(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112514350 B
(45)授权公告日 2023.10.20

(21)申请号 201980051584.6
(22)申请日 2019.06.28
(65)同一申请的已公布的文献号
申请公布号 CN 112514350 A
(43)申请公布日 2021.03.16
(30)优先权数据
1856015 2018.06.29 FR
(85)PCT国际申请进入国家阶段日
2021.02.02
(86)PCT国际申请的申请数据
PCT/FR2019/051609 2019.06.28
(87)PCT国际申请的公布数据
WO2020/002856 FR 2020.01.02
(73)专利权人 奥兰治
地址 法国巴黎
(72)发明人 M.布卡戴尔 C.贾克奎尼特
(74)专利代理机构 北京市柳沈律师事务所 11105
专利代理师 李芳华
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/32(2006.01)
H04L 61/5014(2022.01)
(56)对比文件
CN 103563294 A,2014.02.05
CN 1937499 A,2007.03.28
US 2018041468 A1,2018.02.08
US 2018109554 A1,2018.04.19
审查员 许婵

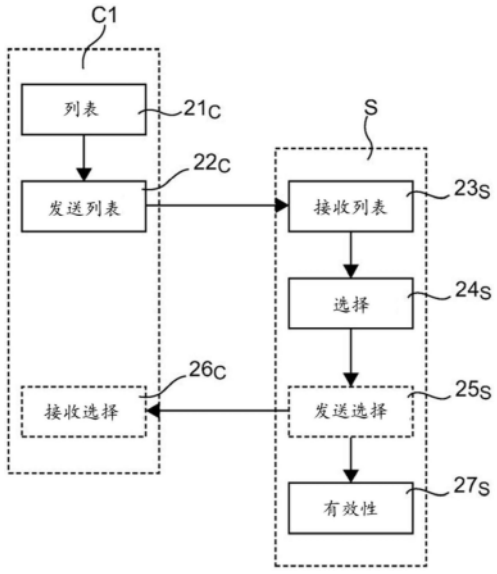
权利要求书4页 说明书20页 附图9页

(54)发明名称

用于核实IP资源的有效性的方法以及相关联的访问控制服务器、验证服务器、客户端节点、中继节点和计算机程序

(57)摘要

本发明涉及一种在访问控制服务器中实施的用于核实与客户端域相关联的IP资源的有效性的方法，所述方法包括：-接收(23S)从所述客户端域的客户端节点发送到所述访问控制服务器的与所述客户端域相关联的至少一个IP资源的列表；-从所述列表当中选择(24S)至少一个待验证的IP资源；以及-核实(27S)所述至少一个所选择的IP资源的有效性。



CN 112514350 B

1.一种用于核实与客户端域相关联的IP资源的有效性的方法,所述方法在被称为访问控制服务器(14)的服务器中实施,所述方法包括:

-接收(23_S)从所述客户端域的客户端节点(111)发送到所述访问控制服务器(14)的、与所述客户端域相关联的至少一个IP资源的列表;

-从所述列表中选择(24_S)至少一个待验证的IP资源;以及

-核实(27_S)所述至少一个所选择的IP资源是否与所述客户端域相关联,

其中,所述客户端域是分布式拒绝服务开放威胁信令(DOTS)域,所述访问控制服务器(14)是DOTS服务器,并且所述客户端节点(111)是DOTS客户端,

其中,所述方法还包括:在由所述访问控制服务器(14)维护的DOTS条目的表中,删除指示不属于由所述客户端节点(111)发送的列表的一部分的IP资源的DOTS条目,或者拒绝指示不属于由所述客户端节点(111)发送的列表的一部分的IP资源的DOTS请求。

2.根据权利要求1所述的方法,其特征在于,所述核实(27_S)包括:

-向至少一个所选择的IP资源发送(31_S)至少一个请求,所述请求旨在由与所述至少一个所选择的IP资源相关联的所述客户端域的至少一个中继节点(112)接收或拦截,所述请求包括控制消息;

-接收(36_S)由所述客户端节点(111)发送到所述访问控制服务器(14)的、包括所述控制消息的信息特征项的响应,所述中继节点(112)先前已经将所述请求中继到所述客户端节点(111);以及

-验证(37_S)通过关联所述请求和所述响应而选择的所述至少一个IP资源。

3.根据权利要求1所述的方法,其特征在于,所述核实包括:

-获得表示所述客户端域的身份的信息项;

-识别与所述至少一个所选择的IP资源相关联的至少一个验证服务器;以及

-向所述至少一个验证服务器发送至少一个请求,所述请求包括所述表示所述客户端域的身份的信息项和所述至少一个所选择的IP资源。

4.一种用于声明与客户端域相关联的IP资源的方法,所述方法在所述客户端域的客户端节点(111)中实施,所述方法包括:

-获得(21_C)与所述客户端域相关联的至少一个IP资源的列表;以及

-将所述列表发送(22_C)到访问控制服务器(14),所述访问控制服务器(14)被配置为核实所述至少一个IP资源是否与所述客户端域相关联,

其中,所述客户端域是分布式拒绝服务开放威胁信令(DOTS)域,所述访问控制服务器(14)是DOTS服务器,并且所述客户端节点(111)是DOTS客户端,

其中,所述访问控制服务器(14)还被配置为:在由所述访问控制服务器(14)维护的DOTS条目的表中,删除指示不属于由所述客户端节点(111)发送的列表的一部分的IP资源的DOTS条目,或者被配置为拒绝指示不属于由所述客户端节点(111)发送的列表的一部分的IP资源的DOTS请求。

5.根据权利要求4所述的方法,其特征在于,所述方法还包括:

-经由与由所述访问控制服务器从所述列表中选择的至少一个IP资源相关联的所述客户端域的至少一个中继节点(112),接收(34_C)源自所述访问控制服务器(14)的至少一个请求,所述请求包括控制消息;以及

-向所述访问控制服务器(14)发送(35_C)包括所述控制消息的信息特征项的响应。

6.根据权利要求4所述的方法,其特征在于,所述方法还包括:

-接收表示所述客户端域的身份的信息项,所述信息项由与由所述访问控制服务器从所述列表中选择的至少一个IP资源相关联的验证服务器生成;以及

-向所述访问控制服务器发送所述表示所述客户端域的身份的信息项。

7.一种用于处理对于与客户端域相关联的至少一个IP资源验证请求的方法,所述方法在与由访问控制服务器(14)从列表中选择的至少一个IP资源相关联的所述客户端域的中继节点(112)中实施,所述列表是与客户端域相关联的至少一个IP资源的列表,所述列表先前从所述客户端域的客户端节点(111)被发送到所述访问控制服务器,

所述方法包括:

-接收或拦截(32_R)源自所述访问控制服务器的至少一个请求,所述请求包括控制消息;以及

-向所述客户端节点发送(33_R)所述至少一个请求,

其中,所述客户端域是分布式拒绝服务开放威胁信令(DOTS)域,所述访问控制服务器(14)是DOTS服务器,并且所述客户端节点(111)是DOTS客户端,

其中,所述访问控制服务器(14)还被配置为在由所述访问控制服务器(14)维护的DOTS条目的表中,删除指示不属于由所述客户端节点(111)发送的列表的一部分的IP资源的DOTS条目,或者被配置为拒绝指示不属于由所述客户端节点(111)发送的列表的一部分的IP资源的DOTS请求。

8.一种用于核实与客户端域相关联的IP资源的有效性的方法,所述方法在与由访问控制服务器从列表中选择的至少一个IP资源相关联的验证服务器中实施,所述列表是与客户端域相关联的至少一个IP资源的列表,所述列表先前从所述客户端域的客户端节点被发送到所述访问控制服务器,

所述方法包括:

-接收至少一个请求,所述请求包括表示客户端域的身份的信息项和所述至少一个所选择的IP资源;

-基于所述表示客户端域的身份的所述信息项来识别所述客户端域;以及

-考虑客户端域的身份,核实所述至少一个所选择的IP资源与客户端域的关联,

其中,所述客户端域是分布式拒绝服务开放威胁信令(DOTS)域,所述访问控制服务器是DOTS服务器,并且所述客户端节点是DOTS客户端,

其中,所述访问控制服务器还被配置为在由所述访问控制服务器维护的DOTS条目的表中,删除指示不属于由所述客户端节点发送的列表的一部分的IP资源的DOTS条目,或者被配置为拒绝指示不属于由所述客户端节点发送的列表的一部分的IP资源的DOTS请求。

9.根据权利要求8所述的方法,其特征在于,所述方法先前实施:

-确定表示所述客户端域的身份的所述信息项(HASH);以及

-向所述客户端节点发送所述表示所述客户端域的身份的信息项。

10.根据权利要求8至9中任一项所述的方法,其特征在于,有效期关联于与客户端域相关联的至少一个IP资源的所述列表。

11.一种访问控制服务器,包括存储器和处理单元,所述存储器存储有计算机程序,所

述处理单元配备有至少一个可编程计算机器或一个专用计算机器,所述计算机程序被所述处理单元执行以实施以下步骤来核实与客户端域相关联的IP资源的有效性:

-接收从所述客户端域的客户端节点发送到所述访问控制服务器的、与所述客户端域相关联的至少一个IP资源的列表;

-从所述列表中选择至少一个待验证的IP资源;以及

-核实所述至少一个所选择的IP资源是否与所述客户端域相关联,

其中,所述客户端域是分布式拒绝服务开放威胁信令(DOTS)域,所述访问控制服务器是DOTS服务器,并且所述客户端节点是DOTS客户端,

其中,所述访问控制服务器还被配置为在由所述访问控制服务器维护的DOTS条目的表中,删除指示不属于由所述客户端节点发送的列表的一部分的IP资源的DOTS条目,或者被配置为拒绝指示不属于由所述客户端节点发送的列表的一部分的IP资源的DOTS请求。

12.一种客户端节点,包括存储器和处理单元,所述存储器存储有计算机程序,所述处理单元配备有至少一个可编程计算机器或一个专用计算机器,所述计算机程序被所述处理单元执行以实施以下步骤来核实与客户端节点所属的客户端域相关联的IP资源的有效性:

-获得与客户端域相关联的至少一个IP资源的列表;以及

-将所述列表发送到访问控制服务器,所述访问控制服务器被配置为核实所述至少一个IP资源是否与所述客户端域相关联,

其中,所述客户端域是分布式拒绝服务开放威胁信令(DOTS)域,所述访问控制服务器是DOTS服务器,并且所述客户端节点是DOTS客户端,

其中,所述访问控制服务器还被配置为在由所述访问控制服务器维护的DOTS条目的表中,删除指示不属于由所述客户端节点发送的列表的一部分的IP资源的DOTS条目,或者被配置为拒绝指示不属于由所述客户端节点发送的列表的一部分的IP资源的DOTS请求。

13.一种中继节点,包括存储器和处理单元,所述存储器存储有计算机程序,所述处理单元配备有至少一个可编程计算机器或一个专用计算机器,所述计算机程序被所述处理单元执行以实施以下步骤来处理对于与中继节点所属的客户端域相关联的IP资源的至少一个验证请求:

-接收或拦截源自访问控制服务器的至少一个请求,所述至少一个请求包括控制消息;以及

-将所述至少一个请求发送到所述客户端域的客户端节点,

所述中继节点由所述访问控制服务器从列表中选择的至少一个IP资源相关联,所述列表是与所述客户端域相关联的至少一个IP资源的列表,所述列表先前从所述客户端域的客户端节点被发送到所述访问控制服务器,

其中,所述客户端域是分布式拒绝服务开放威胁信令(DOTS)域,所述访问控制服务器是DOTS服务器,并且所述客户端节点是DOTS客户端,

其中,所述访问控制服务器还被配置为在由所述访问控制服务器维护的DOTS条目的表中,删除指示不属于由所述客户端节点发送的列表的一部分的IP资源的DOTS条目,或者被配置为拒绝指示不属于由所述客户端节点发送的列表的一部分的IP资源的DOTS请求。

14.一种验证服务器,所述验证服务器与由访问控制服务器从列表中选择的至少一个IP资源相关联,所述列表是与客户端域相关联的至少一个IP资源的列表,所述列表先前从

所述客户端域的客户端节点被发送到所述访问控制服务器，

所述验证服务器包括存储器和处理单元，所述存储器存储有计算机程序，所述处理单元配备有至少一个可编程计算机器或一个专用计算机器，所述计算机程序被所述处理单元执行以实施以下步骤来核实所述至少一个所选择的IP资源的有效性：

-接收至少一个请求，所述请求包括表示客户端域的身份的信息项和所述至少一个所选择的IP资源；

-基于所述表示客户端域的身份的信息项来识别所述客户端域；以及

-考虑客户端域的身份，核实所述至少一个所选择的IP资源与客户端域的关联，

其中，所述客户端域是分布式拒绝服务开放威胁信令(DOTS)域，所述访问控制服务器是DOTS服务器，并且所述客户端节点是DOTS客户端，

其中，所述访问控制服务器还被配置为在由所述访问控制服务器维护的DOTS条目的表中，删除指示不属于由所述客户端节点发送的列表的一部分的IP资源的DOTS条目，或者被配置为拒绝指示不属于由所述客户端节点发送的列表的一部分的IP资源的DOTS请求。

15.一种计算机可读存储介质，存储计算机程序，所述计算机程序在由处理器执行时实施根据权利要求1至10中任一项所述的方法的步骤。

用于核实IP资源的有效性的方法以及相关联的访问控制服务器、验证服务器、客户端节点、中继节点和计算机程序

1.技术领域

[0001] 本发明的领域是通信网络(例如,IP网络)内的通信的领域,尤其是增值(added-value)IP服务的领域。

[0002] 更具体地,本发明提供了一种用于核实与域相关联的IP资源的有效性(validity)的解决方案,即,核实IP地址、IP前缀(一组IP地址)、域名等是否实际上与该域相关联。

[0003] 本发明尤其应用于(但不排他地)缓解DDoS(Distributed Denial of Service,分布式拒绝服务)攻击的领域,特别是促进协调该缓解(mitigation)动作。本发明尤其可以在缓解过程之前或缓解过程期间实施。

