

(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
2024 年 2 月 8 日 (08.02.2024)



(10) 国际公布号
WO 2024/027079 A1

(51) 国际专利分类号:

H04L 9/40 (2022.01)

宇峰 (XIAO, Yufeng); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。

(21) 国际申请号:

PCT/CN2022/140321

(22) 国际申请日:

2022 年 12 月 20 日 (20.12.2022)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

202210930014.8 2022年8月3日 (03.08.2022) CN

(71) 申请人: 中国电信股份有限公司 (CHINA TELECOM CORPORATION LIMITED) [CN/CN]; 中国北京市西城区金融大街31号, Beijing 100033 (CN)。

(72) 发明人: 刘东鑫 (LIU, Dongxin); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。汪来富 (WANG, Laifu); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。史国水 (SHI, Guoshui); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。温展鹏 (WEN, Zhanpeng); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。肖

(74) 代理人: 北京律智知识产权代理有限公司 (BEIJING INTELLEGAL INTELLECTUAL PROPERTY AGENT LTD.); 中国北京市朝阳区慧忠路5号 B1605、B1606、B1607, Beijing 100101 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ,

(54) **Title:** DOMAIN-NAME REFLECTION ATTACK DETECTION METHOD AND APPARATUS, AND ELECTRONIC DEVICE AND STORAGE MEDIUM

(54) 发明名称: 域名反射攻击检测方法及装置、电子设备、存储介质

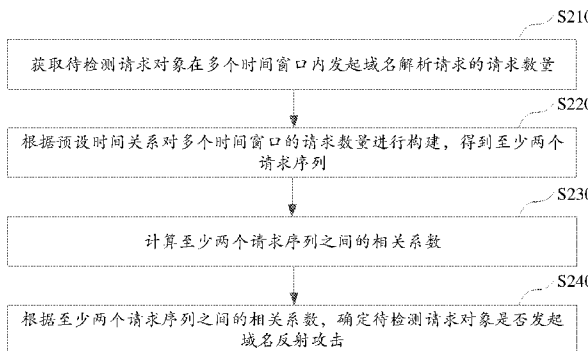


图 2

S210 Acquire the number of domain-name resolution requests, which are initiated, within a plurality of time windows, by a request object to be subjected to detection
S220 According to a preset time relationship, construct the number of requests within the plurality of time windows, so as to obtain at least two request sequences
S230 Calculate a correlation coefficient between the at least two request sequences
S240 According to the correlation coefficient between the at least two request sequences, determine whether said request object has initiated a domain-name reflection attack

(57) **Abstract:** A domain-name reflection attack detection method and apparatus, and an electronic device and a storage medium. The method comprises: acquiring the number of domain-name resolution requests, which are initiated, within a plurality of time windows, by a request object to be subjected to detection; according to a preset time relationship, constructing the number of requests within the plurality of time windows, so as to obtain at least two request sequences; calculating a correlation coefficient between the at least two request sequences; and according to the correlation coefficient between the at least two request sequences, determining whether said request object has initiated a domain-name reflection attack.

(57) **摘要:** 一种域名反射攻击检测方法及装置、电子设备、存储介质, 该方法包括: 获取待检测请求对象在多个时间窗口内发起域名解析请求的请求数量; 根据预设时间关系对多个时间窗口的请求数量进行构建, 得到至少两个请求序列; 计算至少两个请求序列之间的相关系数; 根据至少两个请求序列之间的相关系数, 确定待检测请求对象是否发起域名反射攻击。

NA, RW, SC, 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, ME, 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))。

域名反射攻击检测方法、电子设备、存储介质

交叉引用

本公开要求于 2022 年 8 月 3 日提交的申请号为 202210930014.8、名称为“域名反射攻击检测方法、电子设备、存储介质”的中国专利申请的优先权，该中国专利申请的全部内容通过引用全部并入本文。

