(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2015 年 10 月 22 日 (22.10.2015)

WIPO | PCT

(10) 国际公布号
WO 2015/158194 A1

(51) 国际专利分类号:
H04L 29/12 (2006.01)

(21) 国际申请号: PCT/CN2015/074614

(22) 国际申请日: 2015 年 3 月 19 日 (19.03.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410158695.6 2014 年 4 月 18 日 (18.04.2014) CN

(71) 申请人: **北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED)** [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室（德胜园区）, Beijing 100088 (CN)。 **奇智软件（北京）有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED)** [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。

(72) 发明人: **谭晓生 (TAN, Xiaosheng)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **齐向东 (QI, Xiangdong)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **濮灿 (PU, Can)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: **北京智汇东方知识产权代理事务所（普通合伙） (WISEAST INTELLECTUAL PROPERTY LAW FIRM)**; 中国北京市海淀区花园路 13 号 5 幢 320 房间, Beijing 100088 (CN)。

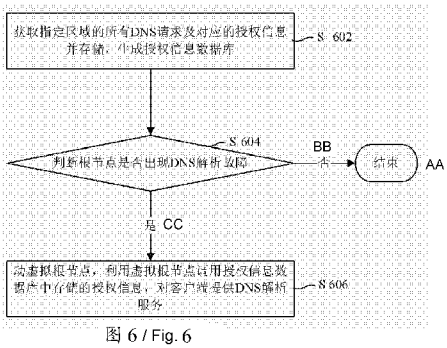
(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) **Title**: DNS SECURITY SYSTEM AND METHOD THEREOF FOR PROCESSING A FAILURE

(54) **发明名称** : DNS 安全系统及其故障处理方法



S 602 OBTAINING AND STORING ALL DNS REQUESTS AND CORRESPONDING AUTHORIZATION INFORMATION IN DESIGNATED AREA AND GENERATING AUTHORIZATION INFORMATION DATABASE
S 604 DETERMINING WHETHER DNS RESOLUTION FAILURE HAS HAPPENED
S 606 INITIATING VIRTUAL ROOT NODE AND USING VIRTUAL ROOT NODE TO INVOKE AUTHORIZATION INFORMATION STORED IN AUTHORIZATION INFORMATION DATABASE AND TO PROVIDE DNS RESOLUTION SERVICE CLIENT
AA END
BB NO
CC YES

图 6 / Fig. 6

(57) **Abstract**: The present invention provides a DNS security system and method thereof for processing a failure. The DNS security system comprises: at least one client, configured to initiate a DNS request; a root node, configured to provide authorization information to said DNS request; an authorization information database, configured to store all DNS requests and corresponding authorization information in a designated area; a virtual root node, configured to invoke corresponding authorization information from said authorization information database when a DNS resolution failure happens on said root node, and to provide a resolution service to a corresponding client. Using the present invention enhances the security and stability of DNS resolution.

(57) **摘要**: 本发明提供了一种 DNS 安全系统及其故障处理方法。DNS 安全系统包括：至少一个客户端，配置为发起 DNS 请求；根节点，配置为对所述 DNS 请求提供授权信息；授权信息数据库，配置为存储指定区域的所有 DNS 请求及对应的授权信息；虚拟根节点，配置为当所述根节点出现 DNS 解析故障时，从所述授权信息数据库中调用相应授权信息，为对应客户端提供解析服务。采用本发明能够提高 DNS 解析的安全性和稳定性。

WO 2015/158194 A1

DNS 安全系统及其故障处理方法

技术领域

本发明涉及互联网应用领域，尤其涉及一种 DNS 安全系统，以及应用该 DNS 安全系统进行故障处理的方法。

背景技术

DNS 是域名系统（Domain Name System）的缩写，是因特网（Internet）一项核心服务，它作为可以将域名和 IP 地址相互映射的一个分布式数据库，能够使人更方便的访问互联网，而不用去记住能够被机器直接读取的 IP 数串。

Internet 主机域名的一般结构为：主机名.三级域名.二级域名.顶级域名。Internet 的顶级域名由 Internet 网络协会域名注册查询负责网络地址分配的委员会进行登记和管理，它还为 Internet 的每一台主机分配唯一的 IP 地址。

图 1 示出了根据背景技术的整体 DNS 架构的示意图。DNS 架构是一个层次树状结构，这个树状结构称为 DNS 域名空间，最上面的域名空间被称为“根节点”。参见图 1，整个 DNS 架构形成域名层次空间，从顶级域到某一个子域的路径就构成了一个域名，例如从顶级域.com 到它的二级域 microsoft，再到 microsoft 的子域 departmentA 就构成了一个域名 departmentA.microsoft.com。

其中，DNS 根服务器是 DNS 树型域名空间的“根”，负责 DNS 的解析，对于域名解析起着极其关键的作用。从理论上说，任何形式的标准域名要想被实现解析，按照技术流程，都必须经过全球“层级式”域名解析体系的工作才能完成。

“层级式”域名解析体系第一层就是根服务器，负责管理世界各国的域名信息，在根服务器下面是顶级域名服务器，即相关国家域名管理机构的数据库，如中国的 CNNIC，然后再到下一级的域名数据库和 ISP（Internet Service Provider，因特网服务供应商）的缓存服务器查询。一个域名必须首先经过根数据库的解析后，才能转到顶级域名服务器进行解析。如果 DNS 根节点不能访问，那么一切的域名解析都会

失败。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决或者减缓上述问题的DNS安全系统和相应的故障处理的方法。

根据本发明的一个方面，提供了一种DNS安全系统，包括：

至少一个客户端，配置为发起DNS请求；

根节点，配置为对所述DNS请求提供授权信息；

授权信息数据库，配置为存储指定区域的所有DNS请求及对应的授权信息；

虚拟根节点，配置为当所述根节点出现DNS解析故障时，从所述授权信息数据库中调用相应授权信息，为对应客户端提供解析服务。

根据本发明的另一个方面，提供了一种应用上述任一项所述的DNS安全系统进行故障处理的方法，包括：

获取指定区域的所有DNS请求及对应的授权信息并存储，生成授权信息数据库；

判断根节点是否出现DNS解析故障；

若是，启动虚拟根节点，利用所述虚拟根节点调用所述授权信息数据库中存储的授权信息，对客户端提供DNS解析服务。

根据本发明的又一个方面，提供了一种计算机程序，其包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据上文任一个所述的应用DNS安全系统进行故障处理的方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了上述的计算机程序。

本发明的有益效果为：

在本发明实施例中，设置了虚拟根节点，当根节点出现DNS解析故障时，虚拟根节点能够代替根节点实现DNS解析功能。为实现虚拟根节点这一功能，授权信息数据库中必须存储有足够的信息，即，授权信息数据库中存储指定区域内的所有DNS请求及对应的授权信息，这样虚拟根节点才能够有足够的资源对DNS请求进行应答。因此，虚

