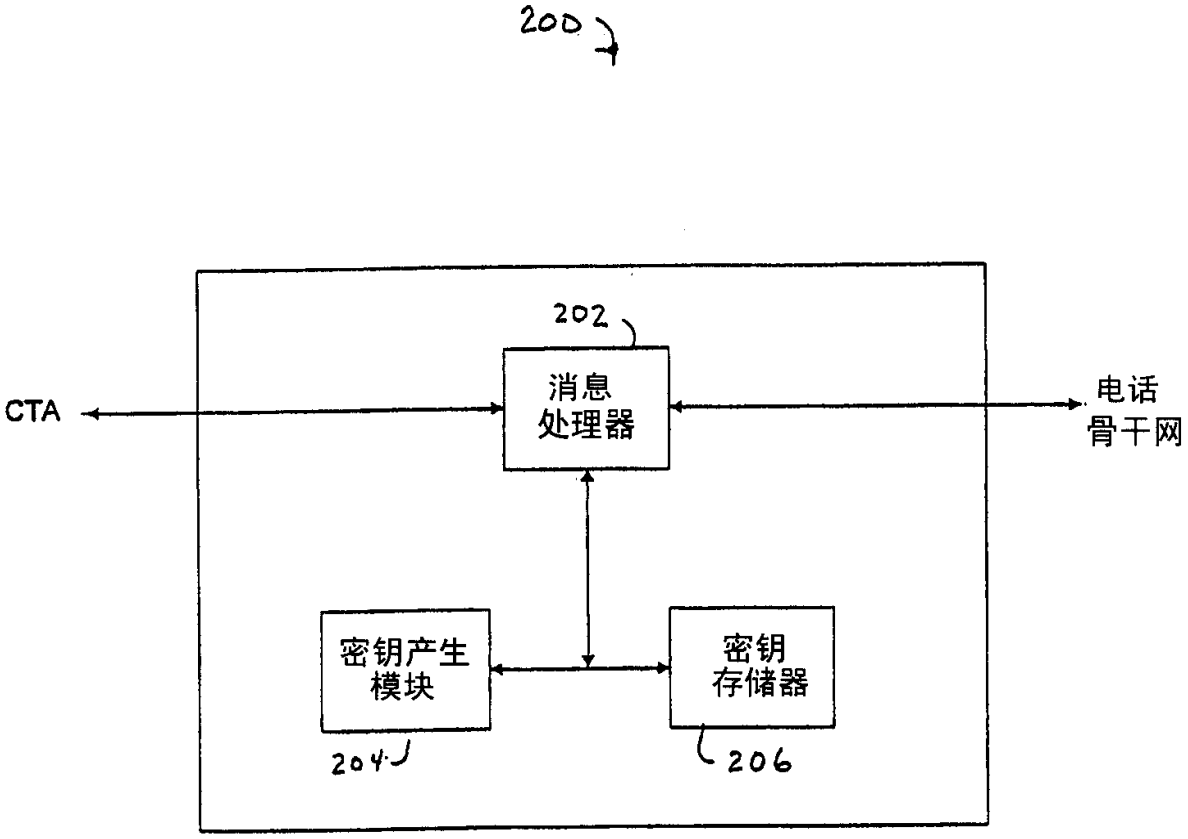