技术领域

本公开涉及安全技术领域，具体而言，涉及一种域名反射攻击检测方法、电子设备、计算机可读存储介质。

背景技术

DNS (Domain Name System, 域名系统)是互联网基础设施，因其隐含的商业价值，逐步被大型企业所重视，各大企业都建立了面向全网的 DNS 系统。这种面向全网的 DNS 系统，无法限制查询源 IP 的范围，客观上成为攻击者可利用的流量反射攻击资源，近年来，因 DNS 低成本、易躲避检测和溯源、流量放大效应明显等特征，DNS 反射攻击屡创攻击流量峰值记录，成为当前互联网基础设施异常流量防护的主要对象。因此，在 DNS 服务器侧，DNS 反射攻击的检测能力，对于应急响应至关重要。

现有针对 DNS 反射攻击的检测方法，主要集中在 DNS 服务器侧或受害者侧，DNS 服务器侧或受害者侧依据网络带宽、服务器的可用性进行监测，超过阈值就告警，但是，这种检测方法具有明显的滞后性，当发出告警时，往往为时已晚，同时，DNS 服务器侧或受害者侧会存在其他原因导致网络带宽或服务器的可用性降低，进而影响对 DNS 反射攻击的检测，使得 DNS 反射攻击检测的准确性较低。一系列的 DDoS (Distributed Denial of Service, 分布式拒绝服务)案例表明，DNS 反射攻击较容易突破异常流量清洗设备的处理能力，使得如何能够及时发现 DNS 反射攻击成为亟待解决的问题。

发明内容

为解决上述技术问题，本公开的实施例提供了一种域名反射攻击检测方法、电子设备、计算机可读存储介质，旨在解决 DNS 反射攻击检测的准确性较低的技术问题。

本公开的其他特性和优点将通过下面的详细描述变得显然，或部分地通过本公开的实践而习得。

根据本公开实施例的一个方面，提供了一种域名反射攻击检测方法，包括：

获取待检测请求对象在多个时间窗口内发起域名解析请求的请求数量；

根据预设时间关系对多个时间窗口的请求数量进行构建，得到至少两个请求序列；

计算至少两个请求序列之间的相关系数；

根据至少两个请求序列之间的相关系数，确定待检测请求对象是否发起域名反射攻击。

根据本公开实施例的一个方面，提供了一种域名反射攻击检测装置，包括：

5 获取模块，配置为获取待检测请求对象在多个时间窗口内发起域名解析请求的请求数量；

构建模块，配置为根据预设时间关系对多个时间窗口的请求数量进行构建，得到至少两个请求序列；

计算模块，配置为计算至少两个请求序列之间的相关系数；

10 确定模块，配置为根据至少两个请求序列之间的相关系数，确定待检测请求对象是否发起域名反射攻击。

根据本公开实施例的一个方面，提供了一种电子设备，包括：一个或多个处理器；存储装置，用于存储一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行时，使得所述电子设备实现如前所述的域名反射攻击检测方法。

15 根据本公开实施例的一个方面，提供了一种计算机可读存储介质，其上存储有计算机可读指令，当所述计算机可读指令被计算机的处理器执行时，使计算机执行如上所述的域名反射攻击检测方法。

根据本公开实施例的一个方面，提供了一种计算机程序产品或计算机程序，该计算机程序产品或计算机程序包括计算机指令，该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该计算机设备执行上述各种可选实施例中提供的域名反射攻击检测方法。

20 在本公开的实施例所提供的技术方案中，在不同的时间窗口中，伪造的域名解析请求行为具有高度自相似性，而正常的域名解析请求行为呈现不可预测性。本公开实施例依据待检测请求对象在多个时间窗口发起域名解析请求的请求次数构建请求序列，请求序列能够表征待检测请求对象在多个时间窗口内的行为特征，根据请求序列计算相关系数，进而依据相关系数能够准确确定待检测请求对象是否发起域名反射攻击，本公开提供的域名反射攻击检测方法能够及时、准确的确定出是否发起域名反射攻击。

附图说明

30 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。显而易见地，下面描述中的附图仅仅是本公开的一些实施例，对于本领域普通技术者来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。在附图中：

