(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1677978 B
(45)授权公告日 2010.11.03

(21)申请号 200510063753.8
(22)申请日 2005.03.31
(30)优先权数据
10/815,232 2004.03.31 US
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 J·T·布赫 苏锦彦 S·纳拉亚南 V·埃德尔曼
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 潘明婤
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
EP 1267548 A2,2002.06.12, 全文.
CN 1423201 A,2003.06.11, 全文.
WO 02/21796 A1,2002.03.14, 全文.
US 2003/0217165 A1,2003.11.20, 说明书第[0023]-[0028]段，第[0034]-[0037]段，第[0041]-[0043]段.
审查员 郑昊

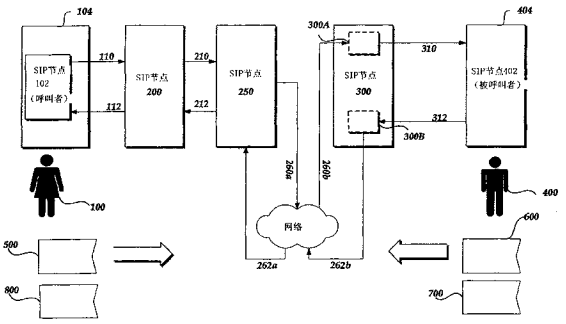
权利要求书 2 页 说明书 21 页 附图 13 页

(54)发明名称

会话启动协议路由标题的签署和确认

(57)摘要

揭示了用于签署和确认会话启动协议(“SIP”)路由标题的方法、具有计算机可执行指令的计算机可读介质、以及具有存储在其中的数据结构的计算机可读出介质。SIP节点可以接收包括消息标题的SIP请求。可以基于至少一部分消息标题和SIP节点标题条目生成签名。然后可以把签名插入到SIP节点标题条目中。



CN 1677978 B

1. 一种处理会话启动协议 SIP 消息的方法，所述方法包括：

在 SIP 节点处接收 SIP 请求，所述 SIP 请求包括消息标题；

确定 SIP 请求的 RECORD-ROUTE 标题；

基于至少一部分消息标题生成签名，其中所述消息标题的部分包括表示网络路由位置的数据；

生成 SIP 节点标题条目；以及

把签名插入到 SIP 节点标题条目中；

其中生成签名包括基于 SIP 请求的至少一部分 RECORD-ROUTE 标题生成签名；且

其中插入签名包括把签名插入到 SIP 节点的 RECORD-ROUTE 标题中。

2. 如权利要求 1 所述的方法，其特征在于，所述 SIP 节点标题条目是返回的标题。

3. 一种处理会话启动协议 SIP 消息的方法，所述方法包括：

在 SIP 节点处接收 SIP 请求，所述 SIP 请求包括消息标题；

基于至少一部分消息标题生成签名；

生成 SIP 节点标题条目，其中 SIP 节点标题条目是 VIA 标题；

把签名插入到 SIP 节点标题条目中；

作为对 SIP 请求的答复，在 SIP 节点处接收 SIP 响应，所述 SIP 响应包括 SIP 节点的 VIA 标题，所述 VIA 标题包括第一接收签名；

验证第一接收签名；

确定到下一 SIP 节点的下一链路，以接收 SIP 请求；以及

判定到下一 SIP 节点的下一链路是否为不可信链路，其中，生成第一签名包括如果下一链路是不可信链路，则只生成第一签名。

4. 一种处理会话启动协议 SIP 消息的方法，所述方法包括：

在 SIP 节点处接收 SIP 请求，所述 SIP 请求包括消息标题；

基于至少一部分消息标题生成签名；

生成 SIP 节点标题条目；

把签名插入到 SIP 节点标题条目中；

作为对 SIP 请求的答复，接收 SIP 响应，所述 SIP 响应包括响应标题；

基于响应标题的 RECORD-ROUTE 标题和 CONTACT 标题生成另一签名；

把另一签名插入到响应的 SIP 节点的 RECORD-ROUTE 标题中；以及

在生成另一签名之前，从 SIP 节点标题条目中移除现有的签名。

5. 如权利要求 1 所述的方法，其特征在于，所述插入签名包括插入签名作为 SIP 节点的 RECORD-ROUTE 标题的标题参数。

6. 如权利要求 1 所述的方法，其特征在于，还包括：

作为对 SIP 请求的答复，在 SIP 节点处接收 SIP 响应，所述 SIP 响应包括包含接收的签名的 SIP 节点的 RECORD-ROUTE 标题；以及

验证所述接收的签名。

7. 如权利要求 1 所述的方法，其特征在于，还包括：

确定到下一 SIP 节点的下一链路，以接收 SIP 请求；以及

判定到下一 SIP 节点的下一链路是否为不可信链路，其中，所述生成签名包括如果下

一链路是不可信链路，则只生成所述签名。

会话启动协议路由标题的签署和确认

技术领域

[0001] 本申请针对用于通过计算机网络在设备之间传递的方法和计算机可读介质，尤其涉及用于签署和确认会话启动协议（“SIP”）路由标题以认证包含在SIP消息中的路由命令的方法和计算机可读介质。

背景技术

[0002] 会话启动协议（“SIP”）是用于建立、管理和终止通信会话的因特网信令协议，所述通信会话包括即时消息通信、因特网电话呼叫以及因特网视频会议。通过引用结合于此的因特网工程任务强制征求意见(Internet Engineering Task Force Request for Comments)2543和征求意见3261的每一个中都规定了SIP。SIP会话涉及一个或多个参与者或客户机（一般是呼叫者和被呼叫者）。通过SIP节点（一般为各种服务器）的网络，在每个端点SIP节点（例如，呼叫者和被呼叫者）之间路由SIP消息。

[0003] 一般有两类SIP消息：从呼叫者（例如，端点SIP节点）发送给被呼叫者的请求，以及从被呼叫者发送给呼叫者以答复请求的响应。在某些情况中，在启动对话会话之后，被呼叫者也可以把请求发送给呼叫者。每个SIP消息，不管是响应还是请求，一般都包括三个部分：起始行、标题和正文。起始行传送消息类型（例如，请求或响应）以及协议版本，而消息正文包括消息内容，并且可以传送起始行中信令信息之外的会话描述信息。SIP标题字段传送消息的属性并修改消息的意义。存储在标题字段中的某些消息属性是如何路由消息以及用文件证明消息实际行进的路由的指令。例如，管理其路由上的请求的每个SIP节点将添加包含标识该SIP节点的信息的“VIA”标题，诸如一个完全合格的域名或因特网协议地址。如此，可以检测路由中的循环，并且响应使用来自请求的VIA标题来确定要行进的路由以返回给呼叫者。然而，消息的特定路径在时间上可能不是固定的，因此，诸如归属服务器(home server)之类的SIP节点可以接收诸如电话呼叫之类的对话的第一请求，但是可能不接收同一对话中的后续请求。为了保留在该对话的“循环”中，SIP节点可以插入包含标识其自身的信息的RECORD-ROUTE标题，诸如统一资源指示符（“URI”）或允许其它服务器或端点到达SIP节点的其它地址。然后接收端客户机（对于请求为被呼叫者，对响应为呼叫者）把RECORD-ROUTE标题的完整列表中的一部分拷贝成一组ROUTE标题。ROUTE SET标题包含某些数据，这些数据向SIP节点提供关于在同一对话会话中如何路由任何未来请求的指令。

发明内容

[0004] 虽然上述SIP标题字段有助于在诸如沿消息的路由的服务器等SIP节点间来回路由消息，但是当根据SIP标准(RFC3261)使用时，这些标题中的许多是不安全的。例如，在服务器处可以用在SIP标题中包括假冒路由信息的多个伪造的SIP消息来引导服务拒绝攻击。可以通过伪造的标题信息来屏蔽假冒消息的真实始发者，可能使之看来正在无知的服务器处始发服务拒绝攻击。此外，伪造的路由标题可以在两个服务器之间创建循环消息。如

此，沿假冒消息的伪造“路由”的每个服务器可能浪费宝贵的资源来处理和转发假冒消息，因此，拒绝把这些资源给合法的用户。

[0005] 本发明的实施例针对用于认证在 SIP 消息中找到的路由标题的方法和计算机可读出介质。具体地，SIP 节点可以接收包括消息标题的 SIP 请求。基于至少一部分消息标题可以生成签名，并插入到 SIP 节点标题条目。如这里所使用的，SIP 节点是指运行在可以作为 SIP 客户机或服务器操作的计算设备上的 SIP 应用程序。

[0006] 例如，可以基于在所接收请求标题中的至少一部分 VIA 标题生成第一签名，并且插入到 SIP 节点的 VIA 标题中。当生成对 SIP 请求的响应时，根据 SIP 标准处理，在响应标题中返回 SIP 节点的 VIA 标题。当 SIP 节点接收响应时，SIP 节点可以验证响应的 SIP 节点 VIA 标题中的第一签名，以认证响应行进的实际路径的完整性。

[0007] 此外或另一方面，可以基于消息标题的至少一部分 RECORD-ROUTE（记录 - 路由）标题和 CONTACT（联系人）标题生成第二签名。可以把第二签名插入到 SIP 节点的 RECORD-ROUTE 标题中。然后被呼叫者系统可以保存附带有第二签名的这个 RECORD-ROUTE 标题的一部分作为 ROUTE 标题来使用，用于在启动会话之后路由和验证被呼叫者系统对呼叫者系统生成的请求。

[0008] 此外或另一方面，可以基于消息标题的至少一部分 RECORD-ROUTE 标题生成第三签名。可以把第三签名插入到 SIP 节点的 RECORD-ROUTE 标题中。当被呼叫者响应 SIP 请求时，在响应标题中返回 SIP 节点的 RECORD-ROUTE 标题。为了验证关于如何路由未来请求的指令的完整性，当 SIP 节点接收到响应时，可以由 SIP 节点来验证第三签名。例如，接收响应的 SIP 节点可以识别包含从请求标题返回的数据的 RECORD-ROUTE 标题，并且从返回的标题中提取签名。SIP 节点可以使用与生成第三签名的过程相同的过程来生成验证签名，例如，基于响应标题中的至少一部分标题生成签名。然后 SIP 节点可以比较验证签名和所提取的签名。如果两个签名是匹配的，则可以正常地处理消息。

[0009] 可以生成第四签名并插入到 SIP 响应标题中。例如，接收响应的 SIP 节点可以基于响应标题的至少一部分 RECORD-ROUTE 标题以及响应标题的 CONTACT 标题生成第四签名。第四签名与上述第二签名相似，然而，由于第四签名是基于响应中的 CONTACT 标题生成的，所以正如请求的情况一样，CONTACT 识别被呼叫者而不是呼叫者。然后可以把第四签名插入到 SIP 节点的 RECORD-ROUTE 标题中。当呼叫者系统接收到响应时，它就可以保存附带有签名的一部分 RECORD-ROUTE 标题作为 ROUTE SET 标题，用于在后续请求中路由指令的使用和验证。

[0010] 在某些情况中，可以通过至少具有第一服务器和第二服务器（可以互换地使用它们来处理同一对话中的消息）的服务器池来提供处理 SIP 消息的 SIP 节点。然而，当交换消息时，对话中的请求可以包含由第一服务器生成，但是可以发送到第二服务器用于处理的签名。这要求第二服务器具有用于验证请求中的签名的会话密钥。为了安全地传送用于生成请求中的签名的会话密钥，生成签名的第一服务器可以把经加密的和经签署的会话密钥附到消息的标题中。例如，可以把会话密钥插入到包括由该密钥生成的签名的同一标题中。为了保护来自其它 SIP 节点的会话密钥，第一服务器可以用服务器池可访问的公钥对会话密钥进行加密。然后第一服务器可以用服务器池可访问的私钥来签署经加密的密钥。接收请求的第二服务器可以验证经加密密钥上的签名，然后对会话密钥进行解密。然后第二服

务器可以基于至少一部分消息标题使用经解密的会话密钥来验证签名。可以理解，可以使用任何合适的安全处理来保护会话密钥，包括例如，包括公钥 / 私钥对的非对称密钥技术。

附图说明

[0011] 在参考下列详细描述的说明书和附图而较好地理解本发明时，可以更容易地理解本发明的上述各方面和伴随的许多优点。

[0012] 图 1 是根据本发明的一个实施例，两个会话启动协议（“SIP”）客户机之间的 INVITE（邀请）请求和响应路由的示意图；

[0013] 图 2 是根据图 1 的示例 INVITE 请求；

[0014] 图 3 是根据图 1 的示例 VIA 标题组；

[0015] 图 4 是根据图 1 的示例 RECORD-ROUTE 标题组；

[0016] 图 5 是对于图 2 的 INVITE 请求的示例响应；

[0017] 图 6 是图 1 的被呼叫者 SIP 节点生成的示例请求；

[0018] 图 7 是图 1 的被呼叫者 SIP 节点生成的示例请求；

[0019] 图 8 是根据本发明一个实施例的示例 SIP 服务器的图示；

[0020] 图 9 是根据本发明一个实施例，来自密钥信息数据库的示例表格的图示；

[0021] 图 10 是根据本发明一个实施例的流程图，描述如何生成 VIA 签名；

[0022] 图 11 是根据本发明一个实施例的流程图，描述如何验证 VIA 标题；

[0023] 图 12 是根据本发明一个实施例的流程图，描述如何生成 ROUTESET 签名和 RECORD-ROUTE 签名；

[0024] 图 13 是根据本发明一个实施例的流程图，描述如何验证 RECORD-ROUTE 签名；以及

[0025] 图 14 是根据本发明一个实施例的流程图，描述如何把会话密钥导入服务器池中的一个服务器。

具体实施方式

[0026] 服务拒绝攻击一般是攻击者启动的计算机化的袭击，以使诸如 Web 服务器或文件服务器之类的网络服务过载或停止。例如，攻击可以导致服务器变得忙于试图对假冒消息作出响应，以致于忽视合法的连接请求。另一方面，可能破坏合法消息的路由，导致 SIP 节点不正确地转发响应。在某些情况中，用于在计算机网络上发送消息的通信协议可能是一个重要的攻击点。例如，如上所述，可以用伪造的 VIA 标题、ROUTE 标题和 / 或 RECORD-ROUTE 标题来发送假冒的 SIP 消息，因此把消息引导到受害的 SIP 节点和 / 或屏蔽攻击者的身份和来源。为了减少服务拒绝攻击，可以使确认包含在 SIP 标题中的路由指令和实际路由路径，以保证它们的完整性。

[0027] 图 1 示出示例会话启动操作，其中 SIP 客户机 102 的用户 100（例如，Alice）希望通过通信网络启动与另一个用户 400(Bob) 的通信会话，通信网络可包括因特网、内联网、广域网、局域网、虚拟专用网络等。为此，驻留在计算机系统 104 中的 SIP 客户机 102 发送将 Bob 标识为预期接收者的 INVITE 请求消息 500。在 SIP 标准下的通信的情况中，发送 INVITE 消息 500 以启动会话的 SIP 客户机 102 被称为“呼叫者”，而 Bob 的计算机系统 404 上的 SIP 客户机 402 被称为“被呼叫者”。如在 SIP 中所定义的，SIP 客户机 102 也被称为

“用户代理客户机”(“UAC”),因为它创建一个新请求,而 SIP 客户机 402 也被称为“用户代理服务器”,因为它生成对于 SIP 请求 500 的响应 600。

[0028] 如在图 1 中所示,把来自 Alice 的 INVITE 消息 500 发送到呼叫者 SIP 客户机的域中的出站 (outbound) 服务器 200。此后,在 INVITE 消息到达 Bob 的域中的 SIP 代理服务器 300 之前,可以令其通过包含在信令操作中的多个 SIP 节点。为了简化起见,在图 1 中仅示出五个 SIP 节点,然而,应该理解,任何链路都可以包括其它服务器、网关、网桥等。SIP 代理 300 把 INVITE 消息转发到 Bob 的计算机的 SIP 客户机 402(被呼叫者)。Bob 的计算机可以自动地,或根据 Bob 的授权,发送对 INVITE 的响应 600,诸如表示成功发送的“200(OK)”消息。

[0029] 如上所述,每个 SIP 消息一般包括起始行、包含关于消息的属性和路由的信息的标题、以及消息的正文。例如,图 2 示出 Alice 的 SIP 客户机 102 发送并由 SIP 节点 200 接收的 INVITE 请求 500 的表示。示例 INVITE 500 包括起始行 502、多个标题 504 以及正文 506。起始行 502 标识消息类型(这里是 INVITE)、一般是被呼叫者的 SIP 地址的请求 URI、以及 SIP 版本。标题 504 是 SIP 标准下可接受的字段。VIA 标题 508 包含表示协议和前一中继段地址的信息。FROM 标题 510 包含表示始发请求的用户(呼叫者)- 这里是 Alice- 的信息。TO 标题 512 包含表示由呼叫者指定的被呼叫者的信息。Call-ID(呼叫 ID) 标题 514 包含表示正在启动的会话的全局唯一标识符的信息。CSEq 标题 516 包含表示一标识符的信息,该标识符在作为同一事务的一部分用相同的 FROM、TO 和 Call-ID 标题发送的多个消息之间进行区分。CONTACT 标题 518 包含表示后续请求的目的地的信息,允许未来消息路由到不在 RECORD-ROUTE 标题中列出的旁路 SIP 节点(下面进一步讨论)。VIA 标题、TO 标题、FROM 标题、CONTACT 标题、RECORD-ROUTE 标题以及 ROUTE 标题的每一个都包含表示网络中的路由位置的数据,诸如 URI、因特网协议地址等。例如,包含表示路由位置的数据的 RECORD-ROUTE 标题可以包括由标题参数跟随着的、包括在“<>”括号中的 URI 部分。在“<>”括号中的 URI 部分可以包括 URI 和 URI 参数。一般而言,至少一个空白行标记标题 504 的结束和正文部分 506 的开始。像 INVITE 请求那样,图 5 中示出的示例响应 600 包括起始行 602、标题部分 604 以及正文 606。