2.背景技术

[0004] 在缓解分布式拒绝服务攻击的领域中的现存问题在本文档的剩余部分中被更具体地描述。本发明当然不限于这个特定的应用领域,但是,更一般地,本发明对于在采取与IP资源相关的任何动作之前需要核实所述资源的有效性的任何技术都是感兴趣的。

[0005] 在此提醒,DDoS攻击是试图使资源(例如,网络或计算资源)对其用户不可用。这种攻击可以通过损害大量主机并使用这些主机放大攻击来大规模地部署。

[0006] 为了缓解这些DDoS攻击,一些访问或服务提供商向其客户提供DDoS攻击检测和缓解服务。这种缓解服务(DDoS保护服务)可以托管在访问提供商所运营的基础设施内或云中。特别地,它们可以区分“合法”流量(即,用户同意的数据)和“可疑”流量。

[0007] 当DPS型服务托管在云中时,很难预先识别出DDoS攻击,因为这种服务(默认情况下)不存在于用于到达受DDoS攻击的网络的路由路径上。

[0008] 为了解决这个问题,注意到,已经提出了建立隧道来强制调用网络中所有(传入或传出)流量的DPS服务。但是,这种方法会显著增加用户观察到的延迟,并对DPS服务的规模施加限制,使其能够处理网络所有用户的所有流量。

[0009] 当DPS型服务托管在由访问提供商运营的基础设施内时,即使DPS服务存在于网络的传入流量的路由路径上,在识别可疑流量时也会出现困难。特别地,随着加密流量的增加,尤其是UDP上携带的加密流量(例如,QUIC(Quick UDP Internet Connection,快速UDP互联网连接)流量)的增加,很难区分合法流量和可疑流量。难以访问纯文本控制消息(诸如在TCP协议中提供的消息(SYN/SYN-ACK/ACK))确实会使确定网络节点是否同意接收流量变得复杂。

[0010] 为了帮助识别出可疑流量,IETF已经标准化了特定的体系结构。这种被称为DOTS(DDoS Open Threat Signaling,DDoS开放威胁信令)的体系结构允许被称为DOTS客户端的客户端节点通知被称为DOTS服务器的服务器:其网络受到DDoS攻击,并且需要采取适当的措施。

[0011] 因此,如果客户端域是DDoS攻击的目标,则附接到该客户端域的DOTS客户端可以向DOTS服务器发送消息以请求帮助。后者与缓解器(mitigator)协调,以确保与拒绝服务攻

击相关联的可疑流量不再被路由到客户端域,而合法流量继续被正常路由到客户端域。

[0012] 该解决方案在DOTS客户端和DOTS服务器之间使用两个通信信道:

[0013] -DOTS信号信道,以及

[0014] -DOTS数据信道。

[0015] DOTS信号信道仅在DDoS攻击正在进行时被使用。因此,DOTS客户端可以使用该信道向DOTS服务器请求帮助。例如,DOTS客户端使用该信号信道向服务器发送请求,以通知它前缀“1.2.3.0/24”受到DDoS攻击,使得服务器可以采取措施来阻止攻击。注意到,这种信号信道在以下文档中有描述:"Distributed Denial-of-Service Open Threat Signaling (DOTS)Signal Channel Specification",draft-ietf-dots-signal-channel,Reddy,T.et al.,2018年1月。

[0016] DOTS数据信道在没有正在进行DDoS攻击时被使用。例如,DOTS客户端可以使用该信道来安装过滤规则,诸如以过滤从特定地址接收的或去往给定节点的流量。例如,DOTS客户端可以使用该DOTS数据信道来指示服务器阻塞到前缀“1.2.3.0/24”的所有流量。这种数据信道在以下文档中有描述:"Distributed Denial-of-Service Open Threat Signaling (DOTS)Data Channel",draft-ietf-dots-data-channel,Reddy,T.et al.2017年12月。

[0017] 应当注意,如果服务器没有一种机制来核实前缀“1.2.3.0/24”是否实际上与DOTS客户端域相关联,则该前缀的合法所有者(即,负责管理该前缀的实体,例如访问提供商)可能会观察到服务中断。特别地,在实施措施以旁路(bypass)与该前缀相关联的流量或过滤具有涉及该前缀的目的地地址的所有流量的情况下,从该前缀提取的地址所分配到的节点可能不再接收流量。

[0018] 此外,尽管合法所有者没有发出缓解请求,但是DDoS缓解服务可能向合法所有者收取费用。

[0019] 此外,为了解决IP地址欺骗(spoofing)的问题,IETF建议激活BCP 38(“Network Ingress Filtering:Defeating Denial of Service Attacks which employ IP Source Address Spoofing”,P.Ferguson et al.,2000年5月)和uRPF功能(Unicast Reverse Path Forwarding,RFC2504:“Users'Security Handbook”E.Guttman et al.,1999年2月)。但是,这些机制仅适用于验证IP分组的源地址。

[0020] 还提出了SAVI(Source Address Validation Improvements,源地址验证改进)解决方案,但是这些解决方案不验证在使用参考的协议(例如,SDP(Session Description Protocol,会话描述协议)、SIP(Session Initiation Protocol,会话初始化协议)或DOTS)的内容(“有效载荷”)中指示的IP地址/前缀。

[0021] 因此,现有技术具有以下缺点中的至少一个:

[0022] -地址验证是基于分组的源地址的,

[0023] -可用的数据库(例如,由RIR(Regional Internet Registry,区域互联网注册中心)管理的数据库)由IP资源的所有者(即,通常是运营商)来填充,或者仅提供IP资源的所有者的身份,

[0024] -没有由不同的参与者(内容和服务提供商以及网络运营商)在互联网上统一部署的IP资源验证解决方案,

[0025] -旨在削弱通信的安全性或连接到互联网的终端的安全性的攻击仍然是可能的。

[0026] 因此,需要一种新技术来核实IP前缀的有效性,或者更一般地,IP资源的有效性,尤其是当DPS服务在云中托管时。

3.发明内容

[0027] 本发明提出了一种用于核实与客户端域相关联的IP资源的有效性的新解决方案,即,用于核实IP资源是否属于客户端域的解决方案。例如,这种IP资源属于包括以下各项的组:

[0028] -IP地址(例如,IPv4或IPv6地址),

[0029] -IP前缀(例如,IPv4或IPv6前缀),

[0030] -域名。

[0031] 根据至少一个实施例,一种用于核实与客户端域相关联的IP资源的有效性的方法在被称为访问控制服务器的服务器中实施以下步骤:

[0032] -接收从客户端域的客户端节点发送到访问控制服务器的与客户端域相关联的至少一个IP资源的列表;

[0033] -从列表中选择至少一个待验证的IP资源;以及

[0034] -核实所选择的(多个)IP资源的有效性,即,核实(多个)资源是否与所述域相关联。

[0035] 根据至少一个实施例,一种用于声明与客户端域相关联的IP资源的方法在客户端域的客户端节点中实施以下步骤:

[0036] -获得与客户端域相关联的至少一个IP资源的列表;以及

[0037] -将列表发送到访问控制服务器。

[0038] 在特定实施例中,访问控制服务器被配置为核实所述至少一个IP资源是否与客户端域相关联。

[0039] 根据至少一个实施例,一种用于处理对于与客户端域相关联的IP资源的验证请求的方法在客户端域的中继节点中实施以下步骤,所述中继节点与由访问控制服务器从列表中选择的至少一个IP资源相关联,所述列表是与客户端域相关联的至少一个IP资源的列表,所述列表先前从客户端域的客户端节点被发送到访问控制服务器:

[0040] -接收或拦截源自访问控制服务器的所述请求,所述请求包括控制消息;以及

[0041] -向客户端节点发送(多个)请求

[0042] 根据至少一个实施例,一种用于核实与客户端域相关联的IP资源的有效性的方法在验证服务器中实施以下步骤,所述验证服务器与由访问控制服务器从列表中选择的至少一个IP资源相关联,所述列表是与客户端域相关联的至少一个IP资源的列表,所述列表先前从客户端域的客户端节点被发送到访问控制服务器:

[0043] -接收至少一个请求,所述请求包括表示客户端域的身份的信息项和所选择的(多个)IP资源;

[0044] -基于表示客户端域的身份的信息项来识别客户端域;以及

[0045] -考虑客户端域的身份,核实所选择的(多个)IP资源与客户端域的关联。

[0046] 在特定实施例中,核实方法还包括向访问控制服务器发送确认消息或错误消息。

[0047] 因此,所提出的解决方案可以核实IP资源是否有效地(并且合法地)与客户端域相

关联。

[0048] 特别地，如果客户端域的客户端节点发出请求以要求访问控制服务器在由IP资源识别的至少一个其他节点上执行动作，则所提出的解决方案可以核实识别至少一个其他节点的IP资源是否实际上与客户端域相关联(例如分配给客户端域的至少一个节点)，或者到该IP资源的流量是否被合法地路由到该客户端域。

[0049] 因此，在例如DDoS攻击的上下文中，在采取措施使得可疑流量不再被路由到客户端域之前，访问控制服务器可以核实由客户端域的客户端节点发送的缓解请求或过滤请求是否实际上涉及该客户端节点或客户端域的另一节点。

[0050] 此外，根据至少一个实施例，所提出的解决方案不需要使用访问提供商的基础设施。因此，所提出的解决方案可以核实与客户域相关联的IP资源的有效性，无论DPS缓解服务是托管在由访问提供商运营的基础设施内、在云中还是在其他地方。

[0051] 根据至少一个实施例，所提出的解决方案可以提高对DDoS攻击的响应的可靠性、鲁棒性和/或有效性。

[0052] 特别地，与基于数据库的静态咨询的当前解决方案不同，根据本发明的至少一个实施例的用于核实IP资源的有效性的方法能够实时核实与向客户端分配IP资源相关的信息，而不公开他们的身份，包括在IP资源的动态分配的上下文中。

[0053] 根据至少一个实施例，周期性地更新列表，和/或在添加、删除或修改与客户端域相关联的IP资源的情况下更新列表。

[0054] 因此，所提出的解决方案可以定期验证IP资源，和/或在添加、删除或修改与客户端域相关联的IP资源的情况下验证IP资源。

[0055] 以这种方式，例如在DOTS架构的上下文中，不必等待接收过滤安装请求(这种安装可以例如对应于对攻击的响应)，这使得可以优化DOTS请求的处理时间。

[0056] 此外，根据至少一个实施例，可以将有效期关联到与客户端域相关联的至少一个IP资源的列表、每个IP资源乃至几个IP资源。在这种情况下，当有效期期满时，访问控制服务器可以自动从其表中删除相关的(多个)IP资源。

[0057] 特别地，客户端节点可以更新与客户端域相关联的IP资源列表，而无需等待有效期期满。

[0058] 以这种方式，可以检测到资源验证是过时的，这在网络频繁重新编号(即，分配给网络节点的IP地址或前缀被频繁地修改)的情况下尤其令人关注。例如，作为缓解请求的一部分，如果客户端域的节点请求访问控制服务器在时间T0处过滤到与客户端域相关联的前缀1.2.3.0/24的(传入)流量，则访问控制服务器必须在时间T1处核实前缀1.2.3.0/24是否仍然与同一客户端域相关联，以决定是否应当过滤或路由到该前缀1.2.3.0/24的流量。

[0059] 根据本发明的特定特征，用于核实IP资源有效性的方法还考虑了至少一个先前定义的数据过滤规则。

[0060] 本发明的其他实施例涉及相关联的访问控制服务器、客户端节点、中继节点和验证服务器。

[0061] 在另一实施例中，本发明涉及一个或多个计算机程序，一个或多个计算机程序包括当所述(多个)程序由处理器执行时、用于实施根据本发明的至少一个实施例的一种用于核实与客户端域相关联的IP资源的有效性的方法的指令，一个或多个计算机程序包括当所

述(多个)程序由处理器执行时、用于实施根据本发明的至少一个实施例的一种用于声明与客户端域相关联的IP资源的方法的指令,一个或多个计算机程序包括当所述(多个)程序由处理器执行时、用于实施根据本发明的至少一个实施例的一种用于处理对于与客户端域相关联的IP资源的至少一个验证请求的方法的指令。

[0062] 在又一实施例中,本发明涉及一个或多个不可移动的、或部分或全部可移动的、计算机可读的并且包括来自一个或多个计算机程序的指令的信息介质,该计算机程序用于执行根据本发明的至少一个实施例的用于核实与客户端域相关联的IP资源的有效性的方法的步骤、和/或用于声明与客户端域相关联的IP资源的方法的步骤、和/或用于处理对于与客户端域相关联的IP资源的至少一个验证请求的方法的步骤。

[0063] 因此,根据本发明的方法可以以各种方式实施,尤其是以有线形式和/或软件形式。

4.附图说明

[0064] 在阅读作为简单的说明性非限制性示例而提供的特定实施例的以下描述以及附图后,本发明的其他特征和优点将变得更加清楚,其中:

[0065] -图1示出了根据本发明的一个实施例的实施一种用于核实与客户端域相关联的IP资源的有效性的方法的通信网络的示例;

[0066] -图2示出了根据本发明的至少一个实施例的用于核实与客户端域相关联的IP资源的有效性的方法的主要步骤;

[0067] -图3和图4示出了本发明的两个实施例;

[0068] -图5示出了根据一个实施例的由DOTS客户端实施的用于声明与DOTS域相关联的IP资源的主要步骤;

[0069] -图6A和图6B示出了两个IP资源声明的示例;

[0070] -图7示出了检测到几个域之间的地址冲突;

[0071] -图8示出了删除不是DOTS客户端所声明的列表的一部分的IP资源;

[0072] -图9示出了拒绝对不是DOTS客户端所声明的列表的一部分的地址的缓解请求;

[0073] -图10示出了客户端节点和中继节点之间被授权或未被授权的通信;

[0074] -图11至图15示出了根据被称为“DOTS探测”的第一实施例的核实过程的实施例;

[0075] -图16示出了根据被称为“协作DOTS/ISP”的第二实施例的核实过程的一个实施例;以及

[0076] -图17示出了根据特定实施例的访问控制服务器、验证服务器、客户端节点或中继节点的简化结构。

5.具体实施方式

[0077] 5.1一般原理

[0078] 本发明的一般原理基于向被称为访问控制服务器的服务器声明与客户端域相关联的IP资源,并且基于对这些IP资源的有效性的核实,即,核实所声明的资源是否实际上与客户端域相关联。

