(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 1832477 B
(45)授权公告日 2010.12.08

(21)申请号 200610003796.1

(22)申请日 2006.02.10

(30)优先权数据
60/659,279 2005.03.07 US
11/107,011 2005.04.15 US

(73)专利权人 微软公司
地址 美国华盛顿州

(72)发明人 E·D·特瑞布尔 T·W·弗里曼

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 张政权

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/24(2006.01)

(56)对比文件
US 5958005 A,1999.09.28, 说明书第4-12栏、图3,5A.
WO 00/07355 A3,2000.02.10, 全文.
CN 1509098 A,2004.06.30, 全文.
CN 1522516 A,2004.08.18, 全文.

审查员 王澍

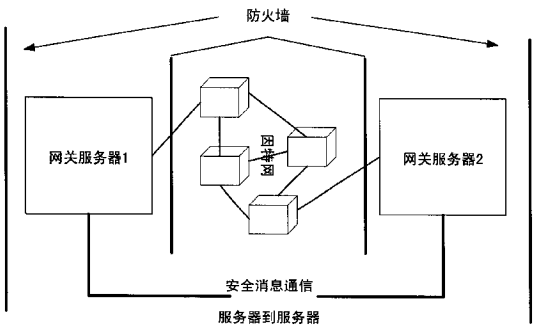
权利要求书 3 页 说明书 10 页 附图 8 页

(54)发明名称

确定服务器和通信者具有兼容安全电子邮件的系统和方法

(57)摘要

发现秘密从源域被发送到通信者域。发现秘密包括对通信者域专用的数据元素。发现秘密包括许可通信者域向其发送消息的源域地址,以便确定潜在通信者具有兼容的安全电子邮件技术,从而可以建立源域与通信者域之间的链路。发现秘密由通信者域接收,包括接收数据元素和源域地址。邀请从通信者域被发送到源域地址。该邀请包括该数据元素或对应于该数据元素的元素。源域在源域接收邀请时启动建立与通信者域的链路的进程。



CN 1832477 B

1. 一种用于确定潜在通信者域具有兼容的安全电子邮件技术，以便在源域与通信者域之间建立链路的方法，包括：

将发现秘密从所述源域发送到所述通信者域，其中，所述发现秘密包括对所述通信者域专用的数据元素，并且其中，所述发现秘密包括源域地址，通信者域被许可向该源域地址发送消息以便在所述源域与所述通信者域之间建立兼容性；以及，

由所述源域经由所述源域地址从所述通信者域接收邀请，其中，所述邀请包括所述数据元素或与所述数据元素相对应的元素，所述数据元素或与所述数据元素相对应的元素可以由所述通信者域用来启动建立与所述通信者域的兼容性的进程，

其中所述数据元素包括秘密，并且其中，所述源域通过重新计算关于所述通信者域的当前秘密并且随后将其与所述发现秘密中所包括的秘密进行比较，来验证从所述通信者域接收的秘密，由此，所述源域只与提供所述秘密的潜在通信者域相对应，以便缓和来自通信者域的服务拒绝攻击。

2. 如权利要求 1 所述的方法，其特征在于，还包括将接受从所述源域发送到所述通信者域，以确定所述通信者域和源域具有兼容的安全电子邮件技术或其他电子邮件或通信技术。

3. 如权利要求 1 所述的方法，其特征在于，所述发现秘密被有选择地发送到以下的至少一个：

通信者域，所述源域已从所述通信者域接收消息；

预先特别地标识的通信者域；以及

经由随机选择的消息的通信者域。

4. 如权利要求 1 所述的方法，其特征在于，所述发现秘密是响应于用户动作而生成的消息；或者所述发现秘密是具有单个通信者域的消息；或者所述发现秘密是到作为操作者的通信者域的消息；或者所述发现秘密是到关于每个密钥的通信者域的单个消息；或者所述发现秘密是在基于时间的确定时发送的消息。

5. 如权利要求 1 所述的方法，其特征在于，所述发现秘密包括附加标题，所述附加标题包括所述数据元素和所述源域地址。

6. 如权利要求 1 所述的方法，其特征在于，所述发现秘密包括截止日期，并且其中，当所述源域在所述截止日期之后接收邀请时，所述源域不确定所述通信者域和源域具有兼容的安全电子邮件技术。

7. 如权利要求 1 所述的方法，其特征在于，所述数据元素是以下的至少一个：

包括关于每个通信者域的随机或伪随机数的每一域秘密；以及

对所述通信者域和所述发现秘密的截止日期加密的所生成的每一域秘密。

8. 如权利要求 1 所述的方法，其特征在于，所述数据元素是从关于每个通信者域的多个同时有效的秘密中选择的，以便有多个有效秘密可以用于从通信者域到源域的管理地址的通信。

9. 如权利要求 1 所述的方法，其特征在于，还包括：对被传递到具有特定数据元素的源域地址的消息的数目施加限制，由此，缓和使用正确数据元素的服务拒绝攻击。

10. 如权利要求 1 所述的方法，其特征在于，还包括覆盖关于给定通信者域的数据元素的要求，以允许带外授权发送来自特定域的邀请消息。

11. 如权利要求 1 所述的方法，其特征在于，所述数据元素是邮件标题中的发现秘密消息内的记号或被嵌入在消息的正文中，或者所述数据元素是邮件标题中的记号而所述消息的正文在通过邮件服务器时保持被加密。

12. 如权利要求 1 所述的方法，其特征在于，还包括：支持关于相同的域的多个同时有效的记号，并且，通过针对关于所述通信者域的记号来验证传入的记号，以验证来自所述通信者域的子域的邀请消息。

13. 如权利要求 1 所述的方法，其特征在于，所述数据元素是关于所述源域的版本信息以及所述源域所支持的功能的叙述。

14. 一种用于确定通信者域和源域具有兼容的安全电子邮件技术的系统，包括：

源域服务器，它将发现秘密发送到所述通信者域，其中，所述发现秘密包括对所述通信者域专用的数据元素，并且其中，所述发现秘密包括源域地址，所述通信者域被许可向所述源域地址发送消息，以便确定所述通信者域和源域具有兼容的安全电子邮件技术；以及

通信者域计算机，它接收包括所述数据元素和所述源域地址的发现秘密，其中，所述通信者域计算机将邀请从所述通信者域传送到所述源域地址，其中，所述邀请包括所述数据元素或与所述数据元素相对应的元素，

所述数据元素是以下的至少一项：

经由散列所述通信者域而生成的秘密；

从关于每个通信者域的多个重叠秘密中选择的数据元素，以便有多个有效秘密可以用于从通信者域到源域的管理地址的通信；以及

关于所述源域的版本信息以及所述源域所支持的功能的叙述。

15. 如权利要求 14 所述的系统，其特征在于，所述源域服务器将接受从所述源域传送到所述通信者域，以确定所述通信者域和源域具有兼容的安全电子邮件技术，并且其中，所述源域服务器启动在所述源域服务器接收邀请时建立与所述通信者域计算机的链路的进程；以及

还包括以下的至少一项：

对被传递到具有特定数据元素的源域地址的消息的数目施加限制，由此，缓和使用正确数据元素的服务拒绝攻击；

覆盖关于给定通信者域的数据元素的要求，以允许带外授权发送来自特定域的邀请消息；以及

支持关于相同的域的多个同时有效的记号，并且，通过对照关于所述通信者域的发现秘密来验证传入的发现秘密，以验证来自所述通信者域的子域的邀请消息。

16. 如权利要求 14 所述的系统，其特征在于，由所述源域服务发送的发现秘密包括以下的至少一项：

被有选择地发送到通信者域的发现秘密，所述源域已从所述通信者域接收到消息；

被有选择地发送到预先特别地标识的通信者域或随机选择的通信者域的发现秘密；

响应于用户动作而生成的消息；

具有单一通信者域的消息；

到作为服务器的操作者地址的通信者域的消息；

到关于每个密钥的通信者域的单一消息；

在基于时间的确定时发送的消息；

包括所述数据元素和所述源域地址的附加标题；以及

截止日期，并且其中，当所述源域在所述截止日期之后接收邀请时，所述源域不启动建立与所述通信者域的链路的进程。

确定服务器和通信者具有兼容安全电子邮件的系统和方法

技术领域

[0001] 本发明的实施例涉及在两个域之间建立兼容的互连的领域，尤其涉及一种用于揭示和发现具有高级性能的邮件服务器的系统和方法。

背景技术

[0002] 一些现有系统试图通过直接通信来识别潜在通信者。但是，这些系统在通信时变得易受攻击者的攻击，特别是，会引起或易受垃圾邮件的攻击和服务拒绝攻击。

[0003] 因此，需要一种系统，该系统通过离散地标识潜在通信者，以便可以建立服务器与潜在通信者之间的安全链路，来解决这些和其他缺点中的一个或多个。

发明内容

[0004] 本发明的实施例包括电子邮件服务器，该电子邮件服务器偶尔将额外标题添加到将被传递到潜在通信者域的消息中。该标题中的数据包括对发送到特定通信者域的消息专用的秘密、以及来自那个通信者域的管理消息可以被指引到服务器的电子邮件地址。如果通信者域处的邮件也被指引通过实现这个实施例的服务器，那么，它将检测到该额外标题，并确定始发域处可能有兼容的服务器。然后，它可以指引管理通信量，例如，建立与所包含的管理电子邮件地址的安全连接的请求。这类管理消息也必须包含为该通信者域提供的秘密。始发域处的管理邮件的邮件接受人随后可以丢弃声称来自通信者域、但不包含与通信者域相对应的秘密的任何邮件。

