(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 103975552 B
(45)授权公告日 2017.06.20

(21)申请号 201280059708.3
(22)申请日 2012.12.05
(65)同一申请的已公布的文献号
申请公布号 CN 103975552 A
(43)申请公布日 2014.08.06
(30)优先权数据
13/311,976 2011.12.06 US
(85)PCT国际申请进入国家阶段日
2014.06.04
(86)PCT国际申请的申请数据
PCT/US2012/068025 2012.12.05
(87)PCT国际申请的公布数据
WO2013/086043 EN 2013.06.13
(73)专利权人 思科技术公司
地址 美国加利福尼亚州
(72)发明人 法彼奥·麦诺 维纳·厄尔玛甘
艾伯特·卡贝罗斯·阿帕里塞奥
(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 李晓冬
(51)Int.Cl.
H04L 9/00(2006.01)
G06F 15/16(2006.01)
H04L 9/32(2006.01)
(56)对比文件
CN 101594339 A,2009.12.02,
WO 2007121787 A1,2007.11.01,
审查员 高伟

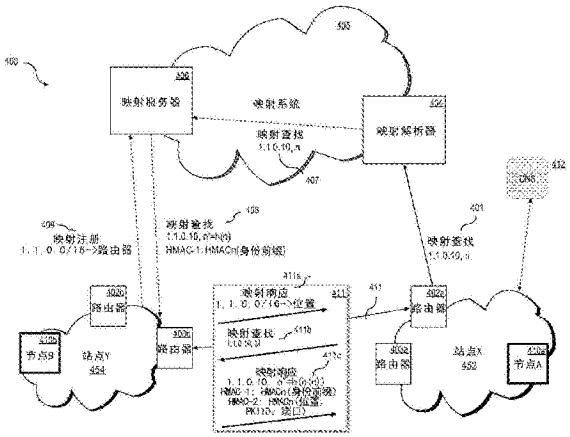
权利要求书2页 说明书15页 附图5页

(54)发明名称

经由经认证的路由器的数据交换

(57)摘要

与第一网络节点(410a)相关联的第一路由器(403a)将第一映射查找发送到映射服务(405),该第一映射查找包括与第二网络节点(410b)相关联的特定设备标识符,该映射服务维护将设备标示符与设备位置相关联的多个映射。第一路由器(403a)从与第二网络节点(410b)相关联的第二路由器(402a)接收映射响应,该映射响应包括对应于第二网络节点(410b)的特定设备标识符的特定设备位置。第一路由器(403a)与第二路由器(402a)建立安全会话,并且基于该安全会话确定第二路由器是否被授权应答与第二网络节点(410b)相关联的特定设备标识符。



CN 103975552 B

1.一种数据交换方法,包括:

在与第一网络节点相关联的第一路由器处:

将第一映射查找发送到映射服务,其中,所述第一映射查找包括与第二网络节点相关联的特定设备标识符,所述映射服务维护将设备标识符与设备位置相关联的多个映射;

从与所述第二网络节点相关联的第二路由器接收映射响应,其中,所述映射响应包括对应于所述第二网络节点的所述特定设备标识符的特定设备位置;

在所述第一路由器与所述第二路由器之间建立安全会话;

基于所述安全会话确定所述第二路由器是否被授权应答包括与所述第二网络节点相关联的所述特定设备标识符的所述第一映射查找。

2.如权利要求1所述的数据交换方法,其中,确定所述第二路由器是否被授权应答所述特定设备标识符包括:通过所述安全会话接收证书链,并且验证所述链包括受信任的根证书。

3.如权利要求1所述的数据交换方法,其中,确定所述第二路由器是否被授权应答所述特定设备标识符包括:

通过所述安全会话接收与所述设备标识符相关联的地址前缀、和所述第二路由器的信任证书,并且指示来自证书授权的发布;

验证所述地址前缀被包括在所述信任证书中。

4.如权利要求1所述的数据交换方法,进一步包括:

确定所述第二路由器未被授权应答所述特定设备标识符,并且响应于此使包括所述第二路由器的先前存储的本地映射无效。

5.如权利要求1所述的数据交换方法,进一步包括:

确定所述第二路由器被授权应答所述特定设备标识符,并且响应于此在所述第一路由器处存储将所述特定设备标识符与所述特定设备位置相关联的本地映射。

6.如权利要求5所述的数据交换方法,进一步包括:

基于存储在所述第一路由器处的所述本地映射,代表所述第一网络节点与所述第二路由器通信。

7.如权利要求1所述的数据交换方法,其中,所述方法是响应于从所述第一网络节点接收一个或多个封包而被执行的,所述封包标识与所述第二网络节点相关联的设备标识符作为目的地。

8.如权利要求1所述的数据交换方法,进一步包括:

在所述第一映射查找中包括密钥,并且在与所述第二路由器建立所述安全会话之前,验证所述映射响应包括所述密钥的预期版本。

9.如权利要求1所述的数据交换方法,其中,确定所述第二路由器是否被授权应答与所述第二网络节点相关联的所述特定设备标识符包括:

确定通过所述安全会话从所述第二路由器接收的公钥的有效性。

10.一种数据交换设备,在与第一网络地址前缀相关联的第一路由器处,该设备包括:

用于将包括特定设备标识符的第一映射查找发送到第二路由器,并且响应于此从所述第二路由器接收包括所述特定设备标识符的特定映射的第一映射响应的装置;

其中,所述第二路由器维护将设备标识符与设备位置相关联的多个映射;

用于向所述第二路由器发送提供证书的请求，并且响应于此从所述第二路由器接收第二映射响应的装置；

用于响应于确定所述第二映射响应包括所述证书，从所述第二映射响应提取所述证书，并且使用所述证书来确定所述第二路由器是否是有权的，并且响应于确定所述第二路由器是有权的而从所述第一映射响应提取所述特定映射并且将所述特定映射安装在所述第一路由器处的装置。

11.如权利要求10所述的数据交换设备，进一步包括：

用于响应于确定所述第二映射响应不包括所述证书，丢弃在所述第一映射响应中提供的所述特定映射的装置；

用于响应于确定所述第二映射响应包括所述证书，但是所述第二路由器不是有权的，丢弃在所述第一映射响应中提供的所述特定映射的装置。

12.如权利要求10所述的数据交换设备，其中，所述特定映射被本地安装在所述第一路由器的缓存中。

13.如权利要求10所述的数据交换设备，其中，所述第二映射响应进一步包括从认证机构(CA)的根发源的完全信任链。

14.如权利要求10所述的数据交换设备，其中，所述特定映射包括所述第一路由器的端口号，DTLS服务器被配置为通过所述端口号来通信。

15.如权利要求14所述的数据交换设备，其中，所述第二映射响应是来自分布式映射系统的被转发的映射响应，并且用于所述发送中的网络地址前缀是在所述第一路由器处接收到的网络地址前缀。

16.如权利要求15所述的数据交换设备，进一步包括：

用于从所述第二路由器接收基于所述端口号建立DTLS会话的请求，并且响应于此向所述第二路由器发送至少一个信任证书的装置，其中所述至少一个信任证书包括由所述第一路由器服务的所述网络地址前缀。

17.如权利要求16所述的数据交换设备，进一步包括：

用于从所述第二路由器接收一个或多个封包，并且将所述一个或多个封包转发到网络节点的装置，所述封包标识所述第一网络地址前缀内的网络节点作为所述一个或多个封包的目的地。

18.如权利要求17所述的数据交换设备，进一步包括：

用于向所述第二路由器指示在所述第一路由器处支持基于公钥的安全的装置。

经由经认证的路由器的数据交换

技术领域

[0001] 本公开涉及网络地址映射系统，更具体地涉及用于网络地址映射系统的安全系统。

背景技术

[0002] 此部分中描述的方法是可以执行的方法，但是不必是之前已经构思或执行的方法。因此，除非另有指示，否则不应认为此部分中描述的任何方法仅因为被包括在此部分中而成为现有技术。

[0003] 已经提出并且开发出各种协议和标准来促进用户与设备之间通过因特网进行通信。一些方法使用设备的IP地址或MAC地址来指示两件事：设备的身份和设备的位置。

[0004] 然而，在一些情况下，使用IP或MAC地址指示设备的身份和位置二者可能会出现问题。例如，当移动设备从一个位置移动到另一个位置时，移动设备的MAC地址保持相同，而设备位置改变。因此，使用设备MAC地址不足以确定设备实际位置。

[0005] 通常，软件应用依赖于设备地址作为设备身份和位置二者的决定因素。例如，促进通过TCP会话进行数据通信的应用可以依赖于设备的IP地址来建立TCP会话。然而，仅依赖于设备IP地址会妨碍基于TCP的应用无缝地继续执行。

[0006] 另外，如果网络设备开始使用另一个端口与因特网通信，则即使设备的物理位置尚未改变，设备也会接收到新的IP地址，这回在维持关于设备的一个连续的通信会话方面产生问题。因此，使用设备地址来指示设备身份和设备位置可能是不准确的。