[0079] 关于图1,呈现了实施一种用于核实与客户端域相关联的IP资源的有效性的方法

的通信网络的不同设备。

[0080] 例如,考虑属于客户端域11的客户端节点C1 111与访问控制服务器S14通信。例如,客户端域11包含一个或多个机器(也称为节点)。特别地,客户端域包括至少一个中继节点R1 112。这里使用的术语“域”是指由同一实体负责的一组机器或节点。

[0081] 第一访问提供商12具有允许客户端域11的客户端访问访问控制服务器14所连接的互联网网络13的设备。根据至少一个实施例,第一访问提供商12包括至少一个验证服务器V1 121。

[0082] 根据示出的示例,访问控制服务器14不属于客户端域11,因此可以经由第二访问提供商连接到互联网网络13。在另一未示出的示例中,访问控制服务器14可以属于客户端域,或者属于经由第一访问提供商12连接到互联网网络13的另一域。

[0083] 图2示出了为核实与客户端域11相关联的IP资源而实施的主要步骤。

[0084] 客户端域11的节点(例如,客户端节点C1 111)获得(21_C)与客户端域11相关联的至少一个IP资源的列表。例如,这种列表包括客户端域11的不同节点的IP地址、与客户端域11的连接路由器相关联的IP前缀、与客户端域11相关联的域名等。

[0085] 客户节点C1 111,或者可能是客户端域11的另一节点,将该列表发送(22_C)到服务器(例如,访问控制服务器14)。换句话说,客户端节点C1 111向访问控制服务器14声明与客户端域11相关联的IP资源。因此,源地址是客户端节点的地址,但是待验证的IP资源是那些在消息的内容中发送到访问控制服务器的IP资源。IP资源的声明可以是显式的(使用专用消息),也可以是隐式的(作为信令或过滤请求的一部分)。

[0086] 根据第一示例,与客户端域相关联的至少一个IP资源的列表在单个消息中被发送。在这种情况下,可以向访问控制服务器发出单个请求(称为聚合请求)。

[0087] 根据第二示例,与客户端域相关联的至少一个IP资源的列表被分布在多个消息上。在这种情况下,可以向访问控制服务器发出几个分开的请求。

[0088] 访问控制服务器14然后接收(23_S)从客户端域11的客户端节点发送到访问控制服务器14的与客户端域11相关联的至少一个IP资源的列表。

[0089] 访问控制服务器14从列表中选择(24_S)至少一个待验证的IP资源。

[0090] 可能的是,访问控制服务器14向客户端节点C1 111发送(25_S)所选择的(多个)IP资源。客户端节点C1 111然后接收(26_C)由访问控制服务器14选择的(多个)IP资源。

[0091] 访问控制服务器14然后核实(27_S)所述至少一个所选择的IP资源的有效性。换句话说,访问控制服务器核实所选择的IP资源是否实际上与客户端域11相关联。

[0092] 图3和图4示出了本发明的两个实施例。第一实施例能够从管理客户端域的访问提供商处解放出来,以验证与该客户端域相关联的IP资源。第二实施例允许使用访问提供商的设备来验证与客户端域相关联的IP资源,同时对客户端域的身份保密。

[0093] 图3示出了根据第一实施例的用于核实IP资源的有效性的方法的主要步骤。

[0094] 根据该实施例,由访问控制服务器14实施的对所选择的(多个)IP资源的有效性的核实(27_S)是基于对于待验证的所述IP资源的至少一个请求的发送(31_S),所述请求由与所述至少一个所选择的IP资源相关联的客户端域的至少一个中继节点(例如,中继节点R1 112)接收或拦截的。可能的是,中继节点R1 112和客户端节点C1 111是相同的。作为变型,中继节点R1 112和客户端节点C1 111是属于同一域的两个不同节点。类似地,客户端节点

和中继节点可以是嵌入在同一物理节点中的两个软件实例。

[0095] 更具体地,所选择的IP资源可以是IP地址。在这种情况下,访问控制服务器将请求发送到IP地址。所选择的资源也可以是IP前缀。在这种情况下,访问控制服务器将请求发送到从该前缀提取的一个或多个地址;这些请求通常会被将客户端域连接到互联网的(多个)路由器拦截。所选择的资源也可以是域名。在这种情况下,访问控制服务器可以实施解析过程(例如,DNS)来获得相关联的域的管理实体(访问提供商)的IP地址。

[0096] 这种请求包括控制消息或数据。特别地,这种控制消息可以与明确识别该请求的任何信息项相关联。这个控制消息必须特别重要,以避免其欺骗。例如,这种控制消息是随机生成的。

[0097] 中继节点R1 112然后拦截(32_R)源自访问控制服务器14并包括控制消息的至少一个请求。如果目的地地址被分配给中继节点所驻留的机器,则该请求可以直接去往中继节点。

[0098] 中继节点R1 112将该(多个)请求发送(33_R)到客户端节点C1 111,即,中继源自访问控制服务器14的(多个)请求。

[0099] 客户端节点C1 111然后经由与由访问控制服务器从列表中选择的至少一个IP资源相关联的客户端域的至少一个中继节点,接收(34_C)源自访问控制服务器并包括控制数据或消息的至少一个请求。

[0100] 特别地,如果中继节点R1 112和客户端节点C1 111是属于同一域的两个不同节点,则中继节点R1 112和客户端节点C1 111之间的交换可以经由安全连接来实施。

[0101] 如果中继节点R1 112和客户端节点C1 111是同一节点,则客户端节点C1 111直接接收源自访问控制服务器14的请求,或者该请求被内部中继。

[0102] 客户端节点C1 111通过向访问控制服务器14发送(35_C)包括控制数据或消息的信息特征项的响应来进行响应。

[0103] 访问控制服务器14接收(36_S)源自客户端节点C1 111的、包括控制消息的信息特征项的响应。控制消息的信息特征项可以与控制消息相同或不同。

[0104] 访问控制服务器14执行对请求和响应的关联(37_S),或者更具体地,对请求中传送的控制数据和响应中传送的控制数据的信息特征项的关联,并且验证所选择的IP资源是否属于客户端域。

[0105] 现在结合图4描述根据第二实施例的用于核实IP资源的有效性的方法的主要步骤。

[0106] 该第二实施例涉及与访问提供商相关联的验证服务器,例如与客户端域11的第一访问提供商12相关联的验证服务器V1 121。

[0107] 更具体地,根据该第二实施例,由访问控制服务器14实施的对所选择的(多个)IP资源的有效性的核实(27_S)是基于对表示客户端域的身份的信息项的接收(41_S)的。例如,这种信息项表示客户域或管理客户端域的实体的身份,诸如连接服务的订户。特别地,这种信息项是客户端域11或管理客户端域的实体的身份的摘要(digest)或“散列(hash)”。

[0108] 访问控制服务器S14还实施与在步骤24_S中选择的(多个)IP资源相关联的至少一个验证服务器(例如,验证服务器V1 121)的识别(42_S)。

[0109] 最后,访问控制服务器S14向所识别的(多个)验证服务器发送(43_S)至少一个请

求,所述请求一方面包括表示客户端域的身份的信息项,另一方面包括所选择的(多个)IP资源。根据该第二实施例,请求因此不被发送到从待验证的IP前缀或IP地址列表中提取的目的地地址,而是被发送到验证服务器。

[0110] 可能的是,这种请求包括与明确识别该请求的任何信息项相关联的控制消息。与第一实施例一样,这种控制消息可以是随机生成的。

[0111] 与由访问控制服务器14从列表中选择的至少一个IP资源相关联的验证服务器V 121接收(44_V)(多个)请求,该列表是与客户端域相关联的至少一个IP资源的列表(先前由客户端节点C1 111发送到访问控制服务器S14的列表),该请求一方面包括表示客户端域的身份的信息项,另一方面包括所选择的(多个)IP资源。

[0112] 基于表示客户端域的身份的信息项,验证服务器V 121可以识别(45_V)客户端域。

[0113] 最后,考虑到客户端域的身份,验证服务器V 121可以核实(46_V)所选择的(多个)IP资源是否与客户端域相关联/属于客户端域。

[0114] 在实施对由访问控制服务器14选择的(多个)IP资源的有效性的核实(27_S)之前,验证服务器V1 121可以直接地或应客户端域的客户端的请求,实施对表示客户端域11的身份的信息项的确定(401_V)。如上所述,这种信息项表示客户端域或管理客户端域的实体的身份,并且可以采取例如客户端域11的身份的摘要的形式。

[0115] 验证服务器V1 121向客户端域11(例如,客户端节点C1 111)发送(402_V)表示客户端域的身份的信息项。

[0116] 客户端节点C1 111然后从附接到客户端域11的验证服务器接收(403_C)表示客户端域的身份的信息项,并且可以直接地或应访问控制服务器14的请求将其发送(404_C)到访问控制服务器14。

[0117] 注意,这些用于接收401_V和发送402_V/接收403_C表示客户端域11的身份的信息项的预备步骤可以在初始化阶段期间实施,或者当客户端域11连接到激活验证服务器的网络时实施,或者当缓解过程被启动时实施,等等。

[0118] 5.2在缓解服务的域中的应用示例

[0119] 下面给出了在DOTS型体系结构中的本发明的实施例的描述,根据该体系结构,客户节点C1 111是DOTS客户,并且访问控制服务器S14是DOTS访问控制服务器,这允许客户节点C1 111通知访问控制服务器S14:客户端域正受到DDoS攻击,并且需要适当的动作。客户节点C1 111和访问控制服务器S14因此可以通过结合现有技术定义的DOTS信号和数据信道进行通信。

[0120] 特别地,当DPS缓解服务不在由连接到客户端域的访问提供商运营的基础设施内托管(即,如果DOTS访问控制服务器不是由连接到客户端域的访问提供商运营的),而是在由另一访问提供商运营的基础设施中或在“云中”时,本发明的至少一个实施例可以被实施来核实与客户端域相关联的IP资源的有效性。

[0121] 5.2.1 DOTS架构的提醒

[0122] DOTS请求可以是,例如:

[0123] -别名(alias)管理消息,例如,其将标识符与位于客户端域中的一个或多个网络资源相关联,

[0124] -从DOTS访问控制服务器请求缓解拒绝服务攻击的信令消息,其中访问控制服务

器能够在接收到这种消息后发起必要的动作来停止攻击,或者

[0125] -过滤规则管理消息,诸如请求DOTS访问控制服务器安装(或已经安装)访问控制列表(access control list,ACL)。

[0126] DOTS请求可以从属于DOTS客户端域的DOTS客户端发送到DOTS访问控制服务器或多个DOTS访问控制服务器。

[0127] DOTS域可以支持一个或多个DOTS客户端。换句话说,客户端域的几个客户端节点可以具有DOTS功能。

[0128] 客户端域和访问控制服务器之间的DOTS通信可以是直接的,也可以经由DOTS网关来建立。这些网关可以托管在客户端域、访问控制服务器域或两者内。换句话说,客户端域的节点可以直接与访问控制服务器通信,或者向直接与访问控制服务器通信的客户端域的网关或服务器域的网关发送请求,或者向与访问控制服务器通信的服务器域的网关发送请求。

[0129] 位于客户端域中的DOTS网关被DOTS访问控制服务器视为DOTS客户端。

[0130] 位于服务器域中的DOTS网关被DOTS客户端视为DOTS访问控制服务器。如果在服务器域中存在DOTS网关,则DOTS客户端的认证可以委派给服务器域的DOTS网关。DOTS访问控制服务器可以在其域内配置有活动DOTS网关列表,并且访问控制服务器可以将其一些功能委派给这些受信任的网关。具体地说,访问控制服务器可以安全地使用由网关提供的、由访问控制服务器通过ad hoc认证过程声明并维护的列表上的信息(例如,由访问控制服务器的授权管理员对列表进行显式配置,从诸如(用于“认证、授权和计费等”的)AAA服务器的认证服务器检索列表)。

[0131] 无论DOTS架构的配置如何(客户端域中的一个或多个DOTS客户端、没有DOTS网关、客户端域或服务器域中的一个或多个DOTS网关、与服务器域分离的客户端域等),都可以实施下面呈现的实施例。

[0132] 可以根据上述文件“Distributed Denial-of-Service Open Threat Signaling (DOTS)Signal Channel Specification”中描述的过程来完成安全DOTS会话的建立。例如,可以使用下列文档之一中描述的过程来建立会话:

[0133] -“Datagram Transport Layer Security Version 1.2”,Rescorla E.et al,RFC 6347,DOI 10.17487/RFC6347,2012年1月,

[0134] -“The Datagram Transport Layer Security(DTLS)Protocol Version 1.3”,Rescorla E.et al,draft-ietf-tls-dtls13-22,2017年11月,

[0135] -“The Transport Layer Security(TLS)Protocol Version 1.2”,Dierks T.et al,RFC 5246,DOI 10.17487/RFC5246,以及

[0136] -“The Transport Layer Security(TLS)Protocol Version 1.3”,Rescorla E.,draft-ietf-tls-tls13-23,2018年1月。

[0137] 在下文中,假设DOTS代理((多个)客户端、(多个)访问控制服务器)相互认证。因此,在DOTS客户端和DOTS访问控制服务器之间存在(例如,类型(D)TLS的)安全通信信道。

[0138] 因此,从模仿合法访问控制服务器的另一服务器接收的消息可以被DOTS客户端拒绝。类似地,来自未被授权访问缓解服务的DOTS客户端的请求可以被DOTS访问控制服务器忽略。在下文中假设该过程由DOTS代理实施。

[0139] (D)TLS交换的细节以及那些关于用于DOTS代理的相互认证的安全密钥的管理的细节并不是本发明的主题,并且在此不详细描述。

[0140] 下面参考图2描述由DOTS客户端和DOTS服务器实施的各种步骤。作为示例,考虑图1中的客户端节点111是DOTS客户端,并且图1中的访问控制服务器14是DOTS服务器。因此,客户端域是DOTS域。

