[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
*H04L 29/06 (2006.01)*
*H04Q 7/38 (2006.01)*

[12] 发明专利说明书

专利号 ZL 01819214.9

[45] 授权公告日 2006 年 11 月 15 日

[11] 授权公告号 CN 1285202C

[22] 申请日 2001.9.21 [21] 申请号 01819214.9
[30] 优先权
[32] 2000. 9.22 [33] US [31] 09/668,426
[86] 国际申请 PCT/US2001/029654 2001.9.21
[87] 国际公布 WO2002/025899 英 2002.3.28
[85] 进入国家阶段日期 2003.5.20
[71] 专利权人 通用器材公司
地址 美国宾夕法尼亚州
[72] 发明人 S·梅德文斯基
审查员 张 鑫

[74] 专利代理机构 上海专利商标事务所有限公司
代理人 洪 玲

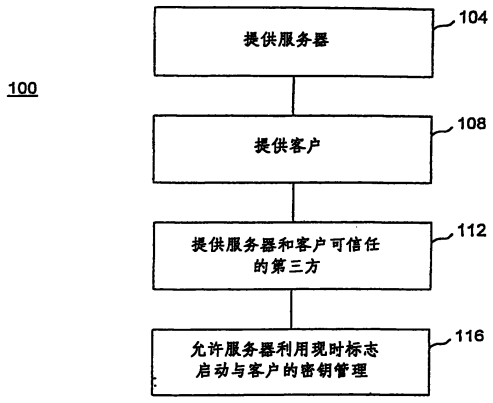
权利要求书 2 页 说明书 6 页 附图 7 页

[54] 发明名称

网际协议电话安全体系结构

[57] 摘要

提供一种系统，在该系统中，当服务器利用一条现时标志启动密钥管理会话时，客户/服务器/网络能实行该密钥管理会话。该现时标志允许将一条唤醒消息或触发消息传送给客户，这样，当服务器接收到一条带有 AP 请求消息的假的现时标志时，可以避免对服务器的服务攻击。因此，服务器可以忽略没有现时标志伴随的 AP 请求信息，该现时标志是由服务器储存的。可以通过电路，电信号和代码实现该方法，达到本方法所述的动作。