[0030] 在 SIP 标准下,当 INVITE 500 在网络上行进时,对它进行管理的每个 SIP 节点把 VIA 标题添加到 INVITE 标题 504 中。如此,在把对于请求的答复返回呼叫者时,被呼叫者可以使用经累加的 VIA 标题来引导响应的路由。如果 SIP 节点愿意继续管理呼叫者和被呼叫者之间该特定对话的消息,则 SIP 节点可以把 RECORD-ROUTE 标题插入到 INVITE 标题 504 中。如此,为了引导可以由被呼叫者生成的未来请求的路由,接收被呼叫者可以保存对话启动请求的 RECORD-ROUTE 标题和 CONTACT 标题的经累加的 URI 部分,作为与所列出的次序相同的标题的 ROUTE SET(路由组)。相似地,为了提供由呼叫者生成的未来请求的路由指令,呼叫者可以按与 ROUTE SET 标题相反的次序来保存在对话启动请求的响应中的 RECORD-ROUTE 标题和 CONTACT 标题的经累加的 URI 部分。

[0031] 考虑到通过处理 SIP 节点的标题添加,图 1 示出了路由 INVITE 请求和响应的具体例子。为了简化起见,未包括无关系的标题和其它消息信息。要理解,所示的 SIP 节点的功能和数量是示例性的,对于特定目的和 / 或网络体系结构可以修改消息路由和验证。

[0032] 如在图 1 中所示,SIP 节点 200 可以是归属服务器,并可接收来自 SIP 客户机 102 的

INVITE 请求。接收消息的 SIP 节点 200 把 VIA 标题插入 INVITE 请求的标题 504 中。作为归属服务器的 SIP 节点 200 可能希望管理来往于 SIP 客户机 102 的任何 SIP 消息。因此，SIP 节点 200 可以在它把消息转发到下一 SIP 节点之前，把 RECORD-ROUTE 标题插入到 INVITE 消息中。在图 1 示出的实施例中，下一 SIP 节点 250 是呼叫者 SIP 客户机 102 的边缘服务器。SIP 节点 250 在把它自己的 VIA 标题和 RECORD-ROUTE 标题插入到消息的标题 504 中之后转发 INVITE 消息。最后，INVITE 消息被路由到 SIP 节点 300，在图 1 所示的实施例中，该节点是被呼叫者 SIP 客户机 402 的边缘代理服务器。边缘代理服务器可以是被设计成在网络边缘处运行的一种代理服务器，例如，使本地网络与因特网分开。像边缘服务器 250 一样，边缘代理服务器 300 在把消息转发到 SIP 客户机 402 之前，把 VIA 标题和 RECORD-ROUTE 标题插入到 INVITE 标题 504 中。在图 3 中示出插入到 INVITE 请求 500 中的 SIP 节点 200 的 VIA 标题 530、SIP 节点 250 的 VIA 标题 532 以及 SIP 节点 300 的 VIA 标题 534 的例子。在图 4 中示出插入到 INVITE 请求 500 中的 SIP 节点 200 的 RECORD-ROUTE 标题 520、SIP 节点 250 的 RECORD-ROUTE 标题 522 以及 SIP 节点 300 的 RECORD-ROUTE 标题 524 的例子。

[0033] Bob 的 SIP 节点 402 可以接受 INVITE，并且发送 OK 响应 600 作为对 INVITE 请求的答复。图 5 示出从 SIP 节点 402 到服务器 300 的示例响应 600。在 SIP 标准下，从所接收的请求中拷贝或返回响应 600 的许多标题字段或至少一部分标题字段。这些返回的标题可以包括，例如在 SIP 标准下确定的，每个 VIA 标题、FROM 标题、TO 标题、每个 RECORD-ROUTE 标题、Call-ID 标题、以及 CSeq 标题。如此，图 5 中示出的响应 600 说明返回的标题。特别地，响应 600 中的 VIA 标题 608、630、632、634 与被呼叫者 SIP 节点 402 接收的 INVITE 500 中的 VIA 标题 508、530、532、534 相同。相似地，RECORD-ROUTE 标题 620、622、624 与 SIP 节点生成并由被呼叫者 SIP 节点 402 接收的 INVITE 500 中的 RECORD-ROUTE 标题 520、522、524 相同。然后如由 VIA 标题 608、630、634 引导的通过网络把响应消息路由到呼叫者 SIP 节点 102。

[0034] 处理响应的 SIP 节点，如 SIP 节点 300、250、200，可以通过确认包含在 VIA 标题中的路由指令来确认响应采用的实际路由的完整性。在一个实施例中，SIP 节点可以把诸如 VIA 标题 508、530、532 等路由信息存储在数据库中，供以后访问和使用，以验证响应 VIA 标题 608、630、632。另一方面，为了减少 SIP 节点上的存储器和访问负载，SIP 节点可以基于至少一个标题中的至少一部分来生成签名，所述至少一个标题包含表示消息的路由中的网络路由位置的数据。例如，签名可以基于包含网络路由位置的所有标题，或可以只基于该标题的一部分，诸如 URI、URI 参数、对等完全合格域名 (“FQDN”) 等。除了至少一个标题之外，签名还可以基于其它信息，包括将在下一个中继段上通过其发送消息的连接的连接标识符、返回标题、TO 标题、FROM 标题、CONTACT 标题、CALL-ID 标题、CSeq 标题以及 Branch-ID。然后可以把基于请求的至少一个标题中的至少一部分的签名传送给响应，并且当 SIP 节点处理响应时被确认。是否应该把标题部分包括在签名中取决于在 SIP 代理验证标题部分之前它是否会改变。例如，包含在为了签名验证而被访问之前可能被移除或改变的信息的标题部分不应包括在签名中。要理解，SIP 消息的路由中的任何或所有的 SIP 节点可以按包括这里讨论的任何合适的方式来生成和存储验证签名。还可以理解，可以根据网络和 SIP 节点的安全性考虑和标准在适当时确认 SIP 消息的标题，包括维护可信链路的列表、符合签署的全局政策以及到 / 自特定域的签名 / 确认消息等。例如，为了实现可信链路列表，每个

服务器可以维护它认为可信的链路的列表。因此，去往 / 来自可信列表的任何消息可能不被签署 / 确认。因此，服务器在生成 / 确认签名之前可以核查可信链路列表，以保证该链路是不可信的，例如，没有列在可信列表中。

[0035] 在一个例子中，可以使用可访问的会话密钥基于请求消息中的至少一个 VIA 标题来生成签名。为了确认消息行进的路由，SIP 节点可以基于所有 VIA 标题或至少 SIP 节点接收到的所有 VIA 标题来生成 VIA 签名。例如，对于图 1 和 2 中示出的 INVITE 消息 500，SIP 节点 200 可以通过使用 SIP 节点 200 可访问的会话密钥，基于包含指定 SIP 客户机 102(Alice) 的信息的 VIA 标题 508 来提供 VIA 签名。可以把所生成的 VIA 签名存储在消息中，传送给响应消息，然后在通过 SIP 节点 200 的消息返回行程上确认。相似地，SIP 节点 300 可以基于所接收的 VIA 标题生成 VIA 签名，以在以后当在 SIP 节点 300 处接收到响应时确认它。为了签署 VIA 标题，SIP 节点 300 可以使用可访问的会话密钥基于 Alice 的 VIA 标题 508、SIP 节点 200 的 VIA 标题 530 以及 SIP 节点 250 的 VIA 标题 532 生成 VIA 签名。

[0036] 要理解，可以签署 VIA 标题和其它标题信息的任何合适的组合，以认证响应标题 604 中的路由指令。例如，除了一部分 TO 标题、FROM 标题或可以从请求标题 504 返回到响应标题 604 的任何其它标题之外，VIA 签名还可以基于一部分 VIA 标题。此外，插入到请求标题 504 中的 VIA 签名 550 可以是表示所生成的数字签名的任何数据或信号。例如，所存储的签名 550 可以是所生成的签名二进制大对象 (blob) 的预定数量的有效位，或可以是整个数字签名。

[0037] 为了保证在处理 INVITE 请求期间生成的 VIA 签名存在，用于 SIP 节点处响应中的验证，可以把所生成的 VIA 签名插入到 INVITE 请求的返回标题中。例如，可以在标准路由位置信息之后插入签名作为 URI 参数或标题参数。因此，当客户机 SIP 节点 402 基于 SIP 请求的返回标题生成响应标题 604 时，所生成的签名从请求自动传送到响应。因此，接收响应的 SIP 节点可以确认传送到响应标题的签名。要理解，基于现有协议由客户机 SIP 节点返回的任何返回标题或自定义标题都可适合于存储签名，用于由 SIP 节点确认。

[0038] 如在图 3 中所示，可以把 VIA 签名插入到生成签名的 SIP 节点的 VIA 标题中。例如，SIP 节点 300 可以基于请求 500 中接收的 VIA 标题 508、530、532 生成 VIA 签名 550。SIP 节点 300 可以把 VIA 签名 550 插入到 SIP 节点 300 的 VIA 标题 534 中。如上所述，在响应标题 604 中返回请求标题中的 VIA 标题。因此，当 SIP 节点 402 形成响应 600 时，它可以把包含在 VIA 标题 534 中的信息拷贝到 SIP 节点 300 的 VIA 标题 634 中 (图 1)。在标准的 SIP 处理下，当返回 VIA 标题时，拷贝标准的 VIA 信息，以及作为标题参数而附加的任何信息，诸如 VIA 签名 550。

[0039] 为了确认所接收的 VIA 签名 650，SIP 节点 300(图 1) 可以剥去和保存图 5 中示出的所接收的 VIA 签名 650。SIP 节点 300 可以使用与用于生成插入到请求中的 VIA 签名 550 的过程相同的过程来生成确认 VIA 签名。根据上述 VIA 签名 550 的生成，SIP 节点 300 可以识别所接收响应 600 中的 VIA 标题，并且基于在 SIP 节点 300 的 VIA 标题 534 下列出的所有 VIA 标题生成确认 VIA 签名。如此，确认 VIA 签名可以基于当在请求消息 500 中生成 VIA 签名 550 时 SIP 节点 300 已知的那些 VIA 标题。因此，SIP 节点 300 的确认 VIA 签名可以基于 SIP 节点 250 的 VIA 标题 632、SIP 节点 200 的 VIA 标题 630 以及呼叫者 SIP 节点 102 的 VIA 标题 608。SIP 节点 300 可以将确认 VIA 签名和所接收的 VIA 签名 650 进行

比较。

[0040] 如果签名是匹配的，则SIP节点300可以继续进行SIP标准下的正常处理，并且把响应转发到在响应标题604的VIA标题中指示的下一SIP节点。如果签名是不匹配的，则SIP节点300可以从它的处理栈中丢弃响应600，和/或把出错消息发送给SIP节点监视服务（未示出）或协议支持的任何合适的监视代理。为了测量签名兼容性和/或攻击检测的消息处理性能，对于每个被拒绝的消息，SIP节点300都递增一签名失败性能计数器。签名失败性能计数器可以是表示SIP节点验证标题签名失败的任何数据或信号。例如，签名失败性能计数器可以对一个时间段内的失败的签名确认的数量进行计数。然后，签名失败性能计数器可以与该时间段内的失败的签名确认的预定阈值（诸如在约1秒的消息处理时间中，大约6个失败的签名确认、大约10个失败的签名确认、或大约25个失败的签名确认）进行比较。当性能计数器超过阈值时，SIP节点可以通知或警告系统管理人员（包括通过电子邮件和/或寻呼机），和/或通知或警告可以基于性能计数器启动预定行动的基于计算机的系统管理员，包括例如，包括撤消路由失败消息的网络连接、锁住网络和/或清洗消息队列。

[0041] 在某些情况中，可以在路由上的每一步处，例如，在返回行程上处理请求和/或响应的每个SIP节点处，生成确认和/或签名。然而，为了减少SIP节点服务器上的计算负担，可以只在需要消息时才确认它。

[0042] 例如，如果请求只包含一个VIA标题，例如，请求500中Alice的SIP节点102的VIA标题508，则在节点处的请求中不生成签名。更具体地，Alice的SIP节点102可能不需要验证响应600中的任何路由指令，因为该响应将由SIP节点102消耗，例如，它将不进一步转发。因此，当请求只包含一个VIA标题时，不生成VIA签名，并且因此，当接收到只包含一个VIA标题的请求时（例如，接收SIP节点的VIA标题时）不需要验证VIA签名。

[0043] 在另一个例子中，如果通过不可信连接接收消息，则服务拒绝攻击更为可能。为了提高消息的安全性，当通过不可信连接接收时，可以确认消息。例如，不可信连接可以包括任何服务器类型的任何客户机连接，因为可以用其它方法来认证从其它服务器接收的消息。不可信连接还可以包括边缘代理服务器的外部服务器连接，尤其可以包括所有外部服务器连接。

[0044] 如在图1中所示，SIP节点200和SIP节点250之间的连接210、212可以是可信连接，因为可以认为这些连接是归属服务器和边缘服务器之间的内部链路。由于服务器可以有认证服务器之间的消息话务的其它方法，所以SIP节点250和SIP节点300之间的链路260、262可以是可信连接；然而，在某些情况中可以认为这些连接是不可信连接，特别是如果认为服务器认证的其它方法不足够的时候。客户机节点402和SIP节点300之间的链路310、312可以是不可信连接，因为SIP消息被发送到客户机SIP节点/从客户机SIP节点发送。因此，可以在SIP节点处确认通过不可信连接（诸如链路312）接收的任何消息，以验证消息完整性和/或真实性。

[0045] 如果不确认通过可信链路接收的响应，则当通过可信链路把请求转发到下一SIP节点时不需要生成VIA签名。例如，SIP节点200和250可以不通过不可信连接接收响应600，因此，在INVITE请求的标题504中，这些节点可以不生成或存储VIA签名，因为它们没有确认响应的路由的要求。因此，在生成VIA签名之前，SIP节点可以判定是否需要对应的

响应的确认。如果不需要验证响应，例如下一个链路是可信连接，则不需要生成 VIA 签名，并且可以继续进行 SIP 请求的正常处理。然而，如果通过不可信连接在 SIP 节点处接收对应的响应，则可以如上所述地生成 VIA 签名。相似地，在接收响应之后，SIP 节点可以首先判定是否从不可信连接接收到响应。如果是这样的，则确认 VIA 签名（如果存在的话）。例如，SIP 节点 300 可以判定响应 600 是否通过可信连接接收的。如在图 1 中所示，链路 312 是不可信连接。结果，SIP 节点 300 就可以识别响应的标题 604 中的 SIP 节点 300 的 VIA 标题 634。SIP 节点 300 可以判定在经识别的 VIA 标题 634 中是否存在签名。如果 VIA 签名不存在，则如果协议允许的话，SIP 节点 300 可以发送出错消息，可以从它的处理栈中丢弃消息，可以递增签名失败性能计数器和 / 或采取任何其它适当的行动。如果存在 VIA 签名 650，如在图 5 中所示，则 SIP 节点 300 可以如上所述地验证签名。

[0046] 如上所述，签署 VIA 标题有助于响应标题 604 中的路由指令的确认。然而，SIP 节点可以另外或可选地要求确认由被呼叫者生成的请求的路由指令。因此，SIP 节点可以基于对话启动请求中的至少一个 RECORD-ROUTE 标题的至少一部分生成签名，然后在来自被呼叫者的后续请求中确认该签名，以保证对话内请求中的路由指令的完整性。

[0047] 为了保证被呼叫者请求行进的路由的完整性，SIP 节点可以基于包含在请求的接收标题字段中的 RECORD-ROUTE 标题和 CONTACT 标题的 URI 部分来生成被呼叫者 ROUTE SET 签名。如果存在一个以上 CONTACT 标题，则被呼叫者 ROUTE SET 签名可以基于 RECORD-ROUTE 标题中所选择的 URI 部分以及第一列出 CONTACT 标题的 URI 部分。更具体地，对于图 1、2 和 4 中示出的 INVITE 消息 500，SIP 节点 300 可以基于 SIP 节点 250 的 RECORD-ROUTE 标题 522 的 URI 部分、SIP 节点 200 的 RECORD-ROUTE 标题 520 的 URI 部分、以及呼叫者 Alice 的 CONTACT 标题 518 的 URI 部分提供被呼叫者 ROUTE SET 签名。可以把所生成的被呼叫者 ROUTE SET 签名存储在消息中，并且传送到被呼叫者 SIP 节点 402，以在由属于同一对话的被呼叫者 SIP 节点 402 生成的任何请求中进行存储和使用。要理解，可以签署 RECORD-ROUTE 标题和其它标题信息的任何合适的组合，以认证被呼叫者 SIP 节点 402 生成的任何后续请求的路由指令。插入到请求标题 504 中的被呼叫者 ROUTE SET 签名可以是表示所生成的签名的任何数据或信号，所生成的签名包括签名二进制大对象的预定数量的有效位和整个数字签名。

[0048] 为了保证存在请求处理期间生成的被呼叫者 ROUTE SET 签名以在呼叫者 SIP 节点 402 生成的后续请求中用于验证，可以把所生成的被呼叫者 ROUTE SET 签名插入到请求的返回标题中。因此，当客户机 SIP 节点 402 基于 SIP 对话启动请求生成新请求时，自动传送所生成的签名。因此，接收请求的 SIP 节点可以确认传送给请求标题的签名。要理解，可以由客户机 SIP 节点基于现有协议返回的任何返回的标题部分或自定义标题都适合于存储被呼叫者 ROUTE SET 签名，用于由 SIP 节点确认。

[0049] 如在图 2 和 4 中所示，可以把被呼叫者 ROUTE SET 签名作为 URI 参数插入到生成签名的 SIP 节点的 RECORD-ROUTE 标题中。例如，SIP 节点 300 可以基于请求 500 中的 RECORD-ROUTE 标题 522、520 和 CONTACT 标题 518 的 URI 部分来生成被呼叫者 ROUTE SET 签名 560。SIP 节点 300 可以把被呼叫者 ROUTE SET 签名 560 插入到 SIP 节点 300 的 RECORD-ROUTE 标题 524 中作为 URI 参数。如上所述，由被呼叫者 SIP 节点在 ROUTE 标题中存储和返回来自呼叫者的对话启动请求的 RECORD-ROUTE 标题he CONTACT 标题的 URI 部分，