拟根节点的实现是在授权信息数据库的基础上实现的。结合新增的授权信息数据库以及虚拟根节点，能够在根节点解析故障的时候为客户端提供 DNS 解析功能，能够降低 DNS 单点故障和提高 DNS 防御攻击能力，同时还可以对虚拟根节点设置访问权限控制，屏蔽 DNS 的攻击数据，提高 DNS 解析的安全性及稳定性。对于危险 DNS 攻击，从授权信息数据库中查询不到具体的授权信息，则虚拟根节点不会为其提供解析服务，因此可以实现防止 DNS 攻击。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示出了根据背景技术的整体 DNS 架构的示意图；

图 2 示出了根据本发明一个实施例的 DNS 安全系统的结构示意图；

图 3 示出了根据本发明一个实施例授权信息数据库对本地 DNS 服务器进行数据备份的示意图；

图 4 示出了根据本发明一个实施例的 DNS 安全系统的具体架构图；

图 5 示出了根据本发明一个实施例的 DNS 安全系统的另一个结构示意图；

图 6 示出了根据本发明一个实施例的利用 DNS 安全系统进行故障处理的方法的处理流程图；

图 7 示意性地示出了用于执行根据本发明的应用 DNS 安全系统进行故障处理的方法的计算设备的框图；以及

图 8 示意性地示出了用于保持或者携带实现根据本发明的应用 DNS 安全系统进行故障处理的方法的程序代码的存储单元。

具体实施方式

下面结合附图和具体的实施方式对本发明作进一步的描述。

为解决上述技术问题，本发明实施例提供了一种 DNS 安全系统，用于在根节点结构故障时能够进行故障处理类的容灾处理。图 2 示出了根据本发明一个实施例的 DNS 安全系统的结构示意图。参见图 2，DNS 安全系统中至少包括：

至少一个客户端 210，配置为发起 DNS 请求；

根节点 220，配置为对任意一个客户端 210 发起的 DNS 请求提供授权信息；

授权信息数据库 230，配置为存储指定区域的所有 DNS 请求及对应的授权信息；

虚拟根节点 240，配置为当根节点 220 出现 DNS 解析故障时，从授权信息数据库 230 中调用相应授权信息，为对应客户端 210 提供解析服务。

在本发明实施例中，设置了虚拟根节点，当根节点出现 DNS 解析故障时，虚拟根节点能够代替根节点实现 DNS 解析功能。为实现虚拟根节点这一功能，授权信息数据库中必须存储有足够的信息，即，授权信息数据库中存储指定区域内的所有 DNS 请求及对应的授权信息，这样虚拟根节点才能够有足够的资源对 DNS 请求进行应答。因此，虚拟根节点的实现是在授权信息数据库的基础上实现的。结合新增的授权信息数据库以及虚拟根节点，能够在根节点解析故障的时候为客户端提供 DNS 解析功能，能够降低 DNS 单点故障和提高 DNS 防御攻击能力，同时还可以对虚拟根节点设置访问权限控制，屏蔽 DNS 的攻击数据，提高 DNS 解析的安全性及稳定性。对于危险 DNS 攻击，从授权信息数据库中查询不到具体的授权信息，则虚拟根节点不会为其提供解析服务，因此可以实现防止 DNS 攻击。

具体地，现对 DNS 攻击行为的处理进行详细描述。在本发明实施例中，对于接收的每个网络数据包，应判断出该网络数据包对应的 DNS 行为类型，并根据确定的 DNS 行为类型确定对该网络数据包进行处理的处理主体，进而将该网络数据包转至确定的处理主体进行处理。在本发明实施例中，处理主体可以由两层组成，分别是内核层、应用层。内核层包括网络层、驱动层等，可以实现高速缓存、攻击防护等功能，

而应用层可以对网络数据包进行基本解析，包括域名解析后的地址、数据存储地址的获取等。与现有技术中的 DNS 行为的处理方法相比较，将网络数据包分别划分至内核层和应用层处理，可以将 DNS 请求根据实际请求处理，若遇到一秒几百万次的 DNS 请求攻击，也可以由处理能力较强的内核对其进行处理，而遇见时效性要求相对较低的 DNS 请求，则可以由应用层处理。采用内核和应用层分别处理 DNS 请求，考虑到内核的巨大的处理能力，能够实现大流量的 DNS 查询。并且，因 DNS 请求所导致的修改或启动导致加载时，因内核和应用层是分别处理的，因此可以利用其中之一处理当前 DNS 请求，另一继续对外提供服务。因此，本发明实施例提高了单机的业务处理能力，大大提高系统的处理能力和安全防护能力的同时，还能实现快速域名动态管理和配置，进而实现很多定制化的复杂功能需求。

当 DNS 行为类型确定为攻击行为时，那么，可以确定处理主体为内核，而当 DNS 行为类型为域名解析行为时，可以确定处理主体为应用层。为了提升域名解析服务的响应速度、处理性能及安全防护能力，根据 DNS 的解析原理，在内核模块中可以实现高速缓存和安全防护，正常情况内核模块能高效、稳定地处理 98%的解析请求和绝大部分的攻击防护。而处理逻辑相对复杂，对性能要求并不是那么高的基础解析和管理功能放在应用层实现。

因此，处理主体为内核时，由内核检测所述网络数据包，过滤将网络数据包中携带的 DNS 攻击行为；以及，将过滤后的网络数据包转发至应用层进行处理。内核检测网络数据包时，可以启动防 DDOS 攻击策略、IP 限速策略、域名限速策略等策略，相应的，可以在内核中为每个策略设置独立的内部模块，用于实现不同策略。

此处需要说明的是，每个网络数据包都具备一个特征码，且每个特征码是独一无二的，因此，可以根据特征码判断网络数据包的 DNS 请求的属性，识破伪装成正常数据包的 DNS 攻击操作。现根据如下步骤判断所述网络数据包中是否携带有 DNS 攻击行为：

步骤 A、计算网络数据包的特征码；

步骤 B、判断特征码是否是 DNS 攻击行为的特征码，若是，执行步骤 C，若否，执行步骤 D；

步骤 C、若是，则确定网络数据包中携带有 DNS 攻击行为；

步骤 D、若否，则确定网络数据包中未携带有 DNS 攻击行为。

其中，数据库中通常存储有已知 DNS 攻击行为的特征码的集合，当需要校验时，将步骤 A 中计算出的特征码与数据库的集合进行匹配，若步骤 A 计算出的特征码存在所述集合中，则是 DNS 攻击行为，反之则不是。

其中，特征码可以根据 IP 或域名等域名信息确定，例如，计算指定时间内接收的来自同一 IP 的网络数据包数得到特征码，和/或计算指定时间内接收的来自同一域名的网络数据包数。若 1 秒内从同一 IP 或同一域名接收的网络数据包数远远大于应该接收的包数，就证明该 IP 地址或域名已被变成攻击源。这也是 IP 限速策略、域名限速策略的基本原理。被证明变为攻击源的 IP 地址或域名，之后再接收到来自这一源头的网络数据包，可以直接舍弃或过滤掉，避免被其攻击，提高系统安全性能及处理效率。