[0141] 5.2.2声明与客户端域相关联的IP资源列表

[0142] 参考图2,DOTS客户端获得(21_C)与DOTS域相关联的至少一个IP资源的列表,然后将其发送(22_C)到一个或多个DOTS访问控制服务器,例如使用DOTS数据或信号通信信道。因此,DOTS客户端可以向DOTS访问控制服务器声明其管理的IP资源,或者更一般地说,与DOTS客户端域相关联的IP资源。

[0143] 这种IP资源的声明的一个优点在于,它可以启动对相关IP资源的有效性的核实,而无需等待DOTS请求的接收,并且因此无需等待攻击的进行。作为结果,可以快速处理从DOTS客户端发送到DOTS访问控制服务器以请求缓解拒绝服务攻击的信令消息。

[0144] 如前所述,IP资源可以是IP地址、IP前缀或域名。域名可以被解析为IP地址。下面的IP前缀表示由DOTS客户端直接传送的IP前缀或经由名称解析系统检索的地址(例如,DNS)。前缀可以具有相同地址家族,或者属于不同家族(IPv4、IPv6)。IP前缀不一定是连续的,也不一定由同一访问提供商管理。此外,这些前缀可以是PA(Provider Assigned,提供商分配的)前缀,即服务提供商拥有的前缀,或者PI(Provider Independent,独立于提供商的)前缀,即应客户请求而分配的前缀,例如由独立于访问提供商的地区互联网注册中心(regional Internet registry,RIR)分配的前缀。

[0145] 由DOTS客户端实施的用于声明与DOTS域相关联的IP资源的主要步骤在下面结合图5进行描述。

[0146] 在初始化步骤51_C期间,建立DOTS客户端和一个或多个DOTS访问控制服务器之间的安全通信信道。

[0147] 在获得步骤52_C期间,类似于步骤21_C,DOTS客户端获得其管理的IP资源列表,或者更一般地说,与其DOTS(客户端)域相关联的IP资源列表。

[0148] 在发送步骤53_C期间,类似于步骤22_C,DOTS客户端通过将IP资源列表发送到一个或多个DOTS访问控制服务器来声明该列表。

[0149] 在更新步骤54_C期间,DOTS客户端核实列表中条目的有效性或发现新资源。该更新步骤可以定期地实施,和/或在每次添加、修改或删除与域相关联的IP资源时实施。一旦列表被更新,该列表就根据发送步骤53_C被发送回DOTS访问控制服务器。这种发送可以定期地实施,也可以在列表更新后立即实施。

[0150] 当将IP资源列表发送到(多个)访问控制服务器时,DOTS客户端可以(例如在“生存期”字段中)指定与该列表或该列表中的某些IP资源相关联的有效期。例如,这种有效期以分钟为单位表示。

[0151] 如果客户端在初始声明请求中定义的有效期期满之前没有更新其声明/列表,则DOTS访问控制服务器可以自动从该客户端/客户端域的其活动前缀/资源表中删除相关联的(多个)IP资源。

[0152] 例如,“生存期”字段可以显示“-1”,以指示不确定的有效期。

[0153] 如图6A所示,DOTS客户端可以发出不同的请求来向(多个)访问控制服务器声明与DOTS客户端的DOTS域相关联的IP资源中的每一个IP资源(例如,声明地址“1.2.3.4”的第一请求,声明地址“11.22.33.44”的第二请求)。可选地,如图6B所示,可以发出单个请求来声明与DOTS客户端的DOTS域相关联的所有IP资源(例如,声明地址“1.2.3.4”和地址“11.22.33.44”的单个请求)。

[0154] 如果几个DOTS客户端部署在同一域中,则IP资源声明只能由一个或几个客户端执行。换句话说,声明在默认情况下与域相关联,而不是与DOTS客户端相关联。

[0155] DOTS访问控制服务器可以识别同一域的DOTS客户端。为此,DOTS访问控制服务器依赖于用于认证的安全密钥,诸如与DOTS客户端相关联的证书的SPKI(Subject Public Key Information,主题公钥信息)(例如,在D.Cooper等人于2008年5月发表的题为“Internet X.509Public Key Infrastructure Certificate and Certificate Revocation List(CRL)Profile”的RFC 5280文档中定义的X.509证书),或者客户在认证过程(“TLS客户端密钥交换(TLS ClientKeyExchange)”)期间使用的PSK身份(shared key identifier,共享密钥标识符)。

[0156] 下面描述用于向其DOTS访问控制服务器声明DOTS客户端的前缀“1.2.3.0/24”的程序示例。“POST”消息用于说明目的,但是当然也可以使用其他消息(例如,“HTTP PUT”):

[0157]
```
POST /restconf/data/ietf-dots-data-channel:dots-data\
        /dots-client=mydotsclient HTTP/1.1
Host: {host}:{port}
Content-Type: application/yang-data+json
{
 "ietf-dots-data-channel:prefixes ": {
   "prefix-list": [
```

[0158]
```
     {
       "name": "my_first_prefix",
       "prefix": "1.2.3.0/24",
       "lifetime": 1504
     }
   ]
 }
}
```

[0159] 如上所述,可以定期地和/或每次添加/修改/删除与客户端域相关联的IP资源时更新与客户端域相关联的IP资源列表。

[0160] 根据第一示例,获取操作可以导致新的IP资源(例如,由活动DOTS客户端管理的新前缀)的分配和使用。DOTS客户端可以声明这种新前缀。为此,例如,DOTS客户端可以发送

POST消息。

[0161] 根据第二示例,DOTS客户端还可以通过删除不再有效的IP资源(例如,不再由访问网络委派的前缀,或者有效期已经期满的前缀)来更新IP资源列表。

[0162] 在这种情况下,DOTS客户端可以删除不再有效的(多个)IP资源,而无需等待声明时指示的有效期期满。

[0163] 下面描述了由DOTS客户端删除前缀“my_first_prefix”的程序示例。同样,“POST”消息用于说明目的,但是当然也可以使用其他消息(例如,“HTTP PUT”):

[0164]
```
DELETE /restconf/data/ietf-dots-data-channel:dots-data\
        /dots-client=mydotsclient
        /prefixes/prefix-list=my_first_prefix HTTP/1.1
  Host: {host}:{port}
```

[0165] 5.2.3选择要由DOTS访问控制服务器验证的IP资源

[0166] 一旦与域相关联的IP资源已经由DOTS客户端向DOTS访问控制服务器声明,DOTS访问控制服务器就可以核实所声明的资源是否实际上与声明客户端域相关联。

[0167] 为此,DOTS访问控制服务器可以从列表中选择一个或多个待验证的IP资源(参考图2的步骤24_S),然后对所选择的IP资源中的每一个IP资源应用核实过程。

[0168] 可能的是,核实过程适用于访问控制服务器所维护的其他条目(例如,过滤条目或属于同一域的其他客户端的条目)。

[0169] 特别地,对于不支持IP资源声明过程的客户端来说,将核实过程推广到访问控制服务器所维护的其他类型的条目是有趣的。如果该域的另一客户端先前已经声明了与该域相关联的所有IP资源,则确实可以核实由不能实施IP资源声明过程的客户所管理的IP资源的有效性。

[0170] 将由DOTS访问控制服务器验证的IP资源的不同选择示例描述如下:

[0171] -DOTS访问控制服务器可以在接收到客户声明后,或在过滤或信号规则的有效期期间,或两者兼有地,系统地执行核实过程;

[0172] -DOTS访问控制服务器可以定期地实施核实过程,以请求DOTS客户端确认过滤规则的有效性,特别是过滤规则中指定的目的地地址;

[0173] -访问控制服务器可以选择待验证的全部或部分条目;为此,访问控制服务器执行选择过程,诸如随机模式、选择已经超过某一生存期的条目(同时借助在条目被创建时由访问控制服务器分配的“生存期”参数的值来保持理论上有效)等;

[0174] -DOTS访问控制服务器可以在检测到属于不同DOTS域的客户端所指示的目的地地址之间的冲突后实施核实过程。

[0175] 根据后一示例,如图7所示,DOTS访问控制服务器可以通过比较DOTS请求中指示的(多个)目的地前缀来检测几个域之间的地址冲突。例如,属于第一域71的第一客户端C1在DOTS请求中指示目的地地址“1.2.3.4/32”,而该地址被属于第二域72的第二客户端C2针对前缀“1.2.3.0/24”的请求所覆盖。由于两个客户端C1和C2不属于同一域,因此访问控制服务器S可以检测到目的地地址之间的冲突,并且不选择任何目的地地址作为“待验证的IP资源”。

[0176] 5.2.4验证所选择的IP资源

[0177] 一旦待验证的IP资源已经被DOTS访问控制服务器选择,DOTS访问控制服务器就实施对所选择的(多个)资源的有效性核实(参考图2的步骤27_S)。

[0178] 根据至少一个实施例,DOTS访问控制服务器可以在核实过程之前或同时删除指示不属于由DOTS客户端声明的列表的一部分的IP资源的DOTS条目。因此,如图8所示,如果客户端C1向访问控制服务器S声明地址“1.2.3.4”,并且DOTS条目包含地址“1.2.3.4”和“11.2.3.4”,则访问控制服务器检测到与客户端C1相关联的过滤规则中的异常,并且可以从其表中删除相对应的条目。可选地,访问控制服务器可以向客户端发送通知以说明清理操作。

[0179] 类似地,在核实过程之前或同时,访问控制服务器可以拒绝指示不属于所声明的IP资源的一部分的IP资源的DOTS请求。因此,如图9所示,如果客户端C1向访问控制服务器S声明地址1.2.3.4,并且访问控制服务器接收到关于地址“15.45.45.78”的信令/缓解请求,则访问控制服务器可以拒绝该信令请求,因为请求中被指示为攻击目标的地址不在由客户端C1或属于同一客户端域的客户端所声明的IP资源列表上。

[0180] 下面描述用于实施包括核实所选择的(多个)资源的有效性(参考图2的步骤27_S)的核实过程的两个实施例。

[0181] 被称为“DOTS探测”的第一实施例能够使自己从访问提供商处解放出来以验证IP资源,其主要步骤在图3中示出。被称为“协作DOTS/ISP”的第二实施例能够在不侵犯客户隐私的情况下处理访问提供商所维护的数据,其主要步骤在图4中示出。

[0182] 下面更详细地描述第一实施例(“DOTS探测”)。

[0183] 根据该第一实施例,客户端域的至少一个节点激活“DOTS_CHECK_RELAY”功能,以检查传入流量并将其重定向到客户端节点。这种节点在下文中称为“中继节点”。

[0184] 可以请求客户端域中具有“DOTS_CHECK_RELAY”功能的几个节点。例如,经由几个链接连接到互联网网络的客户端域(“多归属”上下文)可以在将其连接到互联网网络的所有节点上激活“DOTS_CHECK_RELAY”功能。

[0185] DOTS客户端可以与“DOTS_CHECK_RELAY”功能共存。换句话说,客户端节点可以激活“DOTS_CHECK_RELAY”功能,例如,当DOTS客户端嵌入在网络连接路由器(诸如住宅网关)中时(CPE,客户驻地设备)。那么客户端节点是中继节点。在该情况下,DOTS客户端有利地位于目的地为客户端域的所有流量的路径上。

[0186] 在下文中,假设DOTS客户端具有激活“DOTS_CHECK_RELAY”功能的中继节点的列表。该中继列表可以包含一个或多个中继,并且可以向客户端显式地声明(静态配置)或动态地提供(例如,使用DHCP选项的资源)。然而,没有必要将这种中继列表传送给访问控制服务器。除了到达中继节点的一个或多个地址和安全信息(例如,核实DOTS客户端是否被授权与中继节点通信的认证令牌)之外,还可以提供附加信息,诸如服务的监听端口号或由中继节点管理的IP资源列表。

[0187] 如果没有为中继列表中的中继提供与IP资源相关的规范,则DOTS客户端可以将该中继用于与域相关联的所有IP资源。

[0188] “DOTS_CHECK_RELAY”功能将在下面详细描述。

[0189] “DOTS_CHECK_RELAY”功能可以是:

[0190] -专用于DOTS服务的软件模块，

[0191] -在客户端域的节点上激活的流量捕获功能，例如，将客户端域连接到互联网网络的路由器之一。

[0192] 根据特定实施例，激活“DOTS_CHECK_RELAY”功能的中继和域的DOTS客户端之间的通信可以被保护。例如，激活“DOTS_CHECK_RELAY”功能的中继可以向正式授权的可信客户端传送信息或接收来自正式授权的可信客户端的请求。

[0193] 因此，如图10所示，源自客户端域11的客户端C1和Cm的消息被中继R1和Ri授权，而来自欺骗客户端“F_C”的消息被中继R1和Ri拒绝。

[0194] 根据特定实施例，可以根据请求来激活“DOTS_CHECK_RELAY”功能。根据该实施例，该功能的激活由域的至少一个DOTS客户端控制。该功能被激活达一段有限的时间；然后其被停用。该实施例优选地用于将临时地址或前缀与激活该功能的继电器相关联。

[0195] 根据另一实施例，“DOTS_CHECK_RELAY”功能可以被永久激活。根据该实施例，“DOTS_CHECK_RELAY”功能可以通过重新使用流量捕获功能来实施。当激活“DOTS_CHECK_RELAY”功能的中继节点位于路由去往客户端域的一些或全部流量的路径上时(例如，互联网网络连接路由器，诸如CPE)，优选地使用该实施例。该模式不需要使用临时地址/前缀。

[0196] 下面描述根据第一实施例(“DOTS探测”)的核实过程。

[0197] 如先前结合图2所示，访问控制服务器接收(23_S)与客户端域相关联的至少一个IP资源的列表，并从该列表中选择(24_S)一个或多个待验证的IP资源。注意，该列表的内容可以随时间变化，因为该列表可以被更新(图5中的步骤54_C)。

[0198] 例如，在识别出待由访问控制服务器验证的DOTS条目后，访问控制服务器提取相关联的目的地前缀。

[0199] 可选地，访问控制服务器将所选择的IP资源(或相关联的IP前缀/地址)的列表传送到客户端(图2中的步骤25_S)。例如，当部署专用于DOTS服务的软件模块时，可以将这种列表传送到客户端，该软件模块使用例如虚拟化技术来动态地实例化服务功能(上面的“按需”模式)。