以提供在对话中由被呼叫者生成的任何未来请求的路由指令。因此，如在图 6 中所示，当 SIP 节点 402 形成一个请求时，它可以在标准 SIP 处理下把 RECORD-ROUTE 标题 524 的 URI 部分拷贝到 SIP 节点 300 的 ROUTE 标题 724 中。当返回 RECORD-ROUTE 标题的 URI 部分时，拷贝标准路由信息以及包括被呼叫者 ROUTE SET 签名 560 的任何 URI 参数。

[0050] 为了确认图 6 中所接收的被呼叫者 ROUTE SET 签名 760，SIP 节点 300 可以剥去和保存所接收的被呼叫者 ROUTE SET 签名 760。SIP 节点 300 可以使用与生成插入到对话启动请求（这里是 INVITE）中的被呼叫者 ROUTE SET 签名 560 的过程相同的过程来生成确认 ROUTE SET 签名。根据上述被呼叫者 ROUTE SET 签名 560 的生成，SIP 节点 300 可以识别在所接收的请求 700 中的 RECORD-ROUTE 标题，并且基于除了接收 SIP 节点的 ROUTE 标题之外的、存在于请求中的所有 ROUTE 标题来生成确认 ROUTE SET 签名。如此，确认 ROUTE SET 签名可以基于当在请求消息 500 中生成 ROUTE SET 签名 560 时 SIP 300 已知的那些 RECORD-ROUTE 标题和 CONTACT 标题。例如，在图 1 的设置中，SIP 节点 300 的确认 ROUTE SET 签名可以基于 SIP 节点 250 的 ROUTE 标题 722、SIP 节点 200 的 ROUTE 标题 720、以及基于识别呼叫者 SIP 节点 102 的 CONTACT 标题的 ROUTE 标题 718。SIP 节点 300 可以将确认 ROUTE SET 签名与所接收的被呼叫者 ROUTE SET 签名 760 进行比较。如果签名不匹配，则如果协议允许的话，SIP 节点 300 可以发送出错消息，从它的处理栈中移除请求 700，递增签名失败性能计数器，和 / 或采取任何其它适当的行动。如果签名是匹配的，则 SIP 节点 300 可以在 SIP 标准下继续进行正常的处理，并且把请求转发给在请求标题 704 的 ROUTE 标题中指示的下一 SIP 节点。

[0051] 在某些情况中，可以在路由上的每一步处，例如，在处理请求的每个 SIP 节点处，生成和 / 或确认被呼叫者 ROUTE SET 签名。然而，为了减少 SIP 节点服务器上的计算负担，可以只在需要时才确认请求。

[0052] 例如，如果请求不包含任何 RECORD-ROUTE 标题，例如，甚至连当前处理 SIP 节点也不添加 RECORD-ROUTE 标题，则可以不生成被呼叫者 ROUTE SET 签名。更特别地，如果处理请求的 SIP 节点没有请求保留“在循环中”以进一步在被呼叫者和呼叫者之间通信，则 SIP 节点可以不要求验证未来接收的消息中的路由指令。

[0053] 在又一个例子中，如果请求包含 RECORD-ROUTE 标题但是一个 CONTACT 标题也没有，则 SIP 节点可能不要求确认返回这些 RECORD-ROUTE 标题的任何响应或请求。这会在包括某些类型的 ACK（确认）和 CANCEL SIP（清除 SIP）消息的某些情况中发生。更特别地，如果所接收请求包括至少一个 RECORD-ROUTE 标题和零个 CONTACT 标题，则可能不生成被呼叫者 ROUTE SET 签名而可以继续进行正常处理。

[0054] 在另外的例子中，由于来自不可信链路的请求更有可能是服务拒绝攻击的来源，因此当通过不可信连接接收时，可以确认消息。如果不确认经过不可信链路接收的被呼叫者的请求，则当把来自呼叫者的对话启动请求经过可信链路转发到下一个 SIP 节点时，不需要生成被呼叫者 ROUTE SET 签名 560。例如，如在图 1 中所示，SIP 节点 200 将经过可信连接接收请求 700，或换言之，SIP 节点将不经过不可信连接接收请求 700。因此，这个节点不会生成被呼叫者 ROUTE SET 签名或把它插入到 INVITE 请求的标题 504 中，因为它可能对于使来自被呼叫者的任何请求的确认没有要求。因此，在生成被呼叫者 ROUTE SET 签名之前，SIP 节点可以判定是否需要确认任何被呼叫者请求。如果不要验证被呼叫者请求，例如，

将通过可信连接接收当前请求，则不需要生成被呼叫者 ROUTESET 签名，并且可以继续进行 SIP 节点的正常处理。然而，如果将经过不可信连接在 SIP 节点处接收被呼叫者请求，则可以如上所述地生成被呼叫者 ROUTE SET 签名。相似地，在被呼叫者 ROUTE SET 签名的验证期间，处理 SIP 节点可以首先判定从被呼叫者接收到的请求是否经过不可信连接。如果是的，则可以确认被呼叫者 ROUTE SET 签名（如果存在的话）。例如，SIP 节点 300 可以判定是否经过不可信连接接收请求 700。如在图 1 中所示，链路 312 是不可信连接。结果，SIP 节点 300 就可以识别图 6 中示出的请求 700 的标题 704 中的 SIP 节点 300 的 ROUTE 标题 724。SIP 节点 300 可以判定在所识别的 ROUTE 标题 724 中是否存在签名，如果存在，就验证该签名。

[0055] SIP 节点另外或可选地还要求确认在对话启动请求之后由被呼叫者生成的对话内请求的路由指令。因此，SIP 节点可以基于对于对话启动请求的响应的至少一个 RECORD-ROUTE 标题的至少一部分生成签名，并且然后在来自呼叫者的后一请求中确认该签名，以保证请求的路由指令的完整性。

[0056] 为了保证呼叫者请求行进的路由的完整性，SIP 节点可以基于包含在所接收响应的标题字段中的 RECORD-ROUTE 标题和 CONTACT 标题的 URI 部分生成呼叫者 ROUTE SET 签名。如果存在一个以上 CONTACT 标题，则呼叫者 ROUTE SET 签名可以基于 RECORD-ROUTE 标题的所选择的 URI 部分和第一列出 CONTACT 标题的 URI 部分。更特别地，对于图 1 和 5 中示出的响应消息 600，SIP 节点 200 可以基于 SIP 节点 250 的 RECORD-ROUTE 标题 622 的 URI 部分、SIP 节点 300 的 RECORD-ROUTE 标题 624 的 URI 部分、以及被呼叫者 Bob 的 CONTACT 标题 618 的 URI 部分提供呼叫者 ROUTE SET 签名。可以把所生成的呼叫者 ROUTE SET 签名存储在消息中，并且传送到呼叫者 SIP 节点 102，以在属于同一对话的呼叫者 SIP 节点 102 生成的任何请求中存储和使用。要理解，可以签署 RECORD-ROUTE 标题和其它标题信息的任何合适的组合，以认证呼叫者 SIP 节点 102 生成的任何后续请求的路由指令。插入到响应标题 604 中的呼叫者 ROUTE SET 签名可以是表示所生成的数字签名的任何数据或信号，所生成的数字签名包括签名二进制大对象的预定数量的有效位和整个数字签名。

[0057] 为了保证在响应处理期间生成的呼叫者 ROUTE SET 签名存在，以在呼叫者 SIP 节点 102 生成的后续响应中用于验证，可以把所生成的呼叫者 ROUTE SET 签名插入到响应的返回标题中作为 URI 参数。因此，当客户机 SIP 节点 102 基于来自 SIP 响应的返回标题生成新请求时，自动传送所生成的签名。因此，接收请求的 SIP 节点可以确认传送给请求标题的签名。要理解，由客户机 SIP 节点基于现有协议返回的任何返回标题部分或自定义标题都适合于存储呼叫者 ROUTE SET 签名，用于由 SIP 节点确认。

[0058] 如在图 5 中所示，可以把呼叫者 ROUTE SET 签名插入到生成签名的 SIP 节点的 RECORD-ROUTE 标题中。例如，SIP 节点 200 可以基于响应 600 中的 RECORD-ROUTE 标题 622、624 和 CONTACT 标题 618 的 URI 部分生成呼叫者 ROUTE SET 签名 660。SIP 节点 200 可以把呼叫者 ROUTE SET 签名 660 插入到 SIP 节点 200 的 RECORD-ROUTE 标题 620 中。如上所述，由呼叫者 SIP 节点在 ROUTE 标题中存储和返回对于对话启动请求的响应的 RECORD-ROUTE 标题和 CONTACT 标题的 URI 部分，以提供在对话中的呼叫者生成的任何未来请求的路由指令。因此，如在图 7 的示例请求 800 中所示，当 SIP 节点 102 形成该对话中的后续请求时，它可以在标准的 SIP 处理下把 RECORD-ROUTE 标题 620 的 URI 部分拷贝到 SIP 节点 200 的

RECORD-ROUTE 标题 820 中。当返回 RECORD-ROUTE 标题的 URI 部分时，拷贝标准的路由信息以及包括呼叫者 ROUTE SET 签名 660 的任何 URI 参数。

[0059] 为了确认图 7 的所接收的呼叫者 ROUTE SET 签名 860，SIP 节点 200（图 1）可以剥去和保存图 7 中示出的所接收的呼叫者 ROUTE SET 签名 860。SIP 节点 200 可以使用与生成插入到对于对话创建请求的响应中的呼叫者 ROUTE SET 签名 660 的过程相同的过程来生成确认 ROUTE SET 签名。根据上述呼叫者 ROUTE SET 签名 660 的生成，SIP 节点 200 可以识别在所接收请求 800 中的 RECORD-ROUTE 标题，并且基于除了接收 SIP 节点的 ROUTE 标题之外在请求中存在的所有 ROUTE 标题，来生成确认 ROUTE SET 签名。如此，确认 ROUTE SET 签名可以基于当在响应消息 600 中生成呼叫者 ROUTE SET 签名 660 时 SIP 节点 200 已知的那些 RECORD-ROUTE 标题和 CONTACT 标题。因此，SIP 节点 200 的确认 ROUTE SET 签名可以基于 SIP 节点 250 的 ROUTE 标题 822、SIP 节点 300 的 ROUTE 标题 824 以及根据识别被呼叫者 SIP 节点 402 的 CONTACT 标题的 ROUTE 标题 818。SIP 节点 200 可以将确认 ROUTESET 签名和所接收的呼叫者 ROUTE SET 签名 860 进行比较。如果签名不匹配，则如果协议支持的话，SIP 节点 200 可以发送出错消息，从它的处理栈中移除请求 800，递增签名失败性能计数器，和 / 或采取任何其它适当的行动。如果签名是匹配的，则 SIP 节点 200 可以在 SIP 标准下继续进行正常的处理，并且把请求转发给在请求标题 804 的 ROUTE 标题中指示的下一 SIP 节点。

[0060] 在某些情况中，可以在路由上的每一步处，例如，在处理响应和 / 或请求的每个 SIP 节点处，生成和 / 或确认呼叫者 ROUTE SET 签名。然而，如上相对于插入请求中的 VIA 签名和呼叫者 ROUTE SET 签名所述，通过只在需要时才要求请求中的呼叫者 ROUTE SET 签名确认而减少 SIP 节点服务器上的计算负担。

[0061] 例如，如果对于请求的响应不包含任何 RECORD-ROUTE 标题，例如，甚至连当前处理 SIP 节点也不添加 RECORD-ROUTE 标题，则可以不生成呼叫者 ROUTE SET 签名。更特别地，如果处理响应的 SIP 节点没有请求保留“在循环中”以进一步在呼叫者和被呼叫者之间通信，则该 SIP 节点可以不要求验证未来消息中的路由指令。

[0062] 在又一个例子中，如果响应包含 RECORD-ROUTE 标题但是一个 CONTACT 标题也没有，则 SIP 节点可能不要求确认返回这些 RECORD-ROUTE 标题的任何响应或请求。更特别地，如果所接收的响应包括至少一个 RECORD-ROUTE 标题和零个 CONTACT 标题，则可能不生成呼叫者 ROUTE SET 签名而可以继续进行正常处理。

[0063] 在另外的例子中，当只经过不可信连接接收呼叫者请求的 ROUTESET 标题时，可以确认呼叫者请求的 ROUTE SET 标题。如果不确认经过可信链路接收的请求，则当经过可信链路把响应转发到下一个 SIP 节点时，不需要生成呼叫者呼叫者 ROUTE SET 签名 660。相似地，在接收来自呼叫者的请求之后，如果经过可信连接接收，则不需要确认 ROUTESET 签名。

[0064] 如上所述，在对话启动请求和它的对应响应中包括 RECORD-ROUTE 标题，以生成用于路由后续请求的被呼叫者和呼叫者 ROUTE SET 标题。因此，在某些情况中，SIP 节点可以响应于对话启动请求确认 RECORD-ROUTE 标题，以保证这些 RECORD-ROUTE 标题的完整性。例如，连接节点可以篡改请求中的 RECORD-ROUTE 标题，因此，后续 SIP 节点可能在欺骗性的 RECORD-ROUTE 标题上签署，从而导致 ROUTE 标题具有有效的 ROUTE SET 签名，但是基于欺骗性的路由信息。因此，SIP 节点可以基于请求的至少一个 RECORD-ROUTE 标题的至少一部分

来生成一个签名，然后在来自被呼叫者的响应中确认该签名，以保证消息的 RECORD-ROUTE 标题的完整性。

[0065] 为了保证 RECORD-ROUTE 标题组的完整性，SIP 节点可以基于包含在所接收请求的标题字段中的 RECORD-ROUTE 标题的 URI 部分生成 RECORD-ROUTE 签名。更具体地，对于图 1、2 和 4 中示出的 INVITE 消息 500，SIP 节点 300 可以基于 SIP 节点 250 的 RECORD-ROUTE 标题 522 的 URI 部分和 SIP 节点 200 的 RECORD-ROUTE 标题 520 的 URI 部分提供 RECORD-ROUTE 签名 570。与上述被呼叫者 ROUTE SET 签名相反，RECORD-ROUTE 签名 570 不包括 CONTACT 标题，因为在 SIP 标准下，被呼叫者不在响应中返回 CONTACT 标题。可以把所生成的 RECORD-ROUTE 签名 570 存储在消息中，并且传送到响应消息，并且当通过 SIP 节点处理响应时确认。要理解，可以签署 RECORD-ROUTE 标题和其它标题信息的任何合适的组合，以认证被呼叫者 SIP 节点 402 生成的响应中的路由指令。插入到请求标题 504 中的 RECORD-ROUTE 签名 570 可以是表示所生成的数字签名的任何数据或信号，所生成的数字签名包括签名二进制大对象的预定数量的有效位和整个数字签名本身。

[0066] 为了保证存在处理请求期间生成的 RECORD-ROUTE 签名，用于被呼叫者 SIP 节点 402 生成的响应中的验证，可以把所生成的 RECORD-ROUTE 签名 570 作为标题参数或 URI 参数插入到请求的返回标题中。因此，当客户机 SIP 节点 402 基于 SIP 请求的返回标题生成响应时，将所生成的签名自动从请求传送到响应。因此，接收响应的 SIP 节点可以确认传送到响应标题的签名。要理解，基于现有协议由客户机 SIP 节点返回的任何返回标题或自定义标题都可适合于存储 RECORD-ROUTE 签名，用于由 SIP 节点确认。

[0067] 如在图 4 中所示，可以把 RECORD-ROUTE 签名插入到生成签名的 SIP 节点的 RECORD-ROUTE 标题中。例如，SIP 节点 300 可以把 RECORD-ROUTE 签名 570 作为标题参数插入到 SIP 节点 300 的 RECORD-ROUTE 标题 524 中。如上所述，在响应标题 604 中返回 RECORD-ROUTE 标题。因此，当 SIP 节点 402 形成响应时，诸如图 5 中示出的响应 600，它可以在标准的 SIP 处理下把 RECORD-ROUTE 标题 524 拷贝到 SIP 节点 200 的 RECORD-ROUTE 标题 624 中。当返回 RECORD-ROUTE 标题时，拷贝标准的信息以及包括 RECORD-ROUTE 签名 570 的任何标题参数。

[0068] 为了确认图 5 的所接收的 RECORD-ROUTE 签名 670，SIP 节点 300 可以剥去和保存所接收的 RECORD-ROUTE 签名 670。SIP 节点 300 可以使用与用于生成插入到对应请求（这里是 INVITE）中的 RECORD-ROUTE 签名 570 的过程相同的过程来生成确认 RECORD-ROUTE 签名。根据上述 RECORD-ROUTE 签名 570 的生成，SIP 节点 300 可以基于 SIP 节点 250 的 RECORD-ROUTE 标题 622 的 URI 部分和 SIP 节点 200 的 RECORD-ROUTE 标题 620 的 URI 部分生成确认 RECORD-ROUTE 签名。SIP 节点 300 可以将确认 RECORD-ROUTE 签名和所接收的 RECORD-ROUTE 签名 670 进行比较。如果签名不匹配，则如果协议支持的话，SIP 节点 300 可以发送出错消息，从它的处理栈中移除响应 600，和 / 或递增签名失败性能计数器。如果签名是匹配的，则 SIP 节点 300 可以在 SIP 标准下继续进行正常的处理，并且把响应转发给在响应标题 604 的 VIA 标题中指示的下一 SIP 节点。

[0069] 在某些情况中，可以在路由上的每一步处，例如，在处理响应的每个 SIP 节点处，确认响应的 RECORD-ROUTE 标题。然而，与如上参考 VIA 签名 650 的描述相似，为了减少 SIP 节点的计算负担，只在需要时才确认响应。例如，如果请求不包含任何 RECORD-ROUTE 标题，

则可以不生成 RECORD-ROUTE 签名。在另外的例子中，如果到下一 SIP 节点的连接是可信连接，则可以不生成 RECORD-ROUTE 签名。为了减少通信系统的负担，在验证之后并在把响应转发到下一 SIP 节点之前，SIP 节点可以从 RECORD-ROUTE 标题中移除 RECORD-ROUTE 签名。