[0005] 在一个实施例中，本发明包括用于确定潜在通信者域具有兼容的安全电子邮件技术，以便在源域与通信者域之间建立链路的方法。发现秘密从该源域发送到通信者域。该发现秘密包括对通信者域专用的数据元素以及源域地址，其中准许通信者域将消息发送到该源域地址，以便在源域与通信者域之间建立兼容性。源域经由源域地址从通信者域接收邀请。该邀请包括该数据元素或对应于该数据元素的元素，它可以由通信者域用来启动建立与通信者域的兼容性的进程。

[0006] 根据本发明的一个方面，为将要从源域发送到通信者域的发现秘密提供数据结构，用于确定通信者域和源域具有兼容的安全电子邮件技术或其他电子邮件或通信技术。该发现秘密包括：消息；涉及该消息的标题；以及附加于该消息的附加标题。该附加标题包括：(1) 数据元素，它对通信者域专用并包括源域地址，其中准许通信者域将消息发送到该源域，以便确定通信者域和源域具有兼容的安全电子邮件技术；(2) 发现秘密；以及 (3) 截止日期。

[0007] 按照另一种形式，本发明包括用于确定通信者域和源域具有兼容的安全电子邮件技术或其他电子邮件或通信技术的系统。源域服务器将发现秘密传送到通信者域。该发现秘密包括对通信者域专用的数据元素以及源域地址，其中准许通信者域将消息发送到该源域地址，以便确定通信者域和源域具有兼容的安全电子邮件技术。通信者域计算机接收包括数据元素和源域地址的发现秘密。通信者域计算机将邀请从通信者域发送到源域地址。

该邀请包括数据元素或对应于该数据元素的元素。

[0008] 作为选择，本发明可以包括各种其他的方法和装置。

[0009] 其他特征一部分将显而易见，一部分将在下文中指出。

附图说明

[0010] 图 1 是在其间具有安全消息通信的网关服务器 1 和 2 的示例性框图。

[0011] 图 2 是根据本发明示出源域服务器与潜在通信者（例如，通信者域服务器）之间的工作流程的示例性图表。

[0012] 图 3 是根据本发明示出源消息管理器的示例性框图。

[0013] 图 4 是根据本发明示出安全消息管理 (SMM) 的管理路由的操作的流程图。

[0014] 图 5 是根据本发明示出 SMM 工作者路由的操作的流程图。

[0015] 图 6 是根据本发明示出服务器（管理组织 A）与通信者（管理组织 B）之间的组织间工作流程概述的示例性框图。

[0016] 图 7 是根据本发明示出在服务器与通信者之间实现的新的安全关联之后的状态图的流程图。

[0017] 图 8 是示出其中可以实现本发明的合适的计算系统环境的一个例子的框图。

[0018] 在所有附图中，对应的参考字符指出对应的部分。

具体实施方式

[0019] 本发明涉及一种用于确定潜在通信者具有兼容的安全电子邮件技术，以便开始在服务器与通信者之间建立链路的进程的系统和方法。具体地，本发明涉及一种用于启动为安全电子邮件的部署建立安全链路的进程的系统和方法。本发明允许服务器确定：由于兼容的安全电子邮件技术，可以将潜在通信者建立为目标。结果，一旦标识了潜在通信者，服务器就可以与该潜在通信者交换密钥材料信息，以便建立安全链路。

[0020] 根据本发明的域签署和加密的目标是提供一种传输无关的机制，以在各服务器之间交换机密和服务器认证的消息。图 1 是网关服务器 1 和 2 的示例性框图。网关服务器 1 和 2 在其间具有安全消息通信链路。这些服务器可以被可任选的防火墙隔开；通过该防火墙，它们可以被连接到桥头服务器 (bridgehead server)（未示出），这些桥头服务器可以是单独的安全消息通信系统的一部分。网关服务器 1 和 2 形成可以位于可信内部网络（例如，链接桥头服务器的安全消息通信系统）与非可信外部网络（例如，公用因特网）之间的子网。防火墙也位于网关服务器与因特网之间。网关服务器将所有邮件视作明文，并逐个网关地加密所有邮件。如果网关和桥头服务器不共享相同的加密密钥，那么，网关服务器无法对桥头服务器加密的邮件进行解密。

[0021] 对所有内部和外部关系的官方数据需要单个管理点。可任选地，实现单个主模型而不是多重主模型，这是因为它更简单，并且因为它不必解决复制冲突。安全消息管理 (SMM) 操作通常很少发生，并且，SMM 操作中的延迟不应该延迟邮件传递，而只是延迟新的安全关联的设置。数据库大小通常很小（例如，每个有几 K 的几十万条记录；它可以到达几兆字节，但可能不会是成百上千兆字节），以便有足够的时间来修复或替换硬件或在任何服务损失之前完成系统恢复。在一个实施例中，关于操作的关键数据被复制到其他网关服务

器。由于没有单个管理点，因此，并不是复制所有数据，且所复制的数据是只读的。

[0022] 服务器可能忙于许多其他的通信者域，以便为特定项目设立邮件链路。但是，这类项目的管理协调通常不会缩放。为使安全消息通信能够产生影响，对组织的大多数商业通信者启用安全邮件。这要求能够发现哪些通信者安装了网关服务器并具有简单的组织到组织工作流程，以便确定是否应该有协商来建立安全邮件链路。

[0023] 本发明允许发现被安装在组织的通信者中的网关服务器，以便可以设立安全连接。为了便于发现，服务器通过某个指示（或通告）（此处被称为发现秘密）并利用出站邮件指出（例如，通告）本身的存在。为了最小化易受攻击的发现秘密进程，本发明的系统和方法不在其发现秘密中使用硬编码地址。但是，可以构想，在一个实施例中，单个地址可以用于发现秘密，以被包括在发给那个地址的任何电子邮件中。结果，只有来自已看到发现秘密的各方的消息（包括发现秘密）可被发送到管理地址。所以，在一个较佳实施例中，使用单个地址，并且，必须在每个消息中提供发现秘密。作为选择，指示的地址是可以按合理的时间间隔（例如，每周一次）循环的随机邮箱名称。尽管这个随机方法是一种选择，但它通常是不太首选的实施例。为了确保最小化易受攻击性，发现秘密被绑定到发送域（例如，源域），并绑定到它被发送到那里的域（例如，通信者域）。如果第三方可获得发现秘密，那么，将会受到影响的唯一的域是其邀请地址被泄密的域。

[0024] 按照一种形式，发现秘密可以是822标题，它包含关于协商的短暂的822地址和与何时发送消息有关的822地址的截止时间。入站邮件由接收服务器（例如，通信者或通信者服务器）扫描，以找出来自网关服务器的发现秘密，并与已知网关服务器列表进行比较。对那个列表的任何添加都被传达给本地管理SMM。一发现新的通信者，SMM就可以将探查消息（例如，邀请）发送到另一个SMM处的管理地址，以提供开启域签署和加密或其他服务。一接收到来自另一SMM管理员的邀请，如果消息可在现有的信任策略下验证，那么，本地SMM可以调用策略来自动接受该邀请。作为选择，SMM管理员可以在接受邀请之前要求手动批准。服务器一接收到邀请接受，如果消息可内在地验证，那么，接收SMM将会调用策略来自动开始使用域签署和加密。首先，它现时发送加密查验消息，并等候确认（包括现时），以确保该安全邮件可以被另一方解密。注意，邀请和接受消息利用SMM的官方密钥来签署，而查验和确认利用签署密钥（是官方密钥的子密钥）来签署。完成例行邮件签署和加密的进程只要求官方利用签署密钥来签署（出于安全性起见）。这样，查验和确认也验证安全邮件将与签署密钥一起工作，而不只是官方密钥。新的安全域的配置是异步进程，并且不被用于真实数据，直到在任何管理提示之前通过查验确认的接收而在操作上确认该链路。

[0025] 图2是根据本发明示出源域与潜在通信者（例如，目标域计算机）之间的工作流程的示例性图表。最初，包括管理地址、发现秘密和截止日期的发现秘密从服务器被发送到通信者。发现秘密也应该包含发送域和接收域，以便可以迅速确定它们是否针对你的域（因为作为邮件列表的结果，它们可能已被分程传递）。当通信者识别发现秘密时，通信者将邀请发回到被寻址到作为发现秘密的一部分的管理地址的服务器。在一个实施例中，如果它也已将邮件发送“到”域，那么，它只响应于发现。这样，垃圾邮件发送者无法诱使源域邀请它们（因为你从未首先向它们发送邮件）。来自通信者的邀请包括通信者的管理地址、截止、证书和发现秘密以及其他信息（例如，工作流程ID、联系人信息、发送域和接收域、等等）。作为响应，服务器将接受从服务器的管理地址发送到通信者的管理地址，并且在该接