图2

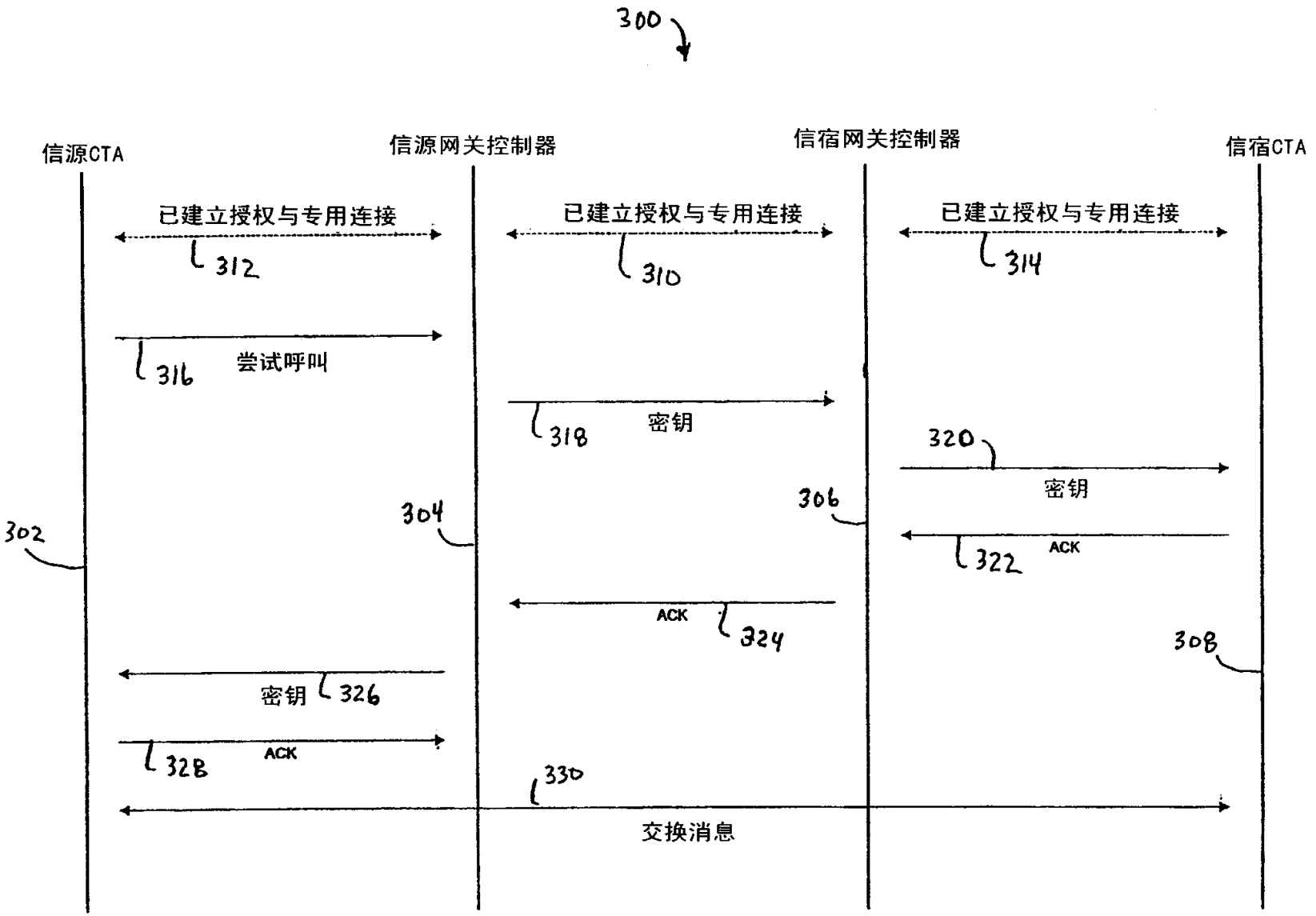