[0070] 为了基于 SIP 消息中的至少一部分标题来生成签名，需要确认和验证能力的 SIP 节点可以包括密码程序，该程序在中央处理单元上执行以执行某些秘码功能，包括加密、解密、签名和 / 或验证。作为一个例子，密码程序能够生成和消灭密钥，诸如用于计算签名时添加随机数，或用于加密 / 解密的目的的对称密钥。另一方面，密码程序可以访问非对称（公有 / 私有）密钥对。在典型的非对称密钥对中，可以使用公钥对信息进行加密，而可以使用对应的私钥对信息进行解密。可以使用私钥来生成数字签名，并且使用公钥来认证该签名。应该理解，任何单向散列机制都可适用于生成基于 SIP 标题的签名，包括基于许多因素（诸如对于攻击的恢复力，相对速度以及生成相关联签名的计算负担）的单独或组合的 MD5、salt、HMAC、SHAI 以及 RSA。还要理解，可以插入整个签名二进制大对象、一部分签名二进制大对象或使用任何编码方案的签名二进制大对象的编码版本，作为 VIA、ROUTE SET、和 / 或 RECORD-ROUTE 签名。在一个例子中，签名可以是 SIP 消息标题的所选择部分和任何其它信息（包括随机数和 / 或会话密钥）的 16 字节单向 MD5 散列。可以用按任何特定次序的相关标题来生成基于 SIP 标题的签名，只要该次序在签名生成和确认之间保持一致。

[0071] 同一 SIP 节点处理的 VIA 签名、ROUTE SET 签名和 RECORD-ROUTE 签名的每一个可以通过相同的会话密钥生成。另一方面，对于每个签名或签名的任何组合，可以使用不同恢复力和速度的密钥。例如，由于一般十分快速地验证 VIA 签名和 / 或 RECORD-ROUTE 签名，例如，在对应的响应中，所以用于生成 VIA 签名的 VIA 密钥可以是计算负担十分小的十分轻量级的密钥 / 密码解决方案。然而，由于 ROUTE SET 标题可以通过整个对话继续验证，所以 ROUTE SET 密钥是重量级的密钥 / 密码解决方案，它比轻量级的密钥 / 密码解决方案较不易受攻击。

[0072] 对于由特定的 SIP 节点在某个时间帧中处理的所有对话请求和 / 或响应，可以生成和使用用于生成签名的会话密钥本身。另一方面，可以向每个对话发出特定的会话密钥，该密钥可以与该 SIP 节点使用的其它对话会话密钥相同或不同，并且可以与其它 SIP 节点使用的对话会话密钥相同或不同。在预定时间段之后、在对话结束处和 / 或接收到密钥和 / 或标题损坏的指示时，密码程序可以消灭这些会话密钥。

[0073] 每个 SIP 节点可以生成它自己的会话密钥，诸如用于生成 VIA 签名的 VIA 密钥、用于生成 RECORD-ROUTE 标题的 ROUTE 密钥以及用于生成 RECORD-ROUTE 签名的 RECORD-ROUTE 密钥。另一方面，SIP 节点的每一个都可以访问会话密钥，诸如通过公钥 / 私钥对的证书来访问，以致使用相同密钥来签署每种类型的标题。

[0074] 为了降低用于生成签名的会话密钥的易损坏性，可以不时地刷新密钥。例如，可以每 4 小时刷新会话密钥。然而，为了保证即使刷新了会话密钥也允许继续进行对话，SIP 节点的密码程序可以存储和保持以前的会话密钥。可以把所存储的密钥存储预定的时间长度，诸如对于 RECORD-ROUTE 和 ROUTE SET 密钥在约 5 分钟到约 24 小时的范围内，而对于 VIA 密钥在约 5 分钟到约 30 分钟的范围内。另外或另一方面，可以保存会话密钥直到已经验证了使用该密钥签署的所有消息。为了保证访问正确的密钥以验证签名，密码程序可以把密钥标识符插入到签名中和 / 或在返回的 SIP 标题中附上作为另外参数的密钥标识符。

[0075] 在某些情况中，可以由服务器池来提供处理 SIP 消息的 SIP 节点。然而，不保证验证签名的服务器与生成签名的服务器是同一服务器。因此，服务器池中的服务器可能需要传送用于生成签名的密钥，以致如果用在池中的其它服务器处理消息，则这些服务器可以验证这些签名。在一个例子中，服务器可以彼此发送密钥或可以通过证书或其它合适的方法从密钥服务访问适当的密钥。然而，在服务器池中的服务器一般使它们之间的通信最小化来减少通信，并且访问密钥服务可能增加消息处理时间。因此，为了将会话密钥安全地从签名生成服务器传送到签名验证服务器，生成签名的服务器可以把经加密和经签署的会话密钥附在具有签名的消息的返回标题上。

[0076] 例如，可以通过包括第一服务器 300A 和第二服务器 300B 的服务器池来提供 SIP 节点 300，如在图 1 中的虚线所示。在某些情况中，可以通过 SIP 节点 300A 路由请求 500，而通过 SIP 节点 300B 路由来自被呼叫者的后续的对话内请求 700。因此，为了验证对话内请求中的 ROUTESET 签名 760，SIP 节点 300B 需要知道 SIP 节点 300A 使用的密钥，以生成 ROUTE SET 签名 560。如在图 4 中的示例请求 RECORD-ROUTE 标题所示，RECORD-ROUTE 标题，诸如 RECORD-ROUTE 标题 534，可以包括标准 SIP 处理下的典型网络位置信息，SIP 节点 300A 生成的 ROUTE SET 签名 560 以及表示 SIP 节点 300A 用来生成签名 560 的 ROUTE SET 密钥 580 的数据。

[0077] 然而，为了保证其它 SIP 节点不能访问消息标题中的 ROUTE SET 密钥 580，SIP 节点 300A 可以用公钥对 ROUTE SET 密钥加密。因此，为了验证该加密的完整性，SIP 节点可以用私钥来签署经加密的 ROUTESET 密钥。然后 SIP 节点 300A 可以把经加密和经签署的会话密钥插入到返回的标题中，诸如 RECORD-ROUTE 标题的 URI 参数，以把安全的会话密钥分发给能够访问用于加密和签署会话密钥的公钥 / 私钥对的服务器。可以插入经加密的会话密钥和经签署的会话密钥作为单个参数或作为多个参数。

[0078] 在某些情况中，可能要求利用两对公钥 / 私钥对来保护消息标题中的会话密钥。例如，可以通过证书系统来安装或访问第一公钥 / 私钥对和第二公钥 / 私钥对。在生成签名的 SIP 节点处，可以使用第一公钥 / 私钥对的第一公钥对会话密钥进行加密，并且可以使用第二公钥 / 私钥对的第二私钥签署会话密钥。如此，能够访问公钥 / 私钥对两者的接收 SIP 节点可以使用第二公钥 / 私钥对的第二公钥来验证签名的有效性，并且可以使用第一公钥 / 私钥对的第一私钥对会话密钥进行解密。

[0079] 通过公钥 / 私钥对加密和签署会话密钥可能有较大计算强度。因此，为了减少 SIP 节点上的负担，可以把经签署的经加密的会话密钥存储在与经解密的密钥信息、密钥的创建的日期 / 时间标记、密钥的到期日 / 时间和或其它信息相关联的密钥数据库中。如此，不需要在每次发送前都计算加密 / 签名。

[0080] 例如，如在图 6 中所示，当 SIP 节点 300B 接收具有包含 ROUTE SET 签名 760 的 RECORD-ROUTE 标题 724 的请求 700 时，SIP 节点 300B 可以检查 ROUTE SET 签名以识别使用了哪个 ROUTE SET 密钥来生成签名 560。在某些情况中，SIP 节点 300B 可以访问存储密钥的数据库以验证是否有经识别的 ROUTE SET 密钥 580 存储其中。如果没有存储 ROUTESET 密钥，则 SIP 节点 300B 可以访问公钥 / 私钥对，以从 ROUTE SET 标题中确定 ROUTE SET 密钥。更特别地，SIP 节点 300B 可以使用证书服务来访问公钥 / 私钥对，或可以从数据库或通过任何合适的方法或过程来检索公钥 / 私钥对。SIP 节点 300B 可以使用公钥来认证会

话密钥的签名。SIP 节点 300B 还可以使用私钥对 ROUTE SET 密钥 580 解密，然后使用该经解密的会话密钥来生成确认 ROUTE SET 签名。按相似的方式，可以把用来生成 VIA 标题和 RECORD-ROUTE 标题的会话密钥插入到返回标题中，尤其，可以插入到包含通过该会话密钥生成的签名的返回标题中。

[0081] 会话密钥可以单独进行加密，或可以在用公钥加密之前使其它信息和会话密钥包括在一起。相似地，可以单独对经加密的会话密钥进行签署，或另一方面，可以把经加密的会话密钥二进制大对象附在其它信息上，这些信息可以在全部用私钥签署之前进行加密或解密。如此，要求诸如密钥标识符、会话密钥到期日或任何其它信息之类的其它信息与经加密的 / 经签署的会话密钥一起发送。可以把另外的信息附到经加密的 / 经签署的会话密钥上，并且可以使用同一公钥 / 私钥对或其它合适的加密过程进行加密和 / 或签署。

[0082] 在某些情况中，接收经签署的和经加密的会话密钥的 SIP 节点可以确认会话密钥的到期时间和 / 或日期。在这方面，SIP 节点 300A 可以对会话密钥与会话密钥的创建的日期和 / 或时间标记一起进行加密和签署。当 SIP 节点 300B 接收对话内请求时，它可以如上所述地认证和解密会话密钥的签名和日期 / 时间标记。此外，SIP 节点 300B 可以将会话密钥的日期 / 时间标记和密钥的预期生命周期或存储的到期日 / 时间进行比较。如果密钥到期，则如果支持的话，SIP 节点 300B 可以发送出错消息，可以从它的处理栈中移除消息，和 / 或可以采取任何其它合适的行动。如果丢弃密钥是活动的，则 SIP 节点 300B 可以继续使用经解密的密钥来确认消息中对应的签名。

[0083] 在图 1 示出的综合性例子中，SIP 节点 300 可以生成 VIA 签名，并把该签名插入到返回的标题中，诸如请求 500 的 VIA 标题的标题参数。然后当被呼叫者发送对于该请求的响应 600 时，可以在 SIP 节点 300 处确认 VIA 签名。相似地，如果请求是对话启动请求，则 SIP 节点 300 可以生成 RECORD-ROUTE 签名，并且把该签名插入到返回的标题中，诸如请求 500 的 RECORD-ROUTE 标题的标题参数。然后当被呼叫者发送对于对话启动请求的响应 600 时，可以在 SIP 节点 300 处确认 RECORD-ROUTE 签名。此外，如果请求是对话启动请求，则 SIP 节点 300 还可以生成被呼叫者 ROUTE SET 签名，并且把该签名插入到返回的标题中，诸如请求 500 的 RECORD-ROUTE 标题的 URI 参数。被呼叫者 SIP 节点可以把 ROUTE SET 签名保存在它处，用作由该对话中的被呼叫者生成的任何未来请求中的 ROUTE 标题组。因此，要到请求中的被呼叫者使用被呼叫者 ROUTE SET 签名时才确认它。相似地，在对于对话启动请求的响应中，SIP 节点 200 可以生成呼叫者 ROUTE SET 签名，并且插入该签名作为 SIP 节点 200 的 RECORD-ROUTE 标题的 URI 参数。可以由呼叫者 SIP 节点保存呼叫者 ROUTE SET 签名，用作由呼叫者 SIP 节点生成的任何请求中的 ROUTE 标题组。如此，要到呼叫者在请求中发送呼叫者 ROUTE SET 签名时才对它进行验证。

[0084] 现在将参考图 8-14 描述 SIP 节点服务器的示例实现。

[0085] 图 1 中示出的呼叫者 SIP 节点 102、SIP 节点 200、SIP 节点 250、SIP 节点 300 和 / 或被呼叫者 SIP 节点 402 的任何组合都可存在，并且可以在作为 SIP 节点处理器的一台或多台计算机或其它设备上操作。这些节点的每一个可以在多个计算机系统或其它设备的全部或一部分上提供，和 / 或可以使用包括有线连接、无线连接等本技术领域中任何已知方法一起组成网络，以提供上述过程。

[0086] 在所示的实施例中，SIP 节点 300 由节点服务器 1300 提供，这将在下面参考图

8-14 来描述。可以通过相似的服务器 / 计算机系统来提供 SIP 节点 102、SIP 节点 250、SIP 节点 200 和 SIP 节点 402。

[0087] 如在图 8 中所示，节点服务器 1300 可以包括一个或多个通信端口 1302，通信端口 1302 可以包括一个或多个处理器 1304、内部日期和时间时钟 1306、以及存储 1308，存储 1308 包括定义指令的一个或多个计算机程序 1322，当执行这些指令时，指令计算机执行 SIP 节点 300 的操作。存储还可以包括联系图 9 更详细地描述的密钥数据库 1310，而下面将相对于图 10-14 讨论程序 1322。

[0088] 图 9 示出密钥数据库 1310 的示例表格 1350，它包括一个或多个记录 1352。一般而言，每个记录将会话密钥 1354 关于该密钥的附加信息相关联。在该例子中，每个记录 1352 包括密钥标识符 1353、会话密钥 1354、用公钥加密的经加密的密钥 1356、创建的日期 / 时间 1358 以及到期日 / 时间 1360。SIP 节点 300 可以生成会话密钥 1354 ；然而，SIP 节点可以从消息本身来识别会话密钥，从密钥服务或通过适合于生成用于签署数据的会话密钥的任何方法检索它。相似地，当 SIP 节点 300、消息本身或其它系统提供密钥信息时，可以初始化并更新其余的数据。

[0089] 密钥数据库可以是任何类型的数据库，包括关系型数据库、面向对象数据库、非结构化数据库、存储器内数据库或其它数据库。可以使用诸如 ACSII 文本、二进制文件、通过通信网络发送的数据之类的平面文件系统或任何其它文件系统来构造数据库。尽管有上述数据库的这些可能实现，然而此处所使用的术语数据库指的是以计算机可访问的任何方式收集和储存的任何数据。

[0090] 现在参考图 10-14，将描述 SIP 节点 300 执行的各种操作。更具体地，参考图 10 描述 VIA 签名的生成，参考图 11 描述 VIA 签名的验证。参考图 12 描述 RECORD-ROUTE 和 ROUTE SET 签名的生成，参考图 13 描述这些签名的确认。图 14 示出在服务器池中将会话密钥从一个服务器导入另一个服务器的操作。

[0091] 参考图 10，生成 VIA 签名的操作包括，但是不限于，接收 (900) SIP 请求。虽然参考 INVITE 请求来讨论上述附图，但是可以根据系统的安全性和处理要求对所有请求或选择的请求生成 VIA 签名。SIP 节点可以判定 (902) 将通过其转发响应的链路是否为不可信链路。如果链路是可信的，则 SIP 节点可以在 SIP 标准过程下继续进行请求的标准处理。如果转发链路是不可信的，则操作可以包括顺序地构造 (904) 除了处理节点的 VIA 标题之外的所有接收的 VIA 标题的 VIA 标题组。特别地，可以检查请求，并可以把所接收消息中存在的 VIA 标题存储在服务器 1300 存储器中。如果 VIA 标题组是空的 (906)，则可以继续进行消息的标准处理。如果存在一个以上 VIA 标题，则操作还包括识别 (908) VIA 密钥，如上所述，该密钥可以由服务器 1300 生成、从消息本身访问 (下面参考图 14 进一步描述)、或通过诸如因特网之类的装置从密钥服务中检索。然后可以生成 (910) VIA 签名，并且可以包括调用密码程序以生成存储在存储器中的 VIA 标题组的散列。可以生成 (912) 用于处理 SIP 节点 300 的 VIA 标题，并且可以把 VIA 签名作为标题参数的插入 (914) 到 SIP 节点 300 的 VIA 标题中。服务器 1300 可以把 VIA 会话密钥存储 (916) 在上面参考图 9 讨论的密钥数据库中，并且可以对诸如密钥标识符、密钥创建日期 / 时间、到期日 / 时间、经加密的密钥和 / 或其它信息之类的密钥参数进行初始化或更新。

[0092] 参考图 11，在生成请求中的 VIA 签名之后，SIP 节点可以接收 (918) 答复以前处理

的请求的响应。服务器可以检查响应的 VIA 标题，并且判定 (920) 是否存在一个以上 VIA 标题。如果只存在一个 VIA 标题，则可以继续进行消息的标准处理。如果存在一个以上 VIA 标题，则 SIP 节点可以判定 (922) 该响应是经过可信连接还是不可信连接接收的。如果链路是可信的，则可以继续进行消息的标准处理。如果链路是不可信的，则 SIP 节点 300 可以检查 SIP 节点 300 的 VIA 标题，并且判定 (924) 是否存在签名。如果不存在签名，则 SIP 节点 300 可以从它处理栈中丢弃该消息。如果存在签名，则 SIP 节点 300 可以从标题中剥去签名，并且把 VIA 签名保存 (926) 在存储器中，然后从消息中剥去 (928) 最上面的 VIA 标题 (例如，SIP 节点 300 的 VIA 标题)。SIP 节点可以从密钥数据库、密钥服务或消息本身检索 (930) 适当的 VIA 会话密钥。可以基于出现在签名本身、消息的日期 / 时间、签名的类型 (例如，VIA) 或适用于识别适当的 VIA 会话密钥的任何其它参数中存在的标识符来选择适当的密钥。SIP 节点可以生成 (932) 在响应中存在的其余 VIA 标题的 VIA 标题组。如果按消息中给出的次序用 VIA 标题生成 VIA 签名，则可以按相同次序生成验证 VIA 标题，以保证签名参数的正确次序。操作还包括基于 VIA 标题组和所检索的会话密钥生成 (934)VIA 确认签名，然后将该确认 VIA 签名和所存储的 VIA 签名进行比较 (936)。如果 VIA 签名匹配，则可以继续消息的标准处理。如果 VIA 签名不匹配，则 SIP 节点可以从它的处理栈中丢弃消息或采取任何其它合适的行动。