1、一种提供密钥管理的方法，其特征在于，包括：

提供一个服务器；

提供一个客户，设置成能连接到所述服务器；

提供可信任第三方，设置成能连接到所述客户；

从所述服务器启动与所述客户的密钥管理会话，其中所述启动包括：

在所述服务器产生触发消息，

在所述服务器产生现时标志，

将所述的触发消息和所述的现时标志传送给所述客户；

所述方法进一步包括：

在所述客户处接收所述触发消息和所述现时标志；

在所述客户处指定一个现时标志作为返回-现时标志；

在所述客户处产生一个第二现时标志；

针对从服务器接收到的触发消息产生一个响应消息；

传送所述响应消息、返回-现时标志和第二现时标志；

将所述返回-现时标志值与服务器处产生的现时标志的值进行比较，以验证消息是否来自所述客户，而不需要使用所述可信第三方。

2、如权利要求 1 中所述的方法，其特征在于，还包括：

为所述现时标志预先确定一个带外值以防止攻击者冒充一个启动密钥管理会话的客户；

检查所述现时标志以确定所述现时标志的值是不是所述带外值。

3、如权利要求 1 中所述的方法，其特征在于，还包括：

在所述服务器确认所述返回_现时标志值；并

将来自所述客户的答复消息传送给所述服务器。

4、如权利要求 1 中所述的方法，其特征在于，还包括：

在所述服务器上，从所述客户接收一条响应消息和一条假的_现时标志；

确定所述假_现时标志是假的；

忽略所述客户响应信息。

5、如权利要求 3 中所述的方法，其特征在于，所述方法基于 Kerberos 的系统，且所述可信第三方是

密钥分配中心，设置成能充当所述客户和所述服务器的可信任第三方。

6、为 IP 电话网络中的有线电话适配器 CTA 和信号传输控制器启动密钥管理会话的一种方法，其特征在于，该方法包括：

提供所述信号传输控制器；

提供所述 CTA，设置成能连接到所述信号传输控制器；

提供密钥分配中心 KDC；

在所述信号传输控制器产生一条触发消息；

在所述信号传输控制器产生一条现时标志；

将所述现时标志连接到所述触发消息；

将与所述触发消息连接的所述现时标志传送给所述 CTA；

给所述触发消息产生一条响应消息；

将所述现时标志值用作为返回_现时标志值；

将所述响应消息连接到所述返回_现时标志；

将所述返回_现时标志与所述响应消息传送给所述信号传输控制器；

比较所述返回_现时标志和所述现时标志；

传送一条 AP 答复信息，以回答所述响应消息；

将一条 SA 恢复消息传送给所述信号传输控制器。

7、一种将来自服务器的密钥传送给客户的方法，其特征在于，包括：

在所述服务器产生一条唤醒消息，而不需要使用可信任第三方；

在所述服务器产生一条服务器_现时标志，其中所述服务器_现时标志是仅能使用一次的随机数；

将所述唤醒消息和所述现时标志传送给所述客户；

在所述客户产生一条 AP 请求消息；

将一条客户_现时标志和所述 AP 请求信息传送给所述服务器；

确认与所述 AP 请求消息一起传送的所述客户_现时标志与在所述服务器产生的所述服务器_现时标志匹配。

# 网际协议电话安全体系结构

本申请要求从共同待批的 PCT 申请号 PCT/US00/09318 的优先权，该专利申请日期为 2000 年 4 月 7 号，标题为“提供设备和服务证明的有线电话适配器的内置厂商证明书”，该专利申请要求从美国申请号 60/128,772，标题为“网际协议电话安全体系结构”，申请日期为 1999 年 4 月 9 号，以及 PCT 申请号 PCT/US00/02174，申请日期为 2000 年 1 月 28 号，标题为“用于保护 CTA 之间的信号传输和呼叫信息包的电话呼叫的密钥管理”中获得优先权，因此，对于有关披露以及各种目的所有资料，都并入一起作参考。

## 技术领域

本发明一般涉及网络安全，特别是涉及用于提供例如在电话或 IP 电话网络内中服务器和客户之间密钥管理的系统。

## 背景技术

在基于客户/服务器结构的网络中，在服务器和客户之间有必要建立一个安全通道。另外，在利用第三方证明信任关系的网络中，有必要提供一个有效机制，允许服务器发送（initiate）密钥管理信息。在利用对服务器和客户来说可信任的第三方的这样的网络中，客户通常可以从可信任的第三方请求加密身份验证令牌，可用于启动对一个特定服务器的密钥管理，然而，服务器通常可直接启动与客户的密钥管理会话（session）。欠佳地，服务器从可信任的第三方获得每个客户的加密身份验证令牌。这种途径会增加服务器的开销，要求服务器为每个客户维持密码状态。如果这样一台服务器失败了，就需要一台备用服务器进行恢复处理，在此处理中新的服务器必须获得每个客户的新身份验证令牌。在预备阶段，需要初始化客户，以允许他们可以成功地鉴别可信任的第三方，并获得加密身份验证令牌。在 PCT 申请号 PCT/US00/09318 中披露了一种客户初始化的建议方法，该专利申请的标题为“提供设备和服务证明的有线电话适配器的内置厂商证明书”。不过，有必要提供一个有效机构，通过这个机构，服务器能启动与客户的密钥管理会话，这与只有客户可以启动这种

会话的一种系统成对比。

这样的客户/服务器网络的例子是在 IP 电话中存在的客户/服务器网络。在 IP 电话系统中，有线电话适配器（CTA）设备可以用于允许用户在 IP 电话网络上发送和接收安全事务处理的信息。在典型操作中，在与另一个用户建立一条安全通道之前，用 IP 电话网络交换记录有 CTA 设备的一系列信号传输信息。因此，CTA 设备需要由 IP 电话系统验证。否则，因为某些提供的交换可以伪造，处理过程会对拒绝服务攻击开放。另外，希望服务提供者鉴别 CTA 设备，以确认在 IP 电话系统中只允许有授权的设备。

## 发明内容

本发明的一个实施例包括在客户/服务器网络中提供密钥管理的一种系统。本发明实施例通过提供一个服务器；提供一个客户，该客户配置成能连接到该服务器；提供可信任的第三方，该第三方配置成能连接到客户；从所述服务器启动与所述客户的密钥管理会话，其中所述启动包括：在所述服务器产生触发消息，在所述服务器产生现时标志，将所述的触发消息和所述的现时标志传送给所述客户；所述方法进一步包括：在所述客户处接收所述触发消息和所述现时标志；在所述客户处指定一个现时标志作为返回-现时标志；在所述客户处产生一个第二现时标志；针对从服务器接收到的触发消息产生一个响应消息；传送所述响应消息、返回-现时标志和第二现时标志；将所述返回-现时标志值与服务器处产生的现时标志的值进行比较，以验证消息是否来自所述客户，而不需要使用所述可信第三方。

一个实施例按一种方法进行工作，该方法能在服务器上产生触发信息；在服务器上产生现时标志；以及将这个触发信息和现时标志传送给客户。在客户上，客户接收触发信息和现时标志，而且通过传送带有返回_现时标志的一条响应信息作为响应。接着，通过比较返回_现时标志值和由服务器产生的现时标志值，服务器可确定响应信息是否有效。