[0200] 特别地，这些服务功能可以被配置为拦截针对由DOTS访问控制服务器传送的至少一个地址的流量。

[0201] 根据特定实施例，客户端可以根据访问控制服务器的指令来配置(多个)“DOTS_CHECK_RELAY”功能。

[0202] 可能的是，客户端可以通知访问控制服务器：客户端域已准备好处理IP资源验证消息。

[0203] 一旦访问控制服务器选择了待验证的IP资源，访问控制服务器就可以对所选择的IP资源或相关联的地址/前缀进行有效性核实(步骤27_S)。

[0204] 为此，根据该第一实施例(“DOTS探测”)，访问控制服务器发送具有待验证地址(即，从所选择的IP资源中提取的地址)作为目的地地址的请求，并被所识别的(多个)中继节点拦截(图3中的步骤31_S)。

[0205] 例如，“DOTS_PROBE_REQUEST”验证消息被发送到所选择的IP资源的列表中的每个地址。

[0206] 一旦选择了待验证的IP资源，或者在某一时段之后，或者在从客户端接收到消息

(例如,当访问控制服务器将所选择的IP资源的列表传送到客户端时(25_S)的接收确认消息)后,访问控制服务器可以发送“DOTS_PROBE_REQUEST”验证消息。

[0207] 向由所选择的(多个)IP资源所识别的(多个)节点发送这种消息可以连续或同时进行。

[0208] 特别地,注意,这种验证消息包括与明确识别验证消息的任何信息项相关联的控制消息。

[0209] 例如,DOTS访问控制服务器生成具有随机有效载荷的“DOTS_PROBE_REQUEST”消息,以防止可疑客户端轻松地猜测消息并发送欺骗响应。因此,作为示例,访问控制服务器可以:

[0210] -插入随机生成的一个或多个唯一标识符,诸如UUID(Universally Unique Identifier,通用唯一标识符)标识符-版本4(如P.Leach于2005年7月发表的RFC 4122文档“A Universally Unique IDentifier(UUID)URN Namespace”中所描述的):

[0211] 1. 263afd79-835c-4ee7-9535-df245cf28d9a

[0212] 2. 246813cd-2bf3-46a9-ad1e-b4bb0f356189

[0213] 3. 730d0839-0267-4216-8b62-66844bb30711

[0214] 4. 61319aa3-555d-445c-8918-f2e9cfd67e06

[0215] -计算其在“DOTS_PROBE_REQUEST”消息中插入的摘要,诸如SHA-256摘要:

[0216] 1.bd10ab3db20f6830feb53a8f295013e2934cdc674c32343341445082a73830f7

[0217] 2. 00ba021fe38dc12c0ceefd709be9a2d08c8ebea3f231c785f25d03623ee566c5

[0218] 3.b9c8740f9a4f59c3311f2b027d055dfdd7ba3184754e7451ed649e05cc779385

[0219] 4.b9e44df1b5f0dc788a068225f422b7cf1b4858b62188a47b7504fe202c25e973

[0220] -使用技术来确保控制消息的完整性和真实性,例如AEAD(具有相关数据的认证加密)类型,如D.McGrew于2008年1月发表的RFC5116文档“An Interface and Algorithms for Authenticated Encryption”中所描述的;

[0221] -使用任何其他随机生成过程,诸如在D.Eastlake于2005年1月发表的题为“Randomness Requirements for Security”的RFC4086文档中规定的过程;

[0222] -使用随机文件(例如,图像);

[0223] -等等。

[0224] 例如,由DOTS访问控制服务器生成“DOTS_PROBE_REQUEST”验证消息包括:

[0225] -生成具有随机数据(控制数据)的分组;

[0226] -定义目的地地址(由所选择的IP资源识别的中继节点的地址);

[0227] -维护对具有随机数据的所述分组的发送的状态特征;

[0228] -向由所选择的IP资源识别的中继发送消息(31_S)。

[0229] 同一消息可以被发送多次,尤其是在其中一条消息在被路由到其目的地时已被销毁的情况下。

[0230] 如果从所选择的IP资源中提取的目的地地址与客户端域不相关联,则访问控制服务器应当考虑两种情况:

[0231] -要么访问控制服务器接收到错误消息(例如,经由ICMP协议);

[0232] -要么访问控制服务器没有接收到任何响应。

[0233] 在两种情况下,访问控制服务器可以断定与DOTS_PROBE_REQUEST消息相关联的地址与DOTS客户端不合法地相关联。因此,访问控制服务器可以使其表中的相对应的条目无效。可以采取其他措施,例如,阻止指示该地址/前缀的DOTS客户端。

[0234] 如果目的地地址实际上与客户端域相关联,则域的至少一个中继可以拦截(多个)DOTS_PROBE_REQUEST消息(图3中的步骤32_R)。这些消息可以显式地去往中继(按需模式)或具有域地址的中继。在两种情况下,这些消息必须被中继(33_R)到DOTS客户端。优选地,中继不修改DOTS_PROBE_REQUEST消息的内容。

[0235] 在客户端接收到(34_C)DOTS_PROBE_REQUEST消息后,DOTS客户端向访问控制服务器发送(35_C)DOTS_PROBE_REPLY响应。优选地,消息的内容不被客户端修改。特别地,响应包括控制消息的信息特征项。

[0236] 在访问控制服务器接收到(36_S)DOTS_PROBE_REPLY消息后,访问控制服务器将响应(DOTS_PROBE_REPLY)与请求(DOTS_PROBE_REQUEST)相关联(37_S),以核实消息的真实性和完整性。

[0237] 如果关联成功,则验证关联的IP资源。

[0238] 例如,DOTS访问控制服务器对“DOTS_PROBE_REPLY”响应消息的处理包括:

[0239] -核实消息的发布者是合法的DOTS客户端:如果不是,则丢弃相对应的IP资源;

[0240] -提取响应消息的内容(控制消息或控制消息的信息特征项);

[0241] -控制消息内容完整性:如果消息的内容与控制消息不相关,则丢弃相对应的IP资源;

[0242] -核实表的内容:如果IP资源与访问控制服务器所维护的表中的任何条目都不匹配,则丢弃该相对应的IP资源;

[0243] -验证相对应的IP资源。

[0244] 可以针对所有所选择的需要被验证的地址来重复这些步骤。

[0245] 图11至图15示出了根据该第一实施例(“DOTS探测”)的核实过程的实施例。

[0246] 图11示出了与DOTS客户端相关联的所有IP资源的成功验证的示例。在该示例中,假设访问控制服务器14向客户端通知所选择的待验证的地址(例如,地址P1到Pi)的列表(25_S)。注意,该步骤是可选的。在接收到该列表(26_C)后,DOTS客户端配置(“设置”)所需的中继,以便它们准备好接收DOTS_PROBE_REQUEST验证消息。DOTS客户端可以向访问控制服务器发送“ACK”确认消息,以指示客户端域已准备好。然后,访问控制服务器可以向每个待验证的地址的中继器发送(31_S)DOTS_PROBE_REQUEST验证消息。这些信息由中继(R1至Ri)成功中继(33_R)到DOTS客户端。DOTS客户端随后向DOTS访问控制服务器发送(35_C)DOTS_PROBE_REPLY消息。DOTS访问控制服务器核实消息的内容的完整性,并在查阅其表之后验证地址。这些地址在可在访问控制服务器上配置的时间段内与该域相关联。因此,地址P1至Pi的状态是“有效的”。

[0247] 图12示出了与DOTS客户端相关的所有IP资源的成功验证的另一示例。根据该第二示例,DOTS_PROBE_REQUEST确认消息被发送(31_S)到同一中继,而无需事先通知客户端。地址P1至Pi的状态也是“有效的”。

[0248] 图13示出了部分成功的地址验证的示例。只有地址P1有效,而地址Pi不是。因此,地址P1的状态是“有效的”,而地址Pi的状态是“无效的”。

[0249] 特别地，注意，如果没有从客户端接收到响应，或者如果接收到的响应没有被验证，则访问控制服务器断定该IP资源与该DOTS客户端域不相关联。因此，它从其表中删除所述地址。

[0250] 图14示出了失败的地址验证的示例，在这种情况下，访问控制服务器没有接收到对DOTS_PROBE_REQUEST消息的任何响应。因此，地址P1和Pi的状态为“无效的”。

[0251] 图15示出了另一示例，根据该示例，客户端生成DOTS_PROBE_REPLY响应消息以模拟其域中的中继实际上已经接收到DOTS_PROBE_REQUEST验证消息。这些DOTS_PROBE_REPLY消息不被访问控制服务器验证，因为DOTS_PROBE_REQUEST和DOTS_PROBE_REPLY消息的有效载荷不相关。

[0252] 现在描述用于核实所选择的(多个)资源的有效性(参考图2的步骤27_S)的第二实施例(“协作DOTS/ISP”)。

[0253] 该第二实施例包括请求访问提供商核实由DOTS客户端声明的地址或前缀是否实际上由该提供商分配给该客户端。该实施例假设访问提供商公开编程接口(API)以向第三方提供增值服务(诸如IP资源验证)。此外，为了保护客户端的数据的机密性，一些信息项不会向这些第三方公开，或者只有在客户端明确同意的情况下才公开。此外，为了避免数据欺骗，客户端的信息不会发送给第三方。

[0254] 还根据该第二实施例来实施由访问控制服务器接收(23_S)与客户端域相关联的至少一个IP资源的列表的步骤、从列表中选择(24_S)至少一个待验证的IP资源的步骤、以及可选地将所选择的待验证的(多个)IP资源发送(25_S)到DOTS客户端的步骤，并且类似于根据第一实施例来实施的步骤。

[0255] 至于核实(27_S)所选择的(多个)IP资源的有效性的步骤，其涉及一个或多个验证服务器。

[0256] 更具体地，如图4所示，根据该第二实施例，访问控制服务器接收(41_S)表示客户端域或管理客户端域的实体的身份的信息项。

[0257] 例如，DOTS访问控制服务器检索拥有IP资源的(多个)提供商的身份。这种信息确实可以公开获得。为此，访问控制服务器查询例如欧洲IP网络(Réseaux IP Européens，RIPE)数据库。

[0258] 下面给出了使用RIPE数据库资源来检索客户端域或管理客户端域的IP资源“80.12.102.157”的实体的身份的请求的示例：

[0259] https://apps.db.ripe.net/db-web-ui\

[0260] /#/query?searchtext＝80.12.102.157#resultsSection

[0261] 如上所述，该第二实施例假设访问提供商公开用于验证IP资源的编程接口(API)，例如在由这些访问提供商托管的一个或多个验证服务器中。验证服务器地址对于这些访问提供商的客户端来说也是可访问/使用的。

[0262] 如果访问提供商公开用于验证IP资源的所述API，并且如果RIPE库被修改以指定(多个)验证服务器，则对该请求的响应指示：根据该示例，IP资源“80.12.102.157”被分配给访问提供商“Orange S.A”，并且该IP资源的(多个)验证服务器由地址“80.12.102.15”和“80.12.102.16”定位。

[0263] 下面给出了对请求的响应的示例：

[0264] Responsible organisation:Orange S.A.

[0265] inetnum:80.12.102.144-80.12.102.159

[0266] validation server(s):80.12.102.15,80.12.102.16

[0267] netname:VISION

[0268] descr:France Telecom NDC

[0269] country:FR

[0270] admin-c:FTO9-RIPE

[0271] tech-c:FTO9-RIPE

[0272] status:ASSIGNED PA

[0273] mnt-by:FT-BRX

[0274] created:2014-11-20T10:56:45Z

[0275] last-modified:2018-02-09T15:00:11Z

[0276] source:RIPE

[0277] 下面将更详细地描述为验证所选择的IP资源而实施的步骤。

[0278] DOTS访问控制服务器向DOTS客户端传送(25_S)，可选地，所选择的IP资源或所选择的IP资源的列表。DOTS访问控制服务器还识别(42_S)资源的所有者和至少一个相关联的验证服务器。

[0279] 一旦DOTS客户端接收到(26_C)列表，DOTS客户端就与由客户端的访问提供商所管理的验证服务器建立安全通信，以检索表示客户端域或管理客户端域的实体的身份的信息项。例如，验证服务器确定(401_V)客户端域的身份的唯一摘要。可以为摘要分配有效期。

[0280] 这种摘要可以容易且明确地识别客户端域，而不泄露关于客户的其他机密信息。

[0281] 例如，验证服务器可以根据“subscriber_45979230632_timestamp_2018-02-08T00:00:11Z”命名法来生成与管理客户机域的实体相对应的摘要，该实体的标识符为“45979230632”，时间戳为“2018-02-08T00:00:11Z”：f4b542f76be38153ecc66b7c4aaa87a04c46def8116d185c132e1c4a1f5152033

[0282] 如果DOTS客户端是托管验证服务器的访问提供商的客户端，则该DOTS客户端可以获得(403_C)摘要。

[0283] 如果没有接收到摘要，则不验证该IP资源。

[0284] 该/这些摘要然后由客户端发送(404_C)到DOTS访问控制服务器。

[0285] 在接收到(41_S)摘要后，DOTS访问控制服务器向验证服务器R1至Ri发送(43_S)DOTS_PROBE_REQUEST验证消息。这些消息包括客户先前传送的摘要，以及待验证的IP资源。在没有摘要的情况下，访问控制服务器不能识别相关的客户端，并且IP资源不被验证。

[0286] 在验证服务器Ri接收到(44_V)验证消息后，验证服务器Ri核实待验证的IP资源(地址/前缀)是否实际上被分配给由所述摘要识别的客户端。

[0287] 如果是，则IP资源是有效的，否则IP资源是无效的。

[0288] 可以向访问控制服务器发送确认消息(DOTS_PROBE_REPLY)或错误消息。

[0289] 接下来的操作类似于第一实施例“DOTS探测”的操作。

[0290] 图16示出了与DOTS客户端相关联的所有IP资源的成功验证的示例。在该示例中，假设访问控制服务器14通知客户端所选择的待验证的地址(例如，地址R1至Ri)的列表

(25_S)。注意，该步骤是可选的。在接收到该列表后，DOTS客户端查询与待验证的IP资源R1至Ri相关联的、第一访问提供商12的验证服务器V1和第i访问提供商16的验证服务器Vi，以获得(403_C)表示客户端域的身份的信息项，然后将该信息项发送(404_C)到访问控制服务器。