[0093] 参考图 12，生成 ROUTE SET 和 RECORD-ROUTE 签名的操作包括在 SIP 节点处接收 (938) 消息，并且判定 (940) 消息是否包含至少一个 RECORD-ROUTE 标题。如果消息不包含任何 RECORD-ROUTE 标题，则可以继续进行消息的标准处理。否则，SIP 服务器可以判定 (944) 是否将经过可信或不可信链路发送消息。更具体地，SIP 服务器可以判定是否将经过可信或不可信链路接收要确认的消息。如果响应链路是可信的，则可以继续进行标准处理。如果链路是不可信的，则 SIP 服务器可以判定 (946) 所接收的消息是否为请求。如果消息不是请求，则 SIP 服务器可以基于响应中的 RECORD-ROUTE 标题构造 (948)RECORD-ROUTE 标题组。如果消息是请求，则 SIP 服务器可以构造 (950)RECORD-ROUTE 标题组，并且识别 (951)RECORD-ROUTE 会话密钥，如上所述，该会话密钥可以由服务器 1300 生成、从消息本身访问 (下面参考图 14 进一步讨论)、或通过诸如因特网之类的装置从密钥服务检索。然后可以生成 (952)RECORD-ROUTE 签名，并且可以包括调用密码程序以生成存储在存储器中的 RECORD-ROUTE 标题组的 URI 部分的散列。可以把 RECORD-ROUTE 签名作为标题参数插入 (954) 到 SIP 节点 300 的 RECORD-ROUTE 标题中。服务器 1300 可以在上面参考图 9 讨论的密钥数据库中存储 (956)RECORD-ROUTE 会话密钥，并且可以对诸如密钥标识符、密钥创建日期 / 时间、到期日 / 时间和 / 或经加密的密钥之类的密钥参数进行初始化和 / 或更新。不管消息是否为请求，SIP 服务器可以判定 (942) 在所接收的消息中是否存在一个 CONTACT 标题。如果不存在，则可以继续进行标准处理 ；否则 SIP 节点可以从 RECORD-ROUTE 标题组和 CONTACT 标题构造 (958)ROUTE 标题组。然后 SIP 服务器可以识别 (960)ROUTE SET 组会话密钥，并且使用该密钥可以生成 (962)ROUTE SET 签名，然后可以把 ROUTE SET 签名作为 URI 参数插入 (962) 到 SIP 节点 300 的 RECORD-ROUTE 标题中。SIP 节点可以在上述密钥数据库中保存 (966)ROUTE SET 会话密钥和密钥参数。然后 SIP 服务器可以继续进行消息的标准处理。

[0094] 参考图 13，当 SIP 节点接收 (968) 响应时，可以发生 RECORD-ROUTE 签名的确认。

SIP 节点可以判定 (970) 在消息中是否存在任何 RECORD-ROUTE 标题。如果没有，则可以继续进行消息的标准处理；否则，SIP 节点可以判定 (972) 是否经过不可信链路接收响应。如果链路是可信的，则可以继续进行消息的标准处理。如果链路是不可信的，则 SIP 节点可以判定 (974)SIP 节点的 RECORD-ROUTE 标题是否包含 RECORD-ROUTE 签名。如果没有，则可以从 SIP 节点 300 的处理栈中丢弃消息。如果存在 RECORD-ROUTE 签名，则 SIP 节点服务器可以剥去和保存 (976)SIP 节点 300 的 RECORD-ROUTE 标题中的所有签名。例如，SIP 节点 300 的 RECORD-ROUTE 标题可以包含 RECORD-ROUTE 签名和 ROUTE SET 签名两者。只要它们的位置在整个对话中是一致的，和 / 或按合适的方式识别签名以区分多个签名，它们中的每一个都可以列出在 RECORD-ROUTE URI 参数的第一个上。例如，插入到具有多个签名的标题中的每个签名可以包括指定标题类型的标识符，和 / 或每个签名都可以伴随有识别所插入的签名的类型的附加参数。SIP 节点可以构造 (978) 包含消息标题中的 RECORD-ROUTE 标题的 URI 部分的 RECORD-ROUTE 标题。SIP 节点还可以根据相对于图 11 的操作 930 所讨论的过程来检索 (980) 适当的 RECORD-ROUTE 会话密钥。SIP 节点可以基于 RECORD-ROUTE 标题组和会话密钥生成 (982) 确认 RECORD-ROUTE 签名，然后将确认 RECORD-ROUTE 签名和所存储的 RECORD-ROUTE 签名进行比较 (984)。如果签名不匹配，SIP 节点可以从它的处理栈中丢弃消息。如果签名匹配，则可以继续进行标准处理。如果存在作为 RECORD-ROUTE 标题的 URI 参数的 ROUTE SET 签名，则 SIP 节点服务器可以把这个签名从消息和 / 或存储器中删除 (986)。更特别地，被呼叫者 ROUTE SET 签名已由被呼叫者 SIP 节点保存，因此，在定向到呼叫者的当前消息中不再需要。为了判定是否应该生成呼叫者的新 ROUTE SET 签名，并且发送给被呼叫者，SIP 节点可以判定 (987) 下一个 SIP 节点是否通过不可信链路，并且存在至少一个 CONTACT 标题。如果不是，则可以继续进行消息的标准处理。如果下一个链路是不可信的，则 SIP 节点服务器可以通过检索 (988)ROUTE SET 会话密钥 (它可以与 RECORD-ROUTE 密钥为相同的密钥) 来生成呼叫者 ROUTE SET 签名。使用该密钥，SIP 节点可以基于 RECORD-ROUTE 标题组和第一列出 CONTACT 标题的 URI 部分来生成 (990)ROUTE SET 签名。可以把 ROUTE SET 签名插入 (922) 到要传送到呼叫者 SIP 节点 102 的 SIP 节点 300 的 RECORD-ROUTE 标题中。SIP 节点可以把 ROUTESET 会话密钥和 / 或 RECORD ROUTE 会话密钥以及密钥参数保存 (994) 在上述密钥数据库中。然后 SIP 服务器可以进行消息的标准处理。在后续请求中的被呼叫者 ROUTE SET 签名和 / 或呼叫者 ROUTE SET 签名的确认可以遵循上述相似的过程。

[0095] 图 14 示出在服务器池中的服务器之间传送会话密钥的一个示例实施中的操作。例如，如上所述，可以由服务器 300A 和服务器 300B 提供 SIP 节点 300。如此，SIP 节点 300A 可以生成具有会话密钥的签名，然后要求 SIP 节点 300B 确认该签名。虽然参考 ROUTE SET 标题描述下列例子，但是可以使用相似的过程对 RECORD ROUTE 会话密钥和 / 或 VIA 会话密钥进行加密、签署和访问。

[0096] 如在图 14 中所示，可以生成 (996) 公钥 / 私钥对的公共证书，并且安装 (998) 在服务器池中的每个服务器上 (300A、300B)。如上所述，可以使用公钥 / 私钥对来签署和加密该节点处理的所有会话密钥，或每个类型的会话密钥 (VIA、RECORD-ROUTE 和 / 或 ROUTE SET) 可以具有不同的公钥 / 私钥对。在操作中，SIP 节点 300A 可以接收 (1000) 需要被签署的请求。如上所述，SIP 节点服务器可以通过生成、访问或检索 ROUTE SET 会话密钥而识

别 (1002) 它。SIP 节点还可以验证 (1004) 该证书被配置成路由关于密钥交换的信息。SIP 服务器可以判定 ROUTESET 会话密钥的创建日期 / 时间标记，并且把日期 / 时间标记附在会话密钥上。SIP 服务器可以使用公钥对会话密钥和日期 / 时间标记进行加密 (1008)，并且用私钥签署 (1010) 结果。可以把经加密和经签署的会话密钥的结果与诸如日期 / 时间标记、会话密钥、会话密钥标识符等密钥参数一起存储 (1012) 在上面参考图 9 描述的密钥数据库中。SIP 节点可以使用 ROUTE SET 会话密钥如上参考图 12 所述地生成 ROUTESET 签名，并且生成 (1014)SIP 节点 300 的 RECORD-ROUTE 标题。SIP 节点服务器可以把 ROUTE SET 签名插入 (1018) 到 SIP 节点的 RECORD-ROUTE 标题中，并且还可以把经签署和经加密的 ROUTE SET 会话密钥作为 URI 参数插入 (1020) 到 SIP 节点 RECORD-ROUTE 标题中。

[0097] 在被呼叫者已经接收到请求之后，它将把 RECORD-ROUTE 标题和 CONTACT 标题的 URI 部分保存在 ROUTE 标题组中。当被呼叫者 SIP 节点生成后续的对话内请求时，被呼叫者 SIP 节点可以包括 ROUTE SET 标题，该 ROUTE SET 标题返回包含 SIP 节点 300A 生成的 ROUTE SET 签名和 ROUTE SET 会话密钥的 RECORD-ROUTE 和 CONTACT 标题。第二 SIP 节点 300B 可以接收 (1022) 具有至少一个 ROUTE 标题的对话内请求。鉴于检索 (930) 上面参考图 12 所述的适当的会话密钥，SIP 节点可以从 ROUTE 标题中提取 (1024) 经签署和经加密的 ROUTE SET 会话密钥，并且将经签署和经加密的密钥和密钥数据库中的条目进行比较 (1026)，以判定服务器节点 300B 是否能够访问经解密的会话密钥。如果是匹配的，则 SIP 节点 300B 可以使用来自密钥数据库的会话密钥确认 ROUTE 标题中的 ROUTE SET 签名。如果不匹配，则 SIP 节点可以提取 (1028) 密钥签名，并且用公钥验证 (1030) 密钥签名。如果没有验证签名，则 SIP 节点可以从它的处理栈中丢弃消息，或采取任何其它合适的行动。如果签名是匹配的，则可以提取 (1032) 经加密的会话密钥。如果密钥不再活动 (例如，到期)，则可以独立于会话密钥对日期 / 时间标记进行解密 (1034)，以使服务器资源最小化。更具体地，在解密以验证日期 / 时间标记在该类型会话密钥的配置生命周期内之后，SIP 节点可以确认 (1036) 日期 / 时间标记。如果不能够验证日期 / 时间标记，则可以从处理栈中丢弃消息。如果验证日期 / 时间标记，则可以用私钥对会话密钥解密 (1038)，然后使用它确认 (1040) ROUTE SET 签名。可以把经解密的会话密钥的结果与诸如日期 / 时间标记、经签署和经加密的会话密钥、会话密钥标识符等密钥参数一起存储 (1042) 在上面参考图 9 描述的密钥数据库中。在某一时刻，诸如当完成该对话时、不再期望使用该会话密钥的更多的标题时，在会话密钥的活动生命周期的结束处、和 / 或在它的到期日之后，会话密钥可以到期，可以从数据库中清除 (1044) 该会话密钥的数据库记录，包括会话密钥、经签署和经加密的会话密钥等。

[0098] 可以用来独立地或组合地实现图 1 和 / 或图 8 的 SIP 节点的各个元件的计算机系统一般包括连接到输出设备 (向用户显示信息) 和输入设备 (从用户接收信息) 两者的至少一个主单元。主单元可以包括经由互连机制连接到存储器系统的处理器。还经由互连机制把输入设备和输出设备连接到处理器和存储器系统。

[0099] 图 1 和 / 或图 8 中示出的计算设备一般包括某些形式的计算机可读介质。计算机可读介质可以是 SIP 服务器中的其它计算设备可以访问的任何可用的介质。作为例子，而不是限制，计算机可读介质可以包括计算机存储介质和通信介质。计算机存储介质包括按任何方法或技术实施的、用于诸如计算机可读出指令、数据结构、程序模块或其它数据之类

的信息存储的易失性和非易失性、可移动和不可移动介质。计算机存储介质包括，但是不限于，RAM、ROM、EEPROM、闪存或其它存储器技术、CD-ROM、数字多功能盘（DVD）和其它光存储器、盒式磁带、磁带、磁盘存储器或其它磁性存储设备、或可以用来存储所需要的信息并且SIP节点中的计算机系统可以访问的任何其它介质。通信介质一般在已调制数据信号（诸如载波或其它传输机制）中包含算机可读指令、数据结构、程序模块或其它数据，，并且包括任何信息传送介质。作为例子，而不是限制，通信介质包括有线介质，诸如有线网或直接的有线连接，以及无线介质，诸如声音、RF、红外和其它无线介质。上述的任何组合也可以包括在计算机可读介质的范围内。

[0100] 可以把一个或多个输出设备和一个或多个输入设备连接到计算机系统。本发明不限于用于计算机系统或对于这里所描述的为特定的输入或输出设备。

[0101] 计算机系统可以是可使用计算机编程语言（诸如SmallTalk、C++、Java、Ada或C#(C-sharp)）或其它语言（诸如脚本语言，甚至汇编语言）编程的通用计算机系统。可以在非编程环境（例如，以HTML、XML或其它格式创建的文件，当在浏览器程序的一个视窗中观看时，呈现图形用户界面的各方面或执行其它功能）中实现本发明的各个方面。本发明的各个方面可以被实现为编程的或非编程的元件或它们的任何组合。计算机系统还可以是特别编程的、专用硬件或专用集成电路（ASIC）。阅读器系统还可以包括寻呼器、电话、个人数字助理或其它电子数据通信设备。

[0102] 在通用通信系统中，处理器一般是市场上可买到的处理器，诸如可从Intel公司得到的众知的Pentium ®处理器。许多其它处理器也是可用的。这种处理器通常执行一个操作系统，例如，操作系统可以是可从Microsoft公司得到的Windows 95 ®、Windows 98 ®、Windows NT ®、Windows 2000 ®或Windows XP ®、可从Apple计算机公司得到的MAC OS系统X、可从Sun Microsystems得到的Solaris操作系统、或从各种来源得到的UMIX。可以使用许多其它操作系统。

[0103] 处理器和操作系统一起定义对其以高级编程语言书写应用程序的计算机平台。应该理解，本发明不限于特定的计算机系统平台、处理器、操作系统或网络。还有，本领域的技术人员应该明白，本发明不限于特定的编程语言或计算机系统。此外，应该理解，也可以使用其它适当的编程语言和其它适当的计算机系统。

[0104] 可以在耦合到通信网络的一个或多个计算机系统（未示出）上分布计算机系统的一个或多个部分。这些计算机系统也可以是通用计算机系统。例如，可以把本发明的各个方面分布在一个或多个计算机系统间，这些计算机系统可以被配置成向一个或多个客户机计算机提供服务（例如，服务器）或作为分布式系统的一部分执行总任务。例如，可以在客户机-服务器系统上执行本发明的各个方面，所述客户机-服务器系统包括根据本发明的各个实施例执行各种功能的一个或多个服务器系统中分布的组件。这些组件可以是可执行的、中间（例如，IL）或解释（例如，Java）代码，这些代码可以使用通信协议（例如，SIP或TCP/IP）经过通信网络（例如，因特网）进行通信。应该理解，本发明不限于在任何特定系统或系统组上执行。

[0105] 现在已经描述了本发明的一些说明性实施例，本领域的技术人员会明白，上述说明只是说明性的而不是限制，只是作为例子而提供。许多修改和其它说明性实施例都在本

领域的技术人员的范围内，并且可以设想为落在本发明的范围内。特别地，虽然这里提供的许多例子涉及方法操作或系统元件的特定组合，但是应该理解，可以按其它方式组合这些操作和这些元件来实现相同的目的。只联系一个实施例所讨论的操作、元件和特征并不意味着排除在其它实施例中相似作用之外。此外，在权利要求书中使用按顺序的术语（诸如“第一”和“第二”）来修改权利要求元素的本身并不意味着任何优先级、特权或一个权利要求元素对于另一个的次序或执行方法的操作的临时次序，而只是用于作为标号来区分具有某个名称的权利要求元素和具有相同名称的另一个元素（但是使用按顺序的术语），来区分权利要求元素。

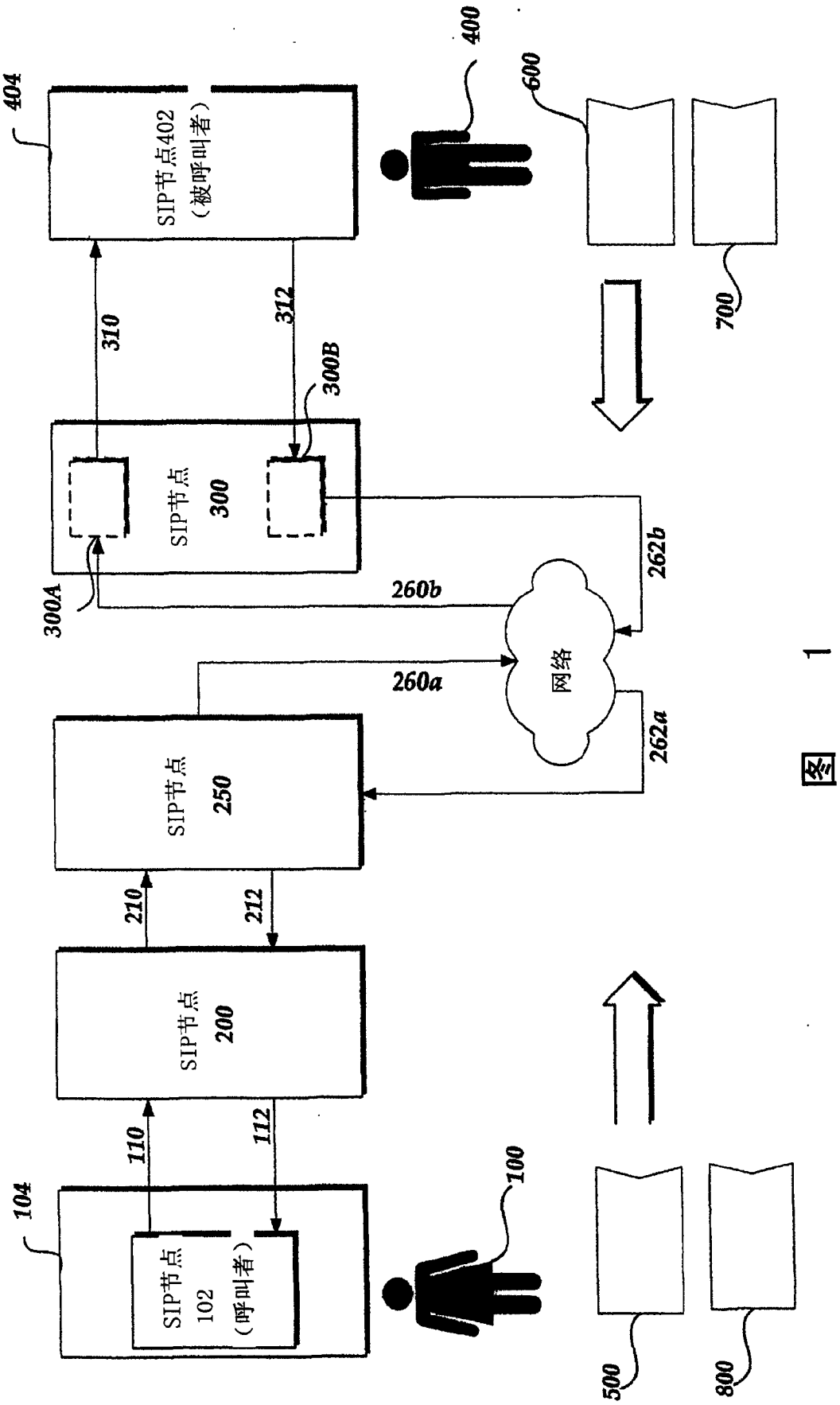

404
SIP节点402
（被呼叫者）
400
600
700
310
312
300B
SIP节点
300
300A
260b
262b
网络
260a
262a
SIP节点
250
210
212
SIP节点
200
110
112
104
SIP节点
102
（呼叫者）
100
500
800