受中包括截止、证书、发现秘密和签名。这在管理上是可任选的，尽管默认策略可以包括自动响应。在一个实施例中，它也可以受限于手动，或者，如果邀请者的证明书符合某个信任策略，则只响应。在接收接受之后，通信者查验服务器，并且，查验被服务器确认，以建立使关联进入就绪状态的连接。它可以涉及可任选地自动化的管理动作，以便从就绪状态前进到活动状态。它可以涉及进一步的步骤，以便从活动状态（使用安全关系，但不相信它）转到认证状态（相信另一端所声明的身份）。如果邀请消息不可如图 2 所示那样使用信任策略来验证，那么，请求可以被暗示等候手动批准。

[0026] 参考图 3，示出了根据本发明的示例性框图，该示例性框图示出了安全消息管理器。通信者对邀请的接受可以在管理 SMM 代理上创建交叉证书，它随后与加密证书一起被推到工作者 SMM 代理。（通常为认证的关联创建交叉证书（以便定义允许它们认证什么）。活动关联具有除交叉证书以外的任何事物。）交叉证书约束新信任所接受的名称集、以及对域网关服务器通信的限制。这时，关于该新关联的证书和信息被分发给所有这些工作者。会话密钥在此情况下也可以从管理 SMM 被分发给所有工作者 SMM，所以，所有工作者使用同一密钥来减小高速缓存大小。为了虑及扩大，用于加密证书的对应的解密私钥应该在面对网关服务器的所有互联网上可用，以允许任何一个解密入站邮件。这在单一的地方（即管理代理处）生成，并被分发给所有工作者服务器。一旦建立信任关系，就应该维持该关系。例如，可以保留原始证书，并且，在该证书到期之前，将续订请求发送到其他 SMM。也可以频繁地更新子加密和签署证书。

[0027] 从服务器的观点来看，根据本发明的方法开始在源域与通信者域之间建立链路的进程。最初，源域服务器经由随机或伪随机消息将发现秘密发送到潜在通信者域。该发现秘密包括诸如被特别地分配给通信者域的叙述或记号或其他秘密等数据元素。发现秘密包括对通信者域（和可能是源域）专用的共享秘密。在该较佳实施例中，它是种子的散列、通信者域和源域（按照某个规定的顺序）。此外，发现秘密包括许可通信者域向其发送消息的源域处的地址，以便在源域服务器与目标计算机之间建立兼容性。源域服务器从通信者域接收邀请，该邀请被寻址到先前提供的源域地址。该邀请包括发现秘密中的数据元素或与发现秘密中的数据元素相对应的元素。这允许源域服务器启动在源域服务器一从通信者域服务器接收到邀请，就在通信者域服务器与源域服务器之间建立兼容性的进程。如图 2 中指出的，源域服务器将接受发送到通信者域服务器，以便在其间建立兼容性。

[0028] 在一个实施例中，源域有选择地将发现秘密发送到源域已从那里发送消息的通信者域。作为选择或除此之外，源域可以将发现秘密发送到预先已特别标识的通信者域。

[0029] 在一个实施例中，可以将发现秘密附加到被特别地发送以携带发现秘密的消息。在本发明的一个实施例中，电子邮件服务器偶尔将附加标题（“x 标题”）添加到将被传递到另一个电子邮件域的消息。该标题中的数据包括对通信者域专用的秘密，以及来自通信者域的管理消息可以被指引回到电子邮件服务器的电子邮件地址，并包括截止、通信者域、发送者域、可任选版本和可任选特征。如果通信者域处的邮件也被指引通过实现本发明的该实施例的服务器，那么，它将检测附加标题，并确定始发域处可能有兼容的服务器。然后，通信者域指引管理通信量（例如，建立与包含的管理电子邮件地址的安全连接的请求）。这类管理消息也必须包含为通信者域提供的秘密（以上被称作“发现秘密”）。始发域处的管理邮件的邮件接受者随后可以丢弃声称来自通信者域、但不包含与通信者域相对应的秘密

的任何邮件。虽然这不绝对保证所接收的管理邮件来自始发域，但是，它的确最小化了对管理地址处的垃圾邮件的易受攻击性，并确保甚至可以看到通信者域的电子邮件的攻击者也只能试图欺骗来自通信者域而非来自任何域的管理地址。

[0030] 在一个实施例中，通过使用被称作“发现秘密”（有时被称作“叙述”）的标题来实施本发明，该发现秘密被附加到来自源域的已出站电子邮件。这个发现秘密揭示了始发该出站电子邮件的邮件服务器上的特定功能的可用性，同时避免对生成附加的、可能不合需要的消息的需求。如上所述，管理电子邮件地址将会被包括在叙述中，并且，将会有每一域的秘密，以减轻垃圾邮件对管理电子邮件地址的危险。这将会支持管理电子邮件地址处的工作流程消息。

[0031] 可以从通信者域的散列和被保持在始发服务器上的秘密种子中生成发现秘密。也可以从源域的散列中生成发现秘密，因为相同的服务器可以表示多个源域。一个实施例可以潜在地具有关于源服务器处的所有域的特殊“来源”。这允许跨越多个服务器共享单个种子，以便每个服务器将生成对于任何通信者域而言是独特的相同的发现秘密。当在始发服务器处接收管理消息时（因为它被指引到叙述中所包括的管理地址），管理消息中所提供的发现秘密由始发服务器来检验。为了检验发现秘密，电子邮件服务器可以生成（或存储）关于使用当前内部种子发送管理消息的域的发现秘密。如果生成的发现秘密与管理消息中的发现秘密相同，那么，那个消息具有正确的发现秘密并被通过到达关于协商消息的适当目的地。协商消息在各域之间传递。如果发现秘密不匹配，那么，将相同的进程应用于先前的发现秘密（直到有界数目）。如果当前有效的种子不能用来生成与传入消息中的发现秘密匹配的发现秘密，那么，消息不被认为是有效的，并被丢弃或拒绝，并且不被传递到关于管理消息的最终目的地。这阻止对管理消息的接收者的未经授权的垃圾邮件攻击，该接收者可能无法应付大量的电子邮件。此外，为了阻止来自接收过有效发现秘密的域的服务拒绝攻击，验证进程许可服务器跟踪最近从特定域或使用特定发现秘密有多少消息被通过到达管理目的地。当那个数目超过容许的限制或容许的比率时，丢弃或拒绝使用该发现秘密的进一步的管理消息。

[0032] 图 4 是根据本发明示出 SMM 管理路由的操作的流程图。签名验证和解密必须在反垃圾邮件处理之前发生，因为要设置反垃圾邮件代理所使用的消息属性标志，来自验证的输出是必要的。签名验证应该在块列表和其他 IP 或协议地址级功能之后发生。这样，该进程在 402 开始，在许可通信者域向其发送消息的源域地址处接收消息。如果在 404 确定发现秘密对于发送域而言无效，那么，在 406 丢弃该消息，并且，路由进程结束。如果发现秘密有效，那么，进程前进到 408，以确定域是否具有已被超过的最大数量或比率。如果该最大值已被超过，那么，在 406 丢弃该消息；否则，如果签名在 410 有效，那么，消息被路由到本地管理代理。但是，签名验证不需要在工作者中发生；它通常在 SMM 中发生。

[0033] 图 5 是根据本发明示出 SMM 工作者路由的操作的流程图。SMM 是安全消息通信管理器；工作者是 SMM 管理 / 控制的并且处理邮件通信量的服务器。SMM 签署和加密通常是最后的功能。每个去往具有安全消息关联的域的消息被签署和加密。这个组件也将包含当前 SMM 短暂地址的标题插入到去往没有安全关系的域的所有邮件中。工作者将适当地添加发现秘密，但它不只是对安全邮件这样做。如图 5 所示，在找到有效的发现秘密之后，域在 502 寻找有效签名，在 504 寻找外部地址。只在声称针对管理员的消息中（不在普通邮件

中）检验发现秘密。如果签名有效，并且没有外部地址，那么，消息在 506 被路由到本地工作者代理。如果有外部地址，那么，它被路由到该外部地址。如果消息看起来是域保护的，那么，同等地对待无效签名，如同签名不存在一样。消息来源不被认证。

[0034] 在一个实施例中，在各个管理组织之间实现如图 6 所示的表示关系的生命周期的组织间的工作流程。其他转滚 (rollover) 是可能的 :密钥具有与它们关联的证书。这些证书可以比这些密钥更频繁地转滚。有签名、加密、以及官方证书和密钥，所有这些都独立地转滚。也会有以后的查验 / 确认序列。该工作流程由 SMM 管理代理执行，并可以经历交换，以便实现转滚（转滚是用于更新到新的密钥或证书的术语）。图 7 是示出新的安全关联的状态图。该图只考虑肯定的情况和终端情况。它不包括诸如在重发限制之前重发消息等其他方面。