内核对攻击行为进行过滤之后，将网络数据包发至应用层进行处理。应用层可以对网络数据包进行解析，获取域名对应的地址信息，从而获取相关数据反馈给客户端。以及，应用层可以对域名信息等数据进行管理，实现数据管理功能。

目前全球仅有 13 台根服务器，且目前的分布是：主根服务器（A）美国 1 个，设置在弗吉尼亚州，辅根服务器（B 至 M）美国 9 个，瑞典、荷兰、日本各 1 个。由上述数据可知，根服务器（即根节点）数量较少，且主要设置在部分区域，那么其他区域在域名分析的过程中缺乏主动性和风险控制功能。

域名系统是互联网的基础服务，而根服务器更是整个域名系统的基础，控制了域名解析的根服务器，也就控制了相应的所有域名和 IP 地址。若存在根服务器的国家突然屏蔽某一地区的域名，那么这些域名所指向的网站就会从互联网上中消失。因此，虚拟根节点的设立十分重要。

在本发明实施例中，在根节点 220 DNS 解析故障的情况下，使用虚拟根节点 240 进行 DNS 解析，为加快解析速度，某些常用的、访问量比较大的 DNS 解析记录，或者某些重要域名的 DNS 解析记录，可以单独存储在授权信息数据库 230 的指定区域中，以便虚拟根节点 240 到授权信息数据库 230 中查询时能够进行快速回复，实现紧急应答。

即，在授权信息数据库 230 中，授权信息可以包括存储访问量超过访问阈值的 DNS 解析记录，和/或，重要域名的 DNS 解析记录。

其中，需要说明的是，授权信息数据库 230 中的授权信息与根节点 220 解析的过程相匹配，能够根据授权信息的相互关系，组成域名层次空间，对应域名空间的第一级。并且，授权信息数据库 230 中的数据信息均能够实时更新。此处的实时更新是指每隔一段时间，会将网络中新的解析记录添加到授权信息数据库中，也可以将授权信息数据库中长期不使用的部分解析记录后移可删除。对于互联网而言，授权信息数据库 230 是互联网域名层次的镜像。图 3 示出了根据本发明一个实施例授权信息数据库对本地 DNS 服务器进行数据备份的示意图。

以中国为例，在采集 DNS 解析记录时，因根节点和国际域名的授权服务器都在国外，可以在中国骨干网出口进行抓包，将 DNS 解析记录进行提取分析，存储对应的 DNS 记录信息，保证抓取包的安全性和可靠性。

在本发明实施例中，虚拟根节点 240 采用分布式部署，通过 BGP（Border Gateway Protocol，边界网关协议，用来连接 Internet 上独立系统的路由选择协议）方式对客户端 210 提供 DNS 解析服务。需要说明的是，优选地，BGP 方式可以为任播（anycast）模式。

前文提及，虚拟根节点 240 控制的是指定区域范围，在正常运行情况下，临界范围的 DNS 请求也可能会被应答，但是为保证本区域的应答正常，当出现解析异常时，虚拟根节点会 240 优先保证本区域的 DNS 正常应答。为实现这一目的，可以在授权信息数据库 230 或虚拟根节点 240 中设置本区域 DNS 请求记录或列表，当客户端 210 发起的 DNS 请求在记录或列表中存在，那么优先对其进行应答。

为保证虚拟根节点 240 能够及时获知根节点解析故障，虚拟根节点 240 可以在骨干网对指定区域的临界区域出口处进行 DNS 数据报文的监听，以确定是否出现 DNS 解析故障。具体的，以中国为例，可以在中国对境外的出口处监听 DNS 数据报文，对 DNS 解析记录的正确性进行监控，一旦发现根节点和其他不可控的域名解析异常情况，在出口处可以将对应的请求包传送到虚拟根节点 240 进行应答，防止数据继续到国外服务器而导致被篡改。

根域名解析的结果一般是不会轻易修改，如果当前返回的解析结果与历史记录中预存的结果不匹配，则证明解析出现篡改，需要告警或采取人工干预。另外，如果当某个顶级域的授权无法正常工作或者返回的都为 SERVFAIL 也直接可以判断为解析结果错误。DNS 的解析结果不正确的一种处理方法为：解析结果出现篡改后，根据告警信息进行判断，对界面操作点击，系统自动批量切换至虚拟根节点的 DNS 解析。

以上告警信息可以结合预先采集的非法 DNS IP 和合法的 DNS IP 地址白名单列表地址确定，例如预先收集的恶意 DNS IP 地址列表可以是由安全厂商预先收集的一组非法 DNS IP 地址，该预先收集的恶意 DNS IP 地址列表可以为客户端数据库中预先收集的恶意 DNS IP 地址列表，或者也可以为从网站上下载至客户端数据库中的恶意 DNS IP 地址列表。该预先设置的合法的 DNS IP 地址白名单列表可以预先存储在客户端数据库中，也可以从网站的服务器（例如：云安全服务器）上下载。

在具体实现中，主要的安全等级包括“危险”、“警告”和“安全”，其中，安全等级为“危险”的表示对用户的威胁最大，为“警告”的次之，为“安全”的最弱。界面上提示也可以据此进行。

图 4 示出了根据本发明一个实施例的 DNS 安全系统的具体架构图。参见图 4，虚拟根节点会与本地 DNS 服务器以及其他 DNS 服务器间建立数据链路。为实现这一目的，图 4 中的各 DNS 服务器可以被视为至少一个递归 DNS，在根节点出现 DNS 解析故障时，将本地保存的根节点地址修改为指向虚拟根节点的地址；或者，将本地的域名解析发送至虚拟根节点。从而能够使得根节点根据授权信息数据库存储的数据记录提供域名解析服务。

进一步，本地 DNS 服务器中设置有缓存，存储有之前一段时间内的域名解析记录。在域名解析过程中，本地 DNS 服务器会先在自己的空间内查看是否有这个域名的缓存，如果没有，就会向根节点（根服务器）发送这个域名的域名解析请求。若根节点故障，则本地 DNS 服务器在自己的空间内未查看到这个域名的缓存，则会向虚拟根节点发送这个域名的域名解析请求。

图 5 示出了根据本发明一个实施例的 DNS 安全系统的另一个结构

示意图，与图 2 所示的 DNS 安全系统相比，图 5 中增加了至少一个递归 DNS 510。图 5 中仅仅示意了一个递归 DNS，在实际应用中，可以存在多个，且每个递归 DNS 均可以为多个客户端进行服务。

在本发明实施例中，需要说明的是，若部分 DNS 服务器无法快速修复，会极大影响用户的感受体验，此时，客户端可以紧急将用户的 DNS 修改到能够正常运行的其他 DNS 服务器上，以保证用户能够正常使用网络。