[0007] 另外，即使可获得关于设备位置的准确信息，取得这种信息通常易受安全攻击。

附图说明

[0008] 在附图中通过示例的方式而非限制的方式示出了本发明，并且在附图中相同的参考标号指代相同的元件，其中：

[0009] 图1示出了使用一次性密钥来保护网络地址映射系统的方法的一个示例；

[0010] 图2示出了使用PKI密钥来保护网络地址映射系统的方法的一个示例；

[0011] 图3示出了保护网络地址映射系统的方法的一个示例；

[0012] 图4示出了网络地址映射系统的一个示例；

[0013] 图5示出了本发明的实施例可以在其上实现的计算机系统的一个示例。

具体实施方式

[0014] 在以下的描述中，出于说明的目的，阐述了许多具体细节来提供对本发明的全面理解。然而，显而易见的是，本发明可以在没有这些具体细节的情况下实施。在其他实例中，以框图形式示出了公知结构和设备，以避免不必要地模糊本发明。

[0015] 这里根据以下提纲描述实施例：

[0016] 1.0概述

[0017] 2.0结构和功能概述

[0018] 3.0安全网络地址映射系统的示例

[0019] 3.1使用一次性密钥保护网络地址映射系统

[0020] 3.2使用PKI密钥保护网络地址映射系统

[0021] 4.0实现机构——硬件概述

[0022] 5.0扩展和替代

[0023] 1.0 概述

[0024] 在一个实施例中，处理被配置成利用基于证书的协议来保护不完全受信任的分布式映射系统。在一个实施例中，设备的身份与设备的位置信息是分开的。设备身份(在一个实施例中称为身份)和设备位置(在一个实施例中称为位置)被划分到两个不同的命名空间，并且不同的网络地址被用于身份和位置。

[0025] 将用于身份和位置的地址分开的功能提供了以下好处：改善的路由系统的可扩展性、更大的位置集合、和输入流量工程的提高的多宿主效率。身份与位置的分开允许克服许多因特网应用正在经历的一些问题。

[0026] 在一个实施例中，提出了一种用于表示捕获设备身份和设备位置的信息的方法。在一种实现方式中，从设备发送的封包包括设备的IP地址信息和设备的位置信息。IP地址信息对应于基于设备IP地址的传统设备标识，并且对设备而言直接已知。然而，位置信息是由被配置成在特定时间确定设备的物理位置、并且使用和维护映射的路由器确定的。

[0027] 例如，位于特定建筑物中的一个会议室中的用户使用移动设备连接到网络。服务于设备连接的路由器可以确定移动设备在给定时刻的位置。在用户和移动设备移动到同一个建筑物中的另一个会议室时，路由器可以确定移动设备的新位置，并且可以在由网络维护的数据库中更新移动设备的位置信息。

[0028] 服务于移动设备对网络的访问的路由器可以在任何特定时间确定移动设备的当前位置。尽管移动设备的IP地址和/或MAC地址不变，但是移动设备的位置的改变可以由网络中的路由器追踪。

[0029] 在一个实施例中，该方法是基于会话(诸如，TCP会话)的连续性的，即使移动设备已经改变它的位置。因此，从支持为移动设备建立的TCP会话的应用的观点看，即使移动设备改变位置，也可以维持连续的TCP会话。依赖于设备所提供的设备IP地址和路由器所提供的设备位置标识，TCP支持应用可以连续执行。

[0030] 在一个实施例中，设备的身份与设备的位置是分开的。虽然身份仍可以由设备的IP地址表示，但是设备的位置是由与设备通信的路由器或服务器确定的。

[0031] 本文所提供的将设备身份与设备位置分开的处理可以防止依赖于设备位置的准确信息并且在仅提供设备的IP地址作为设备标识信息的情况下将会失败的应用的失败。

[0032] 将设备的身份信息与设备的位置信息分开允许依赖于设备的身份信息的应用继续绑定到身份信息。因此，当移动设备移动到另一个位置时，另一个路由器检测并更新设备的位置信息，但是设备的身份信息不需要被更新。这提高了会话连续性，而与设备的移动性无关。设备身份信息与设备位置信息之间的关联可以被存储在由映射系统维护的映射中。

[0033] 在一个实施例中，可以使用一次性密钥来保护对分布式映射系统的访问。一次性密钥可应用于被认为安全的映射系统。可以使用一次性密钥来例如在将从映射系统获得的

位置信息提供给请求者之前保护该位置信息。

[0034] 在一个实施例中，使用基于公钥基础设施(PKI)的安全处理来保护映射系统，从而保护映射系统免受针对映射系统中存在的实体的安全漏洞攻击。

[0035] 可以使用基于PKI的方法来认证映射系统的实体。例如，基于PKI的方法可以允许验证针对特定身份获得的位置信息是否是由被授权与映射系统通信并且被授权向其他实体提供位置信息的实体提供。

[0036] 2.0 结构和功能概述

[0037] 图4示出了网络地址映射系统400的一个示例。在一个实施例中，映射系统400包括站点452(站点X)、映射系统405、以及站点454(站点Y)。在实际实施例中，额外的站点452和454以及额外的替代拓扑结构405可以存在于映射系统400中。

[0038] 在一个实施例中，站点452包括一个或多个节点A 410a、一个或多个入口隧道路由器402a、以及一个或多个出口隧道路由器403a。节点A410a可以与一个或多个域名系统(DNS)412通信，节点410a可以从域名系统请求并获得一个或多个因特网协议(IP)地址。此外，节点410a可以通过连接411与站点452中的任何其他节点以及站点454中的任何节点通信。

[0039] 一个或多个入口隧道路由器402a负责与映射系统405交互，而一个或多个出口隧道路由器403a负责从映射系统405接收信息。

[0040] 在一个实施例中，站点454包括一个或多个节点B 410b、一个或多个入口隧道路由器402b、以及一个或多个出口隧道路由器403b。节点B410b可以通过连接411与站点454中的任何其他节点以及站点452中的任何节点通信。

[0041] 一个或多个入口隧道路由器402b负责与映射系统405交互，而一个或多个出口隧道路由器403b负责从映射系统405接收信息。

[0042] 如果节点410a请求与节点410b建立通信连接411，则入口隧道路由器402a建立与出口隧道路由器403b的通信连接411。然而，在一个实施例中，为了获得节点410b的当前位置信息，在建立连接411之前，入口隧道路由器402a通过映射系统405建立隧道，该隧道是节点410a和410b不知道的，但是该隧道允许入口隧道路由器402a获得节点410b的当前位置信息。

[0043] 在一个实施例中，入口隧道路由器402a被配置成在站点452与站点454之间建立隧道，其中该隧道包括映射系统405。

[0044] 在一个实施例中，站点452与站点454之间通过映射系统405的隧道是虚拟隧道，该隧道的存在没有被传达到站点452中的设备和站点454中的设备。因此，如果(例如)节点410a与节点410b通信，则入口隧道路由器402a和出口隧道路由器403b可以通过映射系统405设立隧道。

[0045] 在一个实施例中，映射系统405包括一个或多个映射解析器404和一个或多个映射服务器406。在一些实现方式中，映射系统405可以是包括彼此通信地耦合的各种服务器的分布式系统，所述服务器包括一个或多个映射解析器404、一个或多个映射服务器406、以及其他服务器。

[0046] 映射解析器404和映射服务器406负责创建和维护站点452和454中存在的设备的身份信息与位置信息之间的映射。

[0047] 在一个实施例中，映射解析器404接收解析设备位置的请求，处理该请求以获得所请求的位置信息，并且将设备的位置信息返回给请求者。

[0048] 映射解析器404解析设备标识已知的设备的位置信息问题。例如，在提供特定设备的IP地址之后，映射系统405的映射服务器404可以确定该特定设备的当前位置的信息。

[0049] 在一个实施例中，映射服务器406维护网络中的设备的标识信息与位置信息之间的映射，并且被配置成在设备的位置信息被请求时提供此信息。

[0050] 在一个实施例中，映射解析器404和映射服务器406彼此合作来对网络设备的位置信息的请求提供响应。接收请求、处理请求、以及获得对请求的响应的处理可以类比由诸如域名系统(DNS)的设备执行的处理，除了DNS处理针对IP地址的请求而映射解析器404和映射服务器406处理针对位置信息的请求。

[0051] 在一个实施例中，网络地址映射系统400包括多个隧道路由器(诸如，两个或更多个入口隧道路由器402a、402b和两个或更多个出口隧道路由器403a、403b)或与多个隧道路由器合作。隧道路由器负责建立路由器之间的隧道并且封装位置信息请求和响应。

[0052] 在一个实施例中，通过映射系统405以下面的方式建立虚拟隧道，在此方式中诸如节点410a、410b的端节点不知道所述隧道的存在。例如，对于节点410b和节点410a来说，出口隧道路由器403b可以下面的方式建立与入口隧道路由器402a的隧道，在此方式中节点410a、410b不知道该隧道的存在。

[0053] 所提出的方法的实现可以基于包括TCP/IP的多个数据通信协议中的任意一个，其中在该数据通信协议中设备可以封包(如在IP中)或分段(如通过TCP)的形式交换数据。因此，在以下描述中，对数据封包的引用也可以理解为对含有封包的数据段的引用。

[0054] 在一个实施例中，诸如节点A 410a和节点B 410b的端节点不知道均可以被分配给每个相应节点的身份与IP地址之间的差异。例如，当生成去往节点A 410a的数据封包或数据段时，节点B 410b可以在不知道所包括IP地址确实是分配给节点410a的IP地址还是只是分配给节点410a的身份的情况下将节点410a的IP地址包括在封包/分段的头部中。

[0055] 身份与IP地址之间的区别不被节点直接使用；然而，诸如出口隧道路由器403a/b和入口隧道路由器402a/b的隧道路由器使用不同的值。

[0056] 在一个实施例中，隧道路由器负责确定接收到的数据封包包括端点节点的身份信息还是端点节点的IP地址。例如，在接收到来自端点410b并且去往端点节点410a的数据封包时，出口隧道路由器403b确定该数据封包包括节点410a的身份还是节点410a的IP地址。