[0035] 本发明的其他可任选特征包括可以个别地或组合地实现的以下内容。活动与认证的关联之间的区别是“可任选的”，如同可以被应用来自动进行管理转移的所有各项策略那样。发现秘密可以包括截止日期，在此情况下，源域服务器将不会启动当源域服务器接收邀请的时间在截止日期之后时建立与通信者域计算机（例如，服务器）的兼容性的进程，以便共享秘密不会随着时间的推移而变得越来越显露。数据元素可以是以下的至少一项 :每一域秘密，它包括关于每个通信者域计算机（例如，服务器）的随机或伪随机数、经由散列通信者域计算机（例如，服务器）而生成的秘密、以及被用来为一个以上的域生成每一域秘密的秘密种子 ;以及通过加密通信者域计算机（例如，服务器）和秘密的截止日期而生成的每一域秘密。数据元素可以包括秘密，在此情况下，通过重新计算关于通信者域计算机（例如，服务器）的当前秘密并且随后将其与发现秘密中包括的秘密进行比较，源域服务器可以记住秘密或可以验证从通信者域计算机（例如，服务器）接收的秘密。数据元素可以从多个秘密中选择，这些秘密在重叠时间内对于每个通信者域计算机（例如，服务器）而言有效，以便有多个有效秘密可以用于从通信者域计算机（例如，服务器）到发信域的管理地址的通信。可以对被传递到具有特定数据元素的源域服务器地址的消息的数目施加限制，以便缓和使用正确数据元素的服务拒绝攻击。源域服务器可以包括覆盖关于给定通信者域计算机（例如，服务器）的数据元素的要求的能力，以允许带外授权发送来自特定域的邀请消息。数据元素可以是邮件标题中的发现秘密消息内的记号或被嵌入在消息的正文中，或者，数据元素可以是邮件标题中的记号，并且，消息的正文在通过邮件服务器时保持被加密。源域服务器可以支持关于相同域的多个同时有效的发现秘密，并且通过对照关于通信者域计算机（例如，服务器）的发现秘密来验证传入的发现秘密，可验证来自通信者域计算机（例如，服务器）的子域的邀请消息。数据元素可以是发现秘密，并包括关于源域服务器的版本信息，并包括源域服务器支持的功能。

[0036] 在一个实施例中，本发明包括关于将要从源域服务器发送到通信者域计算机（例如，服务器）的发现秘密的数据结构。如上所述，这个发现秘密被用来建立源域服务器与通信者域计算机（例如，服务器）之间的兼容性。作为选择，它可以用于这两个域之间的其他目的。例如，它可以用于这两个域以同意它们将发送与加密或安全无关的专有 TNEF 格式（而不是文本或 HTML）。该数据结构包括消息和其涉及该消息的通常的标题。此外，数据结构包括附加于消息和消息标题并且包括对通信者域计算机（例如，服务器）专用的数据元素的附加标题。该标题也包括许可通信者域计算机（例如，服务器）将消息发送到源域服

务器的源域服务器地址，以便建立源域服务器与通信者域计算机（例如，服务器）之间的兼容性。如上所述，该额外标题应该包括截止日期，尽管这是可任选的。

[0037] 作为选择或除此之外，发现秘密可以是具有单个通信者域的消息和/或到作为操作者的通信者域的消息。到通信者域的单个消息可以是针对每个密钥，并且，它可以在基于时间的确定时（例如，每小时一条消息）发送。例如，用户动作可以是NDR或返回收条。具体地，发送单独的消息或附加于已被发送的消息的选择独立于是在每个消息上这样做还是只是偶尔这样做。一个跨接情况是等候具有单个域（通信者域）处的接收者的消息，而不是将发现秘密附加于具有多个域处的接收者的消息。在一项实现中，消息被分离，以便去往通信者域处的接收者的副本具有关于该域的发现秘密。

[0038] 图8示出了采取计算机130的形式的通用计算设备的一个例子。在本发明的一个实施例中，诸如计算机130等计算机适用于这里所示出和描述的其他附图。计算机130具有一个或多个处理器或处理单元132和系统存储器134。在所示的实施例中，系统总线136将包括系统存储器134的各种系统组件耦合到处理器132。总线136表示任何几种类型的总线结构中的一个或多个，包括存储总线或存储控制器、外围总线、加速图形端口、以及使用任种总线体系结构中的任一种的处理器或局部总线。举例来讲（不作限制），这类体系结构包括工业标准体系结构（ISA）总线、微通道体系结构（MCA）总线、增强型ISA(EISA)总线、视频电子技术标准协会（VESA）局部总线和外围部件互连（PCI）总线（也被称作Mezzanine总线）。

[0039] 计算机130通常至少具有某种形式的计算机可读介质。计算机可读介质（包括易失性和非易失性介质、可移动和不可移动介质）可以是可由计算机130访问的任何可用介质。举例来讲（不作限制），计算机可读介质包括计算机存储介质和通信介质。计算机存储介质包括易失性和非易失性的可移动和不可移动介质，该介质以用于信息（例如，计算机可读指令、数据结构、程序模块或其他数据）存储的任何方法或技术来实现。例如，计算机存储介质包括RAM、ROM、EEPROM、闪存或其他存储技术、CD-ROM、数字多功能盘（DVD）或其他光盘存储器、盒式磁带、磁带、磁盘存储器或其他磁存储设备、或可以用来存储所需信息并可以由计算机130访问的其他任何介质。通信介质通常具体化为已调制数据信号（例如，载波或其他传送机制）中的计算机可读指令、数据结构、程序模块或其他数据，它包括任何信息传递介质。本领域的技术人员熟悉已调制数据信号，其一个或多个特征按为该信号中的信息编码的这样一种方式来加以设置或更改。有线介质（例如，有线网络或直线连接）和无线介质（例如，声音、RF、红外线和其他无线介质）是通信介质的例子。以上任何内容的组合也被包括在计算机可读介质的范围以内。

[0040] 系统存储器134包括采取可移动和/或不可移动的易失性和/或非易失性存储器的形式的计算机存储介质。在所示的实施例中，系统存储器134包括只读存储器（ROM)138和随机存取存储器（RAM)140。基本输入/输出系统142(BIOS)通常被存储在ROM 138中，该基本输入/输出系统包含有助于在计算机130内的各个元件之间传送信息（例如，在启动期间）的基本例程。RAM 140通常包含可立即由处理单元132访问和/或目前正由处理单元132操作的数据和/或程序模块。举例来讲（不作限制），图8示出了操作系统144、应用程序146、其他程序模块148和程序数据150。

[0041] 计算机130也可以包括其他可移动/不可移动的易失性/非易失性计算机存储介

质。例如，图 8 示出了从不可移动的非易失性磁介质读取或对其写入的硬盘驱动器 154。图 8 也示出了从可移动的非易失性磁盘 158 读取或对其写入的磁盘驱动器 156，以及从可移动的非易失性光盘 162（例如，CD-ROM 或其他光学介质）读取或对其写入的光盘驱动器 160。可以用于该示例性操作环境中的其他可移动 / 不可移动的易失性 / 非易失性计算机存储介质包括（但不局限于）卡型盒式磁带机、闪存卡、数字多功能盘、数字录像带、固态 RAM、固态 ROM 等。硬盘驱动器 154、磁盘驱动器 156 和光盘驱动器 160 通常通过非易失性存储接口（例如，接口 166）而被连接到系统总线 136。

[0042] 以上所讨论的和图 8 中所示的这些驱动器或其他大容量存储设备及其相关联的计算机存储介质为计算机 130 提供计算机可读指令、数据结构、程序模块和其他数据的存储。例如，在图 8 中，硬盘驱动器 154 被示为存储操作系统 170、应用程序 172、其他程序模块 174 和程序数据 176。注意，这些组件可以等同于或不同于操作系统 144、应用程序 146、其他程序模块 148 和程序数据 150。这里为操作系统 170、应用程序 172、其他程序模块 174 和程序数据 176 提供不同的标号，以说明它们至少是不同的副本。

[0043] 用户可以通过输入设备或用户界面选择设备，例如，键盘 180 和定点设备 182（例如，鼠标、跟踪球、笔或触垫），来将命令和信息输入计算机 130。其他输入设备（未示出）可以包括话筒、操纵杆、游戏垫、圆盘式卫星电视天线、扫描仪或类似的输入设备。这些和其他的输入设备通过被耦合到系统总线 136 的用户输入接口 184 而被连接到处理单元 132，但也可能由其他接口和总线结构（例如，并行端口、游戏端口或通用串行总线 (USB)）来连接。监视器 188 或其他类型的显示设备也经由接口（例如，视频接口 190）而被连接到系统总线 136。除监视器 188 以外，计算机经常包括诸如打印机和扬声器等其他外围输出设备（未示出），这些外围输出设备可以通过输出外围接口（未示出）来连接。