基于同一发明构思，本发明实施例还提供了一种应用上述任意一个优选实施例或其组合所提供的 DNS 安全系统进行故障处理的方法。图 6 示出了根据本发明一个实施例的利用 DNS 安全系统进行故障处理的方法的处理流程图。参见图 6，该流程图至少包括步骤 S602 至步骤 S606：

步骤 S602、获取指定区域的所有 DNS 请求及对应的授权信息并存储，生成授权信息数据库；

步骤 S604、判断根节点是否出现 DNS 解析故障，若是，触发步骤 S606，若否，流程结束；

步骤 S606、若是，启动虚拟根节点，利用虚拟根节点调用授权信息数据库中存储的授权信息，对客户端提供 DNS 解析服务。

在一个优选的实施例中，授权信息包括存储访问量超过访问阈值的 DNS 解析记录，和/或，重要域名的 DNS 解析记录。

在一个优选的实施例中，授权信息数据库根据授权信息的相互关系形成域名层次空间。

在一个优选的实施例中，授权信息数据库为互联网域名层次的镜像。

在一个优选的实施例中，利用虚拟根节点对客户端提供 DNS 解析服务，包括：虚拟根节点采用分布式部署，通过 BGP 方式对客户端提供 DNS 解析服务。

在一个优选的实施例中，BGP 方式包括 anycast 模式。

在一个优选的实施例中，判断根节点是否出现 DNS 解析故障，包括：在骨干网对指定区域的临界区域出口处进行 DNS 数据报文的监听，以确定是否出现 DNS 解析故障。

在一个优选的实施例中，上述方法还包括：

在根节点出现 DNS 解析故障时，至少一个递归 DNS 将保存的根节点地址修改为指向虚拟根节点的地址；或者，将本地的域名解析发送至虚拟根节点。

采用本发明实施例提供的 DNS 安全系统及其故障处理方法，能够达到如下有益效果：

在本发明实施例中，设置了虚拟根节点，当根节点出现 DNS 解析故障时，虚拟根节点能够代替根节点实现 DNS 解析功能。为实现虚拟根节点这一功能，授权信息数据库中必须存储有足够的信息，即，授权信息数据库中存储指定区域内的所有 DNS 请求及对应的授权信息，这样虚拟根节点才能够有足够的资源对 DNS 请求进行应答。因此，虚拟根节点的实现是在授权信息数据库的基础上实现的。结合新增的授权信息数据库以及虚拟根节点，能够在根节点解析故障的时候为客户端提供 DNS 解析功能，能够降低 DNS 单点故障和提高 DNS 防御攻击能力，同时还可以对虚拟根节点设置访问权限控制，屏蔽 DNS 的攻击数据，提高 DNS 解析的安全性及稳定性。对于危险 DNS 攻击，从授权信息数据库中查询不到具体的授权信息，则虚拟根节点不会为其提供解析服务，因此可以实现防止 DNS 攻击。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块

进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的 DNS 安全系统中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图 7 示出了可以实现根据本发明的应用 DNS 安全系统进行故障处理的方法的计算设备。该计算设备传统上包括处理器 710 和以存储器 720 形式的计算机程序产品或者计算机可读介质。存储器 720 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 720 具有用于执行上述方法中的任何方法步骤的程序代码 731 的存储空间 730。例如，用于程序代码的存储空间 730 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 731。这些程序代码可以从一个或者多个计算机程序产品

中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图 8 所述的便携式或者固定存储单元。该存储单元可以具有与图 7 的计算设备中的存储器 720 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 731’，即可以由例如诸如 710 之类的处理器读取的代码，这些代码当由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求

1、一种 DNS 安全系统，包括：

至少一个客户端，配置为发起域名系统 DNS 请求；

根节点，配置为对所述 DNS 请求提供授权信息；

授权信息数据库，配置为存储指定区域的所有 DNS 请求及对应的授权信息；

虚拟根节点，配置为当所述根节点出现 DNS 解析故障时，从所述授权信息数据库中调用相应授权信息，为对应客户端提供解析服务。

2、根据权利要求 1 所述的系统，其中，所述授权信息包括存储访问量超过访问阈值的 DNS 解析记录，和/或，重要域名的 DNS 解析记录。

3、根据权利要求 1 或 2 所述的系统，其中，所述授权信息数据库，还配置为根据所述授权信息的相互关系，组成域名层次空间。

4、根据权利要求 3 所述的系统，其中，所述授权信息数据库为互联网域名层次的镜像。

5、根据权利要求 1 所述的系统，其中，所述虚拟根节点还配置为：采用分布式部署，通过边界网关协议 BGP 方式对所述客户端提供 DNS 解析服务。

6、根据权利要求 5 所述的系统，其中，所述 BGP 方式包括任播 anycast 模式。

7、根据权利要求 1 所述的系统，其中，所述虚拟根节点还配置为：在骨干网对所述指定区域的临界区域出口处进行 DNS 数据报文的监听，以确定是否出现 DNS 解析故障。

8、根据权利要求 1 至 7 任一项所述的系统，其中，所述系统还包括：

至少一个递归 DNS，配置为在所述根节点出现 DNS 解析故障时，将本地保存的根节点地址修改为指向所述虚拟根节点的地址；或者，将本地的域名解析发送至所述虚拟根节点。

9、一种应用权利要求 1 至 8 任一项所述的 DNS 安全系统进行故障处理的方法，包括：

获取指定区域的所有域名系统 DNS 请求及对应的授权信息并存

储，生成授权信息数据库；

判断根节点是否出现 DNS 解析故障；

若是，启动虚拟根节点，利用所述虚拟根节点调用所述授权信息数据库中存储的授权信息，对客户端提供 DNS 解析服务。

10、根据权利要求 9 所述的方法，其中，所述授权信息包括存储访问量超过访问阈值的 DNS 解析记录，和/或，重要域名的 DNS 解析记录。

11、根据权利要求 9 或 10 所述的方法，其中，所述授权信息数据库根据所述授权信息的相互关系形成域名层次空间。

12、根据权利要求 11 所述的方法，其中，所述授权信息数据库为互联网域名层次的镜像。

13、根据权利要求 9 所述的方法，其中，利用所述虚拟根节点对客户端提供 DNS 解析服务，包括：所述虚拟根节点采用分布式部署，通过边界网关协议 BGP 方式对所述客户端提供 DNS 解析服务。

14、根据权利要求 13 所述的方法，其中，所述 BGP 方式包括任播 anycast 模式。

15、根据权利要求 9 所述的方法，其中，所述判断根节点是否出现 DNS 解析故障，包括：在骨干网对所述指定区域的临界区域出口处进行 DNS 数据报文的监听，以确定是否出现 DNS 解析故障。

16、根据权利要求 9 至 15 任一项所述的方法，其中，还包括：

在所述根节点出现 DNS 解析故障时，至少一个递归 DNS 将保存的根节点地址修改为指向所述虚拟根节点的地址；或者，将本地的域名解析发送至所述虚拟根节点。

17、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求 9 至 16 中的任一项所述的应用 DNS 安全系统进行故障处理的方法。