另外，可以用代码和能产生该方法动作的电路实现一个实施例。

通过参考本说明书的剩余部分和附图，可以更加理解这里披露的本发明的特性。

## 附图说明

图 1 显示一张流程图，示范了本发明实施例的概况。

图 2A 和 2B 显示更详细的流程图，示范了服务器和客户之间密钥管理会话。

图 3 显示了启动密钥管理会话后的密钥管理会话的步骤。

图 4 显示一张客户/服务器/可信任第三方网络的一张概括方框图。

图 5 显示一张 IP 电话网络的方框图，在这个网络中，有线电话适配器，信号传输控制器和密钥分配中心互相连接。

图 6 显示用于建立密钥管理会话的数据结构的实施，如本发明的一个实施例所实现的。

**具体实施方式**

图 1 显示一张流程图，示范了本发明实施例的概况。在流程图 100，在 104，提供服务器，并在 108，提供与服务器连接的客户。在 112，为服务器和客户提供可信任的第三方，然后在 116，允许服务器利用一条现时标志启动与客户的密钥管理会话。

必须理解：服务器是网络上一台共享的计算机，例如用在 IP 电话网中的信号传输控制器。此外，还必须理解：客户是由另一台网络计算设备服务的一台计算机或设备，例如由信号传输控制器（服务器）经 IP 电话系统服务的有线电话适配器（客户）。另外，必须理解：服务器和客户的可信任第三方是一台设备或计算机，该设备或计算机可由至少两个实体使用，有利于加密处理，例如证明两个实体相互之间的身份。最后，必须理解：所产生的现时标志是仅能使用一次的一个数字。使用现时标志能有助于防止攻击者实行重复攻击。这种现时标志可以随机产生。

参考图 2A 和图 2B 可以更好地理解图 1 的方法。在图 2A 和图 2B 设计的方法 200 中，在 204，提供一个服务器，例如在 IP 电话系统中的信号传输控制器。另外在 208，提供一个客户，例如在 IP 电话系统中的有线电话适配器。同样在 212，提供客户和服务器的可信任第三方，例如在 IP 电话系统中的密钥分配中心。服务器、客户和可信任第三方互相连接。通常，客户启动与服务器的密钥管理会话，然而，有时候，服务器需要启动与客户的密钥管理会话。本发明能够利用现时标志检验来自客户的随后的 AP 请求消息，而不是验证触发信息（例如用数字签名和证书）。本发明的这个实施例不能防止对手（冒充一台合法服务器）给客户发送非法触发信息，以及哄骗该客户以 AP 请求信息响应。取而

代之，它（本发明实施例）提供：通过合法服务器拒绝这样一条 AP 请求信息。这个机构设计成能减少服务器与其客户交流的启动密钥管理的总开销，与此同时仍然保持足够的安全。因而在 216，服务器产生一条触发消息以启动密钥管理会话。然后在 220，服务器产生现时标志，并在 224，这个现时标志与触发消息耦合在一起，并传送给客户。在 228，客户接收触发消息和现时标志。然后在 232，客户将该现时标志指定为返回_现时标志。这样，客户可以把接收到的现时标志返回给服务器以确认该信息来自客户。在 236，客户产生第二个现时标志。该第二个现时标志由服务器和客户使用，作为启动密钥管理会话的一部分。在 240，客户对从服务器接收到的触发消息产生一条响应消息。然后在 244，将该响应消息、返回_现时标志和第二条现时标志传送给服务器。

在服务器上，将返回_现时标志的值和由服务器产生的现时标志的值进行比较。如果返回_现时标志值和保存在服务器中的现时标志的值相等，则密钥管理会话可以继续进行。但是，如果返回_现时标志值不等于保存在服务器中的现时标志值，那么在 252，就确定这条返回_现时标志实际上是错误的现时标志。在这种情况，很可能是信号被破坏了，或者可能是攻击者试图进行服务攻击。在服务攻击中，攻击者试图欺骗性地启动一个重复的密钥会话以使服务器利用处理器周期，从而妨碍处理器利用那些周期进行其他操作。因此在这种攻击下，服务器会变得不如在正常情况下那样有效。通过重复这种攻击，攻击者能够妨碍服务器有效地操作，从而能够威胁到例如 IP 电话网络这样的客户服务器网络的操作安全。如果返回_现时标志确实是与保存在服务器中的现时标志值不相等，那么在 256，认为和该返回_现时标志一起发送的响应消息是不可靠的。然而，如果返回_现时标志与保存在服务器中的现时标志值相等，那么在 260，密钥管理会话继续进行。

图 3 显示了如图 2B 中的模块 260 所强调的一个典型的密钥管理会话的附加步骤。在图 3 中，方法 300 显示：在 364，服务器产生一个申请（AP）答复信息。在 368，将该 AP 答复信息与客户产生的第二个现时标志一起传送给客户。AP 请求是申请请求的缩写，AP 答复表示申请答复信息。例如，Kerberos 密钥管理标准中规定了这两种信息（请查阅 IETF RFC 1510）。作为又一个例子，在 Kerberos 的上下文中，第二个现时标志可以是以微秒表示的客户时间。在 372，当客户接收到 AP 答复信息和第二个现时标志时，就将一个安全关联（SA）恢复消息传送给服务器。就完成了可用的 Kerberos 密钥管理会话。