[0057] 如果接收到的封包包括目的地节点的端点标识符，则隧道路由器将目的地节点的端点标识符传输到映射解析器404以确定目的地节点的位置。一旦映射解析器404(与映射服务器406协作)确定目的地节点的位置，目的地节点的位置信息就被传输到隧道路由器。隧道路由器将接收到的封包封装为包括目的地节点的位置信息，并且将封装的封包转发到目的地。

[0058] 然而，如果接收到的封包包括目的地节点的IP地址，则隧道路由器根据已经被包括在接收到的封包中的IP地址将接收到的封包传输到目的地。

[0059] 将身份与位置分开实现了端点移动性。例如，可以向移动节点410b静态地提供用于其所有连接的身份。具有来自身份命名空间的头部的封包可以由移动节点410b封装在来自位置空间的外层报头(outer header)中，从而建立到目的地站点的隧道。封包基于外层

报头被路由到目的地站点。一旦封包到达目的地站点，封包的外层报头被移除并且封包被传递到终端主机或应用。

[0060] 在一个实施例中，映射系统存储身份与位置之间的关联。在一个实施例中，映射被设计成经受对手进行的映射的操纵。映射受到保护而免受其中对手能够重定向流量并且扰乱网络的可靠性和安全性的情况。

[0061] 在一个实施例中，身份-位置映射受到保护，尤其是在动态地更新映射(这是移动设备的情况)的情况下。例如，与移动节点的身份相关联的位置在移动节点从一个位置移动到另一个位置时改变，并且因此身份与位置之间的映射被频繁地更新以反映移动设备的当前位置。可能难以将映射系统所执行的位置信息的合法更新与对手所执行的位置信息的不合法更新进行区别。

[0062] 可以用多种方式提供用于映射系统的安全措施。在一个实施例中，使用映射注册(map registration)和保护映射-响应消息来实现安全措施。

[0063] 在一个实施例中，为了支持隧道路由器对节点标识符的使用，网络中的节点需要向映射系统注册。最初可以使用类似于向设备分配IP地址的处理来向节点或设备分配身份。例如，可以使用动态主机配置协议(DHCP)来分配身份。DHCP允许网络设备从服务器自动地获得有效IP地址。DHCP还可以允许节点或设备从服务器自动地获得有效身份。事实上，可以DHCP不会在IP地址与身份之间进行区别的方式来配置DHCP。

[0064] 为了注册，节点向映射系统提供节点身份信息和节点位置信息。例如，移动设备410b可以通过映射注册消息来将其自己的身份和位置注册到相关联的映射服务器406中。映射服务器406可以是用于身份的有权实体(authoritative entity)，并且可以被配置成能够验证注册的授权、真实性和完整性。

[0065] 例如，出口节点403b可以通过向映射服务器406发送映射注册消息409来发起向映射系统的注册处理，可以在该消息中提供其身份和位置信息，并且可以请求由映射服务器406注册身份和位置信息。在图4中所描绘的示例中，映射注册消息409包括作为前缀的身份信息1.1.0.0/16和位置信息。

[0066] 在接收到映射注册消息409之后，映射服务器406在服务器上的数据库或任何其他数据存储结构中注册接收到的身份和位置信息。

[0067] 在一个实施例中，对端节点(correspondent node，CN)执行DNS查找以便找出节点的身份，并且使用该身份开始将封包发往该节点。

[0068] 如果路由器402a在其缓存中还没有关于该身份的映射条目，则路由器402a可以在映射系统中执行查找。路由器402a可以通过将映射查找消息401发送到映射解析器404来完成查找。在图4中所描绘的示例中，映射查找消息401包括身份前缀“1.1.0.10”和对应于随机数的“n”，以下进行描述。

[0069] 包括身份前缀和随机数的映射查找消息401通过映射系统405被运送到映射服务器406。

[0070] 在一个实施例中，映射服务器406接收包括身份的映射查找消息407，并且解析该身份的位置信息。

[0071] 在一个实施例中，为了解析所提供的身份的位置信息，映射服务器406获得与所提供的身份相关联的位置信息，将该位置信息包括到映射查找408中，并且将映射查找消息

408发送到出口隧道路由器403b。

[0072] 在识别出与身份相关联的位置信息后，映射服务器406将映射查找408传输到出口隧道路由器403b。如以下所描述的，映射查找消息408可以包括随机数的散列(表示为n'＝h(n))。此外，映射查找消息408可以包括加密的信息(表示为HMAC-1)。以下描述生成HMAC-1的处理。

[0073] 在一个实施例中，在接收到映射查找消息408后，出口隧道路由器403b将映射查找消息408作为映射响应消息411a发送到入口隧道路由器402a以提供对应于特定身份的位置信息。

[0074] 替换地，在接收到映射查找消息408后，出口隧道路由器403b在将该消息作为映射响应发送到入口隧道路由器402a之前加密该消息的内容。例如，使用随机数散列n'＝h(n)，出口隧道路由器可以加密包括在消息中的位置信息，生成HMAC-2(以下描述)，并且发送包括散列的随机数(n'＝h(n))、映射服务器406生成的HMAC-1、和出口隧道路由器403b生成的HMAC-2的映射响应消息411c。

[0075] 在一个实施例中，映射响应消息411c还包括PKI-ID和端口标识符。PKI-ID是指示用以认证出口隧道路由器403b的PKI的公钥基础设施(PKI)标识符。例如，PKI-ID可以指示发布密钥的认证机构(CA)。

[0076] 端口标识符是出口隧道路由器403b可以在其上接收关于提供给该出口隧道路由器的证书的查询的端口的标识符。例如，如果在接收到映射响应消息411c之后，入口隧道路由器402a想要验证出口隧道路由器403b是否被授权与映射系统通信，则入口隧道路由器402a可以向由包括在映射响应消息411c中的端口标识符所指示的出口隧道路由器端口发送相应的查询。参照图2提供关于验证出口隧道路由器的授权的详情。

[0077] 在一个实施例中，一旦入口隧道路由器402a确定接收到的消息的内容被折中并且该消息是从被授权的实体接收的，则入口隧道路由器402a开始将数据封包封装在数据平面中并且将数据封包传输到预期目的地。

[0078] 在一个实施例中，映射响应411(a、b或c)包括路由位置信息，并且可选地包括与特定映射相关联的权重和优先级。

[0079] 如果移动设备(例如，节点410b)改变其位置，则该移动设备可以生成另一个映射注册消息409，在该消息中移动设备可以提供其身份和更新后的位置信息。映射注册消息409被映射服务器406接收。映射服务器406更新身份的映射信息并且更新与身份相关联的位置信息。

[0080] 一旦在映射系统中注册或更新了与特定身份相关联的位置信息，则将该位置信息用于去往包括由该特定身份标识的节点的站点的数据封包的封装中。

[0081] 在一个实施例中，数据封包的转发在路由器的数据平面中被执行，而数据封包的封装在路由器的控制平面中被执行。在一个实施例中，需要保护控制平面中的处理。

[0082] 3.0 安全网络地址映射系统的示例

[0083] 在一个实施例中，用于映射系统的安全处理具有以下效果：提供所涉及的成员(诸如，映射解析器404、映射服务器406、路由器402a/b和403a/b)的认证，以及确保所涉及的成员被授权提供映射信息和服务。例如，可能期望保护映射系统免受想要拦截关于映射系统的信息并且干扰映射系统的功能的假冒者的危害。还可能期望防止未被授权的实体操纵映

射系统、由映射服务器存储的信息、以及提供给映射服务器的更新信息。

[0084] 在一些情况下，可以假定映射系统安全并且功能良好，并且因此将映射查找消息传递到其预期目的地。替换地，可以假定封包被传输到除预期目的地之外的位置。

[0085] 此外，本文的安全方法可以假定不可以通过GRE隧道对映射系统进行中间人攻击，并且包括在映射查找消息中的信息(包括随机数)不能由第三方实体读取。在隧道安全时或者如果使用GRE和IPSec来部署隧道，这种假定是合理的，并且因此对映射系统提供了加强的保密性。

[0086] 在一个实施例中，额外的安全机制被用来防止来自位于映射系统外部的实体以及来自可以位于映射系统内的中间人实体的对映射系统的攻击。

[0087] 在一个实施例中，映射系统被实现用于IP前缀，而不必仅用于个别IP地址。实现映射系统以处理IP前缀可以使得映射系统稳健且高效。例如，如果将身份表达为前缀1.1.0.0/32，则一般的服务器将发送对应于1.1.0.0/32的最大IP前缀。因此，如果下一个请求是对于指定为1.1.0.0/32的身份前缀的，则隧道路由器可以依赖于已经接收到的针对前缀1.1.0.0/32的信息。

[0088] 在一个实施例中，映射系统利用与IP地址和IP前缀相关联的额外参数。例如，映射系统可以利用生存时间参数、新鲜度指标和其他参数的特定值。例如，对于移动设备而言，生存时间参数的值可能相对较小，因为移动设备被预期频繁地改变其位置。