图1是本公开涉及的一种实施环境的示意图。

图 2 是本公开涉及的一种域名反射攻击检测方法的流程图。

图 3 是本公开涉及的一个实施例中步骤 S210 的流程图。

图 4 是本公开涉及的一个实施例中步骤 S220 的流程图。

图 5 是本公开涉及的一个实施例中步骤 S410 的流程图。

5 图 6 是本公开涉及的一个实施例中确定第一时间窗口和第二时间窗口的示意图。

图 7 是本公开涉及的另一个实施例中确定第一时间窗口和第二时间窗口的示意图。

图 8 是本公开涉及的一个实施例中步骤 S230 的流程图。

图 9 是本公开涉及的一个实施例中步骤 S820 的流程图。

图 10 是本公开涉及的一个实施例中步骤 S240 的流程图。

10 图 11 是本公开涉及的一种域名反射攻击检测方法的流程图。

图 12 是本公开涉及的一种域名反射攻击检测装置的框图。

图 13 示出了适于用来实现本公开实施例的电子设备的计算机系统的结构示意图。

具体实施方式

15 这里将详细地对示例性实施例执行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

20 附图中所示的方框图仅仅是功能实体，不一定必须与物理上独立的实体相对应。即，可以采用软件形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

25 附图中所示的流程图仅是示例性说明，不是必须包括所有的内容和操作/步骤，也不是必须按所描述的顺序执行。例如，有的操作/步骤还可以分解，而有的操作/步骤可以合并或部分合并，因此实际执行的顺序有可能根据实际情况改变。

30 还需要说明的是：在本公开中提及的“多个”是指两个或者两个以上。“和/或”描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B 可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。字符“/”一般表示前后关联对象是一种“或”的关系。

DNS(Domain Name System, 域名系统)是因特网上作为域名和 IP 地址(Internet Protocol Address, 互联网协议地址)相互映射的一个分布式数据库，能够使用户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。通过主机名，最终得到该主机名对应的 IP 地址的过程叫做域名解析。

在正常域名解析过程中，源 IP 地址向 DNS 服务器发起 DNS 请求，DNS 服务器将依据 DNS 请求进行域名解析，得到 DNS 回复包，将 DNS 回复包返回给源 IP 地址，经过域名解析后，得到 DNS 回复包比 DNS 请求大，而反射攻击正是利用 DNS 回复包比 DNS 请求大的特点，放大流量，伪造受害者网络的 IP 地址，并以该受害者网络的 IP 地址向 DNS 服务器发送 DNS 请求，以此将 DNS 回复包的流量引入受害者网络的服务器。请参阅图 1，图 1 是本公开涉及的一种实施环境的示意图。该实施环境包括僵尸网络 Zombie110、DNS 服务器 120，以及受害者网络 Victim130，僵尸网络 Zombie110、DNS 服务器 120，以及受害者网络 Victim130 相互之间通过有线或者无线网络进行通信。

假设 DNS 请求的数据部分长度约为 40 字节，而 DNS 回复包的数据部分的长度可能会达到 4000 字节，这意味着攻击者利用此手法能够产生约 100 倍的放大效应。因此，攻击者只需要控制一个能够产生 150M 流量的僵尸网络 Zombie110 就能够进行约 15G 的 DDoS 攻击。如图 1 所示，僵尸网络 Zombie110 向 DNS 服务器 120 发送 DNS 请求，经过 DNS 服务器 120 的解析处理，放大了 DNS 回复包，DNS 服务器 120 将放大后的 DNS 回复包发送给了受害者网络 Victim130，攻击者通过僵尸网络 Zombie110 进行多次的实施，以此达到攻击受害者网络 Victim130 的目的。