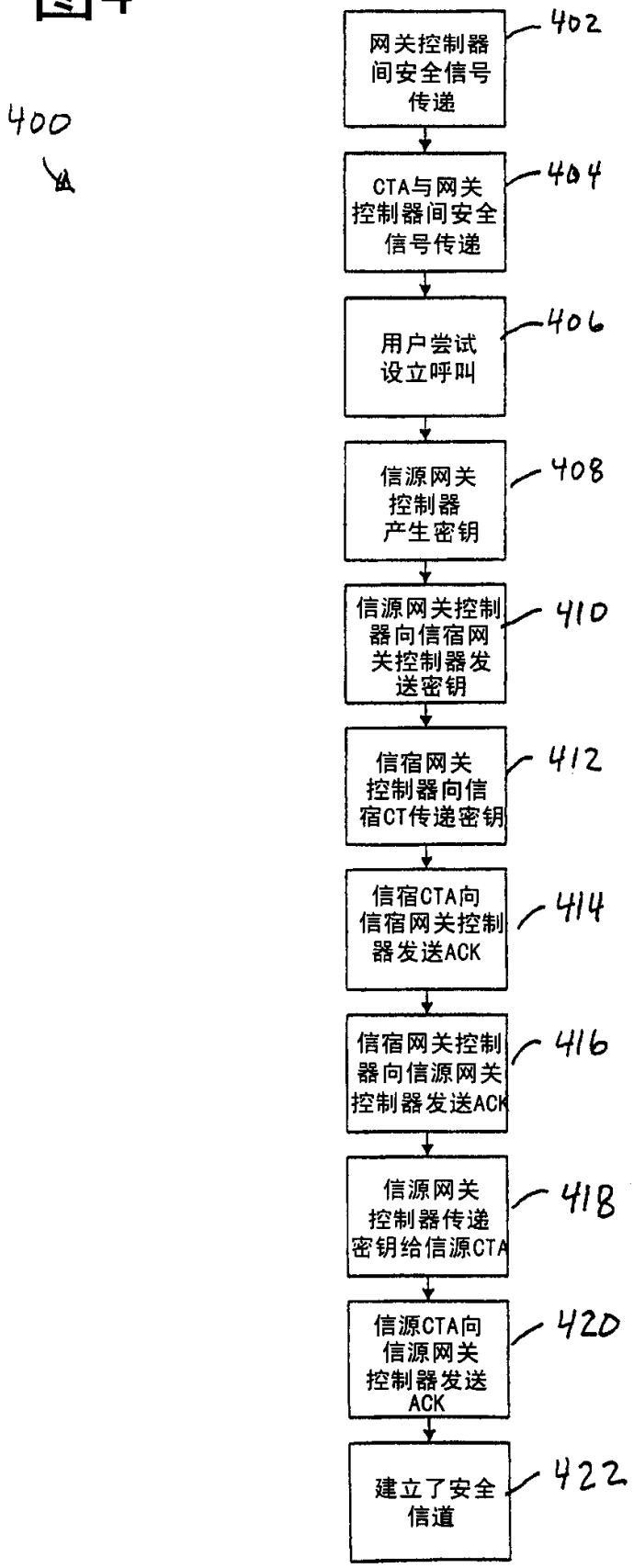