[0089] 在一个实施例中，安全机制被设计成防止其中隧道路由器通过在映射响应消息中提供关于其不拥有的身份的位置来请求该身份的情况下的攻击。

[0090] 例如，如果侵入者(攻击者)拦截映射注册消息，改变包括在映射注册消息中的信息，并且将改变后的信息发送到映射系统，则映射系统可以接收到将指示特定设备的两个或更多个不同位置的两个或更多个映射注册消息。存储在映射系统数据库中的信息将由非相干信息建立。

[0091] 根据另一个实例，如果侵入者拦截映射响应消息，改变包括在映射响应消息中的信息，并且将改变后的消息发送到映射系统，则侵入者可能能够将数据流量重定向至他的设备，从而不利地影响数据通信的安全性。

[0092] 根据其他示例，从各个来源(包括侵入者)发送到映射系统的消息可以对网络中的带宽提出高要求。发送高容量的消息可能会拖延网络内的通信，从而不利地影响映射系统的效率。

[0093] 在一个实施例中，可以使用一次性密钥方法和PKI密钥方法来对抗对映射系统的各种攻击。以下分别描述每种方法。

[0094] 3.1 使用一次性密钥保护网络地址映射系统

[0095] 在一个实施例中，假定映射系统本身是可信的，但是与映射系统通信的节点、设备和其他实体是不可信的。

[0096] 安全架构的一个方面是在不对映射系统增加太多复杂性的情况下提供合理的安全等级。

[0097] 在一个实施例中，保护网络地址映射系统是基于实现随机数的一次性密钥方法的。随机数是由在接收到去往特定目的地节点的一个或多个封包后发起与映射系统的通信的节点或隧道路由器生成的随机数。

[0098] 在一个实施例中，假定入口隧道路由器与映射服务器之间的连接是可信且安全的，且因此可以在从入口隧道路由器发送到映射服务器的消息中安全地传送随机数。替换地，如果入口隧道路由器与映射服务器之间的连接不可信，则可以使用仅入口隧道路由器和映射服务器知道的共享密钥来加密该随机数。

[0099] 然而，一旦映射服务器接收到具有随机数的消息，映射服务器就必须在将该消息传输到出口隧道路由器之前保护该消息。因为映射服务器与出口隧道路由器之间的连接被假定为不可信的，所以映射服务器使用随机数来加密消息中的内容并且将具有加密的有效载荷的消息发送到出口隧道路由器。作为加密密钥，映射服务器可以使用例如随机数的散列，如以下将描述的。因此，随机数被称为一次性密钥。

[0100] 随机数本身(或者随机数的散列)可以用来在映射服务器处接收到的消息被从映射服务器发送到出口隧道路由器之前对该消息的内容进行加密。由于出口节点不知道一次性密钥(随机数)，所以出口节点不能解密使用该随机数加密的内容。因此，如果出口隧道路由器确实不可信，则出口节点不能领会拦截到的消息的内容。

[0101] 图1示出了使用一次性密钥保护网络地址映射系统100的方法的一个示例。在方框101，第一前缀中的第一路由器接收去往节点B的一个或多个封包。术语“第一路由器”用来指示隧道路由器或端点节点中的任意一个。例如，第一路由器可以是如图4中所描绘的入口隧道路由器402a/b，或者同样如图4中所描绘的端点节点410a/b(诸如，移动设备)。

[0102] 在接收到去往节点B的一个或多个封包后，第一路由器生成随机数。在一个实施例中，随机数是用来保护发送到映射系统和从映射系统接收的消息的一次性密钥。

[0103] 随机数可以是随机生成的数字。随机数可以在隧道路由器每次接收到去往新目的地的封包时被重新生成。替换地，可以在每次通信会话、拒绝周期、或对于每个特定的网络设备生成一次随机数。也可以实现用于定时随机数生成的其他方法。

[0104] 在一个实施例中，将随机数与身份相关联地进行本地存储，其中针对该身份映射查找被生成。可以将随机数存储在与生成映射查找消息的隧道路由器相关联的存储装置中或者隧道路由器可以与其通信的任何存储装置中。

[0105] 在方框102，第一路由器将第一映射查找消息发送到分布式映射服务。第一映射查找包括如前所述的设备标识符(诸如，身份)和随机数。在一个实施例中，以清楚(未加密)的形式传输包括在消息中的随机生成的随机数(n)。

[0106] 替换地，可以加密随机数。加密的随机数的使用保护消息交换免受被描述为中间人攻击的攻击。如果映射服务器和入口隧道路由器属于相同的域，则可以使用共享密钥来加密随机数。如果映射服务器和入口隧道路由器不属于相同的域(例如，当入口隧道路由器是来自外部网络的访问设备并且动态地获得对映射解析器的访问时)，则可以实现保护路径的其他方法。

[0107] 在一个实施例中，用来加密随机数的密钥在诸如入口隧道路由器的第一路由器与映射服务器之间共享。可以使用密钥来保护在第一路由器与映射服务器之间交换的消息的完整性。

[0108] 在一个实施例中，入口隧道路由器不使用随机数作为加密密钥。随机数在消息中被运送到映射服务器，作为映射服务器用作一次性密钥的信息，在消息被传送到出口隧道路由器之前对消息的内容进行加密。映射服务器使用随机数作为加密密钥来保护通过映射

服务器与出口隧道路由器之间的可能不安全的连接发送的消息的内容。

[0109] 在一个实施例中，在接收到具有加密的随机数的映射查找消息后，映射解析器解密随机数并且将映射查找消息作为解密的消息转发到映射系统。具体来说，将映射查找消息发送到映射服务器。

[0110] 在一个实施例中，可以使用随机数(n)作为密钥来加密身份前缀并且生成HMAC。因此，随机数(n)表示在入口隧道路由器与包括映射解析器和映射服务器二者的映射系统之间共享的一次性密钥。

[0111] 随机数因为其仅被使用一次而被称为一次性密钥，其仅被用来获得特定身份的位置信息。每当生成新的映射查找消息时，可以生成新的随机数并且由入口隧道路由器和映射系统共享该随机数。

[0112] 然而，随机数(共享的秘密)是出口隧道路由器不知道并且未向其公开的，因为假定出口隧道路由器是不可信的实体。例如，如果攻击者获得对于出口隧道路由器的访问，则与出口隧道路由器共享密钥可能会导致映射系统中的安全性的破坏。另外，如果攻击者拦截消息并且确定消息中存在散列值，则与出口隧道路由器共享密钥可能帮助攻击者反转散列处理并且确定随机数(n)的原始值。因此，设计不与出口隧道共享密钥，以保护消息免受获得了对于出口隧道路由器的访问的可能攻击者的篡改。

[0113] 在一个实施例中，发送到出口隧道路由器的消息包括随机数的散列。使用随机数来加密身份前缀并生成HMAC。随机数的散列或HMAC都不可被出口隧道路由器领会。

[0114] 在一个实施例中，在出口隧道路由器将消息发送到入口隧道路由器之前，出口隧道路由器使用随机数的散列作为密钥来进一步加密消息的一部分。包括在由出口隧道路由器从映射服务器接收到的消息中的随机数散列可以用作额外密钥。图3中描述了出口隧道路由器将散列的随机数用作额外密钥的示例。

[0115] 图3示出了保护网络地址映射系统的方法300的一个示例。

[0116] 在方框301，出口隧道路由器使用散列的随机数来加密映射查找消息的内容。在一个实施例中，在消息被从出口隧道路由器传输到入口隧道路由器之前，出口隧道路由器使用散列的随机数来保护消息的内容。散列的随机数被用作密钥来保护出口隧道路由器与入口隧道路由器之间的连接。

[0117] 随机数本身被用作密钥来保护由映射服务器传输到出口隧道路由器的位置信息，而散列的随机数被用作另一个密钥来保护出口隧道路由器与入口隧道路由器之间的连接。

[0118] 在一个实施例中，出口隧道路由器使用散列的随机数加密的消息的一部分包括映射服务器从对于特定身份的映射获得的身份信息和/或位置信息。位置信息可能已经由映射服务器使用随机数加密。出口隧道路由器可以使用散列的随机数来加密包括在从映射服务器接收到的消息中的已经加密的路由器位置信息。

[0119] 由于出口隧道路由器不知道原始随机数的值，所以出口隧道路由器不能解密由映射系统加密的信息。但是，出口隧道路由器可以使用散列的随机数来加密已经加密一次的位置信息。出口隧道路由器通过加密已经加密一次的信息生成的双加密的信息在本文中被称为HMAC-2。

[0120] 在方框302，出口隧道路由器生成已经散列的随机数的散列。出口隧道生成已经散列的随机数的散列，从而生成散列的随机数的散列。如上所述，随机数的第一散列可以由映

射服务器生成。在从映射服务器接收到映射查找消息后，出口隧道路由器可以再次对散列的随机数进行散列。散列的随机数的散列在本文称为n”＝h(h(n))。

[0121] 在方框303，出口隧道路由器生成映射响应消息。映射响应可以包括身份信息(以上描述的)、散列的随机数的散列(n”＝h(h(n)))、由映射服务器使用随机数加密的加密一次的位置信息(HMAC-1)、以及由出口隧道路由器通过对加密一次的位置信息进行加密生成的双加密的位置信息(HMAC-2)。消息可以被格式化为在图4中描绘的映射响应消息411c。

[0122] 在方框304，出口隧道路由器将映射响应消息发送到入口隧道路由器。在一个实施例中，出口隧道路由器发送包括身份信息、散列的随机数的散列(n”＝h(h(n)))、由映射服务器使用随机数加密的加密一次的位置信息(HMAC-1)、以及由出口隧道路由器通过对加密一次的位置信息进行加密生成的双加密的位置信息(HMAC-2)的消息。图4中描绘了映射响应消息411c。