攻击者为了提高流量放大效果，往往会伪造响应类型为 Non-Exist Domain 类型的 DNS 请求，强制 DNS 服务器 120 发起递归查询，导致 DNS 服务器 120 的 CPU (Central Processing Unit, 中央处理器)、Ram (Random access memory, 随机存取存储器) 突然上涨，而现有的位于 DNS 服务器侧的，基于 DNS 服务器 120 可用性监测的域名反射攻击检测方案往往难以发现异常，但现实中攻击者经常使用多个不同的公共 DNS 服务器发起攻击，单个 DNS 服务器往往不存在可用性异常。而靠近受害者网络 Victim130 侧的城域网对链路可用性监测的域名反射攻击检测方案，会受到其他 DDoS 攻击类型的干扰，还需要结合 Netflow 信息判断是否为域名反射攻击，因此，该种检测方案的判断时延较大。一系列创纪录的域名反射攻击流量峰值都可以使受害者网络 Victim130 的上游链路瘫痪，导致相关的研判系统无法工作。

本公开实施例提供的域名反射攻击检测方法能够依据待检测请求对象在多个时间窗口发起域名解析请求的请求数量构建请求序列，请求序列能够表征待检测请求对象在多个时间窗口内的行为特征，在不同的时间窗口中，伪造的域名解析请求行为具有高度自相似性，而正常的域名解析请求行为呈现不可预测性。根据请求序列计算相关系数，进而依据相关系数确定待检测请求对象是否发起域名反射攻击，能够及时、准确的确定出是否发起域名反射攻击。

图 2 是根据一示例性实施例示出的一种域名反射攻击检测方法的流程图。该方法

可以应用于图 1 所示的实施环境，并由图 1 所示实施例环境中的 DNS 服务器 120 具体执行。

如图 2 所示，在一示例性实施例中，该域名反射攻击检测方法可以包括步骤 S210 至步骤 S240，详细介绍如下：

- 5 步骤 S210，获取待检测请求对象在多个时间窗口内发起域名解析请求的请求数量。

本公开实施例中，待检测请求对象即为向 DNS 服务器发送域名解析请求的源 IP，对 DNS 网络流量或 DNS 系统日志进行解析，即可得到源 IP，以及该源 IP 发送域名解析请求的时间戳。依据时间戳，获取待检测请求对象在多个时间窗口
10 内发起域名解析请求的请求数量，若待检测请求对象在某个时间窗口内没有发起过域名解析请求，则该时间窗口对应的请求数量记为 0。

在本公开的一示例性实施例中，请参阅图 3，在步骤 S210 获取待检测请求对象在多个时间窗口内发起域名解析请求的请求数量之前，方法还包括步骤 S310 和步骤 S320，详细介绍如下：

- 15 步骤 S310，获取指定时间窗口内发起域名解析请求的请求对象，并统计请求对象在指定时间窗口内发起域名解析请求的请求数量。

本公开实施例中，在确定待检测请求对象时，通过解析对 DNS 网络流量或 DNS 系统日志，得到指定时间窗口内向 DNS 服务器发送域名解析请求的请求对象，统计每个请求对象在该指定时间窗口内发送域名解析请求的请求数量，如指
20 定时间窗口内，共有 X 个请求对象向 DNS 服务器发送域名解析请求，分别统计这 X 个请求对象在指定时间窗口的请求数量。

步骤 S320，根据请求数量和预设数量阈值的关系，从请求对象中确定待检测请求对象。

本公开实施例中，预先设置有预设数量阈值，将 X 个请求对象中，请求数量
25 小于预设数量阈值的请求对象进行过滤，剩下的请求对象即可作为待检测请求对象。经过过滤后，确定出的待检测请求对象若为多个，可依据请求数量对待检测请求对象进行降序排列，再依据降序排列后的顺序检测各个待检测请求对象其是否发送域名反射攻击。

- 30 步骤 S220，根据预设时间关系对多个时间窗口的请求数量进行构建，得到至少两个请求序列。

本公开实施例中，依据预设时间关系个待检测请求对象在各个时间窗口的请求数量构建请求序列，对于同一个待检测请求对象，在不同的时间窗口中，伪造的域名解析请求行为具有高度自相似性，根据请求数量，即可构建出能够表征待检测请求对象的行为的请求序列，每个请求序列中由对应的时间窗口的请求数量