[0291] 然后，访问控制服务器可以向(多个)验证服务器发送(43_S)DOTS_PROBE_REQUEST验证消息，其携带待验证的IP资源和表示客户端域的身份的信息项。

[0292] (多个)验证服务器核实由DOTS_PROBE_REQUEST验证消息携带的IP资源实际上与由表示客户端域的身份的信息项所识别的域相关联。如果是的话，地址R1至Ri的状态因此是“有效的”。

[0293] 可能的是，(多个)验证服务器向DOTS访问控制服务器发送DOTS_PROBE_REPLY响应。

[0294] 5.3结构

[0295] 最后，上面结合图17描述了根据一个实施例的访问控制服务器、客户端节点、中继节点和验证服务器的简化结构。

[0296] 根据特定实施例，访问控制服务器包括含有缓冲存储器的存储器171_S、配备有例如可编程计算机器或专用计算机器的处理单元172_S(例如，P处理器)，并由实施根据本发明的一个实施例的用于核实IP资源的有效性的方法步骤的计算机程序173_S控制。

[0297] 在初始化时，计算机程序173_S的代码指令例如在被处理单元172_S的处理器执行之前被加载到RAM中。

[0298] 处理单元172_S的处理器根据计算机程序173_S的指令来实施先前所述的用于核实IP资源的有效性的方法步骤，以：

[0299] -接收从客户端域的客户端节点发送到访问控制服务器的、与客户端域相关联的至少一个IP资源的列表；

[0300] -从列表中选择至少一个待验证的IP资源；

[0301] -核实所选择的(多个)IP资源的有效性。

[0302] 根据特定实施例，客户端节点包括存储器171_C(存储器171_C包括缓冲存储器)、配备有例如可编程计算机器或专用计算机器的处理单元172_C(例如，P处理器)，并由实施根据本发明的一个实施例的用于声明IP资源的方法步骤的计算机程序173_C控制。

[0303] 在初始化时，计算机程序173_C的代码指令例如在被处理单元172_C的处理器执行之前被加载到RAM中。

[0304] 处理单元172_C的处理器根据计算机程序173_C的指令来实施先前描述的用于声明IP资源的方法步骤，以：

[0305] -获得与客户端节点所属的客户端域相关联的至少一个IP资源的列表；

[0306] -将列表发送到访问控制服务器。

[0307] 根据特定实施例，中继节点包括含有缓冲存储器的存储器171_R、配备有例如可编程计算机器或专用计算机器的处理单元172_R(例如，P处理器)，并由实施根据本发明的一个实施例的用于处理IP资源验证请求的方法步骤的计算机程序173_R控制。

[0308] 在初始化时，计算机程序173_R的代码指令例如在被处理单元172_R的处理器执行之前被加载到RAM中。

[0309] 处理单元172_V的处理器根据计算机程序173_R的指令来实施先前描述的用于处理IP

资源验证请求的方法步骤,以:

[0310] -接收源自访问控制服务器的、包括控制消息的至少一个请求,

[0311] -向客户端域的客户端节点发送(多个)请求,

[0312] 所述中继节点与由访问控制服务器从与客户端域相关联的至少一个IP资源的列表中选择的至少一个IP资源相关联,该列表是先前从客户端域的客户端节点发送到访问控制服务器的。

[0313] 特别地,这种中继节点可以激活先前定义的"DOTS_CHECK_RELAY"功能。

[0314] 根据特定实施例,验证服务器包括含有缓冲存储器的存储器171_V、配备有例如可编程计算机器或专用计算机器的处理单元172_V(例如,P处理器),并由实施根据本发明的一个实施例的用于核实IP资源的有效性的方法步骤的计算机程序173_R控制。

[0315] 在初始化时,计算机程序173_R的代码指令例如在被处理单元172_V的处理器执行之前被加载到RAM中。

[0316] 处理单元172_V的处理器根据计算机程序173_R的指令来实施先前描述的用于核实IP资源的有效性的方法步骤,以:

[0317] -接收或拦截至少一个请求,该请求包括表示客户端域的身份的信息项和至少一个所选择的IP资源,

[0318] -基于表示客户端域的身份的信息项来识别客户端域,

[0319] -考虑客户端域的身份,核实所选择的IP资源与客户端域的关联。

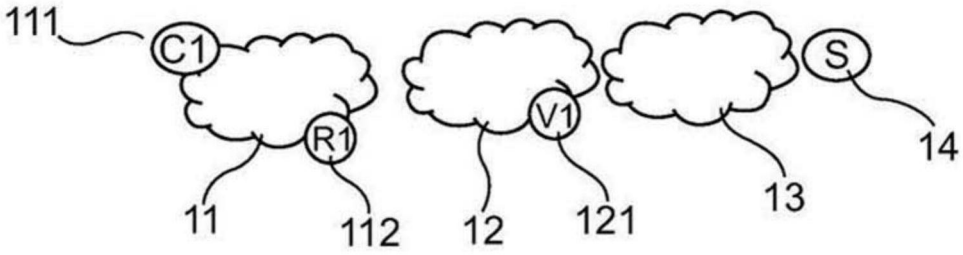

111
C1
R1
11
112
12
V1
121
13
S
14

图1

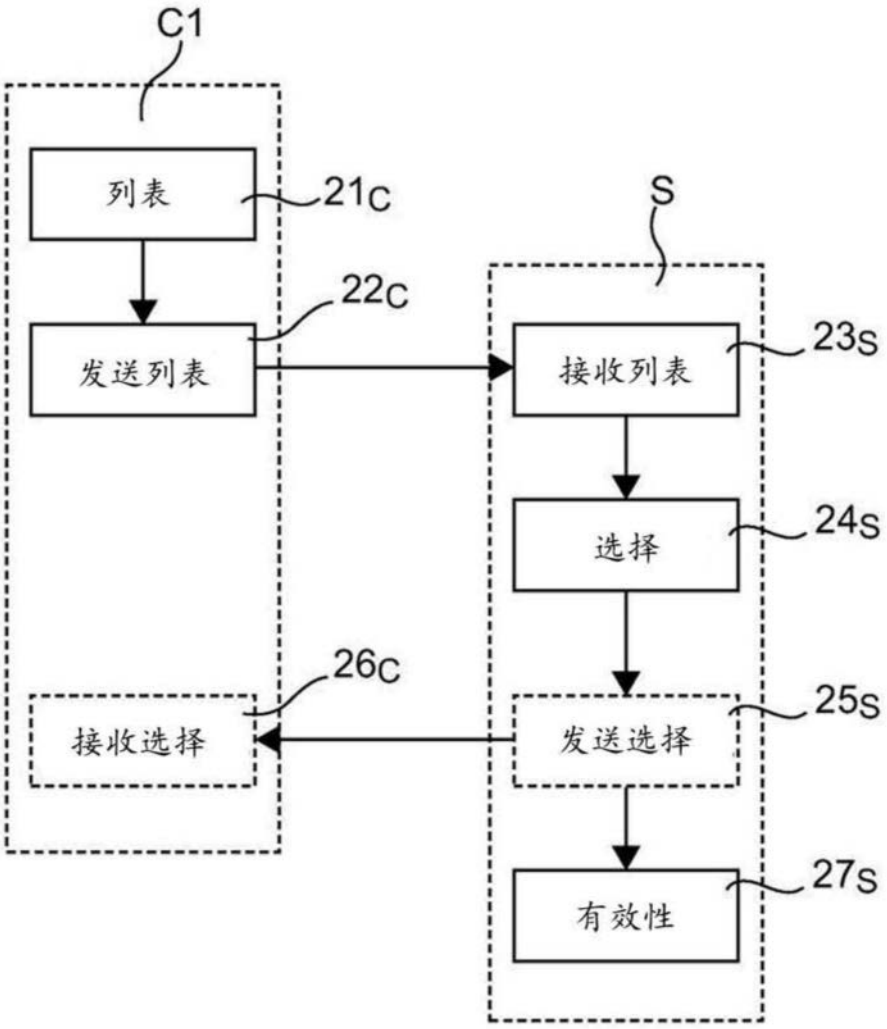

C1
列表
21C
22C
发送列表
S
接收列表
23S
选择
24S
26C
接收选择
发送选择
25S
有效性
27S

图2

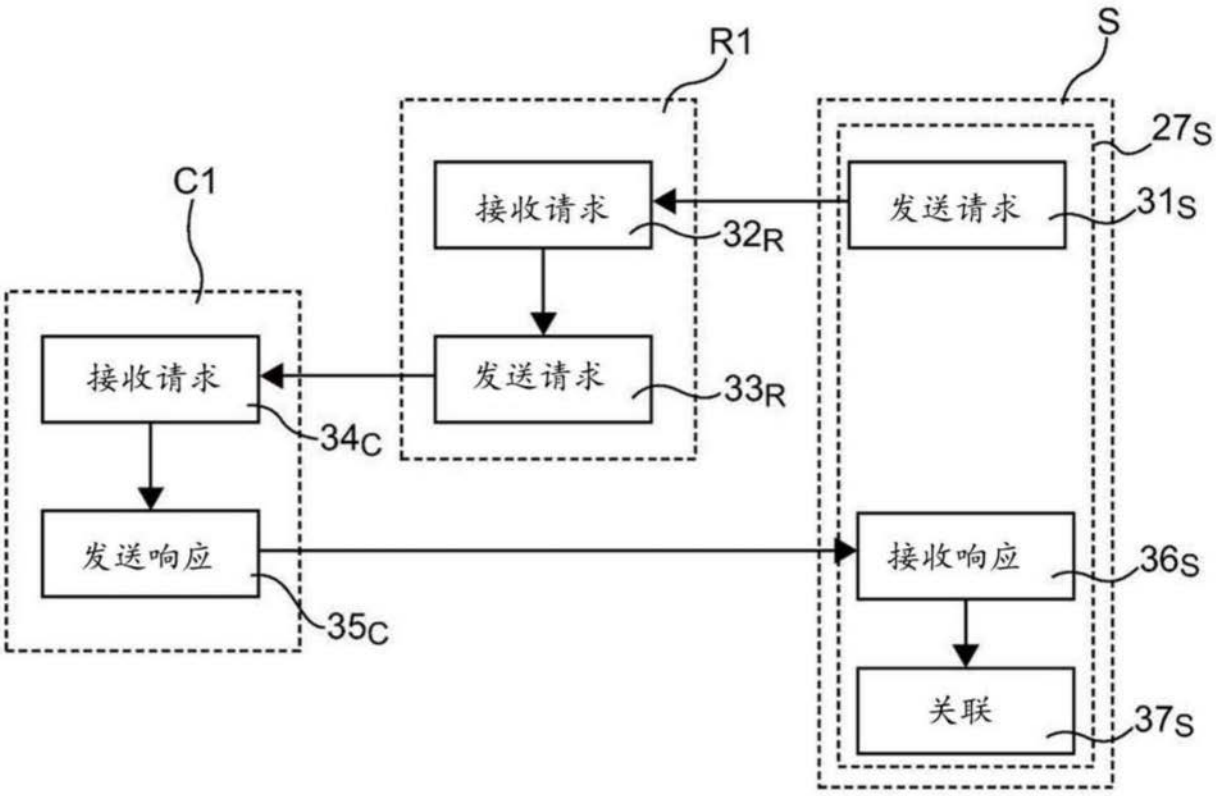

R1
S
27S
C1
接收请求
32R
发送请求
31S
接收请求
发送请求
33R
34C
发送响应
接收响应
36S
35C
关联
37S

图3

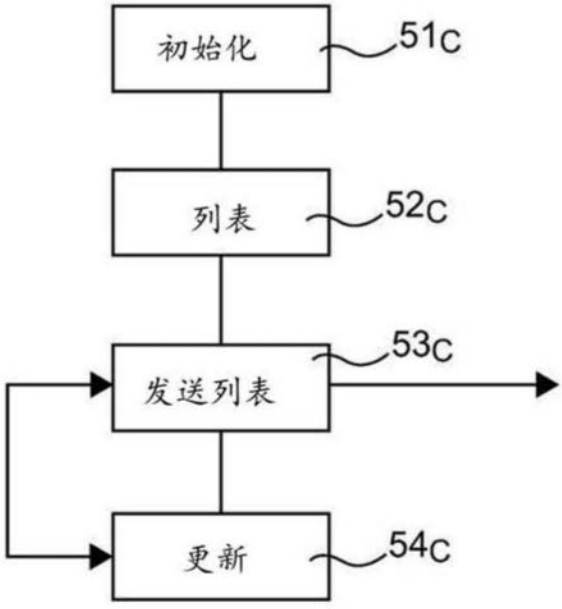

初始化
51C
列表
52C
53C
发送列表
更新
54C

图5

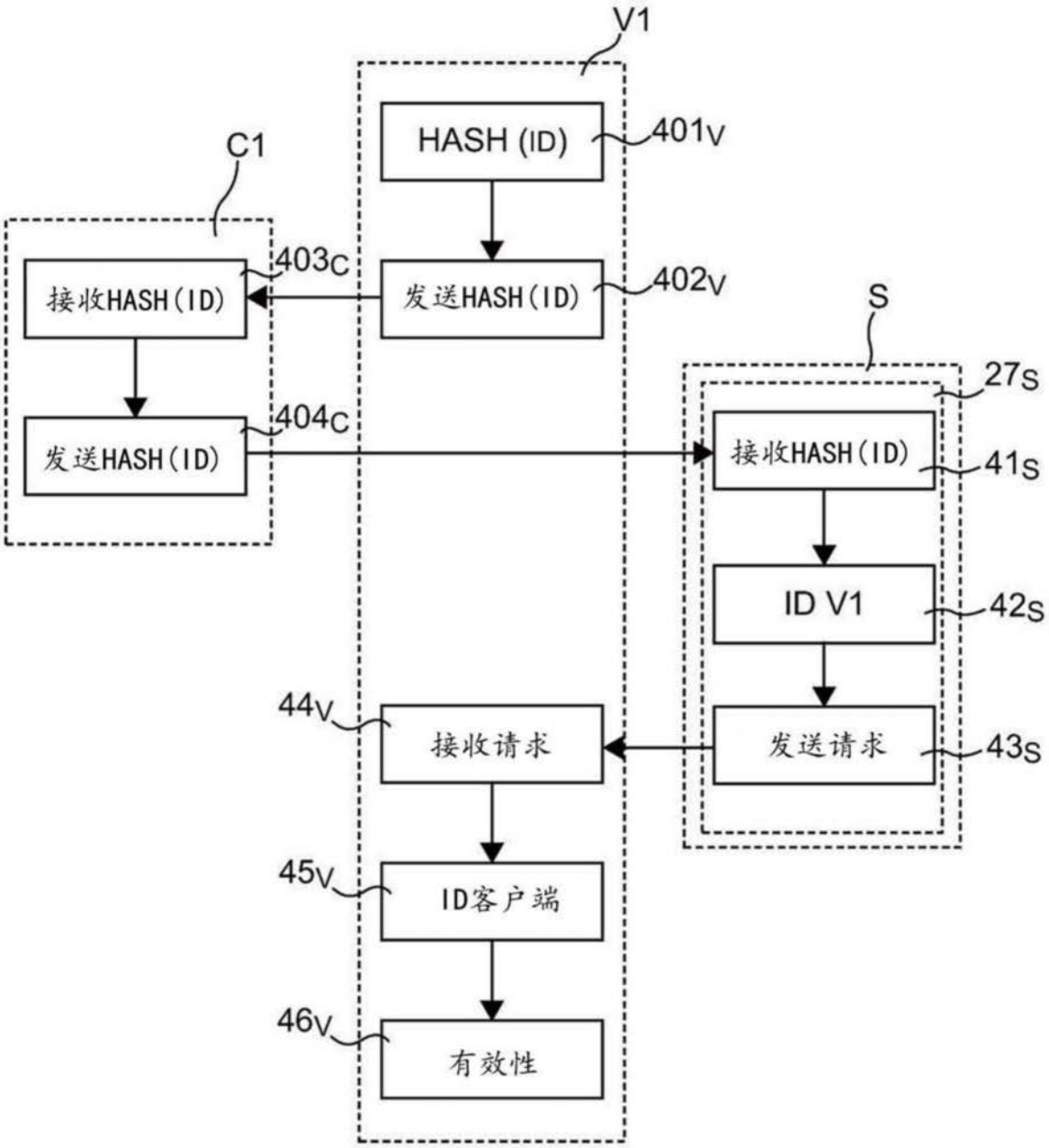

V1
HASH (ID)
401V
C1
403C
接收HASH(ID)
发送HASH(ID)
402V
S
27S
404C
发送HASH(ID)
接收HASH(ID)
41S
ID V1
42S
44V
接收请求
发送请求
43S
45V
ID客户端
46V
有效性

图4

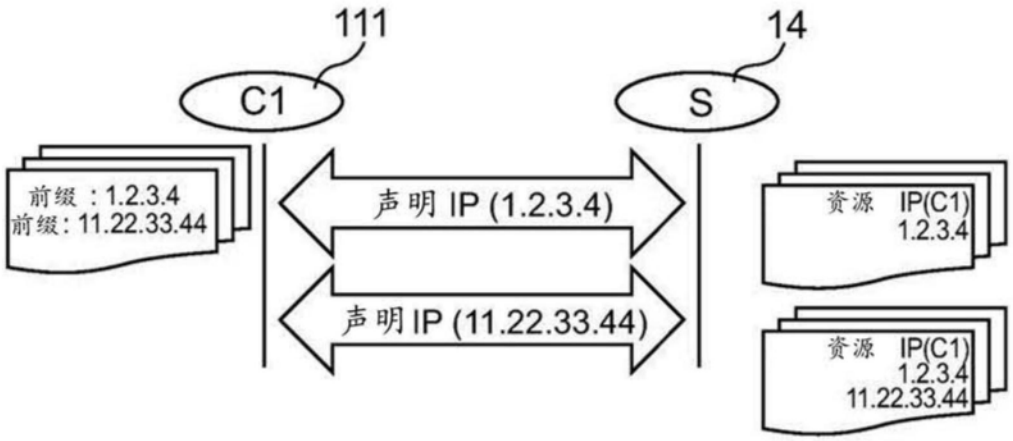

111
14
C1
S
前缀 ：1.2.3.4
前缀：11.22.33.44
声明 IP (1.2.3.4)
声明 IP (11.22.33.44)
资源 IP(C1)
1.2.3.4
资源 IP(C1)
1.2.3.4
11.22.33.44

图6A

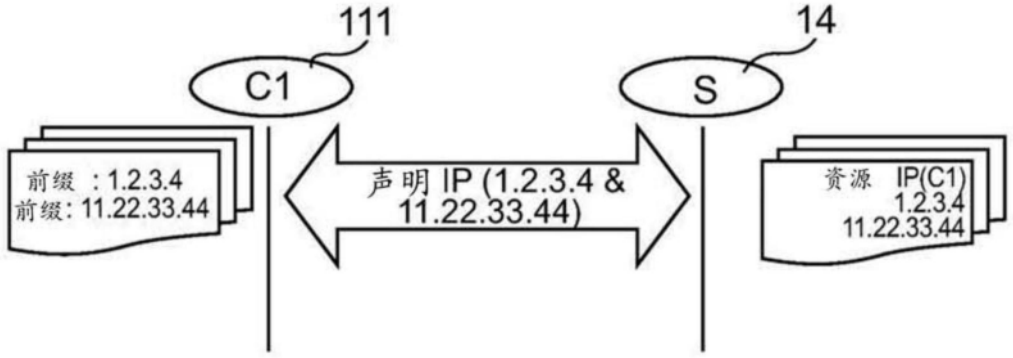

111
14
C1
S
前缀 ：1.2.3.4
前缀：11.22.33.44
声明 IP (1.2.3.4 &
11.22.33.44)
资源 IP(C1)
1.2.3.4
11.22.33.44

图6B

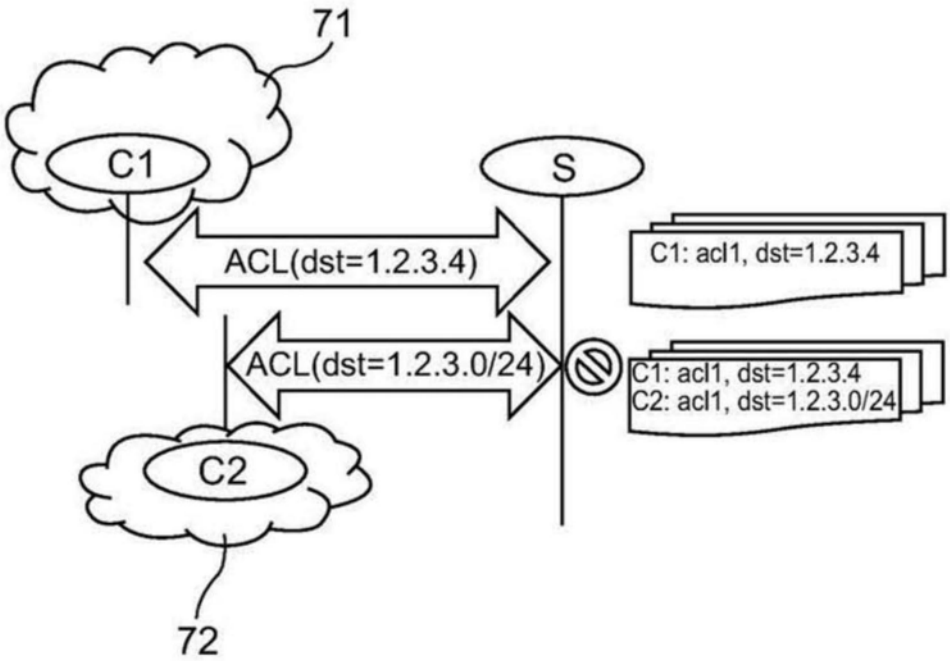

71
C1
S
ACL(dst=1.2.3.4)
C1: acl1, dst=1.2.3.4
ACL(dst=1.2.3.0/24)
C1: acl1, dst=1.2.3.4
C2: acl1, dst=1.2.3.0/24
C2
72

图7

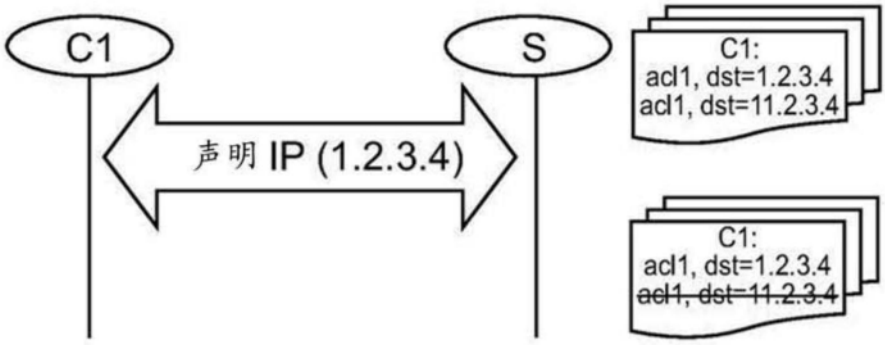

C1
S
C1:
acl1, dst=1.2.3.4
acl1, dst=11.2.3.4
声明 IP (1.2.3.4)
C1:
acl1, dst=1.2.3.4
~~acl1, dst=11.2.3.4~~

图8

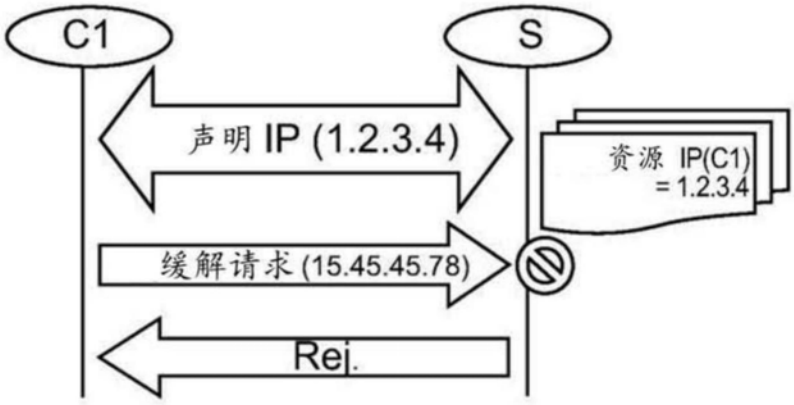

C1
S
声明 IP (1.2.3.4)
资源 IP(C1)
= 1.2.3.4
缓解请求 (15.45.45.78)
Rej.

图9

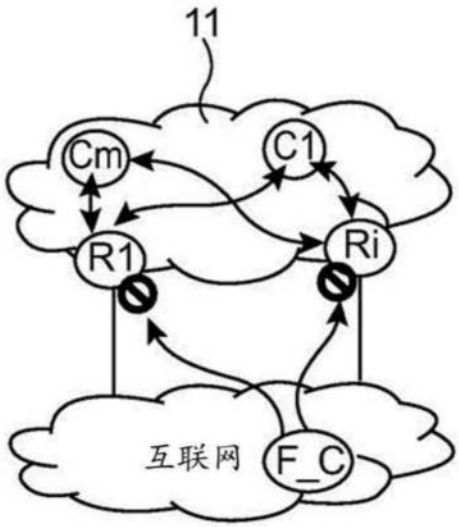

11
Cm
C1
R1
Ri
互联网
F_C

图10

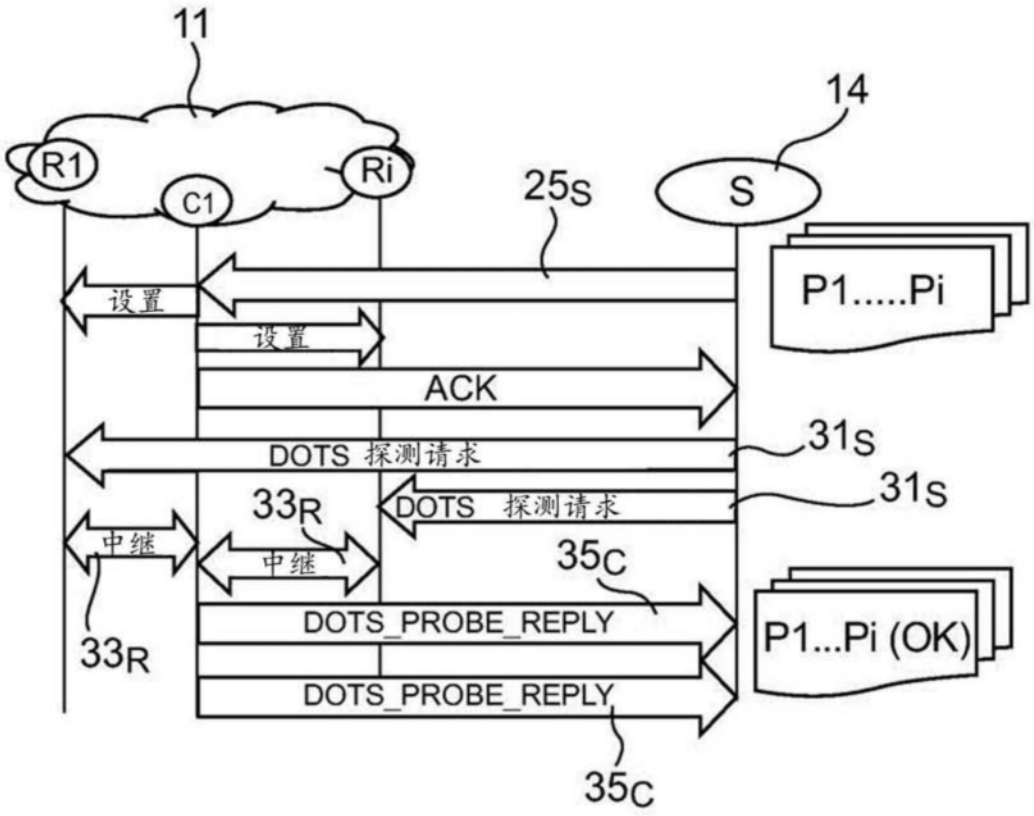

11
14
R1
C1
Ri
25S
S
P1.....Pi
设置
设置
ACK
DOTS 探测请求
31S
33R
DOTS 探测请求
31S
中继
中继
35C
DOTS_PROBE_REPLY
P1...Pi (OK)
33R
DOTS_PROBE_REPLY
35C