[0044] 计算机 130 可以使用与一台或多台远程计算机（例如，远程计算机 194）的逻辑连接而在网络化环境中操作。远程计算机 194 可以是个人计算机、服务器、路由器、网络 PC、对等设备或其他共同的网络节点，它通常包括以上相对于计算机 130 而描述的许多或所有这些元件。图 8 中所描绘的逻辑连接包括局域网 (LAN) 196 和广域网 (WAN) 198，但也可以包括其他网络。LAN 136 和 / 或 WAN 138 可以是有线网络、无线网络、其组合、等等。这类网络环境在办公室、企业范围的计算机网络、内联网和全球计算机网络（例如，因特网）中很普遍。

[0045] 当被用于局域网环境中时，计算机 130 通过网络接口或适配器 186 而被连接到 LAN 196。当被用于广域网环境中时，计算机 130 通常包括调制解调器 178 或用于通过 WAN 198（例如，因特网）建立通信的其他装置。调制解调器 178（可以是内置的，也可以是外置的）经由用户输入接口 184 或其他适当的机制而被连接到系统总线 136。在网络化环境中，相对于计算机 130 或其各个部分而描绘的程序模块可以被存储在远程记忆存储设备（未示出）中。举例来讲（不作限制），图 8 将远程应用程序 192 示为驻留在存储设备上。所示的这些网络连接起示例性的作用，可以使用在计算机之间建立通信链路的其他手段。

[0046] 通常，计算机 130 的数据处理器通过在不同时刻存储在计算机的各种计算机可读存储介质中的指令来编程。例如，程序和操作系统通常分布在软盘或 CD-ROM 上。从那里，它们被安装或载入计算机的辅助存储器。在执行时，它们至少被部分地载入计算机的主电子存储器。当这些和其他各种类型的计算机可读存储介质包含用于协同微处理器或其他数据处理器来实现下述步骤的指令或程序时，这里所描述的本发明包括这类介质。当根据这

里所描述的方法和技术编程时，本发明也包括计算机本身。

[0047] 出于举例说明的目的，程序和其他可执行程序组件（例如，操作系统）在这里被示为离散块。但是，可认识到：这类程序和组件在各个不同的时刻驻留在计算机的不同的存储组件中，并且由计算机的数据处理器来执行。

[0048] 虽然结合示例性计算系统环境（包括计算机 130）来描述，但是，本发明可利用众多其他的通用或专用计算系统环境或配置来操作。计算系统环境并不意在对本发明的使用范围或功能性提出任何限制。而且，不应该将计算系统环境解释为对示例性操作环境中所示的任何一个组件或组件组合具有任何依赖性或要求。可适用于本发明的众所周知的计算系统、环境和 / 或配置的例子包括（但不局限于）个人计算机、服务器计算机、手持设备或便携式设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费者电子设备、移动电话、网络 PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境等。

[0049] 本发明可以在由一台或多台计算机或其他设备执行的计算机可执行指令（例如，程序模块）的一般上下文中描述。通常，程序模块包括（但不局限于）执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件和数据结构。本发明也可以在分布式计算环境中实践，在分布式计算环境中，由通过通信网络连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括记忆存储设备的本地和远程计算机存储介质中。

[0050] 软件体系结构的上下文中的接口包括软件模块、组件、代码部分、或计算机可执行指令的其他序列。例如，接口包括第一模块，该第一模块访问第二模块，以便代表该第一模块来执行计算任务。在一个例子中，第一模块和第二模块包括诸如由操作系统提供的应用程序编程接口 (API)、组件对象模型 (COM) 接口（例如，用于对等应用程序通信）、以及可扩展标记语言元数据交换格式 (XMI) 接口（例如，用于各 web 服务之间的通信）。

[0051] 接口可以是例如在 Java 2 平台企业版本 (J2EE)、COM 或分布式 COM(DCOM) 例子中的紧密耦合的同步实现。作为选择或除此之外，接口可以是例如在 web 服务（例如，使用简单对象访问协议）中的松散耦合的异步实现。一般而言，接口包括以下特征的任何组合：紧密耦合、松散耦合、同步和异步。另外，接口可以符合标准协议、专有协议、或标准协议和专有协议的任何组合。

[0052] 这里所描述的接口都可以是单一接口的一部分，或者可以作为单独的接口或其中的任何组合来实现。接口可以本地或远程地执行，以提供功能。另外，接口可以包括与这里所示或描述的相比更多或更少的功能。

[0053] 在操作中，计算机 130 作为源域服务器或通信者域计算机（可能是服务器）来操作，以执行如上所述的计算机可执行指令（例如，图 2-7 中所示的计算机可执行指令）。

[0054] 这里所示和描述的方法的执行或实行顺序不是重要的，除非另有规定。即，方法的元素可以按任何顺序来执行，除非另有规定；并且，方法可以包括比这里所揭示的元素更多或更少的元素。例如，可以构想，在另一个元素之前、同时或之后执行或实行特定元素是在本发明的范围以内。

[0055] 当介绍本发明或其实施例的元素时，冠词“一”、“一个”、“该”和“所述”意味着：有这些元素中的一个或多个元素。术语“包括”、“包含”和“具有”意在起包含的作用，并意味着可能有除列出的元素以外的额外元素。

[0056] 鉴于上述内容，将会看到，实现了本发明的几个目标，并达到其他有利的结果。

[0057] 由于在不脱离本发明的范围的前提下可以在以上的构造、产品和方法方面进行各种更改，因此，上文中所包含的和附图中所示的所有内容意在被解释为起说明的作用，而没有限制的意义。