组成，每个请求序列所对应的时间窗口的数量相同。

在本公开的一示例性实施例中，请参阅图 4，在步骤 S220 中根据预设时间关系对多个时间窗口的请求数量进行构建，得到至少两个请求序列，包括步骤 S410 和步骤 S420，详细介绍如下：

- 5 步骤 S410，根据预设时间关系，将多个时间窗口划分为多个第一时间窗口和多个第二时间窗口。

本公开实施例中，从多个时间窗口划分出第一时间窗口和第二时间窗口，多个第一时间窗口和多个第二时间窗口的数量之和可小于等于多个时间窗口，通过第一时间窗口和第二时间窗口，以此形成两个请求序列。

- 10 预先定义相关的配置参数，配置参数包括时间窗口 t 和缓存时间 T ，其中， $T=n*t$ ， n 为 >30 的自然数；同时配置有第一时间窗口和第二时间窗口的指定数量 k ，其中， $k*t$ 应大于 $30s$ ，可以较好地克服合理的数值波动。

- 15 在确定多个时间窗口时，可获取待检测请求对象的相邻的前一个缓存时间内的 n 个时间窗口；或获取待检测请求对象的相邻的后一个缓存时间内的 n 个时间窗口；或
15 获取与指定时间窗口相邻的前 p 个时间窗口和与指定时间窗口相邻的后 q 个时间窗口形成多个时间窗口，其中， $p+q+1$ 的和等于缓存时间的时间窗口个数 n ，同时， p 或 q 均大于等于 k 。在一个缓存时间内，从 n 个时间窗口划分出第一时间窗口和第二时间窗口，第一时间窗口与第二时间窗口的数量相等，同时，第一时间窗口与第二时间窗口的数量之和可不等于 n 。

- 20 每经过一个时间窗口 t ，缓存时间 T 将新增最近时间窗口 t 内的请求对象，将缓存时间 T 前的请求对象清零、释放，DNS 服务器中始终保持每时间窗口 t ，新增请求对象，同时在缓存时间 T 中释放不需要的请求对象，以此减轻 DNS 服务器的存储压力。

- 25 步骤 S420，根据多个第一时间窗口的请求数量构建得到第一请求序列，以及根据多个第二时间窗口的请求数量构建得到第二请求序列。

- 30 本公开实施例中，依据第一时间窗口的请求数量构建第一请求序列，将多个第一时间窗口依据时间的先后顺序进行排列，然后依据排列顺序，基于第一时间窗口的请求数量构建第一请求序列，按 {src IP: [请求数量 1, 请求数量 2, ..., 请求数量 k]} 的字典格式，生成第一请求序列，如 1.1.1.1: [20, 20, ...]，共有 k 个时间窗口的请求数量，1.1.1.1 表征源 IP 地址为 1.1.1.1 的待检测请求对象。

同样的，依据第二时间窗口的请求数量构建第一请求序列，将多个第二时间窗口依据时间的先后顺序进行排列，然后依据排列顺序，基于第二时间窗口的请求数量构建第二请求序列，按 {src IP: [请求数量 a , 请求数量 b , ..., 请求数量 j]} 的字典格式，生成第二请求序列。

在本公开的一示例性实施例中，请参阅图 5，多个时间窗口是连续的时间窗口；在步骤 S410 中根据预设时间关系，将多个时间窗口划分为多个第一时间窗口和多个第二时间窗口，包括步骤 S510 和步骤 S520，详细介绍如下：

5 步骤 S510，在多个连续的时间窗口中，确定指定数量个连续的时间窗口作为多个第一时间窗口。

本公开实施例中，多个时间窗口是获取待检测请求对象的指定时间窗口的相邻的前一个缓存时间内的 n 个时间窗口，或获取待检测请求对象的指定时间窗口的相邻的后一个缓存时间内的 n 个时间窗口得到时，在这 n 个时间窗口内，依据各个时间窗口的顺序，可获取前 k 个连续的时间窗口作为第一时间窗口。如图 6 所示，图 6 所示的多个时间窗口是获取待检测请求对象的指定时间窗口的相邻的前一个缓存时间内的 n 个时间窗口，直接将第 1 至第 k 个时间窗口作为第一时间窗口。