图 1

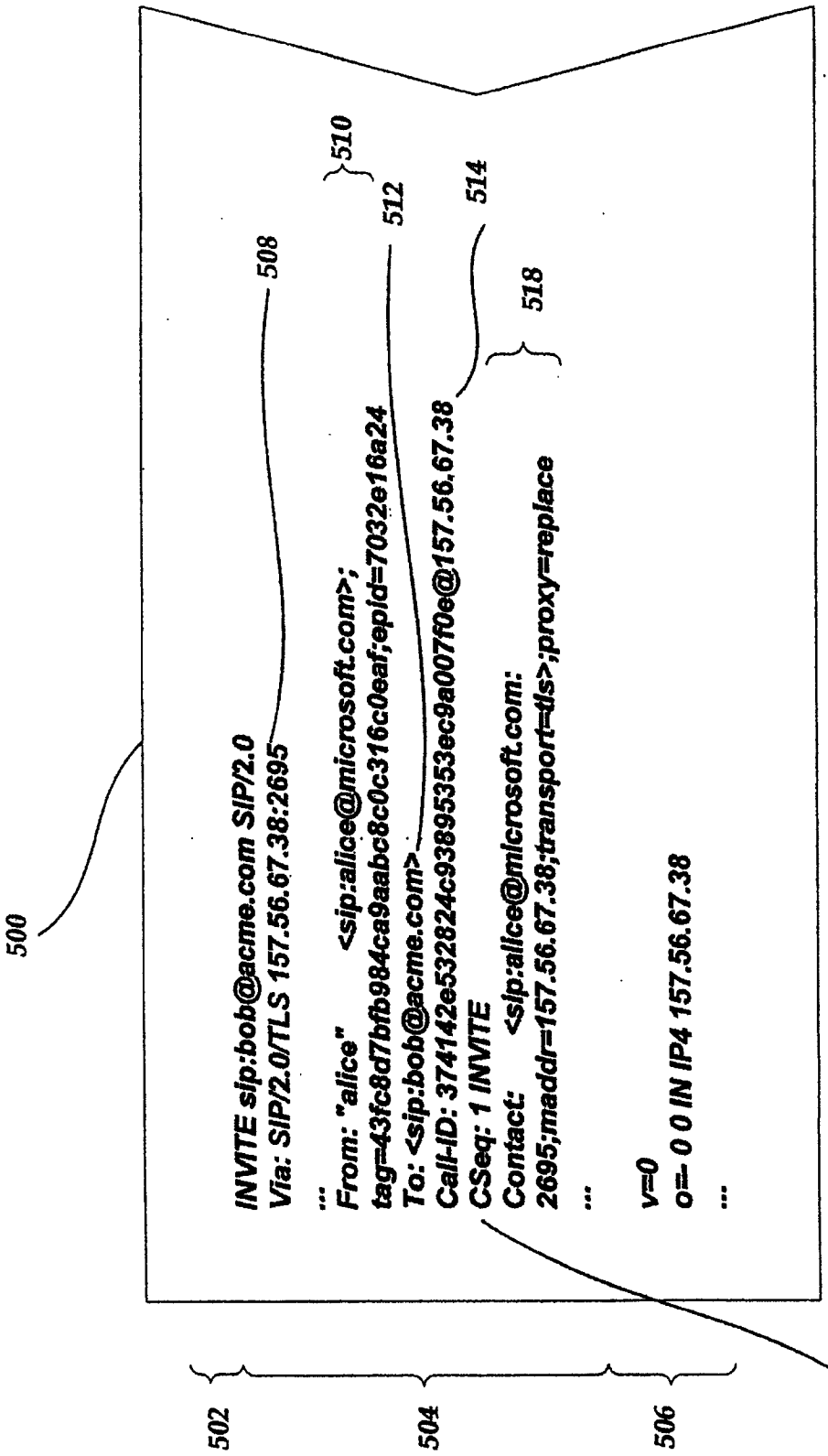

500
INVITE sip:bob@acme.com SIP/2.0
Via: SIP/2.0/TLS 157.56.67.38:2695
...
From: "alice" <sip:alice@microsoft.com>;
tag=43fc8d7bfb984ca9aabc8c0c316c0eaf;epid=7032e16a24
To: <sip:bob@acme.com>
Call-ID: 374142e532824c93895353ec9a007f0e@157.56.67.38
CSeq: 1 INVITE
Contact: <sip:alice@microsoft.com:
2695;maddr=157.56.67.38;transport=tls>;proxy=replace
...
v=0
o=- 0 0 IN IP4 157.56.67.38
...
502
504
506
508
510
512
514
516
518

图 2

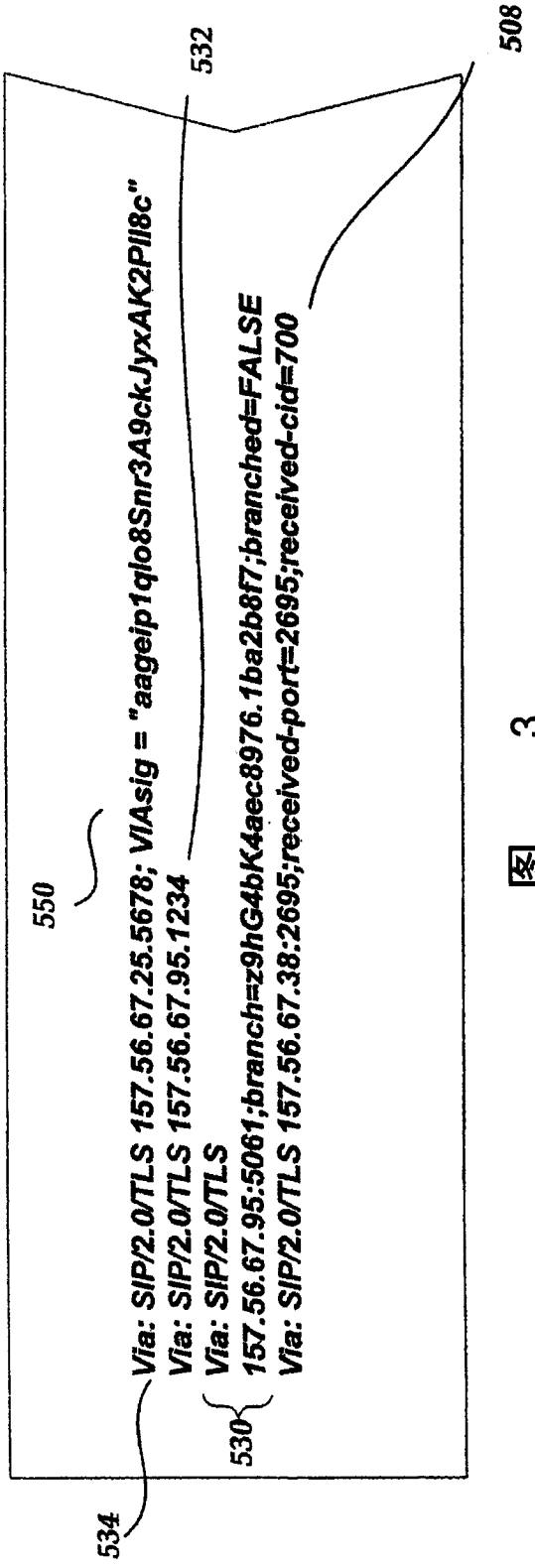

550
Via: SIP/2.0/TLS 157.56.67.25.5678; VIAsig = "aageip1qlo8Snr3A9ckJyxAK2Pll8c"
Via: SIP/2.0/TLS 157.56.67.95.1234
Via: SIP/2.0/TLS
157.56.67.95:5061;branch=z9hG4bK4aec8976.1ba2b8f7;branched=FALSE
Via: SIP/2.0/TLS 157.56.67.38:2695;received-port=2695;received-cid=700
532
508
534
530

图 3

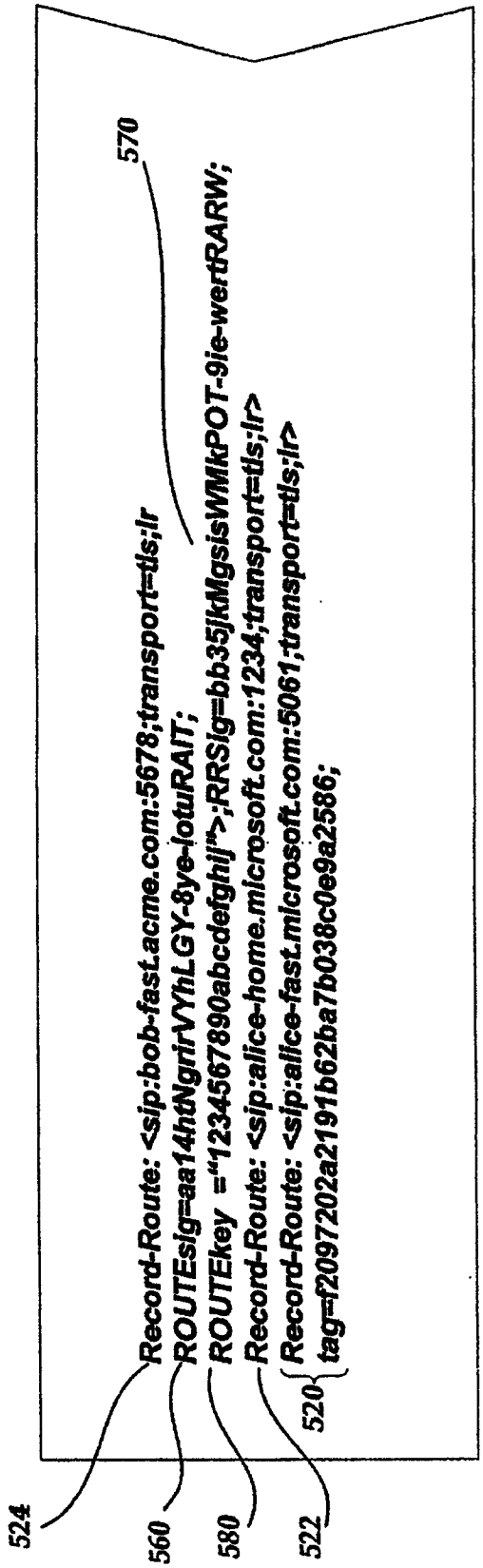

570
Record-Route: <sip:bob-fast.acme.com:5678;transport=tls;lr
ROUTEsig=aa14htNgrirVYhLGY-8ye-ioturAIT;
ROUTEkey ="12345678900abcdefghij">;RRSig=bb35jkMgsisWMkPOT-9ie-wertRARW;
Record-Route: <sip:alice-home.microsoft.com:1234;transport=tls;lr>
Record-Route: <sip:alice-fast.microsoft.com:5061;transport=tls;lr>
tag=f2097202a2191b62ba7b038c0e9a2586;
524
560
580
522
520

图 4

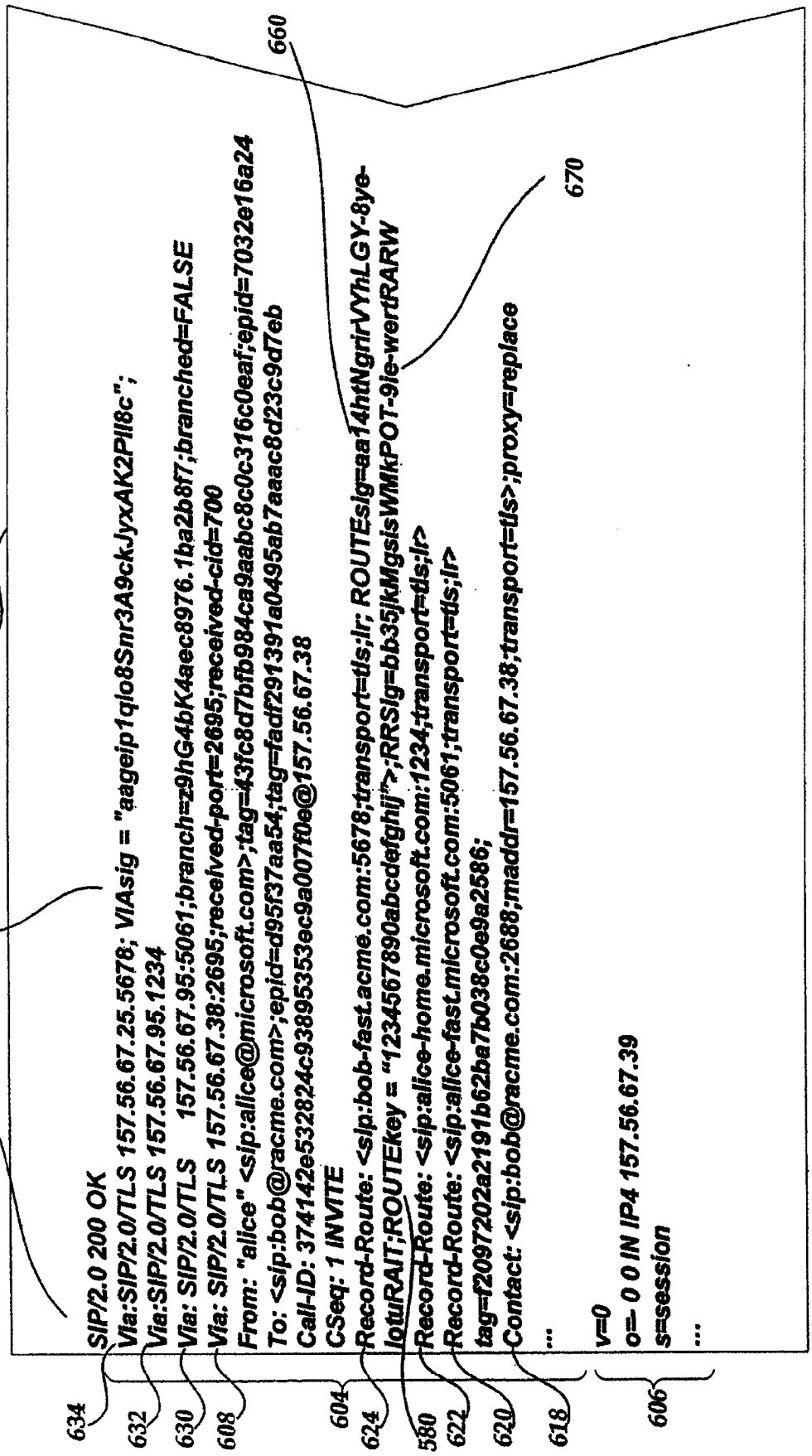

600
602
650
660
670
SIP/2.0 200 OK
Via:SIP/2.0/TLS 157.56.67.25.5678; VIAsig = "aageip1qlo8Snr3A9ckJyxAK2Pll8c";
Via:SIP/2.0/TLS 157.56.67.95.1234
Via: SIP/2.0/TLS 157.56.67.95:5061;branch=z9hG4bK4aec8976.1ba2b8f7;branched=FALSE
Via: SIP/2.0/TLS 157.56.67.38:2695;received-port=2695;received-cid=700
From: "alice" <sip:alice@microsoft.com>;tag=43fc8d7bfb984ca9aabc8c0c316c0eaf;epid=7032e16a24
To: <sip:bob@racme.com>;epid=d95f37aa54;tag=fadf291391a0495ab7aaac8d23c9d7eb
Call-ID: 374142e532824c93895353ec9a007f0e@157.56.67.38
CSeq: 1 INVITE
Record-Route: <sip:bob-fast.acme.com:5678;transport=tls;lr; ROUTEsig=aa14htNgrirVYhLGY-8ye-
IoturAIT;ROUTEkey = "1234567890abcdefghij">;RRSig=bb35jkMgsisWMkPOT-9ie-wertRARW
Record-Route: <sip:alice-home.microsoft.com:1234;transport=tls;lr>
Record-Route: <sip:alice-fast.microsoft.com:5061;transport=tls;lr>
tag=f2097202a2191b62ba7b038c0e9a2586;
Contact: <sip:bob@racme.com:2688;maddr=157.56.67.38;transport=tls>;proxy=replace
...
v=0
o=- 0 0 IN IP4 157.56.67.39
s=session
...
634
632
630
608
604
624
580
622
620
618
606