18、一种计算机可读介质，其中存储了如权利要求 17 所述的计算机程序。

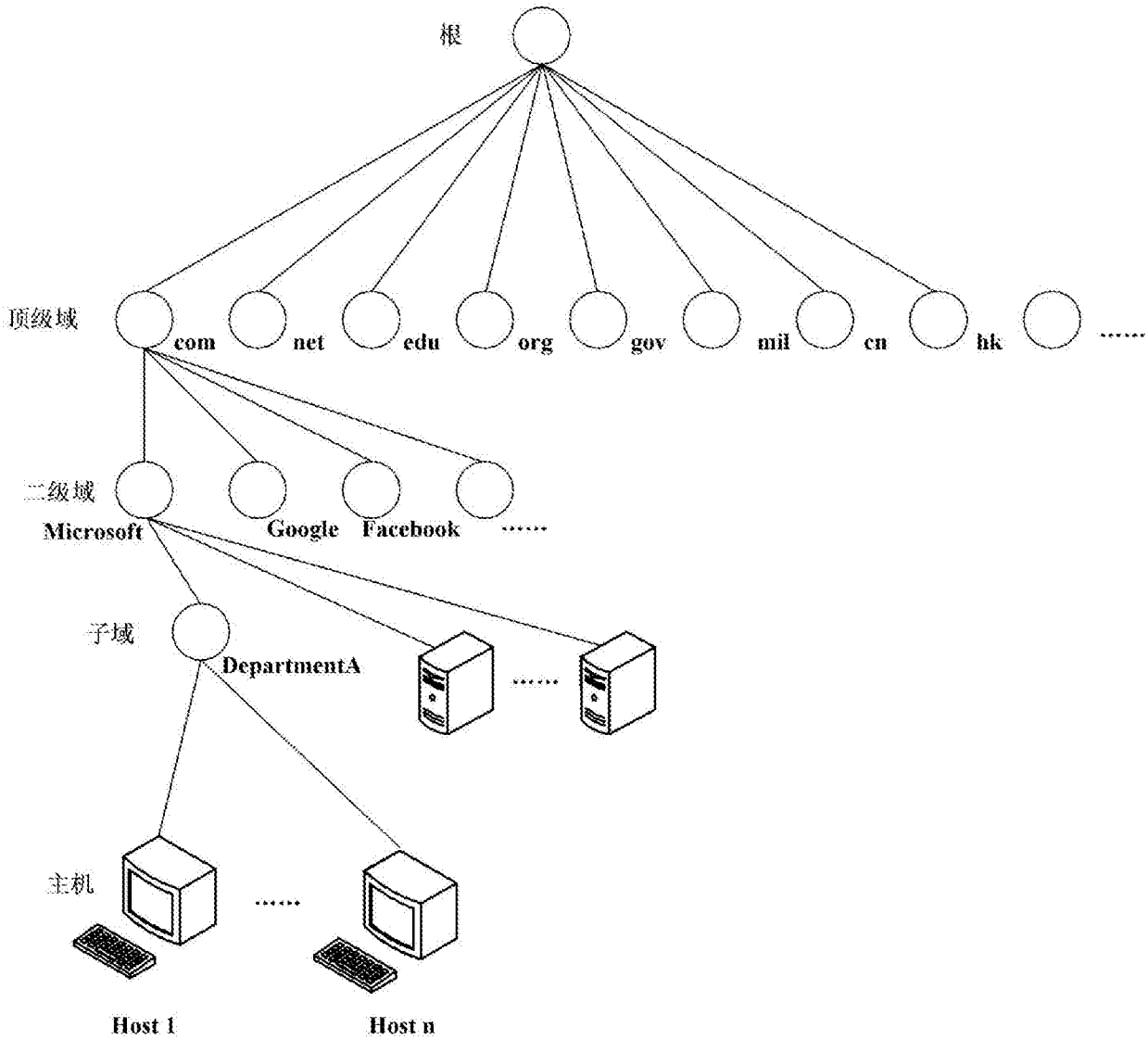

根
顶级域
com
net
edu
org
gov
mil
cn
hk
.....
二级域
Microsoft
Google
Facebook
.....
子域
DepartmentA
.....
主机
.....
Host 1
Host n