15 在另一实施例中，多个时间窗口是获取与指定时间窗口相邻的前 p 个时间窗口和与指定时间窗口相邻的后 q 个时间窗口得到时，在前 p 个时间窗口中确定连续的 k 个时间窗口作为第一时间窗口，或在后 q 个时间窗口中确定连续的 k 个时间窗口作为第一时间窗口，如图 7 所示，在图 7 展示的多个时间窗口中，A 表示指定时间窗口，A 左侧的时间窗口即为前 p 个时间窗口，A 右侧的时间窗口即为后 q 个时间窗口，直接将前 p 个时间窗口中第 1 至第 k 个时间窗口作为第一时间窗口。

20 步骤 S520，在除第一时间窗口之外的其他时间窗口中，确定指定数量个时间窗口作为多个第二时间窗口；其中，多个第一时间窗口中最晚的第一时间窗口早于多个第二时间窗口中最早的第二时间窗口。

本公开实施例中，在除第一时间窗口后的其他时间窗口内，随机获取 k 个时间窗口作为第二时间窗口。

25 具体的，如图 6 所示，当多个时间窗口是获取待检测请求对象的指定时间窗口的相邻的前一个缓存时间内的 n 个时间窗口，或获取待检测请求对象的指定时间窗口的相邻的后一个缓存时间内的 n 个时间窗口得到时，通过 Shuffle 算法在第 $k+1$ 至第 n 个时间窗口内随机确定 k 个时间窗口作为第二时间窗口，即获取当前系统时间，将当前系统时间作为随机因子，计算得到一个随机数，计算随机数的公式为： $m = \text{rand}(\text{time}) * (i+1) \bmod (n-k)$ ，上述公式表示依据系统时间获取一个范围在 $[1, (n-k)]$ 的随机数， time 表示当前系统时间， $i+1$ 表示正在计算第几个第二时间窗口， i 的取值范围为 $[0, k-1]$ ，通过上述公式计算出随机数后，取第 $m+k$ 个时间窗口作为第二时间窗口，重复 k 次就可以得到需要的 k 个时间窗口，若计算出的随机数存在重复的情况，则重新进行计算，直到取出 k 个不同的时间窗口

作为第二时间窗口。

如图 7 所示, 当多个时间窗口是获取与指定时间窗口相邻的前 p 个时间窗口和与指定时间窗口相邻的后 q 个时间窗口得到时, 在 p 个时间窗口确定第一时间窗口后, 在后 q 个时间窗口内随机确定 k 个时间窗口作为第二时间窗口, 同样的, 在随机
5 确定 k 个时间窗口作为第二时间窗口时, 通过 Shuffle 算法在后 q 个时间窗口内随机确定 k 个时间窗口作为第二时间窗口, 即获取当前系统时间, 将当前系统时间作为随机因子, 计算得到一个随机数, 计算随机数的公式为: $m = \text{rand}(\text{time}) * (i+1) \bmod (q)$, 上述公式表示依据系统时间获取一个范围在 $[1, q]$ 的随机数, time 表示当前系统时间, $i+1$ 表示正在计算第几个第二时间窗口, i 的取值范围为 $[0, k-1]$, 通过上述公式计算出随机
10 数后, 取第 $m+p+1$ 个时间窗口作为第二时间窗口, 重复 k 次就可以得到需要的 k 个时间窗口, 若计算出的随机数存在重复的情况, 则重新进行计算, 直到取出 k 个不同的时间窗口作为第二时间窗口。

在其他实施例中, 当多个时间窗口是获取待检测请求对象的指定时间窗口的相邻的前一个缓存时间内的 n 个时间窗口, 或获取待检测请求对象的指定时间窗口的相邻
15 的后一个缓存时间内的 n 个时间窗口得到时, 在 n 个时间窗口内, 可获取后 k 个连续的时间窗口作为第一时间窗口, 然后在剩余的时间窗口中, 随机确定 k 个时间窗口作为第二时间窗口。在随机确定 k 个时间窗口时, 与前述一致, 通过 Shuffle 算法随机确定 k 个时间窗口作为第二时间窗口。