[0123] 再次参照图1，在方框103，第一路由器(入口隧道路由器)从第二路由器(出口隧道路由器)接收映射响应消息。

[0124] 在一个实施例中，映射响应包括以上描述的双散列的随机数(n”＝h(h(n)))、加密一次的位置信息(HMAC-1)、以及双加密的位置信息(HMAC-2)，在图4中被描绘为映射响应411c。

[0125] 在方框104，第一路由器确定随机数是否有效。

[0126] 响应于发送具有身份和随机数的映射查找消息，隧道路由器接收映射响应消息。基于映射响应消息的内容，隧道路由器确定映射响应消息是否合法。例如，在响应于发送具有特定身份和特定随机数的映射查找消息而接收到映射响应消息后，隧道路由器生成存储在入口隧道路由器处的随机数的散列，并且比较所生成的散列的随机数是否匹配包括在映射响应消息中的散列的随机数。如果随机数匹配，则隧道路由器确定映射查找消息和映射响应消息未由敌对方拦截，并且通信是安全的。

[0127] 由于在入口隧道路由器与映射系统之间共享随机数，所以入口隧道路由器可以检索其自身的随机数复本，生成随机数的散列，并且将随机数的散列与从接收到的映射响应提取的散列的随机数进行比较。

[0128] 在一个实施例中，使用嵌入在映射查找和映射响应中的随机数的方法允许确定接收到的映射响应消息是否是未经请求的映射响应消息。如果嵌入在映射响应消息中的随机数不匹配用于相同身份的映射查找中的随机数，则最有可能的是映射响应消息是未经请求的并且可能是由侵入者生成的。

[0129] 另外，使用随机数，入口隧道路由器可以对加密的位置信息(HMAC-1)进行解密，并且使用散列的随机数，入口隧道路由器可以对双加密的位置信息(HMAC-2)进行解密。

[0130] 如果随机数有效，则处理进行到执行步骤106；否则，处理进行到执行步骤105，其中第一路由器破坏映射(如果这是必要的)。

[0131] 在方框106，第一路由器建立与第二路由器的数据报传输层安全(DTLS)会话，并且将第二映射查找直接发送到第二路由器。DTLS协议为诸如UDP的数据报协议提供通信隐私。DTLS允许基于数据报的应用以被设计成防止偷听、篡改或消息伪造的方式来通信。图2中描述了建立DTLS会话。

[0132] 还可以使用GRE和IPsec来保护来自节点和隧道路由器的数据封包的通信。

[0133] 在方框107，第一路由器确定第二路由器是否被授权与映射系统通信。第一路由器可以是入口隧道路由器，而第二路由器可以是出口隧道路由器。以下在图2中描述了用于确定第二路由器是否被授权与映射系统通信的方法之一。

[0134] 再次参照图1，如果第二路由器被授权与映射系统通信，则处理进行到执行步骤109；否则，处理进行到执行步骤108，其中在步骤108第一路由器终止先前建立的安全会话并且破坏与第二路由器相关联的任何映射。

[0135] 在方框109，第一路由器本地安装映射并且将一个或多个数据封包发送到节点B。映射可以包括身份与位置之间的映射，从而指示与设备的位置相关联的设备标识符。

[0136] 使用随机数允许确认接收到的映射响应消息是否匹配先前发送的映射查找消息。最有可能的，侵入者(攻击者)不知道存在于消息中的随机数并且没有认识到需要消息中的随机数。因此，即使他生成了不合法的映射响应消息，该消息也将不会包括有效的随机数。没有有效随机数的消息可以容易地被映射系统识别为不合法。

[0137] 例如，侵入者(攻击者)拦截具有特定身份的映射查找消息，并且从拦截到的映射查找消息中提取身份；然而，他没有认出消息中的随机数。侵入者生成映射响应消息，关联和由特定身份标识出的设备的实际位置信息不同的位置信息，并且传播所生成的具有不正确的设备位置信息的映射响应消息。一旦这样的映射响应消息被隧道路由器接收到，则隧道路由器分析消息的内容，确定在消息中缺少有效随机数并且忽略该消息。因此，使用随机数提供了用于使用映射查找和映射响应消息来交换信息的安全机制。然而，在一些应用中，可能需要更强的安全机制。

[0138] 在一个实施例中，通过允许假定不能信任映射系统的额外机制来加强基于随机数的安全措施。

[0139] 3.2 使用PKI密钥保护网络地址映射系统

[0140] 在本部分中，假定映射系统是不可信系统。例如，当映射系统是由不同的组织外包、维护或者在不同的国家维护时，不能信任系统的完整性。维护映射系统的完整性可能需要实现特定的安全机制。

[0141] 图2示出了使用PKI密钥保护网络地址映射系统200的方法的一个实例。

[0142] 在一个实施例中，使用PKI密钥保护映射系统200包括将证书与出口隧道路由器相关联。

[0143] 在一些情况下，路由器可能不信任映射系统、目的地映射服务器、或出口隧道路由器(其可能是映射系统的一部分)。对于这些情况，路由器可以尝试验证映射系统设备的证书来确定设备是否被授权与映射系统合作。

[0144] 在一个实施例中，一次性密钥安全基础设施被修改并且扩展以并入提供路由器所拥有的身份前缀的强认证的PKI。

[0145] 在一个实施例中，入口隧道路由器可以请求出口隧道路由器证明出口隧道路由器确实被授权将消息传达到映射系统和从映射系统传达消息。例如，入口隧道路由器可以请求出口隧道路由器提供其证书以证明出口隧道路由器的授权。

[0146] 在一个实施例中，当路由器请求特定身份的位置信息时，路由器将映射查找消息传输到映射系统，并且响应地接收映射响应消息。

[0147] 在方框201，诸如入口隧道路由器的服务器从出口隧道路由器接收包括特定身份

的位置信息的映射响应消息。

[0148] 在一个实施例中，映射响应消息含有向路由器指示是否支持基于PKI的安全的字段。

[0149] 如果路由器支持基于PKI的安全，则路由器可以通过数据报传输层安全(DTLS)会话将另一个映射查找消息直接传输到最近获悉的路由器位置以便向该路由器请求证书。图4中描绘的映射查找消息411b包括身份和服务器向路由器请求证书的指示。

[0150] 响应于接收到映射查找消息，路由器可以将证书连同从认证机构(CA)的根发出的完全信任链一起包括到DTLS协议数据报中，并且通过映射响应消息来应答。

[0151] 在方框202，响应于将另一个映射查找消息发送到出口隧道路由器，入口隧道路由器接收具有证书的消息。

[0152] 在方框202，入口隧道路由器从消息提取证书并且确定出口隧道路由器是否是有权的。例如，路由器可以验证证书列表和包括在证书中的身份前缀链。此外，路由器可以验证包括在消息中的身份前缀是否是有效路由器证书。

[0153] 在方框204，如果确定出口隧道路由器有权与映射系统通信，则处理进行到步骤205，其中在步骤205路由器可以将包括在先前接收到的映射响应消息中的映射安装在其本地缓存中。然而，如果确定出口隧道路由器未经授权，则处理进行到步骤206，其中在步骤206中入口隧道路由器不安装映射，并且可选地破坏映射。

[0154] 在一个实施例中，基于PKI的安全方法允许验证映射系统的组件是否可信。例如，如果出口隧道路由器和入口隧道路由器位于不同的国家并且入口隧道路由器无法肯定出口隧道路由器是否可信，则所呈现的基于PKI的方法允许验证出口隧道路由器是否确实可信。仅在出口隧道路由器可以呈现有效证书(和从认证机构(CA)的根发出的完全信任链)的情况下，才可以认为出口隧道路由器是可信实体。

[0155] 在一个实施例中，将证书预先分发给各个路由器并且在分发证书时建立信任链。例如，证书可以使用DTLS来分发，并且可以涉及在实体之间交换几个消息以便为实体提供相应证书。

[0156] 在一个实施例中，映射服务器用作出口隧道路由器。映射服务器和出口隧道路由器可以是相同的设备。因此，也可以预先向映射服务器提供证书。

[0157] 4.0 实现机构——硬件概述

[0158] 根据一个实施例，本文描述的技术由一个或多个专用计算设备实现。专用计算设备可以被硬接线以执行这些技术，或者可以包括被永久编程以执行这些技术的诸如一个或多个专用集成电路(ASIC)或现场可编程门阵列(FPGA)的数字电子设备，或者可以包括被编程以根据固件、存储器、其他存储装置或组合中的程序指令来执行这些技术的一个或多个通用硬件处理器。这些专用计算设备还可以将定制的硬接线逻辑、ASIC或FPGA与定制的编程组合来实现这些技术。专用计算设备可以是台式计算机系统、便携式计算机系统、手持设备、联网设备或并入有硬接线和/或程序逻辑以实施这些技术的任何其他设备。

[0159] 例如，图5是示出本发明的实施例可以在其上实现的计算机系统500的框图。计算机系统500包括用于传送信息的总线502或其他通信机制、以及与总线502耦合用于处理信息的硬件处理器504。硬件处理器504可以是例如通用微处理器。

[0160] 计算机系统500还包括耦合到总线502用于存储将由处理器504执行的信息和指令

的主存储器506，诸如随机存取存储器(RAM)或其他动态存储设备。主存储器506还可以用于在由处理器504执行的指令的执行期间存储临时变量或其他中间信息。这些指令在被存储在处理器504可访问的非瞬态存储媒体中时使得计算机系统500成为被定制为执行指令中指定的操作的专用机器。