图 1

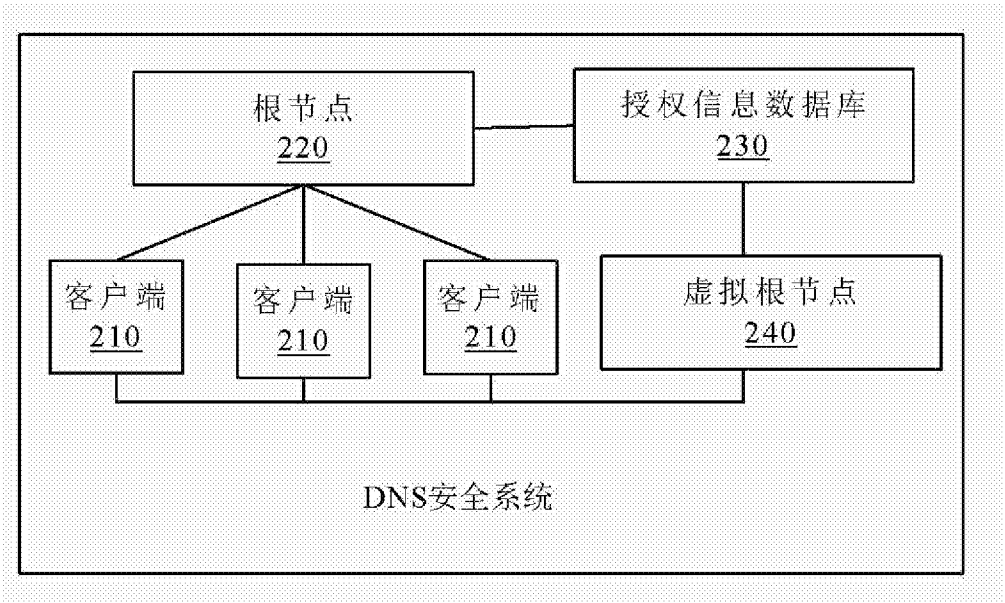

根节点
220
授权信息数据库
230
客户端
210
客户端
210
客户端
210
虚拟根节点
240
DNS安全系统

图 2

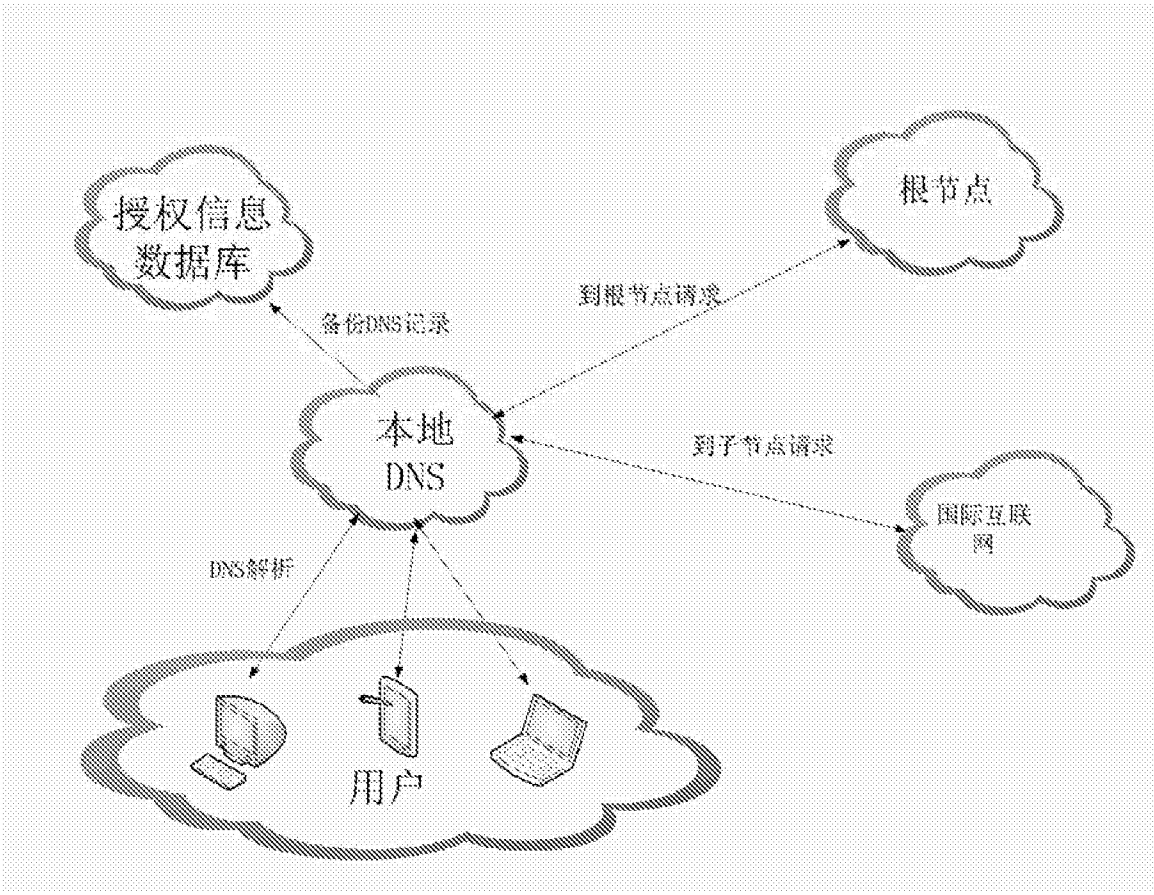

授权信息数据库
根节点
备份DNS记录
到根节点请求
本地DNS
到子节点请求
国际互联网
DNS解析
用户

图 3

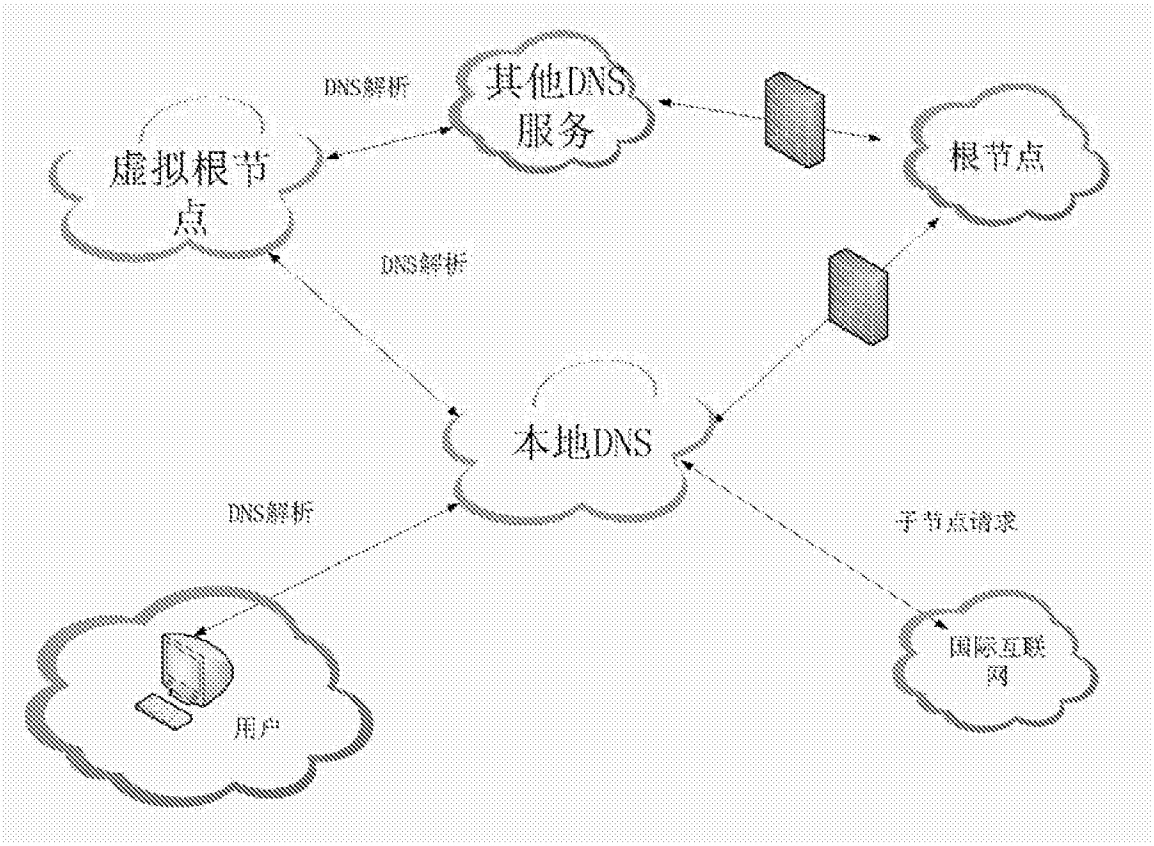


图 4