图4显示了客户/服务器/可信任第三方网络的框图。客户401与服务器402连接。另外，客户与可信任的第三方404连接。可信任的第三方还和服务器402连接。因此图4示范了可实现本发明一个实施例的网络。

图5中，示范了实现本发明的一个实施例的IP电话网络。例如有线电话适配器501的客户，与例如信号传输控制器502的服务器连接。此外，有线电话适配器和信号传输控制器还与可信任的第三方连接，该第三方描述为密钥分配中心504。而且，信号传输控制器也与IP电话网络508连接。图5中描述的网络有利于建立从一个用户到另一个用户的IP电话呼叫。前一个用户通过IP电话网络508连接到有线电话适配器，后一个用户连接到相似网络。因此，在IP电话网络中发生呼叫时，可以通过有线电话适配器和信号控制器将该用户鉴定为呼叫方。这种网络的更详细内容在并入作参考的参考资料中作了说明。

图6描述了用于实行Kerberos密钥管理会话的数据结构，该密钥管理会话是由客户/服务器网络中的服务器启动。在图6中，现时标志号1与一个例如触发或唤醒消息的初始信号连接，并将该混合信号通过接口601传送给客户。客户保存现时标志号1。接着，在数据结构中添加现时标志号2和申请请求信息，例如图6所示。然后，这组数据跨过接口送回给服务器。服务器把所接收的现时标志号1的值和保存在服务器中的现时标志号1的值进行比较，以确定AP请求信息的真实性。依据AP请求信息的鉴别，服务器产生一条AP答复信息并将它与客户所产生的现时标志号2连接。然后，将混合的现时标志号2和AP答复信息跨过接口传送给客户。客户可通过比较从服务器接收到的现时标志号2的值和保存在客户中的现时标志号2的值，来检验AP答复信息的真实性。依据AP答复信息的鉴别，客户产生一条安全关联（SA）恢复消息，并跨过接口传送给服务器。因此，该基于Kerberos的密钥管理协议是按一种有效的方式实行的，此外，还允许服务器仅利用一条附加的现时标志作为初始消息的总开销，启动密钥管理会话。因此，这种方法是很有效的，在这种方法中，仅需一条现时标志用于初始信息的鉴别处理过程中。

除了用硬件实行本发明的那些实施例之外，应当注意：这些实施例可以通过使用制成品来实现，包括在其上记录有计算机可读程序代码的计算机可读媒体，这使本说明书披露的硬件功能及/或结构成为可行的。例如，这可以通过使用硬件描述语言（HDL），寄存器传送语言（RTL），VERILOG,VHDL，或类似的编程工具来实现，这些技术都为本领域技术人员所熟知。由J.Bhasker和Star

Galaxy Pr.在1997年写的《Verilog HDL入门》一书中提供Verilog和HDL的很多详情，并因此并入所披露的各种目的所有内容作参考。因此可以想象，如上述的本发明实现的功能可以按某一核心表示，该核心可以按程序代码实现，并可转换到硬件，作为集成电路产品的一部分。因此，希望上述的在其程序代码方法中的实施例也被考虑受本专利保护。

应当注意，本发明的实施例可用电信号将相关的信号传送给接收机来实现，该电信号例如为载波中的计算机数据信号。因此，在将数据描述为储存在计算机媒体上的地方，也可理解为可像电信号一样进行传送。同样地，也应该认为：在描述消息的数据结构的地方，可以用跨媒体（例如因特网）传送的电信号来实现。

也应注意，这里所述的许多结构和动作可以被分别叙述成用于执行一种功能的方法或用于执行一种功能的步骤。因此，应该了解这种语言是要覆盖所有在本说明书或类似的说明中披露的结构或动作，包括并入作参考的内容。

应该认为：从本说明可了解本发明实施例的设备和方法和许多附带优点，并且应该明白：其中部件的格式、结构和排列上可以作许有多种不同改变，并没有脱离本发明宗旨和范围或者牺牲所有实质的优势，这儿描述前的格式仅仅是示范性实施例。