图 5

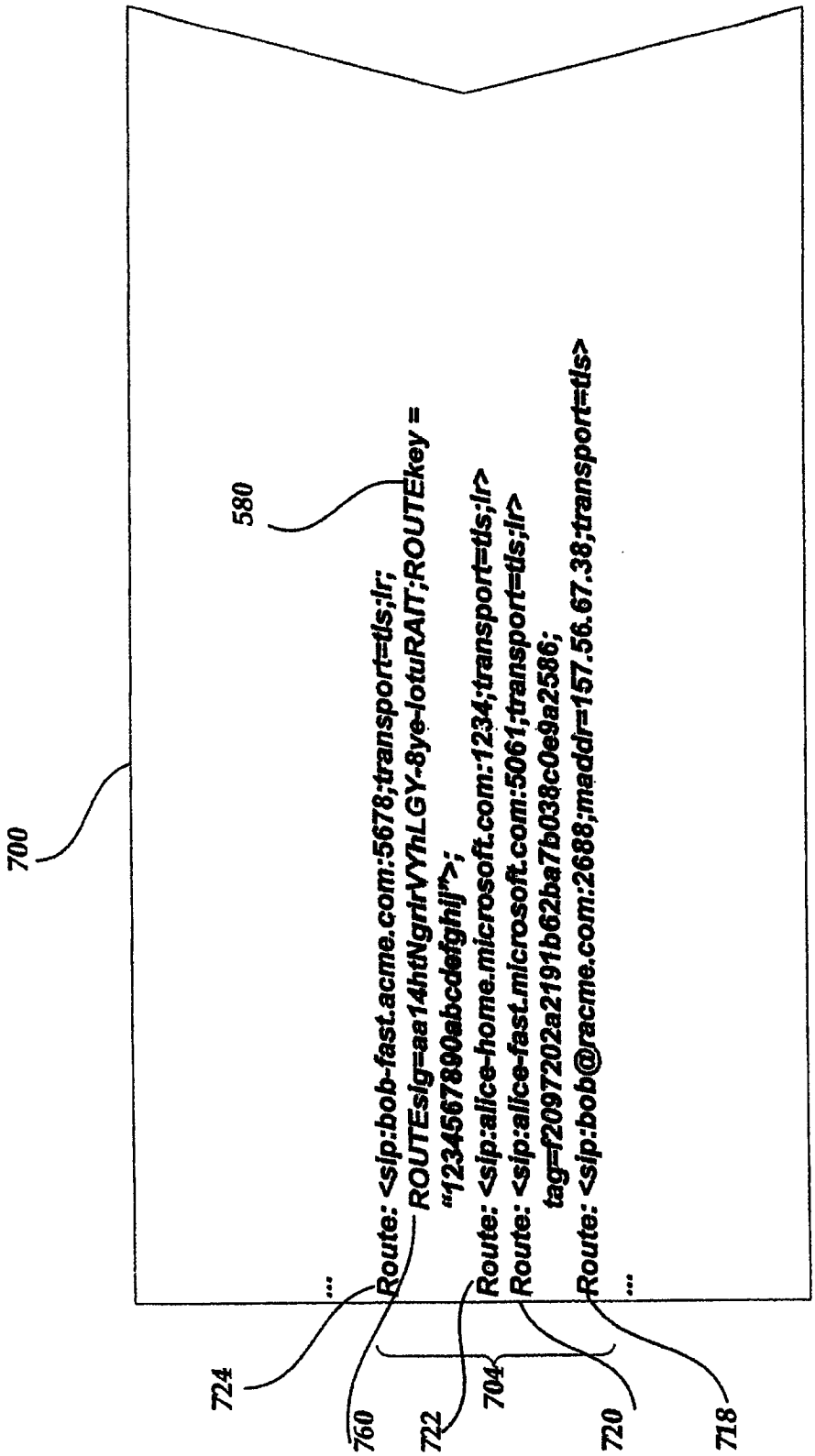

700
580
...
Route: <sip:bob-fast.acme.com:5678;transport=tls;lr;
ROUTEsig=aa14htNgrirVYhLGY-8ye-IotuRAIT;ROUTEkey =
"1234567890abcdefghij">;
Route: <sip:alice-home.microsoft.com:1234;transport=tls;lr>
Route: <sip:alice-fast.microsoft.com:5061;transport=tls;lr>
tag=f2097202a2191b62ba7b038c0e9a2586;
Route: <sip:bob@racme.com:2688;maddr=157.56.67.38;transport=tls>
...
724
760
722
704
720
718

图 6

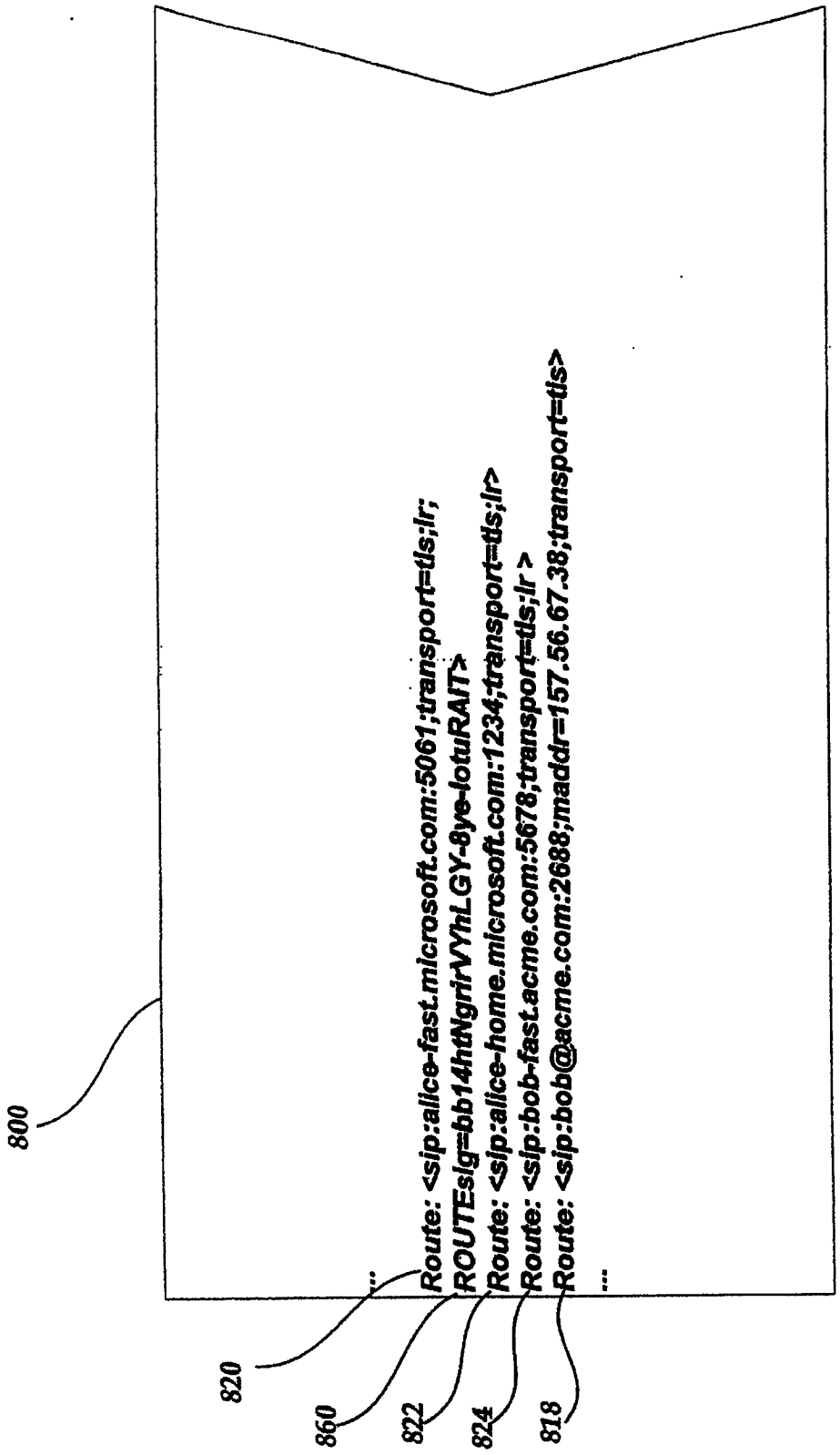

800
820
860
822
824
818
...
Route: <sip:alice-fast.microsoft.com:5061;transport=tls;lr;
ROUTEsig=bb14htNgrirVYhLGY-8ye-IotuRAIT>
Route: <sip:alice-home.microsoft.com:1234;transport=tls;lr>
Route: <sip:bob-fast.acme.com:5678;transport=tls;lr >
Route: <sip:bob@acme.com:2688;maddr=157.56.67.38;transport=tls>
...

图 7

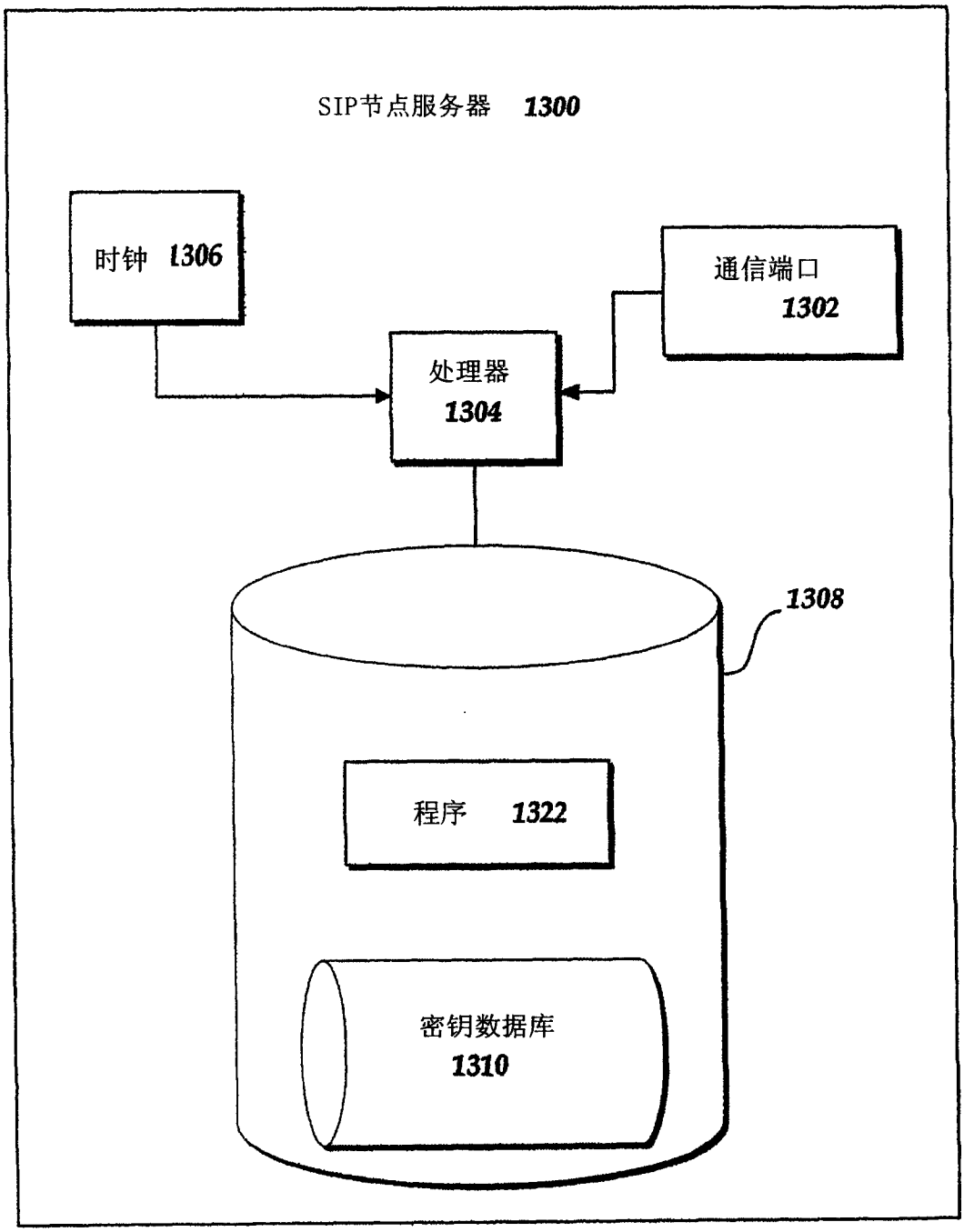

SIP节点服务器 1300
时钟 1306
通信端口 1302
处理器 1304
1308
程序 1322
密钥数据库 1310

图 8

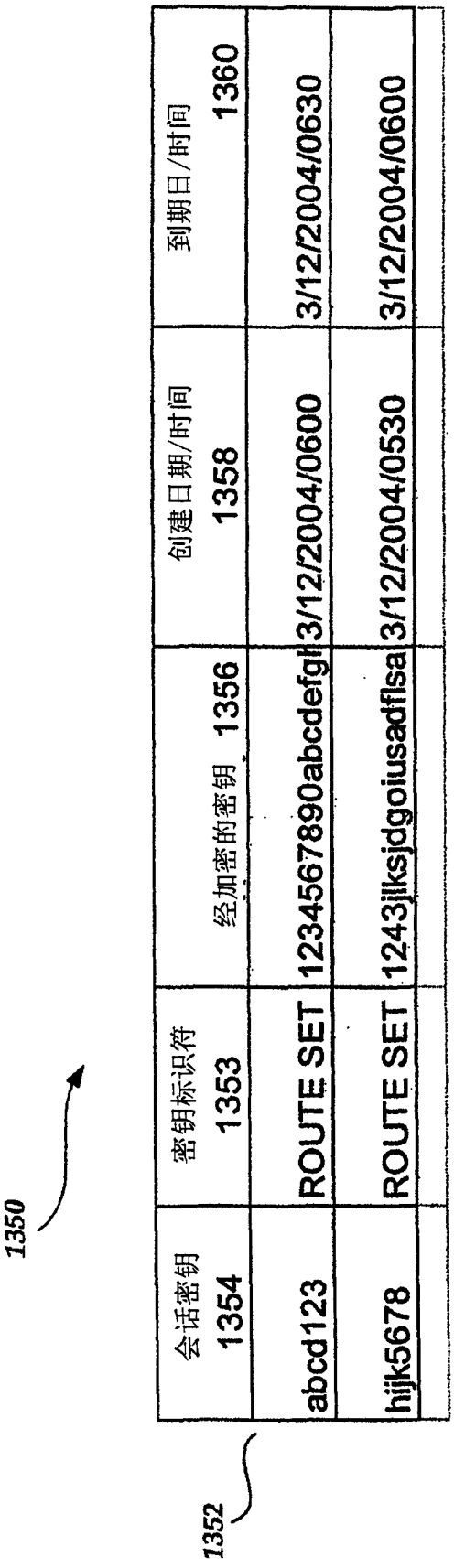

1350
1352
会话密钥 1354
密钥标识符 1353
经加密的密钥 1356
创建日期/时间 1358
到期日/时间 1360
abcd123
ROUTE SET
1234567890abcdefgh
3/12/2004/0600
3/12/2004/0630
hijk5678
ROUTE SET
1243ijksjdgoiusadflsa
3/12/2004/0530
3/12/2004/0600

图 9

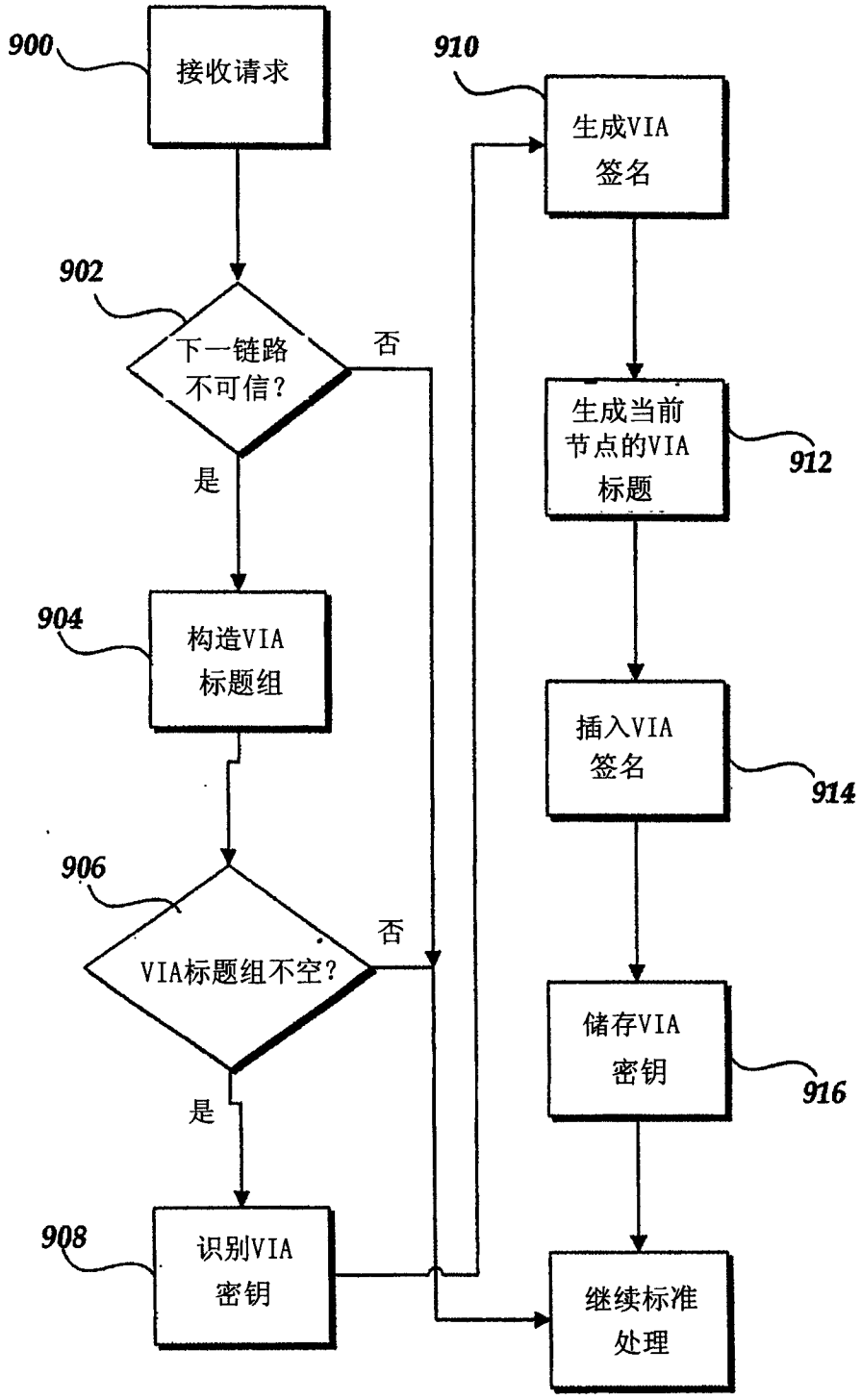

900
接收请求
902
下一链路不可信?
否
是
904
构造VIA标题组
906
VIA标题组不空?
否
是
908
识别VIA密钥
910
生成VIA签名
生成当前节点的VIA标题
912
插入VIA签名
914
储存VIA密钥
916
继续标准处理