[0161] 计算机系统500进一步包括耦合到总线502、用于存储用于处理器504的静态信息和指令的只读存储器(ROM)508或其他静态存储设备。诸如磁盘或光盘的存储设备510被提供并且被耦合到总线502，用于存储信息和指令。

[0162] 计算机系统500可以通过总线502耦合到显示器512(诸如，阴极射线管(CRT))，用于将信息显示给计算机用户。包括字母数字和其他键的输入设备514耦合到总线502，用于将信息和命令选择传送给处理器504。另一种类型的用户输入设备是光标控制器516，诸如鼠标、轨迹球或光标方向键，用于将方向信息和命令选择传送给处理器504并且用于控制显示器512上的光标移动。此输入设备通常具有沿两个轴线(第一轴线(例如x)和第二轴线(例如y))的两个自由度，这允许设备指定平面中的位置。

[0163] 计算机系统500可以使用定制的硬接线逻辑、一个或多个ASIC或FPGA、固件和/或与计算机系统组合使得或编程计算机系统500成为专用机器的程序逻辑来实现本文描述的技术。根据一个实施例，本文的技术由计算机系统500响应于处理器504执行包含在主存储器506中的一个或多个指令的一个或多个序列来执行。这些指令可以被从诸如存储设备510的另一个存储介质读入主存储器506中。包含在主存储器506中的指令序列的执行使得处理器504执行本文描述的处理步骤。在替代实施例中，硬接线电路可以替代软件指令使用或者与之组合使用。

[0164] 本文使用的术语“存储媒体”指代存储促使机器以特定方式进行操作的数据和/或指令的任何非瞬态媒体。这种存储媒体可以包括非易失性媒体和/或易失性媒体。非易失性媒体包括例如光盘或磁盘，诸如存储设备510。易失性媒体包括动态存储器，诸如主存储器506。普通形式的存储媒体包括例如软盘、软磁盘、硬盘、固态驱动器、磁带或任何其他磁性数据存储介质、CD-ROM、任何其他光学数据存储介质、具有孔图案的任何物理介质、RAM、PROM和EPROM、FLASH-EPROM、NVRAM、任何其他存储器芯片或磁片盒。

[0165] 存储媒体与传输媒体不同，但是可以与其结合使用。传输媒体参与在存储媒体之间传递信息。例如，传输媒体包括同轴电缆、铜线或光纤，包括含有总线502的导线。传输媒体也可以采用声波或光波的形式，诸如在无线电波或红外线数据通信期间生成的那些波。

[0166] 在将一个或多个指令的一个或多个序列运载到处理器504以供执行的过程中可能涉及各种形式的媒体。例如，指令最初可以被承载于远程计算机的磁盘或固态驱动器上。远程计算机可以将指令载入其动态存储器中并且使用调制解调器通过电话线发送指令。计算机系统500本地的调制解调器可以接收电话线上的数据并且使用红外线发射器来将数据转换成红外线信号。红外线检测器可以接收在红外线信号中运载的数据并且适当的电路可以将数据放置于总线502上。总线502将数据运载到主存储器506，处理器504从该主存储器检索指令并执行指令。主存储器506接收到的指令可以在由处理器504执行之前或之后可选地存储在存储设备510上。

[0167] 计算机系统500还包括耦合到总线502的通信接口518。通信接口518提供耦合到网络链路520(网络链路520连接到本地网络522)的双向数据通信。例如，通信接口518可以是

综合业务数字网络(ISDN)卡、电缆调制解调器、卫星调制解调器或提供到相应类型的电话线的数据通信连接的调制解调器。作为另一个实例，通信接口518可以是提供到兼容的LAN的数据通信连接的局域网(LAN)卡。也可以实现无线链路。在任何这些实现方式中，通信接口518发送和接收运载表示各种类型的信息的数字数据流的电、电磁或光学信号。

[0168] 网络链路520通常提供通过一个或多个网络到其他数据服务的数据通信。例如，网络链路520可以提供通过本地网络522到主机计算机524或到由因特网服务提供商(ISP)526所操作的数据设备的连接。ISP 526进而提供通过全球封包数据通信网络(现在通常称为“因特网”)528的数据通信。本地网络522和因特网528都使用运载数字数据流的电、电磁或光学信号。通过网络链路520并且通过将数字信号运载到计算机系统500以及从计算机系统500运载数字信号的通信接口518的信号、以及通过各种网络的信号是传输媒体的示例性形式。

[0169] 计算机系统500可以通过网络、网络链路520和通信接口518来发送消息和接收数据(包括程序代码)。在因特网实例中，服务器530可以通过因特网528、ISP 526、本地网络522和通信接口518传输用于应用程序的所请求的代码。

[0170] 接收到的代码可以在其被接收和/或存储在存储设备510中时由处理器504执行，或者存储在其他非易失性存储器中以供稍后执行。

[0171] 在以上说明书中，已经参照可能根据实施方式而变化的若干特定细节描述了本发明的实施例。因此，说明书和附图被认为是说明性而非限制性意义。本发明的范围唯一且排他性指标并且申请人打算作为本发明的范围的是由此申请生成的权利要求的集合的字面和等效范围，以其中这些权利要求生成的包括任何随后的校正的特定形式。

[0172] 5.0 扩展和替代

[0173] 在以上说明书中，已经参照可能根据实施方式而变化的若干特定细节描述了本发明的实施例。因此，说明书和附图被认为是说明性而非限制性意义。

[0174] 实施例包括：

[0175] 1.一种由映射服务器执行的方法，所述方法包括：

[0176] 在维护将网络设备标识符与网络设备位置相关联的多个映射的映射服务器处：

[0177] 接收包括特定网络设备标识符和密钥的第一版本的映射查找；

[0178] 生成所述密钥的第二版本；

[0179] 生成多个地址前缀，与所述特定网络设备标识符相关联的路由器对所述地址前缀是有权的；

[0180] 向所述路由器发送所述密钥的所述第二版本和所述多个地址前缀。

[0181] 2.如权利要求1所述的方法，其中，生成所述多个地址前缀包括将散列函数应用于所述多个网络地址前缀，其中所述散列函数使用密钥作为散列关键字。

[0182] 3.如权利要求1所述的方法，其中，所述映射查找由第一路由器在尝试将一个或多个封包发送到与所述特定设备标识符相关联的网络节点时发出。

[0183] 4.如权利要求2所述的方法，其中，所述网络节点与由所述路由器服务的所述多个地址前缀中的特定地址前缀相关联。

[0184] 5.如权利要求4所述的方法，进一步包括：在所述发送之前，与所述路由器建立DTLS会话，并且基于所述DTLS会话向所述路由器发送所述密钥的所述第二版本和所述多个