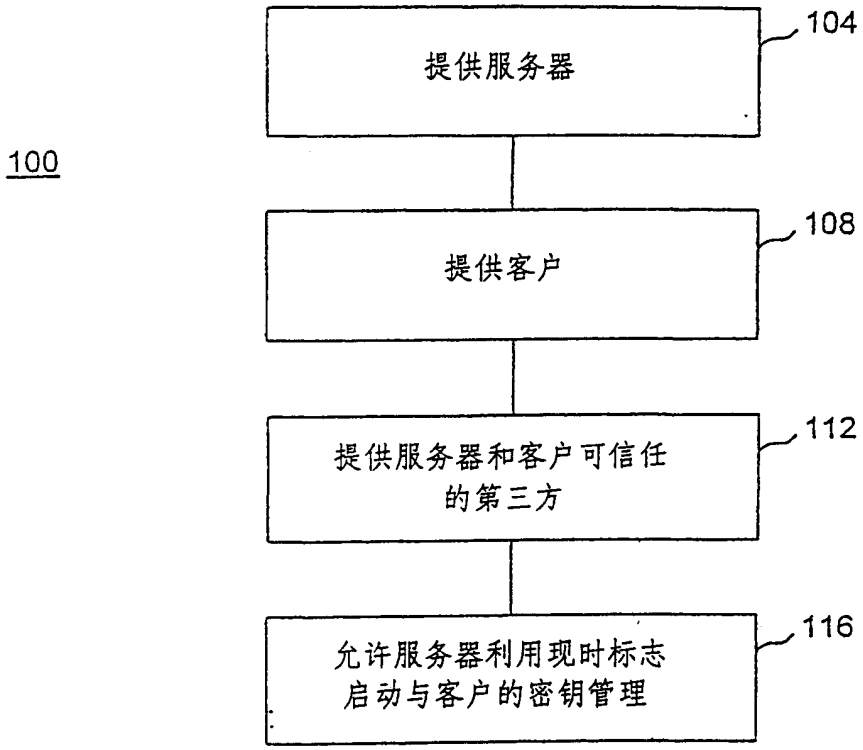

100
提供服务器
104
提供客户
108
提供服务器和客户可信任的第三方
112
允许服务器利用现时标志启动与客户的密钥管理
116

图 1

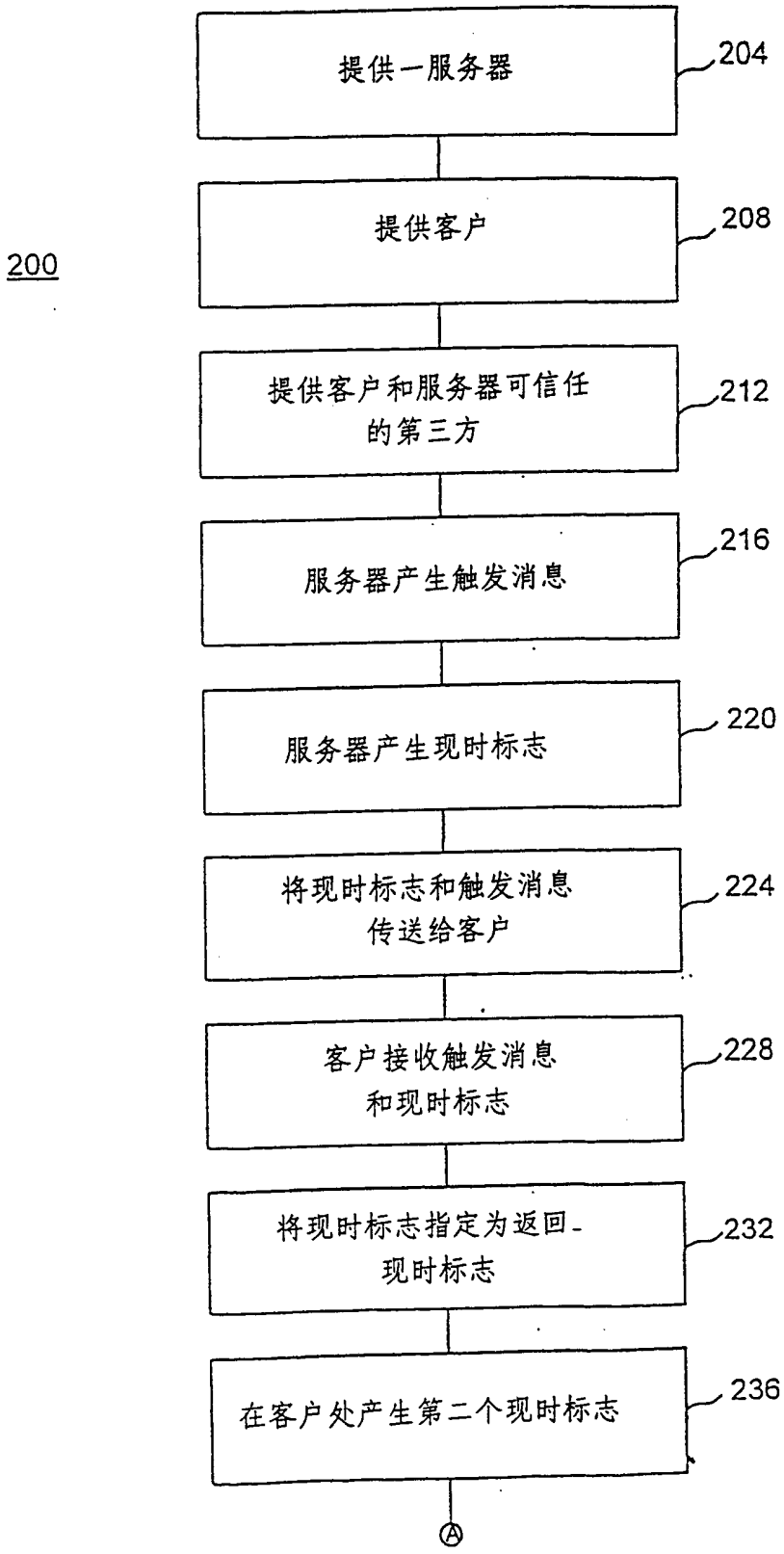

200
提供一服务器
204
提供客户
208
提供客户和服务器可信任的第三方
212
服务器产生触发消息
216
服务器产生现时标志
220
将现时标志和触发消息传送给客户
224