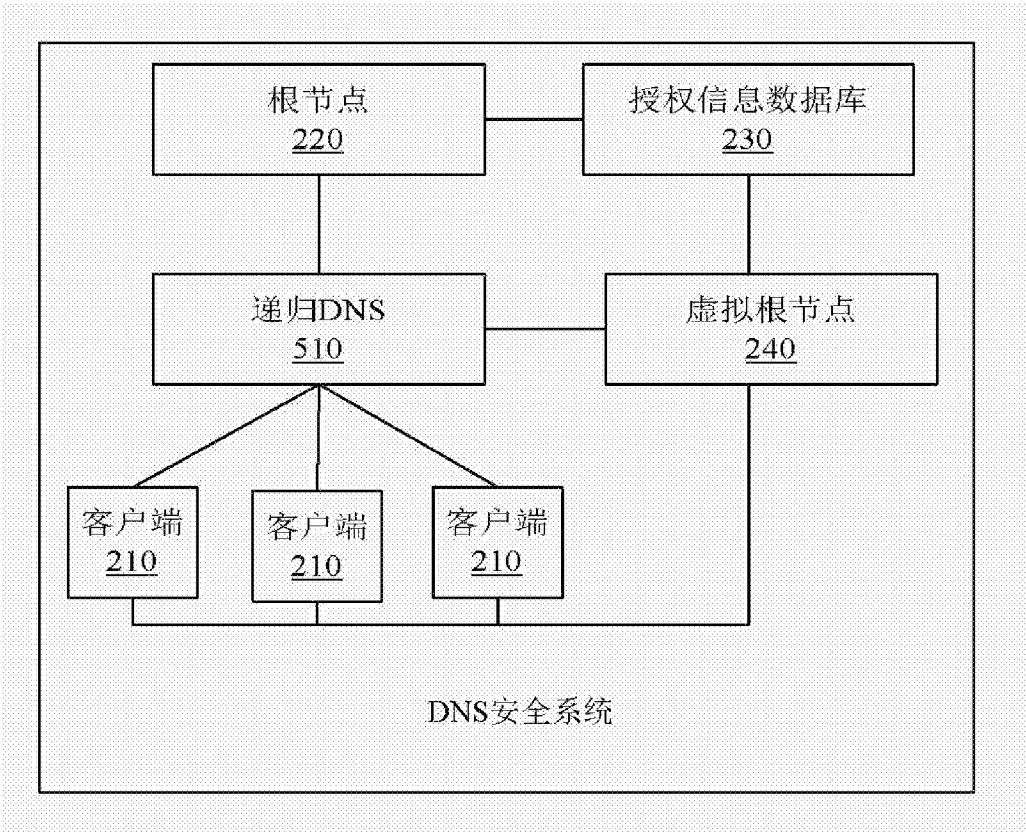

根节点
220
授权信息数据库
230
递归DNS
510
虚拟根节点
240
客户端
210
客户端
210
客户端
210
DNS安全系统

图 5

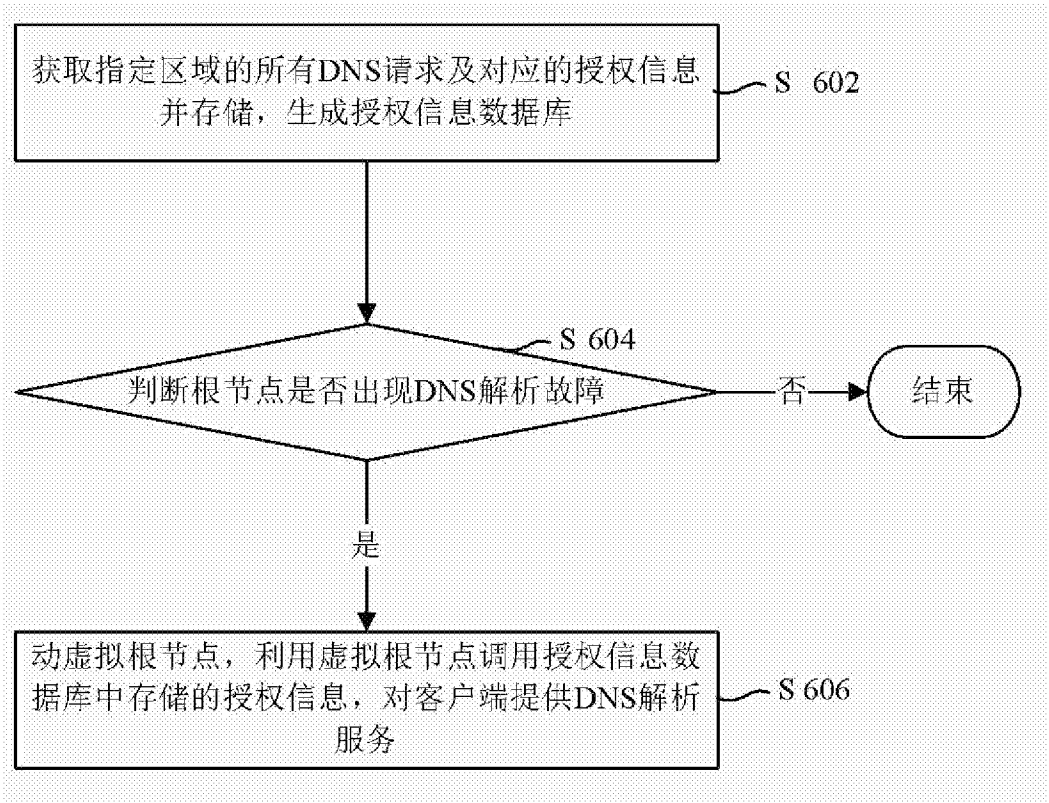

获取指定区域的所有DNS请求及对应的授权信息并存储，生成授权信息数据库
S 602
S 604
判断根节点是否出现DNS解析故障
否
结束
是
动虚拟根节点，利用虚拟根节点调用授权信息数据库中存储的授权信息，对客户端提供DNS解析服务
S 606