地址前缀。

[0185] 6.如权利要求1所述的方法，进一步包括：基于所述多个映射，验证所述特定设备标识符对应于特定设备位置或地址前缀。

[0186] 7.如权利要求1所述的方法，进一步包括：从被配置成转发来自多个其他地址前缀的映射请求的映射解析器接收所述映射查找。

[0187] 8.一种由映射解析器执行的方法，所述方法包括：

[0188] 从与第一网络节点相关联的第一路由器接收包括与第二网络节点相关联的特定设备标识符和密钥的映射查找；

[0189] 将所述映射查找转发到维护将设备标识符与设备位置相关联的多个映射的映射服务器。

[0190] 9.如权利要求8所述的方法，进一步包括：在接收所述映射请求之前，与所述第一路由器建立安全连接。

[0191] 10.如权利要求9所述的方法，其中，所述安全连接是DTLS连接。

[0192] 11.如权利要求9所述的方法，进一步包括：确定所述映射查找无效并且将负映射响应发送到所述第一路由器。

[0193] 12.如权利要求9所述的方法，其中，所述第一路由器和所述第二路由器在不同的地址前缀中。

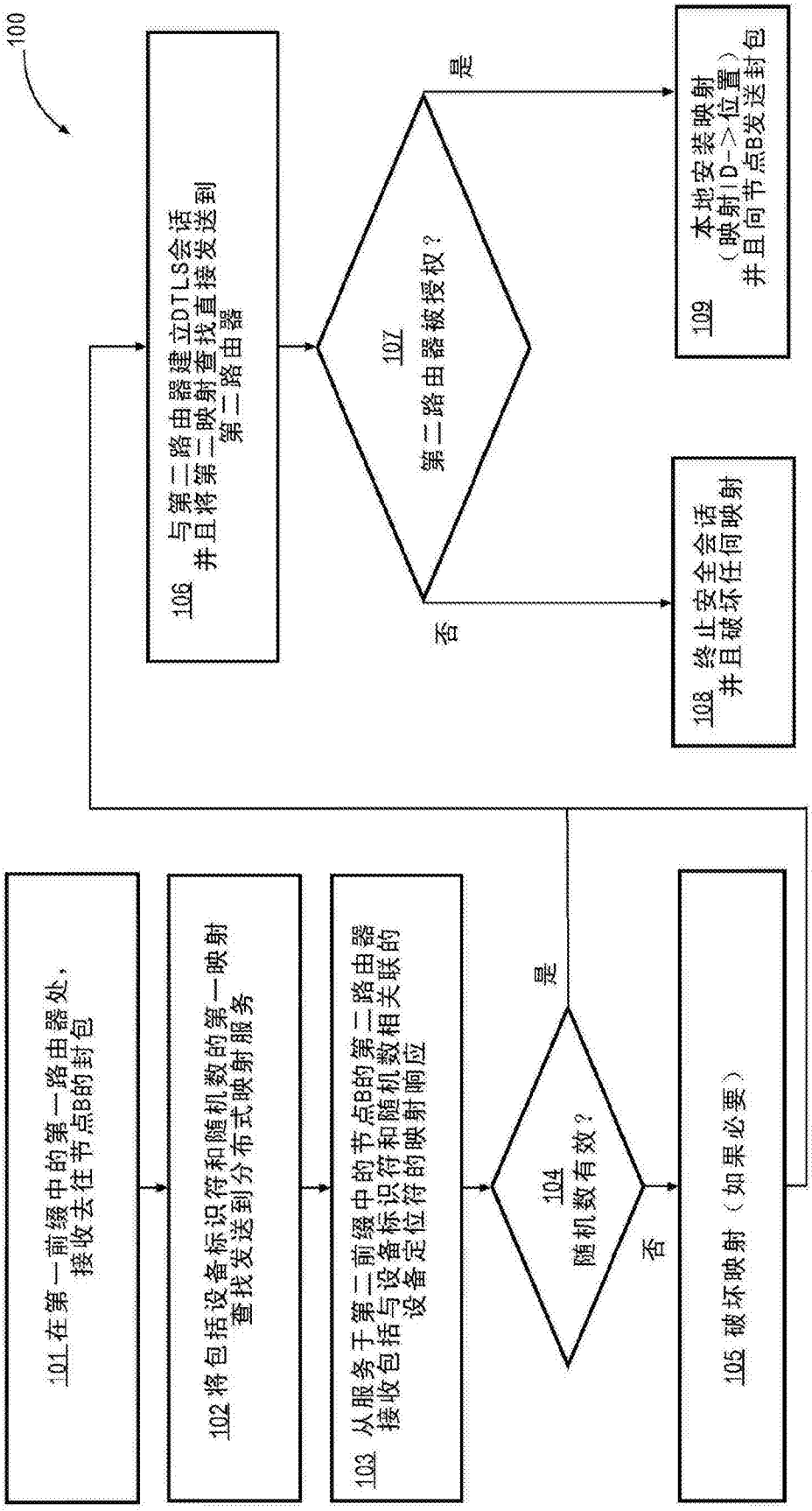

100
101 在第一前缀中的第一路由器处，
接收去往节点B的封包
102 将包括设备标识符和随机数的第一映射
查找发送到分布式映射服务
103 从服务于第二前缀中的节点B的第二路由器
接收包括与设备标识符和随机数相关联的
设备定位符的映射响应
104
随机数有效？
否
是
105 破坏映射（如果必要）
106 与第二路由器建立DTLS会话
并且将第二映射查找直接发送到
第二路由器
107
第二路由器被授权？
否
是
108 终止安全会话
并且破坏任何映射
109 本地安装映射
（映射ID->位置）
并且向节点B发送封包

图1

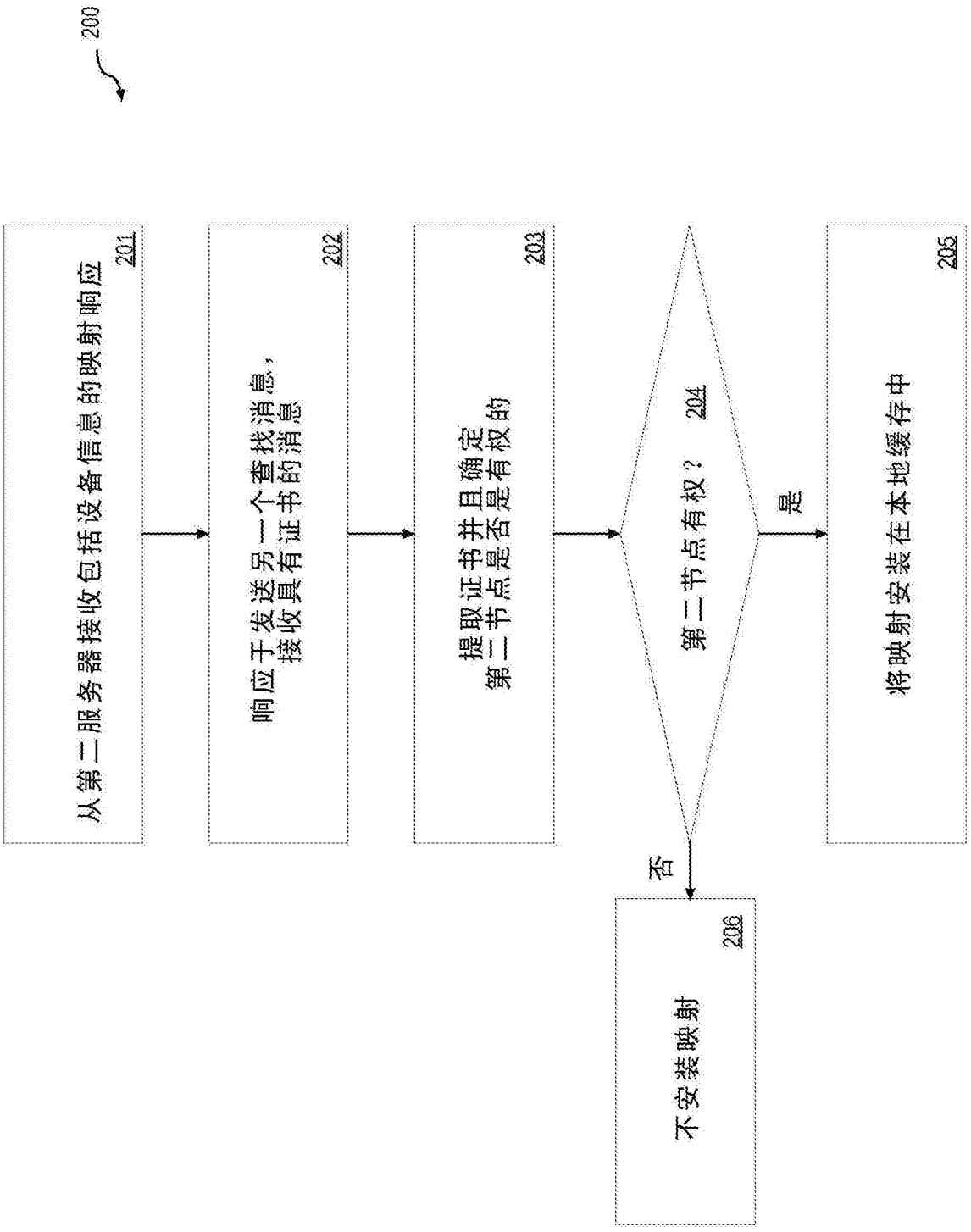

200
从第二服务器接收包括设备信息的映射响应
201
响应于发送另一个查找消息，
接收具有证书的消息
202
提取证书并且确定
第二节点是否是有权的
203
第二节点有权？ 204
是
否
将映射安装在本地缓存中
205
不安装映射
206