客户接收触发消息和现时标志
228
将现时标志指定为返回-现时标志
232
在客户处产生第二个现时标志
236
A

图 2a

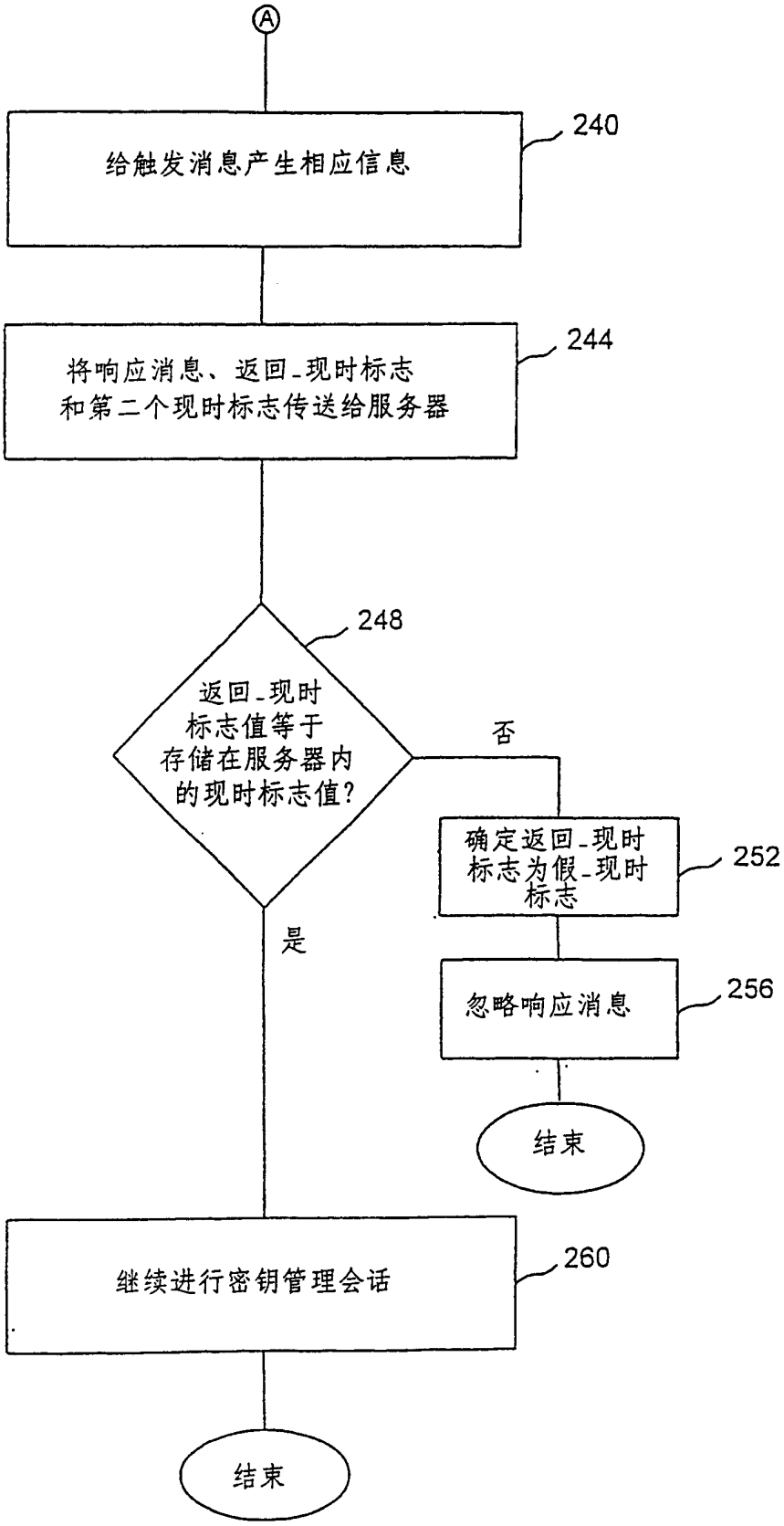

A
给触发消息产生相应信息
240
将响应消息、返回_现时标志
和第二个现时标志传送给服务器
244
248
返回_现时
标志值等于
存储在服务器内
的现时标志值?
否
是
确定返回_现时
标志为假_现时
标志
252
忽略响应消息
256
结束
继续进行密钥管理会话
260
结束