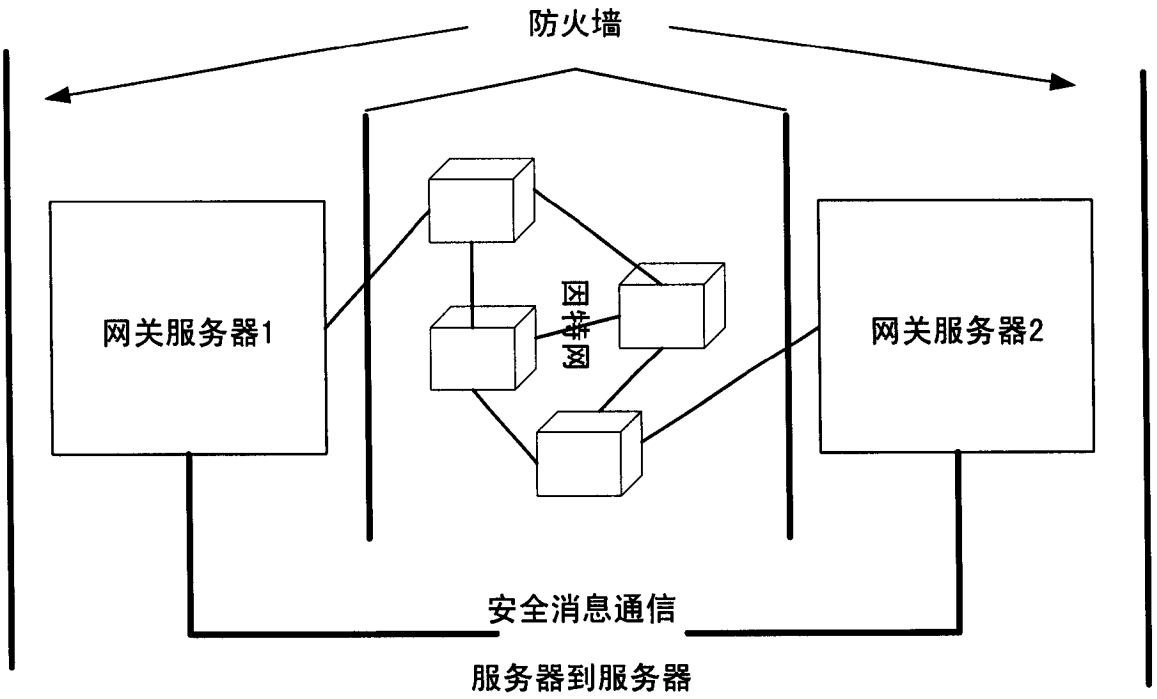


图 1

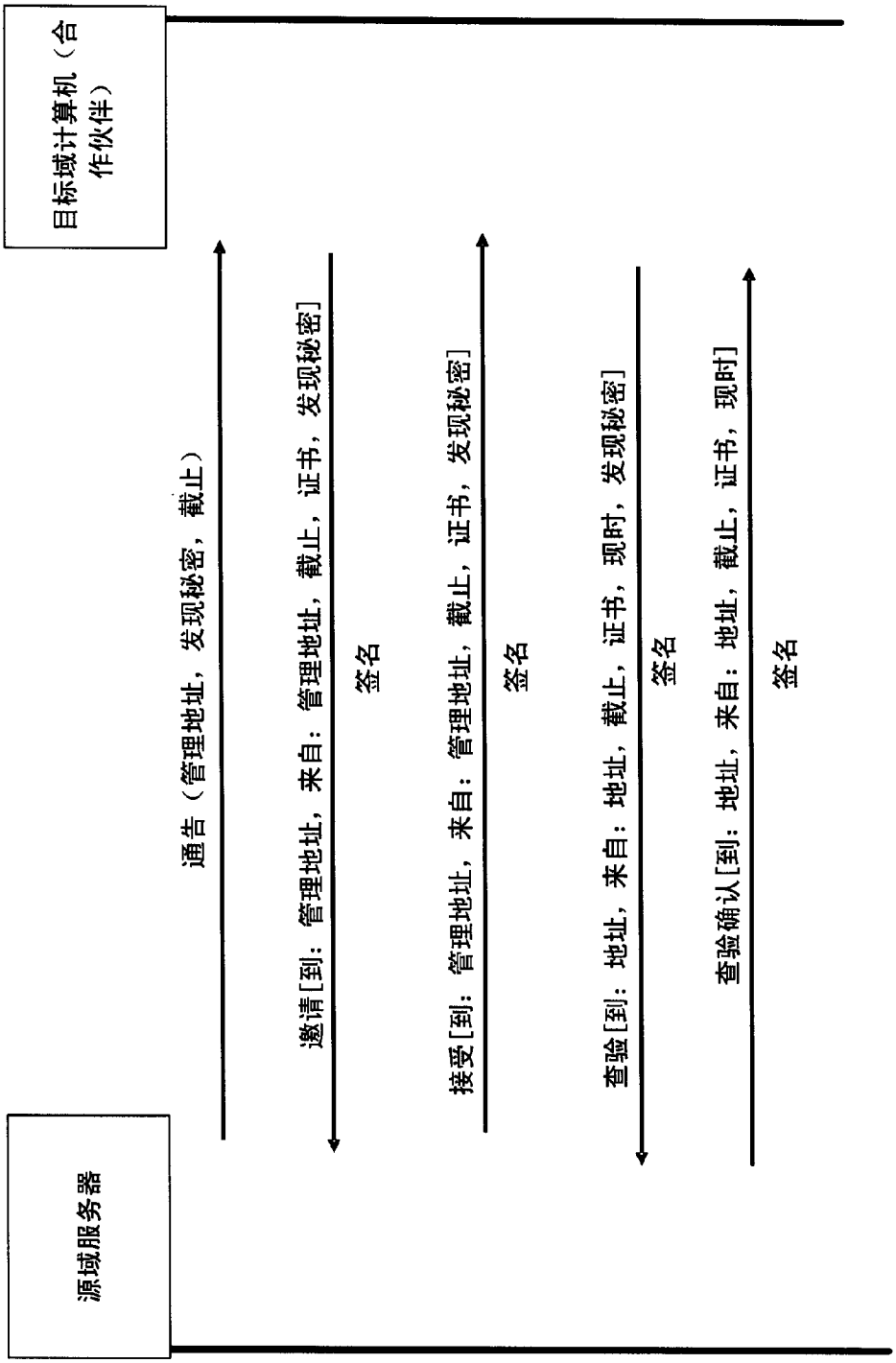

源域服务器
目标域计算机（合作伙伴）
通告（管理地址，发现秘密，截止）
邀请[到：管理地址，来自：管理地址，截止，证书，发现秘密]
签名
接受[到：管理地址，来自：管理地址，截止，证书，发现秘密]
签名
查验[到：地址，来自：地址，截止，证书，现时，发现秘密]
签名
查验确认[到：地址，来自：地址，截止，证书，现时]
签名

图 2

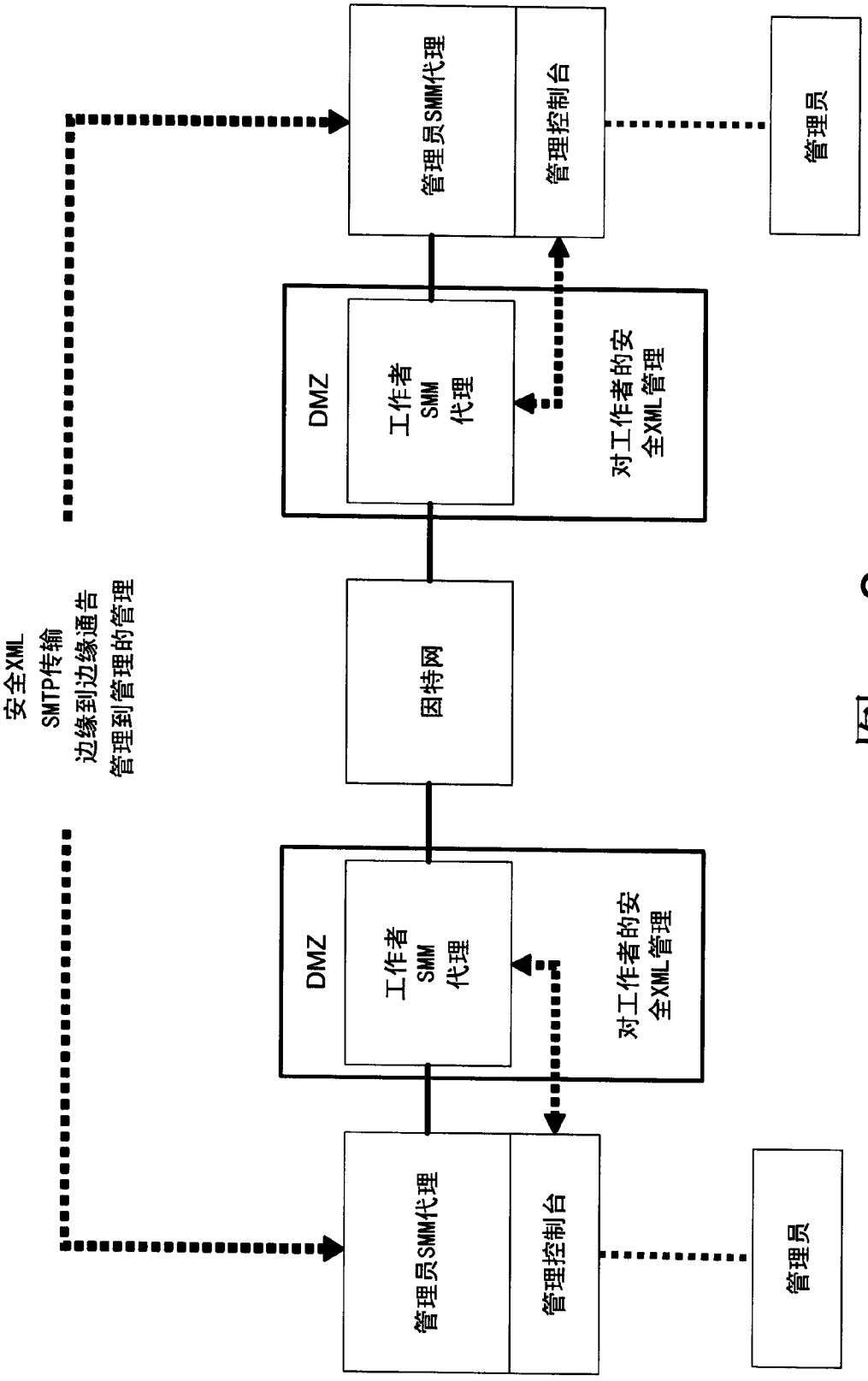

管理员SMM代理
管理控制台
管理员
DMZ
工作者
SMM
代理
对工作者的安
全XML管理
因特网
DMZ
工作者
SMM
代理
对工作者的安
全XML管理
管理员SMM代理
管理控制台
管理员
安全XML
SMTP传输
边缘到边缘通告
管理到管理的管理