300
信源CTA
信源网关控制器
信宿网关控制器
信宿CTA
已建立授权与专用连接
312
已建立授权与专用连接
310
已建立授权与专用连接
314
316
尝试呼叫
318
密钥
320
密钥
306
304
302
ACK
322
ACK
324
308
密钥
326
328
ACK
330
交换消息

图3

图4


400
网关控制器间安全信号传递
402
CTA与网关控制器间安全信号传递
404
用户尝试设立呼叫
406
信源网关控制器产生密钥
408
信源网关控制器向信宿网关控制器发送密钥
410
信宿网关控制器向信宿CT传递密钥
412
信宿CTA向信宿网关控制器发送ACK
414
信宿网关控制器向信源网关控制器发送ACK
416
信源网关控制器传递密钥给信源CTA
418
信源CTA向信源网关控制器发送ACK
420
建立了安全信道
422

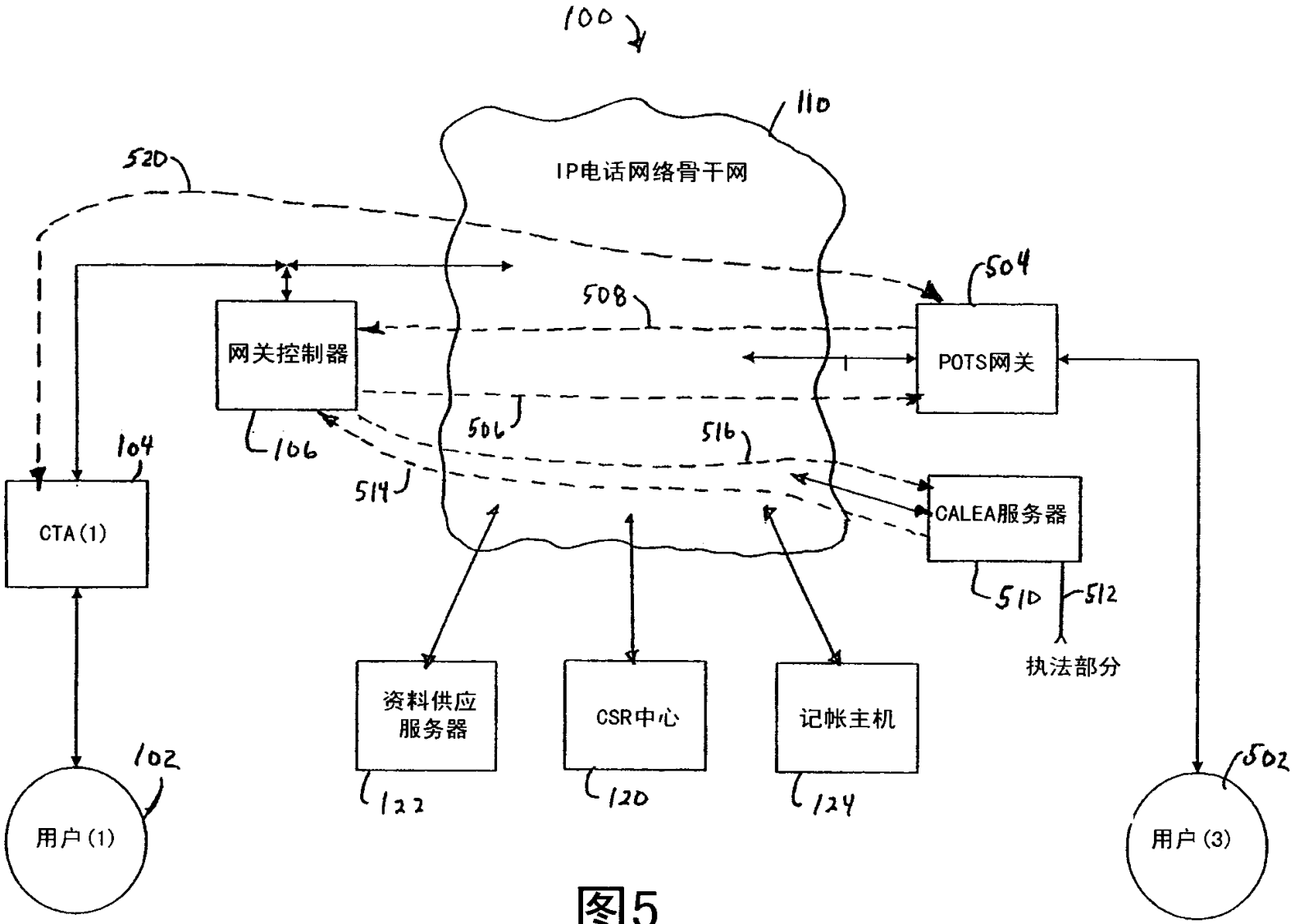

100
110
IP电话网络骨干网
520
504
508
网关控制器
POTS网关
106
506
516
514
104
CTA(1)
CALEA服务器
510
512
执法部分
资料供应
服务器
CSR中心
记帐主机
122
120
124
102
用户(1)
502
用户(3)

图5