图 2b

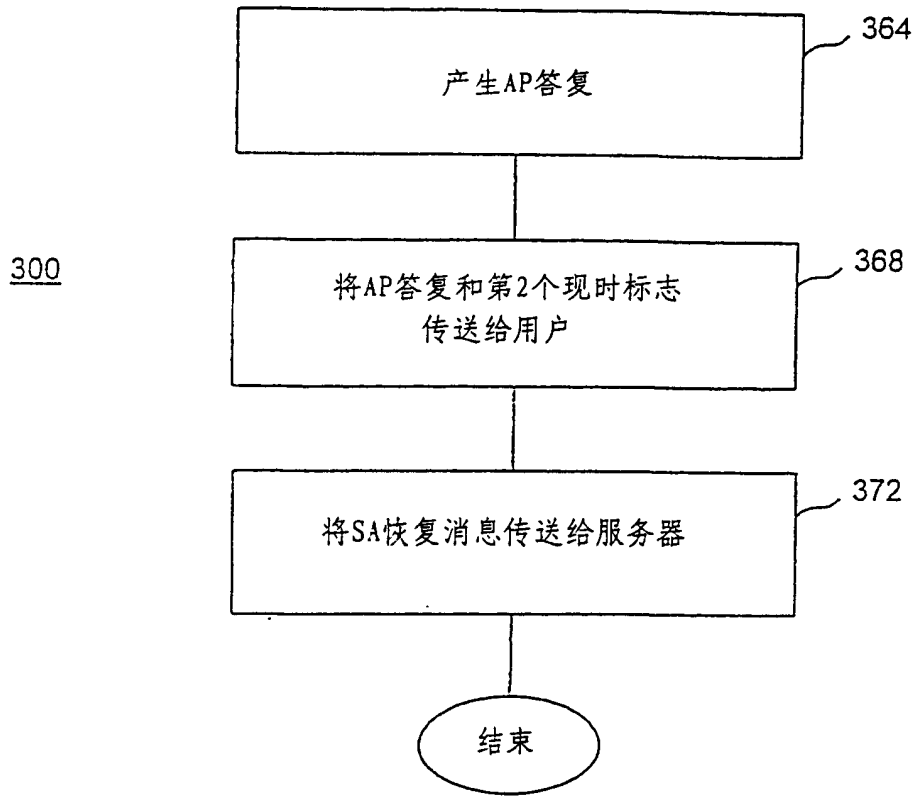

300
产生AP答复
364
将AP答复和第2个现时标志
传送给用户
368
将SA恢复消息传送给服务器
372
结束

图 3