图11

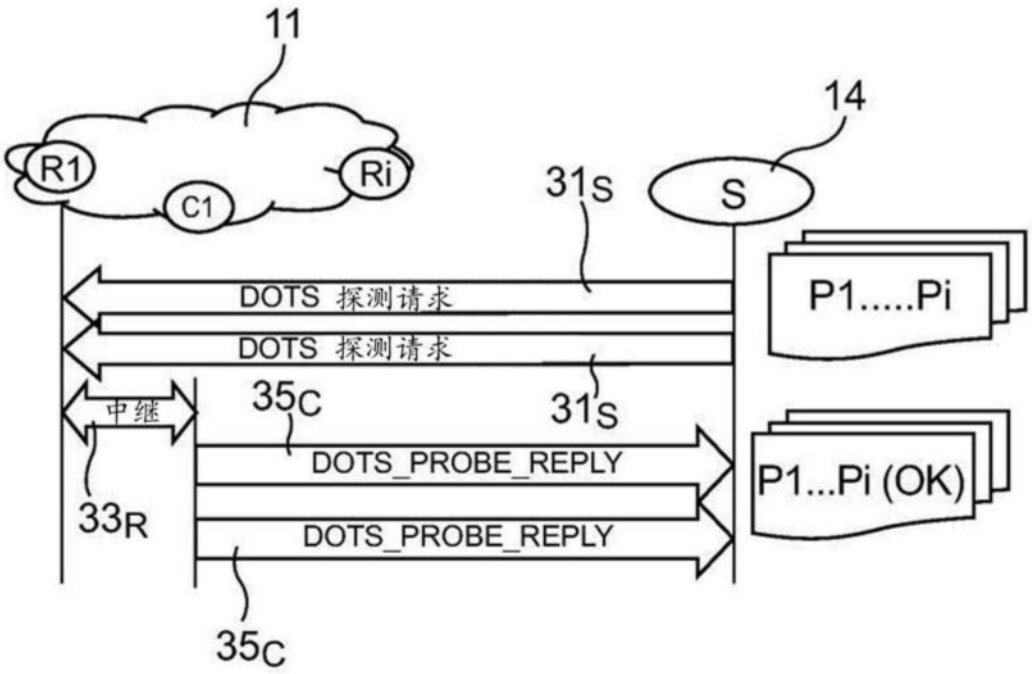

11
14
R1
Ri
C1
31S
S
DOTS 探测请求
P1.....Pi
DOTS 探测请求
中继
35C
31S
DOTS_PROBE_REPLY
P1...Pi (OK)
33R
DOTS_PROBE_REPLY
35C

图12

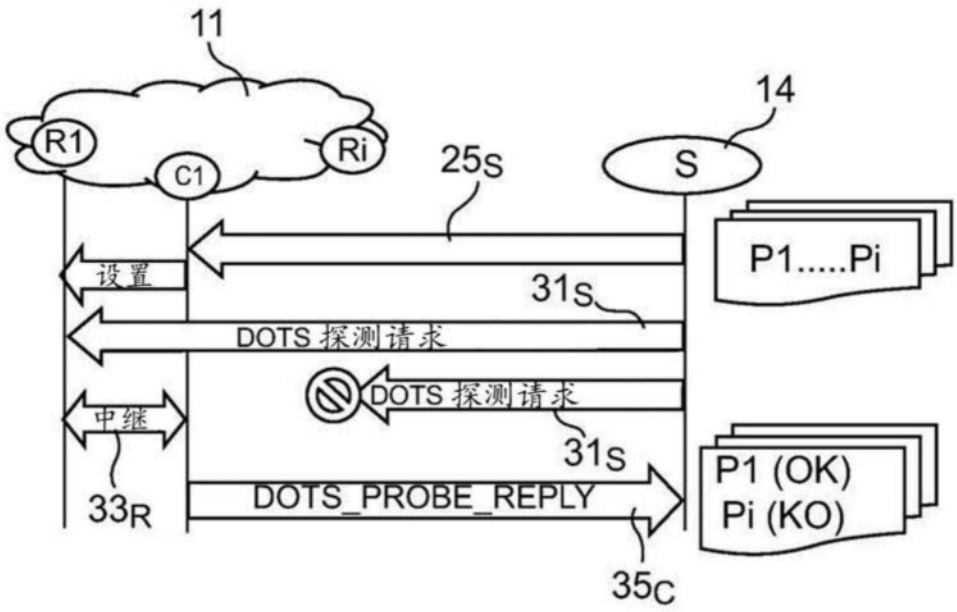

11
14
R1
Ri
C1
25S
S
P1.....Pi
设置
31S
DOTS 探测请求
DOTS 探测请求
中继
31S
P1 (OK)
Pi (KO)
33R
DOTS_PROBE_REPLY
35C

图13

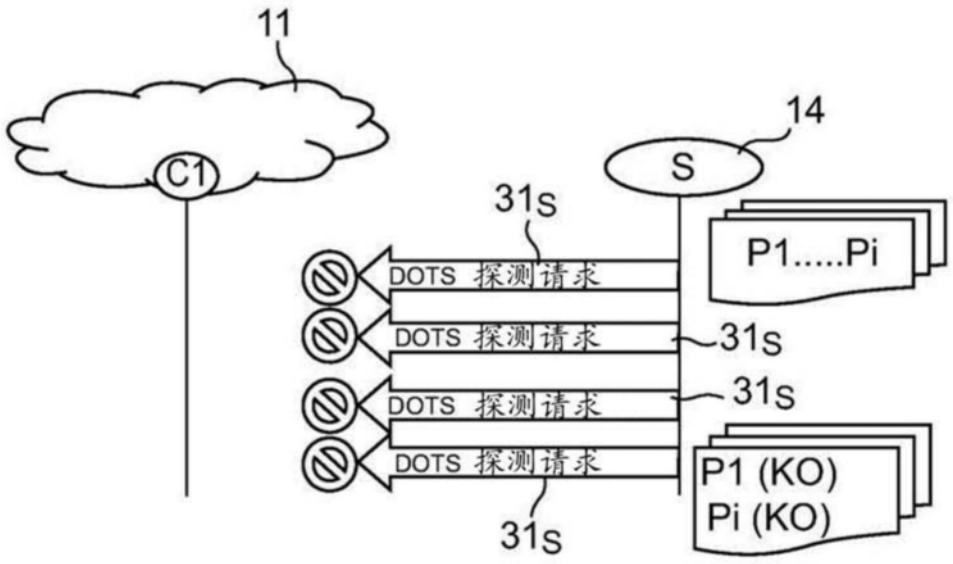

11
C1
14
S
31S
P1.....Pi
DOTS 探测请求
DOTS 探测请求
31S
DOTS 探测请求
31S
DOTS 探测请求
P1 (KO)
Pi (KO)
31S

图14

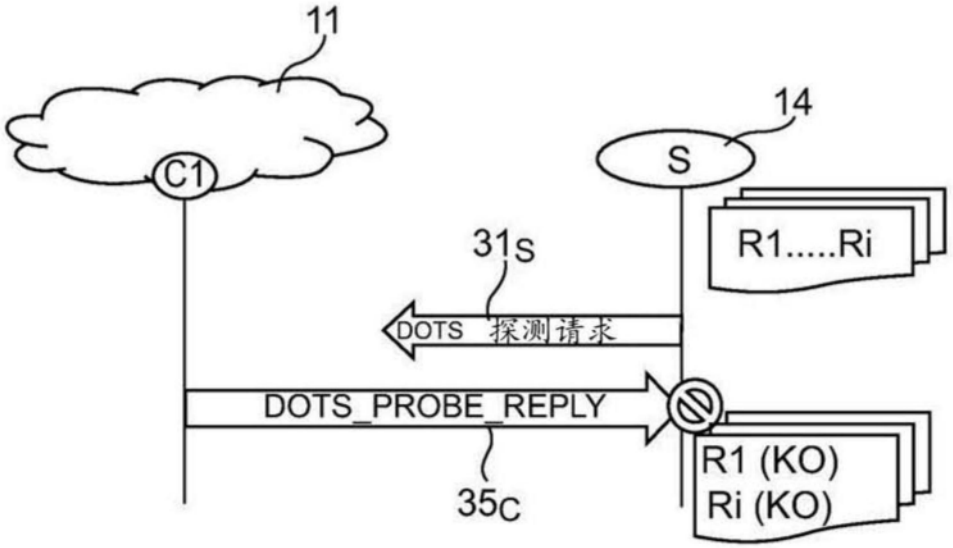

11
C1
14
S
R1.....Ri
31S
DOTS 探测请求
DOTS_PROBE_REPLY
R1 (KO)
Ri (KO)
35C

图15

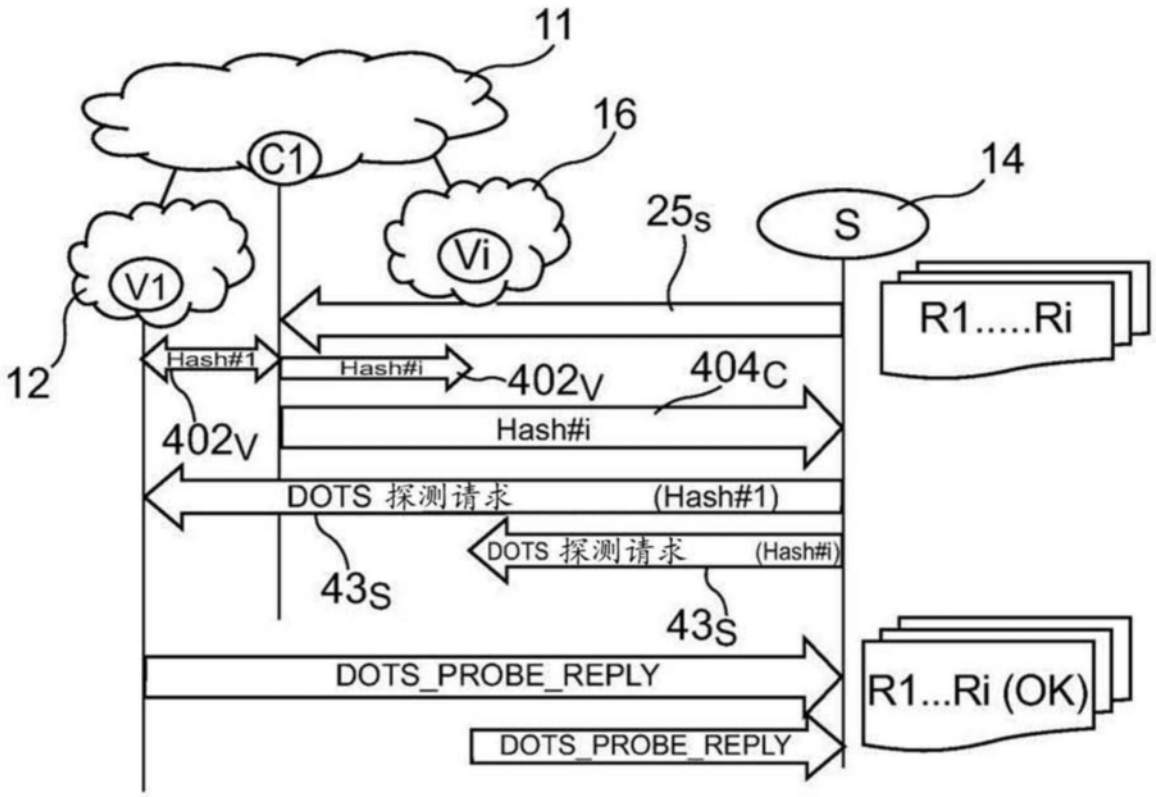

11
16
C1
14
25s
S
Vi
V1
R1.....Ri
12
Hash#1
Hash#i
402V
404C
402V
Hash#i
DOTS 探测请求 (Hash#1)
DOTS 探测请求 (Hash#i)
43S
43S
DOTS_PROBE_REPLY
R1...Ri (OK)
DOTS_PROBE_REPLY

图16

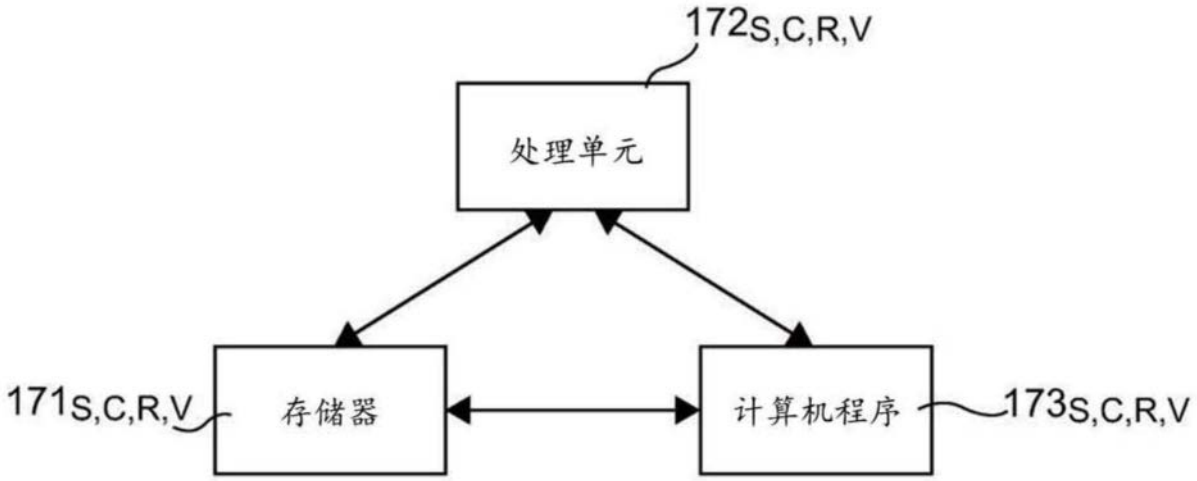

172S,C,R,V
处理单元
171S,C,R,V
存储器
计算机程序
173S,C,R,V

图17