图 3

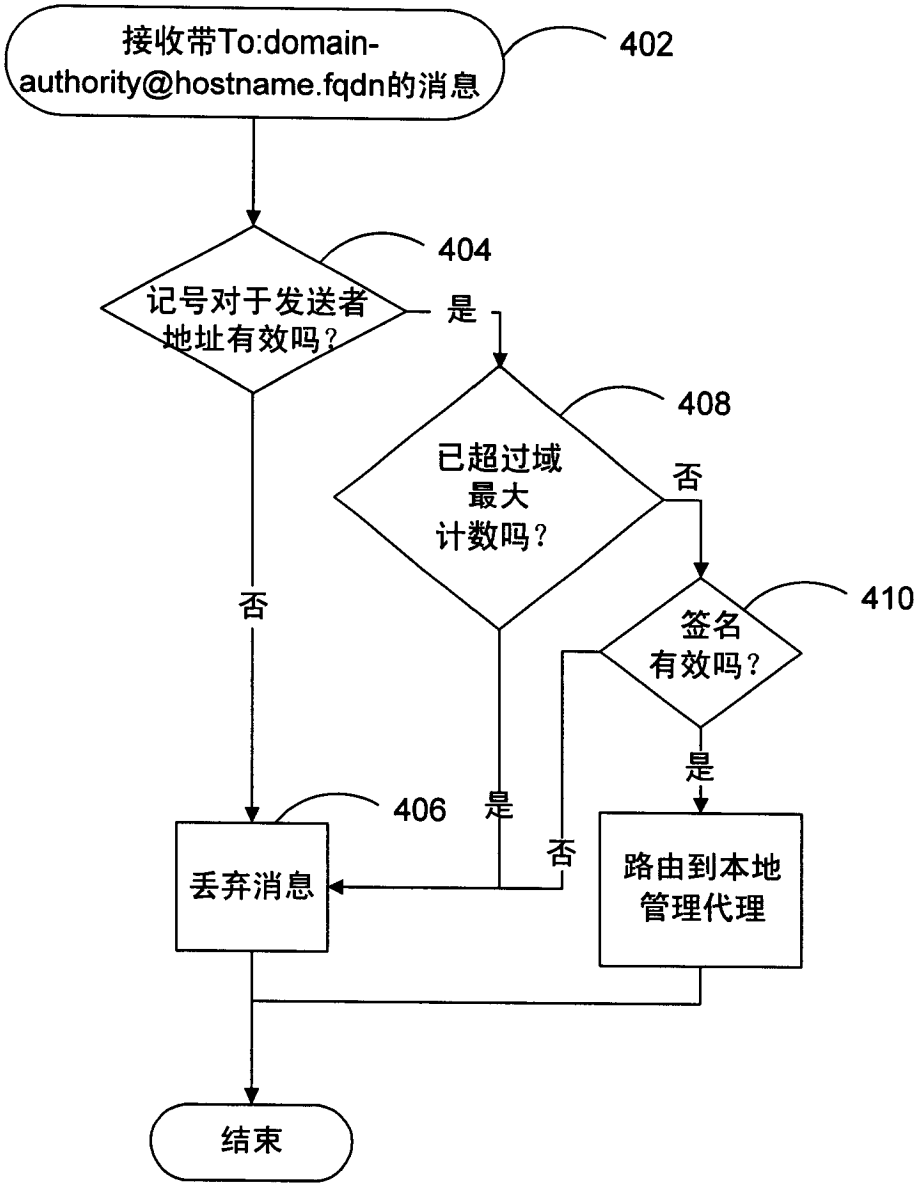

接收带To:domain-authority@hostname.fqdn的消息
402
404
记号对于发送者地址有效吗？
是
否
408
已超过域最大计数吗？
否
是
410
签名有效吗？
是
否
406
丢弃消息
路由到本地管理代理
结束

图 4

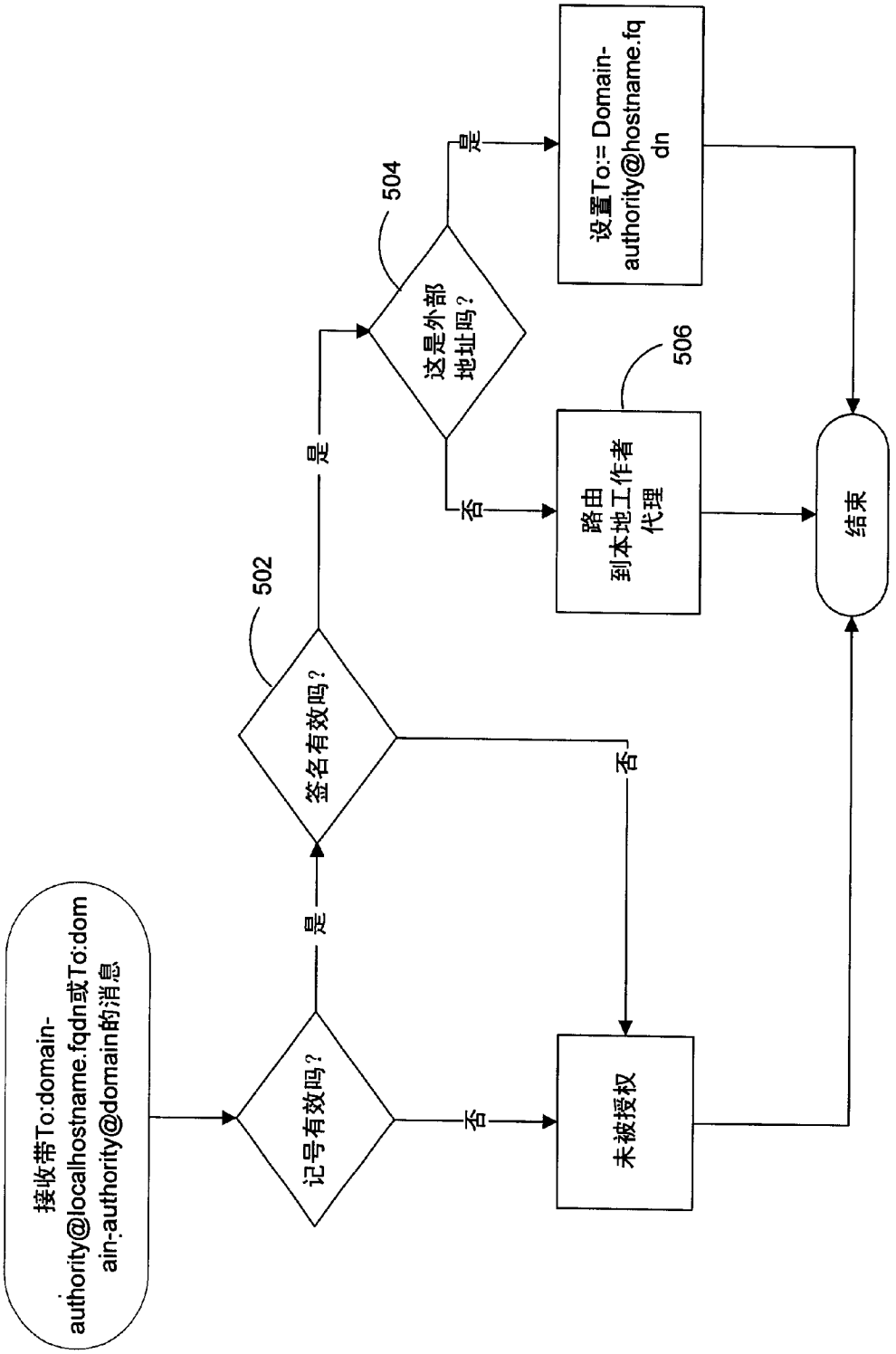

接收带To:domain-authority@localhostname.fqdn或To:domain-authority@domain的消息
记号有效吗?
是
否
未被授权
签名有效吗?
502
是
否
这是外部地址吗?
504
是
否
设置To:= Domain-authority@hostname.fqdn
路由到本地工作者代理
506
结束