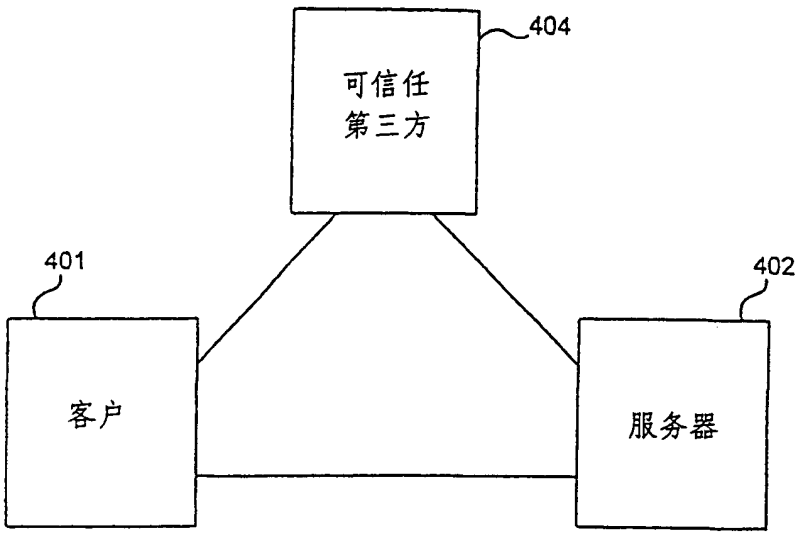



图 4

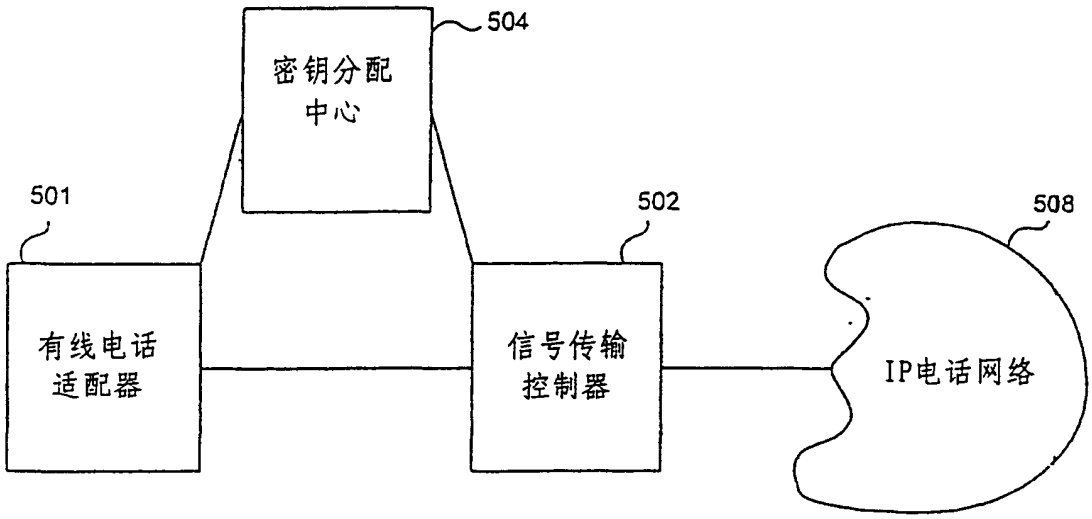



图 5

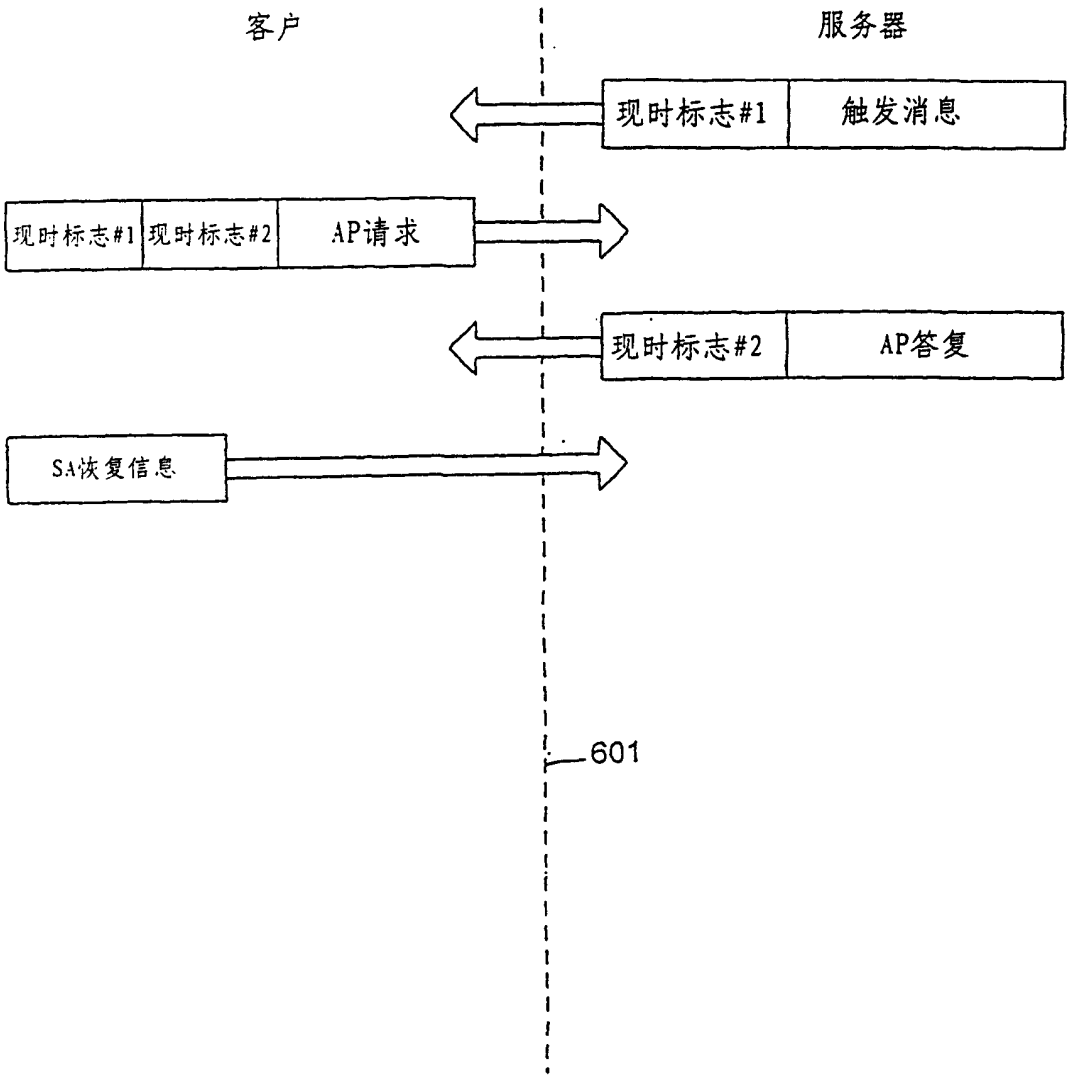



图 6