图2

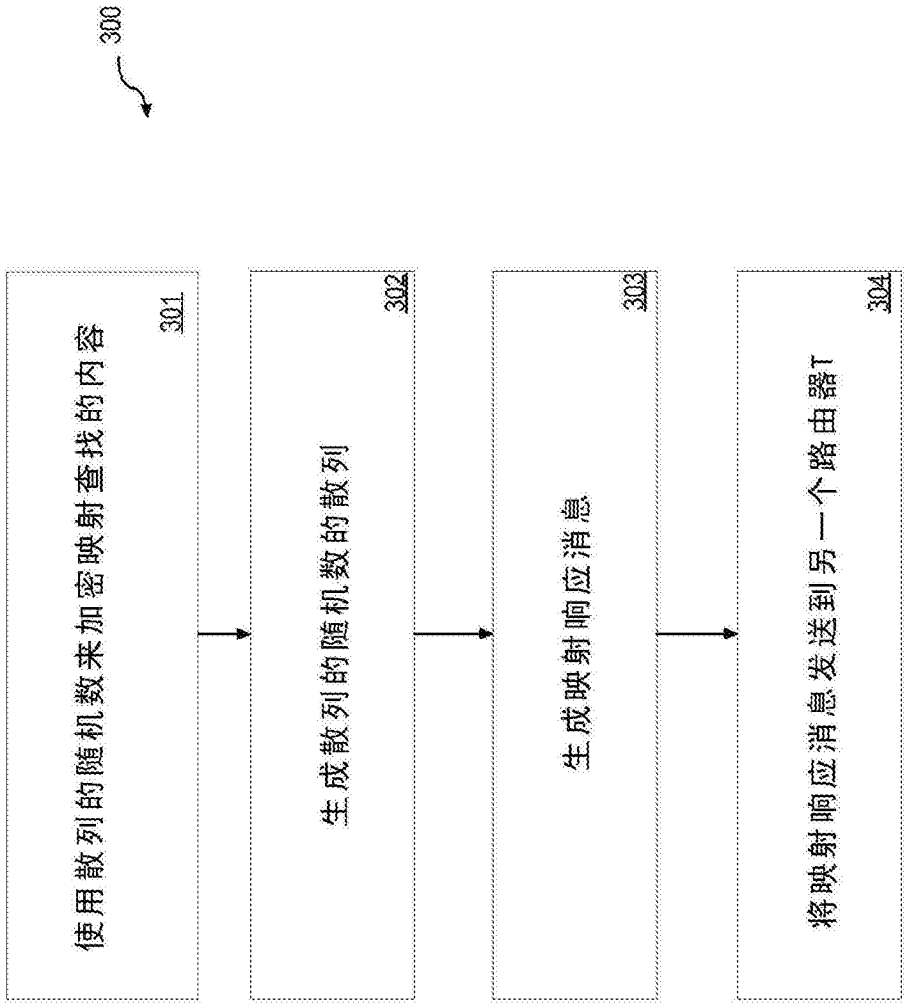

300
使用散列的随机数来加密映射查找的内容
301
生成散列的随机数的散列
302
生成映射响应消息
303
将映射响应消息发送到另一个路由器T
304

图3

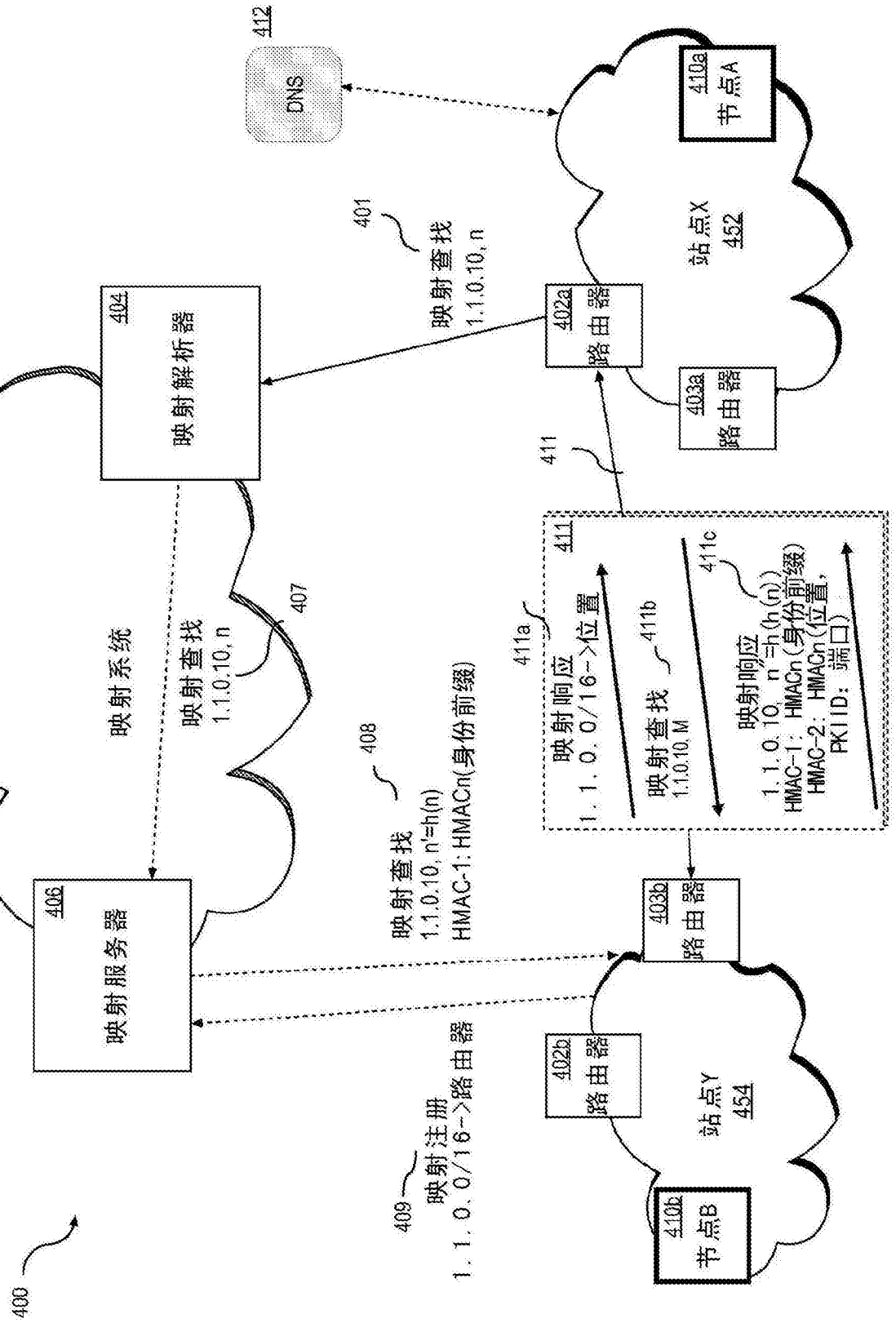

412
DNS
410a
节点A
站点X
452
401
映射查找
1.1.0.10, n
402a
路由器
403a
路由器
404
映射解析器
411
405
映射系统
映射查找
1.1.0.10, n
407
411
411a
映射响应
1.1.0.0/16->位置
411b
映射查找
1.1.0.10, M
411c
映射响应
1.1.0.10, n'=h(n)
HMAC-1: HMACn(身份前缀)
HMAC-2: HMACn(位置, PKI ID: 端口)
408
映射查找
1.1.0.10, n'=h(n)
HMAC-1: HMACn(身份前缀)
406
映射服务器
403b
路由器
402b
路由器
站点Y
454
410b
节点B
409
映射注册
1.1.0.0/16->路由器
400

图4

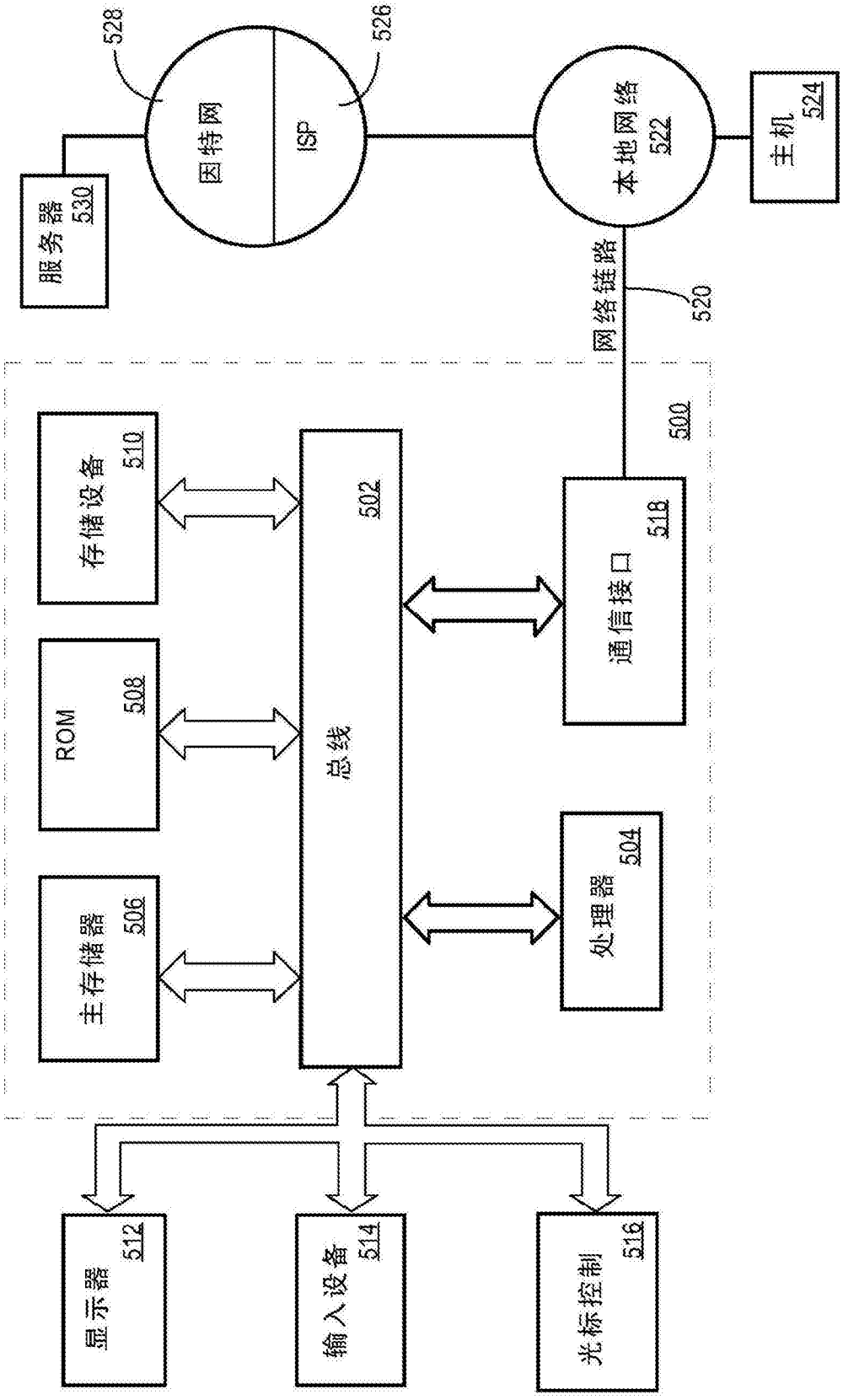

528
因特网
ISP
526
服务器
530
本地网络
522
主机
524
网络链路
520
500
存储设备
510
502
通信接口
518
ROM
508
总线
主存储器
506
处理器
504
显示器
512
输入设备
514
光标控制
516

图5