图 5

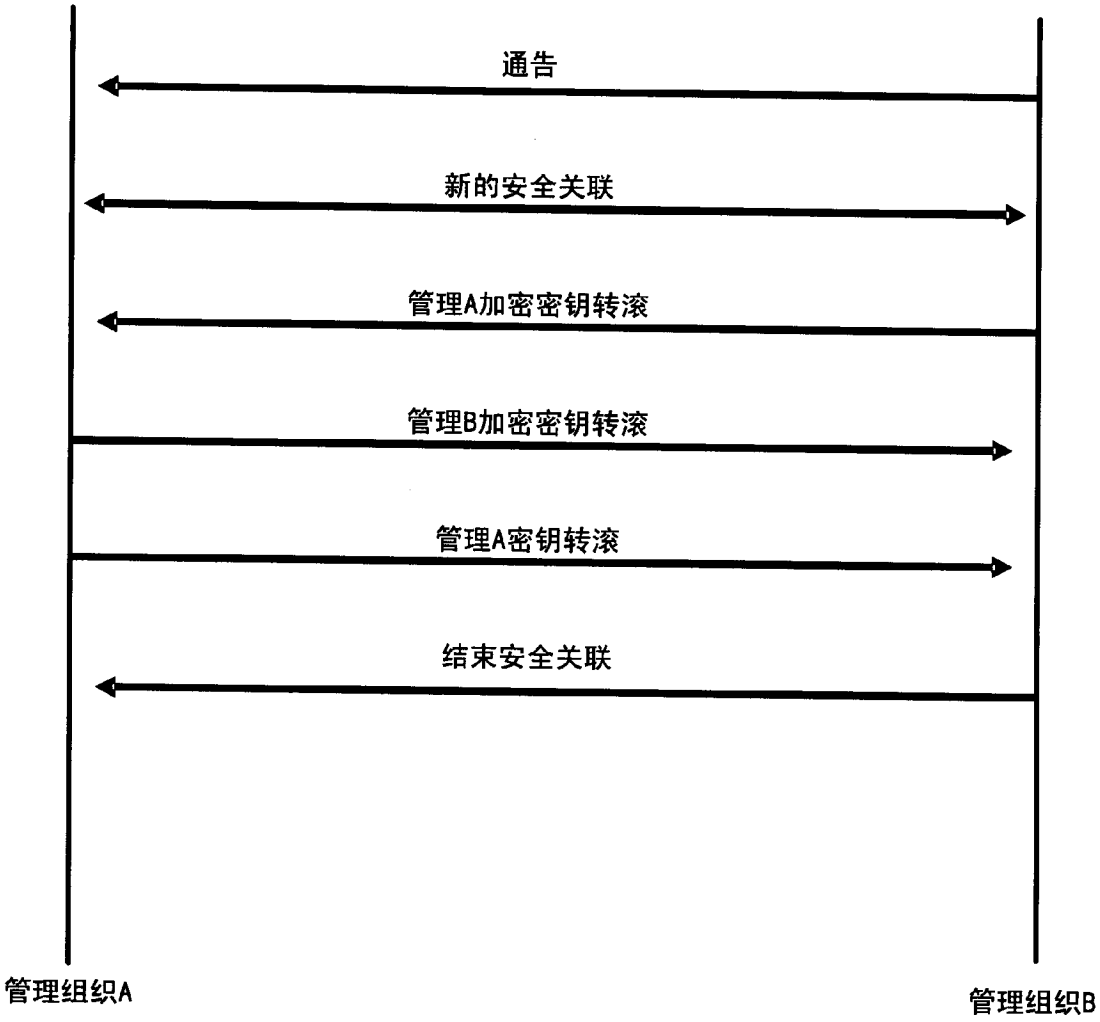


图 6

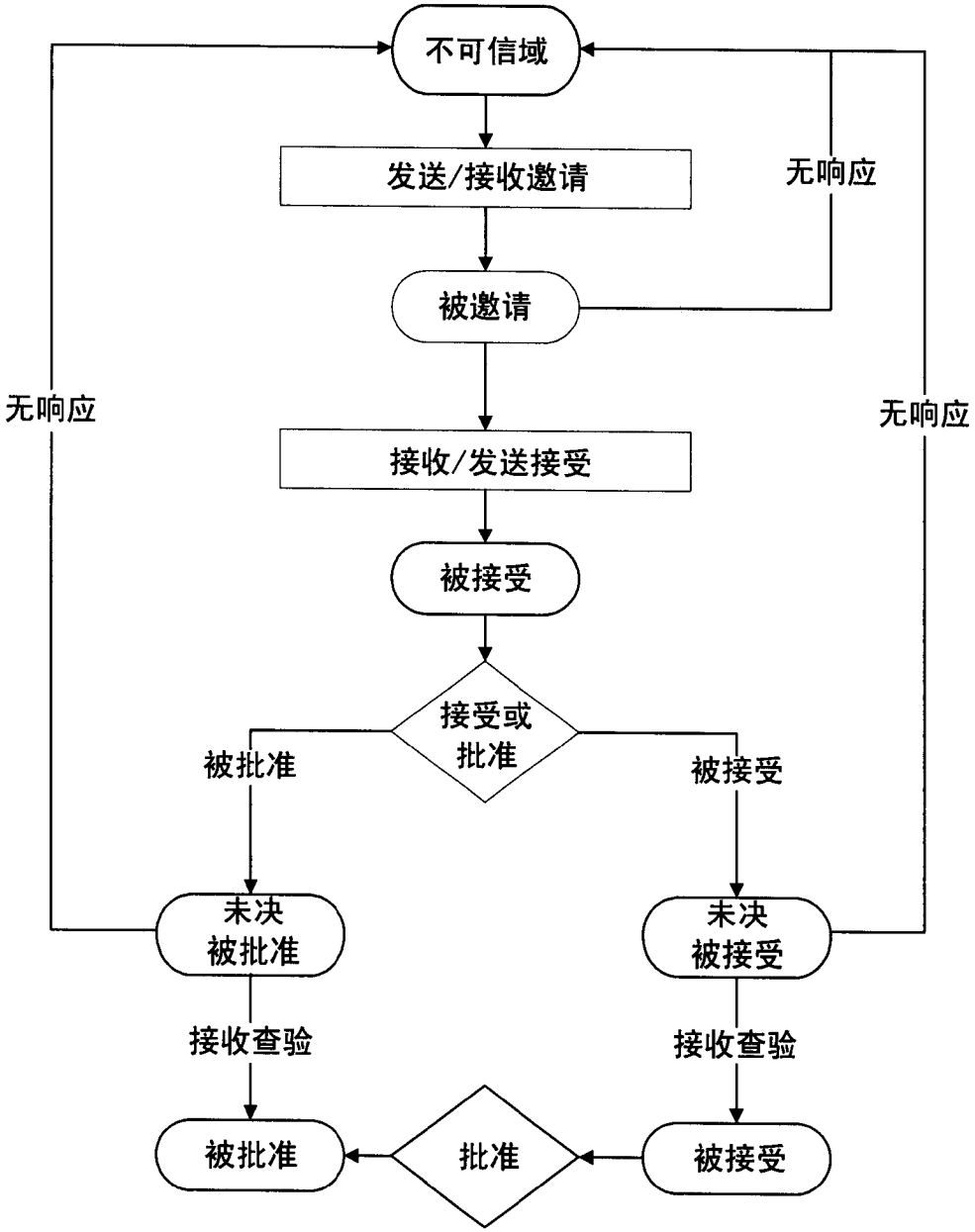
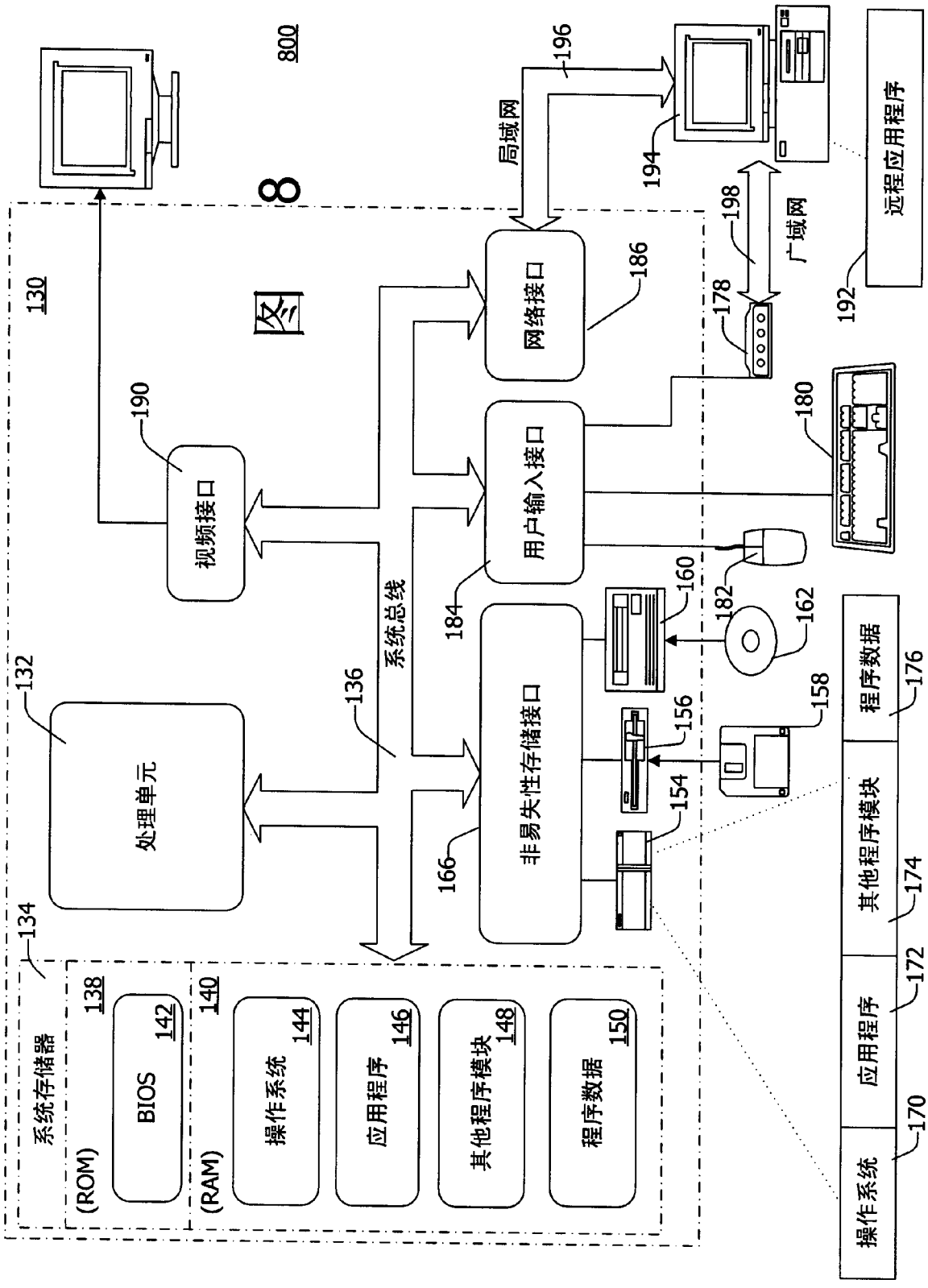

不可信域
发送/接收邀请
无响应
被邀请
无响应
无响应
接收/发送接受
被接受
接受或
批准
被批准
被接受
未决
被批准
未决
被接受
接收查验
接收查验
被批准
批准
被接受

图 7


800
图 8
130
局域网
196
194
198
广域网
远程应用程序
192
网络接口
186
178
视频接口
190
用户输入接口
180
系统总线
184
160
182
162
132
处理单元
136
非易失性存储接口
156
158
154
166
134
系统存储器
(ROM)
138
BIOS
142
(RAM)
140
操作系统
144
应用程序
146
其他程序模块
148
程序数据
150
程序数据
176
其他程序模块
174
应用程序
172
操作系统
170