图 6

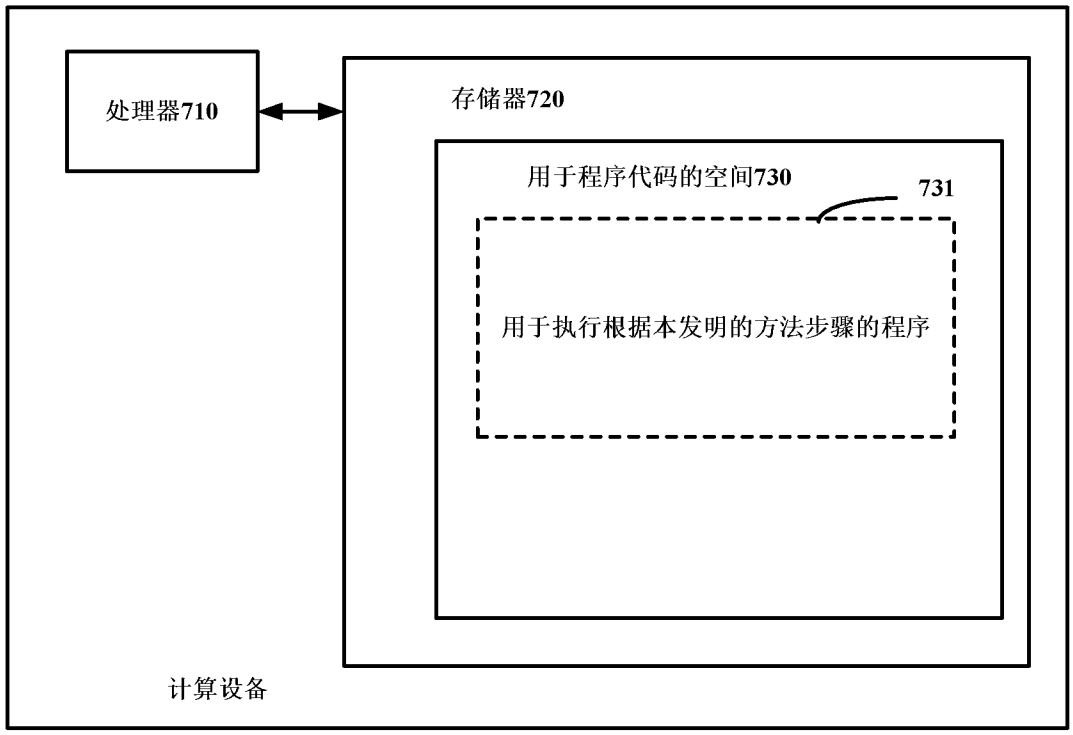

处理器710
存储器720
用于程序代码的空间730
731
用于执行根据本发明的方法步骤的程序
计算设备

图 7

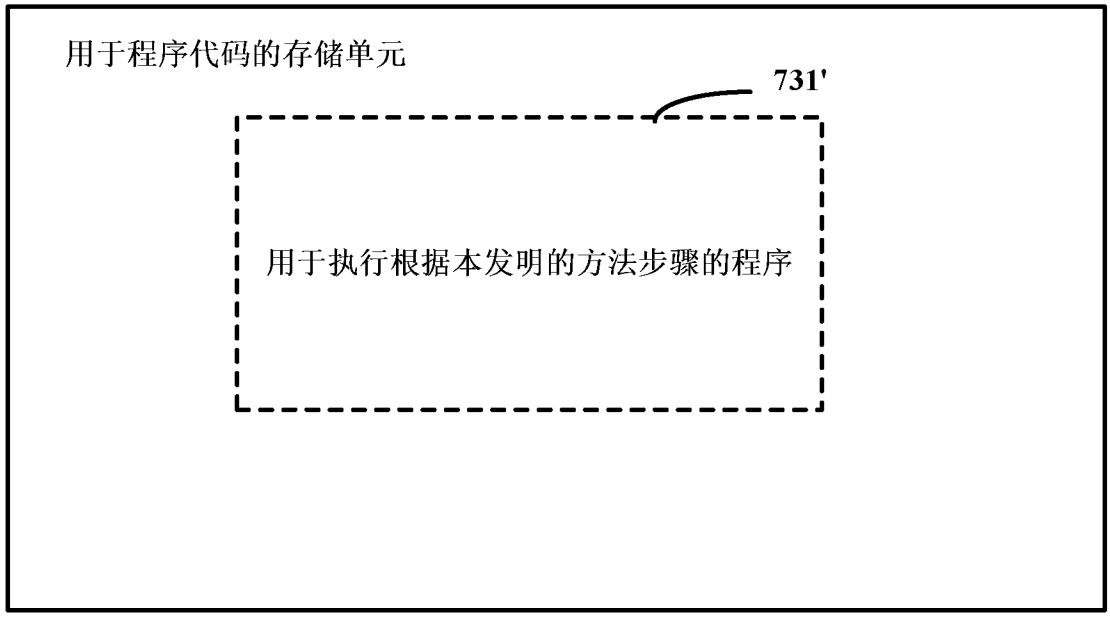

用于程序代码的存储单元
731'
用于执行根据本发明的方法步骤的程序

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/074614

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/12 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS, CNTXT, CNKI: virtual, root server, root node, root domain name, disaster backup, DNS, authentication information database, resolution, domain name, DNS request, failure, authentication

VEN: virtual, root server, root node, root domain name, disaster, backup, DNS, authentication information database, resolution, domain name, DNS request, default, failure, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103957286 A (SHANGHAI JULIU SOFTWARE TECHNOLOGY CO., LTD.), 30 July 2014 (30.07.2014), claims 1-10, and description, paragraph [0119]	1-18
PX	CN 103957284 A (SHANGHAI JULIU SOFTWARE TECHNOLOGY CO., LTD.), 30 July 2014 (30.07.2014), description, paragraphs [0074]-[0171]	1-18
PX	CN 103957285 A (SHANGHAI JULIU SOFTWARE TECHNOLOGY CO., LTD.), 30 July 2014 (30.07.2014), claims 1-10, and description, paragraphs [0053]-[0078]	1-18
A	CN 101431539 A (HUAWEI TECHNOLOGIES CO., LTD.), 13 May 2009 (13.05.2009), the whole document	1-18
A	CN 103354525 A (COMPUTER NETWORK INFORMATION CENTER, CHINESE ACADEMY OF SCIENCES), 16 October 2013 (16.10.2013), the whole document	1-18

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 June 2015 (15.06.2015)	**19 June 2015 (19.06.2015)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **ZHANG, Bo** Telephone No.: (86-10) **62088428**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/074614

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103957286 A	30 July 2014	None	
CN 103957284 A	30 July 2014	None	
CN 103957285 A	30 July 2014	None	
CN 101431539 A	13 May 2009	CN 101431539 B	20 April 2011
CN 103354525 A	16 October 2013	None	

国际检索报告

国际申请号
PCT/CN2015/074614

A. 主题的分类

H04L 29/12(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CPRSABS，CNTXT，CNKI:虚拟，根服务器，根节点，根域名，灾备，DNS，授权信息数据库，解析，域名，DNS请求，故障，授权；VEN：virtual, root server, root node, root domain name, disaster, backup, DNS, authentication information database, resolution, domain name, DNS request, default, failure, authentication

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 103957286 A (上海聚流软件科技有限公司) 2014年 7月 30日 (2014-07-30) 权利要求1-10，说明书第[0119]段	1-18
PX	CN 103957284 A (上海聚流软件科技有限公司) 2014年 7月 30日 (2014-07-30) 说明书第[0074]-[0171]段	1-18
PX	CN 103957285 A (上海聚流软件科技有限公司) 2014年 7月 30日 (2014-07-30) 权利要求1-10，说明书第[0053]-[0078]段	1-18
A	CN 101431539 A (华为技术有限公司) 2009年 5月 13日 (2009-05-13) 全文	1-18
A	CN 103354525 A (中国科学院计算机网络信息中心) 2013年 10月 16日 (2013-10-16) 全文	1-18

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2015年 6月 15日	2015年 6月 19日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451	张博 电话号码 (86-10)62088428

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/074614

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	103957286	A	2014年 7月 30日	无			
CN	103957284	A	2014年 7月 30日	无			
CN	103957285	A	2014年 7月 30日	无			
CN	101431539	A	2009年 5月 13日	CN	101431539	B	2011年 4月 20日
CN	103354525	A	2013年 10月 16日	无			