图 10

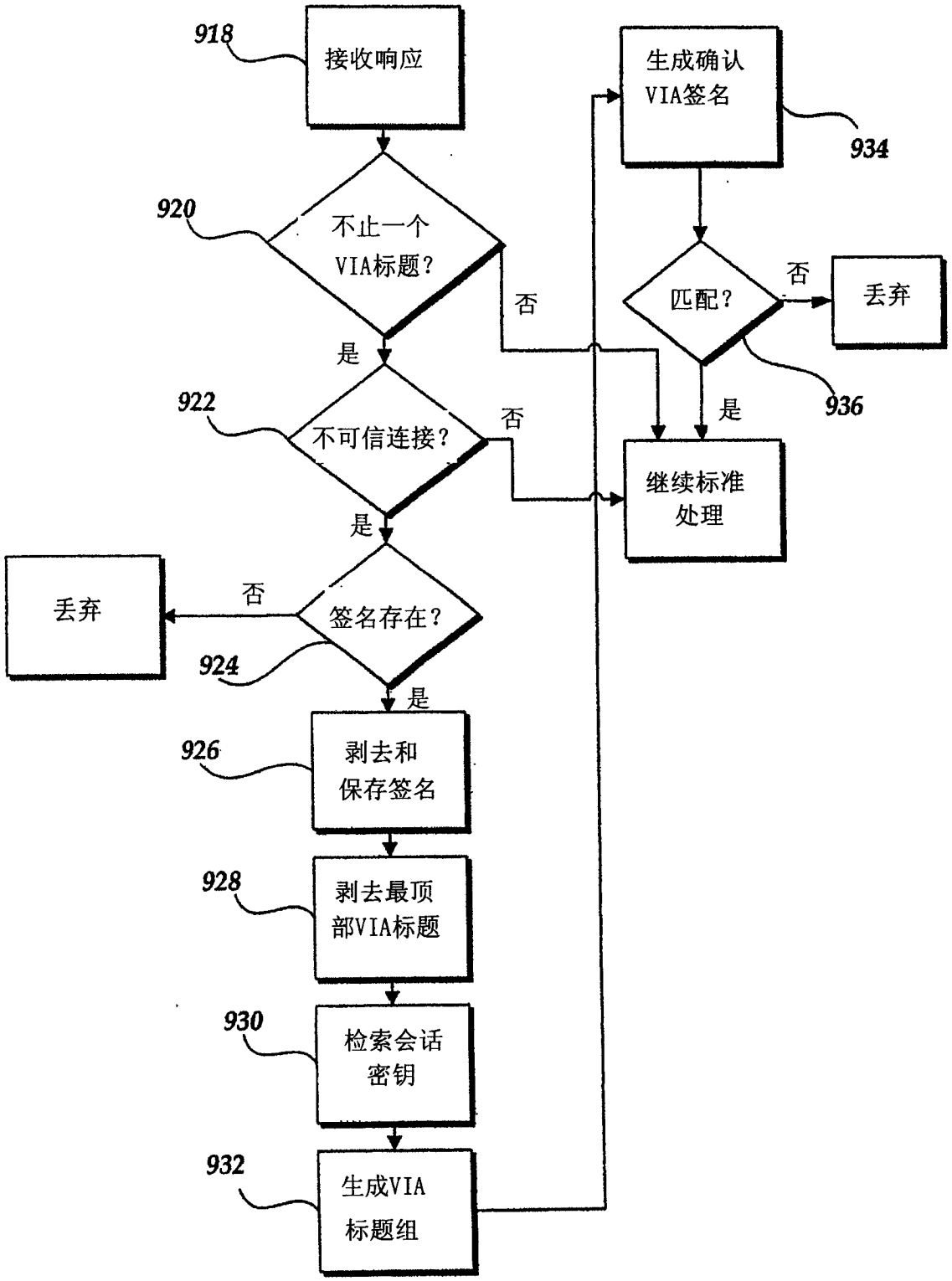

918
接收响应
920
不止一个VIA标题?
否
是
922
不可信连接?
否
是
丢弃
否
签名存在?
924
是
926
剥去和保存签名
928
剥去最顶部VIA标题
930
检索会话密钥
932
生成VIA标题组
生成确认VIA签名
934
匹配?
否
丢弃
是
936
继续标准处理

图 11

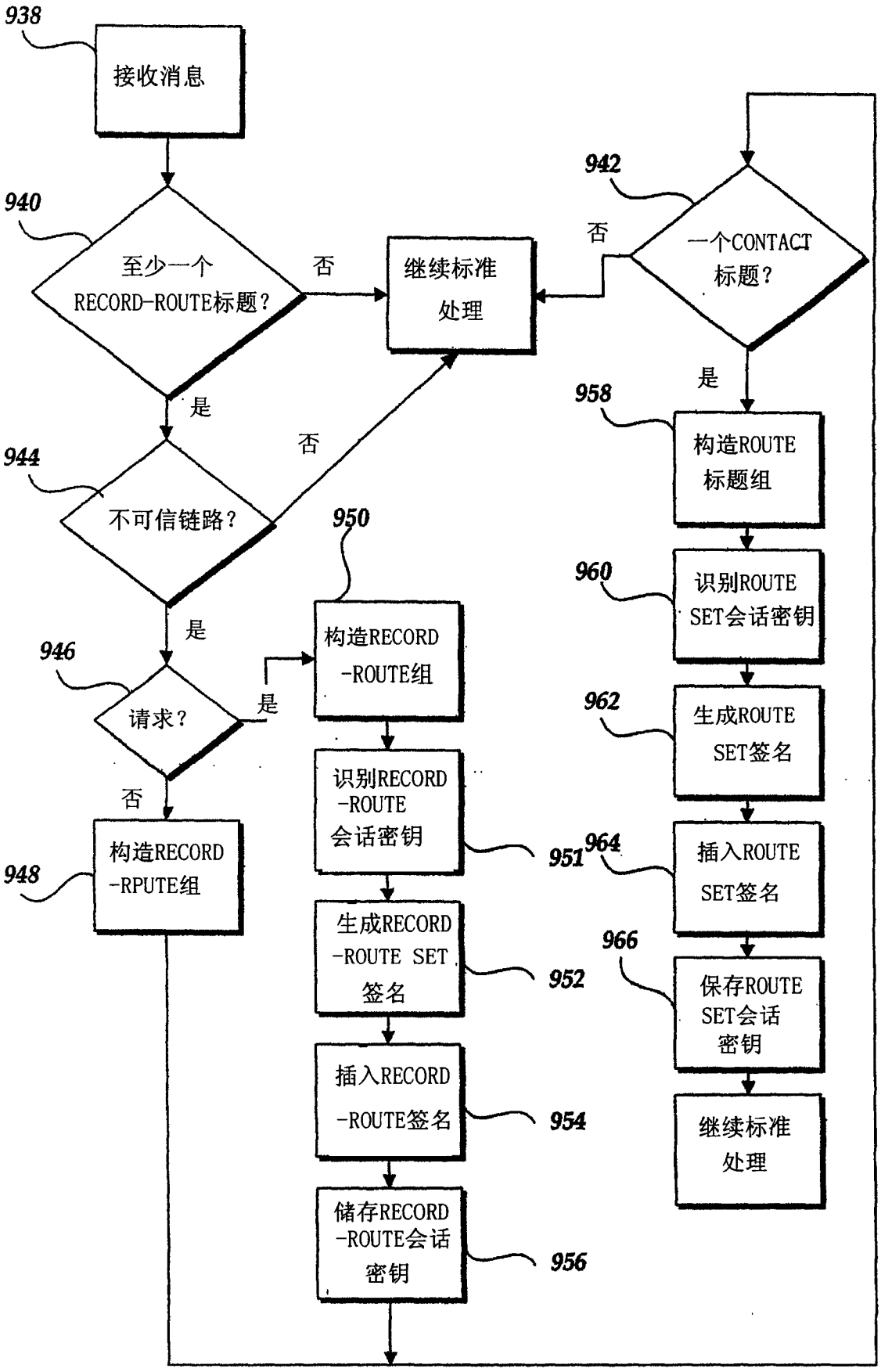

938
接收消息
940
至少一个 RECORD-ROUTE标题?
否
继续标准处理
是
944
不可信链路?
否
是
946
请求?
是
否
948
构造RECORD -RPUTE组
950
构造RECORD -ROUTE组
识别RECORD -ROUTE 会话密钥
951
生成RECORD -ROUTE SET 签名
952
插入RECORD -ROUTE签名
954
储存RECORD -ROUTE会话密钥
956
942
一个CONTACT 标题?
否
是
958
构造ROUTE 标题组
960
识别ROUTE SET会话密钥
962
生成ROUTE SET签名
964
插入ROUTE SET签名
966
保存ROUTE SET会话密钥
继续标准处理

图 12

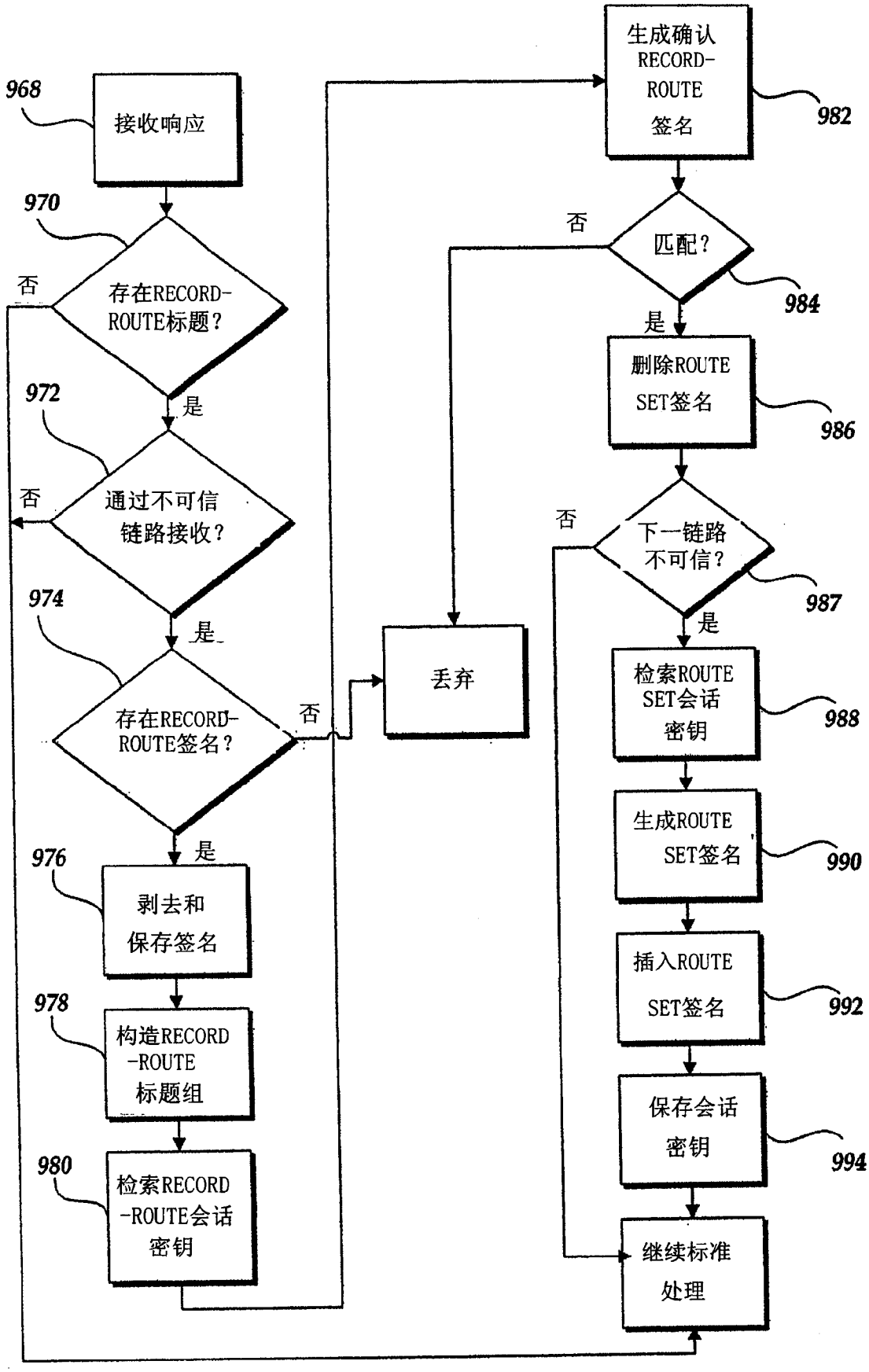

968
接收响应
970
存在RECORD-ROUTE标题?
否
是
972
通过不可信链路接收?
否
是
974
存在RECORD-ROUTE签名?
否
是
976
剥去和保存签名
978
构造RECORD-ROUTE标题组
980
检索RECORD-ROUTE会话密钥
丢弃
生成确认RECORD-ROUTE签名
982
匹配?
否
是
984
删除ROUTE SET签名
986
下一链路不可信?
否
是
987
检索ROUTE SET会话密钥
988
生成ROUTE SET签名
990
插入ROUTE SET签名
992
保存会话密钥
994
继续标准处理

图 13

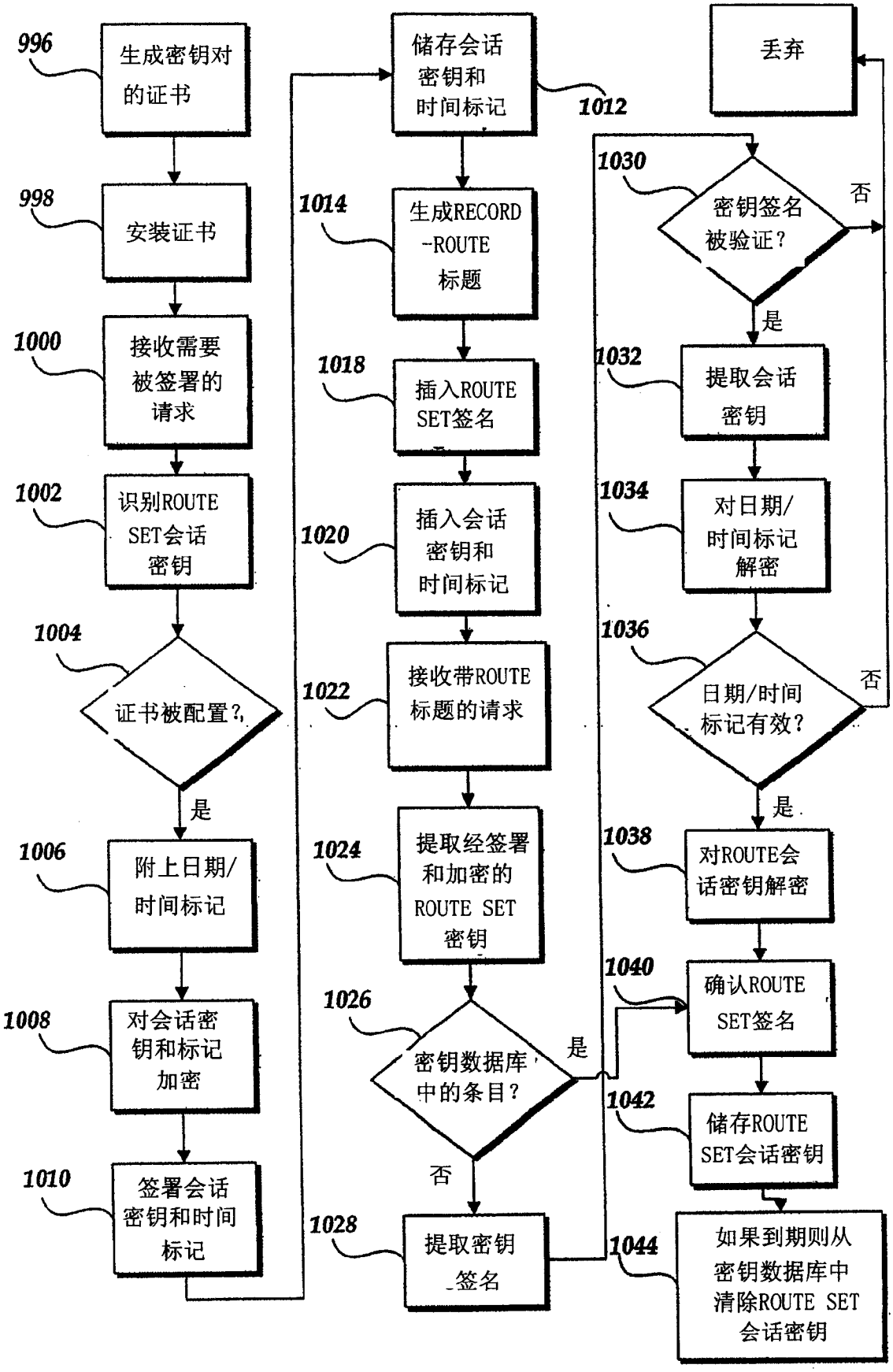

996
生成密钥对的证书
998
安装证书
1000
接收需要被签署的请求
1002
识别ROUTE SET会话密钥
1004
证书被配置?
是
1006
附上日期/时间标记
1008
对会话密钥和标记加密
1010
签署会话密钥和时间标记
储存会话密钥和时间标记
1012
1014
生成RECORD-ROUTE标题
1018
插入ROUTE SET签名
1020
插入会话密钥和时间标记
1022
接收带ROUTE标题的请求
1024
提取经签署和加密的ROUTE SET密钥
1026
密钥数据库中的条目?
是
否
1028
提取密钥_签名
丢弃
1030
密钥签名被验证?
否
是
1032
提取会话密钥
1034
对日期/时间标记解密
1036
日期/时间标记有效?
否
是
1038
对ROUTE会话密钥解密
1040
确认ROUTE SET签名
1042
储存ROUTE SET会话密钥
1044
如果到期则从密钥数据库中清除ROUTE SET会话密钥

图 14