在另一实施例中, 当多个时间窗口是获取与指定时间窗口相邻的前 p 个时间窗口
20 和与指定时间窗口相邻的后 q 个时间窗口得到时, 可从前 p 个时间窗口中随机确定 k 个时间窗口作为第二时间窗口, 再在后 q 个时间窗口中确定连续的 k 个时间窗口作为第二时间窗口。在随机确定 k 个时间窗口时, 与前述一致, 通过 Shuffle 算法随机确定 k 个时间窗口作为第二时间窗口。

步骤 S230, 计算至少两个请求序列之间的相关系数。

25 本公开实施例中, 计算至少两个请求序列之间的相关系数, 若请求序列包括两个时, 直接计算两个请求序列之间的相关系数; 若请求序列具有两个以上时, 计算各个请求序列两两之间的相关系数, 并基于各个请求序列两两之间的相关系数计算系数平均值, 将系数平均值作为至少两个请求序列之间的相关系数。

在本公开的一示例性实施例中, 请参阅图 8, 至少两个请求序列包括第一请求序
30 列和第二请求序列; 在步骤 S230 中计算至少两个请求序列之间的相关系数, 包括步骤 S810 和步骤 S820, 详细介绍如下:

步骤 S810, 对第一请求序列中含有的各个请求数量进行求平均值运算, 得到第一均值, 以及对第二请求序列中含有的各个请求数量进行求平均值运算, 得到第二均值。

本公开实施例中, 根据第一请求序列中的请求数量计算第一均值 $\bar{X}$, 以及根据第

二请求序列中的请求数量计算第二均值 $\bar{Y}$ 。

步骤 S820, 根据第一均值、第二均值、第一请求序列, 以及第二请求序列, 计算第一请求序列和第二请求序列之间的相关系数。

5 本公开实施例中, 根据计算得到的第一均值、第二均值、第一请求序列, 以及第二请求序列, 计算第一请求序列和第二请求序列之间的相关系数。

在本公开的一示例性实施例中, 请参阅图 9, 在步骤 S820 中根据第一均值、第二均值、第一请求序列, 以及第二请求序列, 计算第一请求序列和第二请求序列的相关系数, 包括步骤 S910 和步骤 S920, 详细介绍如下:

10 步骤 S910, 将第一请求序列中含有的各个请求数量分别与第一均值进行求差值运算, 得到多个第一差值, 以及将第二请求序列中含有的各个请求数量分别与第二均值进行求差值运算, 得到多个第二差值。

本公开实施例中, 将第一请求序列中的各个请求数量分别与第一均值进行进行求差值运算, 即第一请求序列中的各个请求数量减去第一均值, 得到多个第一差值, 将第二请求序列中的各个请求数量分别与第二均值进行求差值运算, 即第二请求序列中的各个请求数量减去第二均值, 得到多个第二差值。

步骤 S920, 根据多个第一差值和多个第二差值, 计算第一请求序列和第二请求序列之间的相关系数。

本公开实施例中, 根据多个第一差值和第二差值计算第一请求序列和第二请求序列之间的相关系数。

20 具体的, 通过公式 $r = \frac{\sum_{j=1}^k (X_j - \bar{X})(Y_j - \bar{Y})}{\sqrt{\sum_{j=1}^k (X_j - \bar{X})^2} \sqrt{\sum_{j=1}^k (Y_j - \bar{Y})^2}}$ 计算第一序列和第二序列之间的

相关系数, 其中, r 表示相关系数, X_j 表示第一请求序列中第 j 个请求数量, Y_j 表示第二请求序列中第 j 个请求数量, k 表示第一请求序列和第二请求序列中分别具有 k 个请求数量, $\bar{X}$ 表示第一均值, $\bar{Y}$ 表示第二均值。

25 步骤 S240, 根据至少两个请求序列之间的相关系数, 确定待检测请求对象是否发起域名反射攻击。

本公开实施例中, 在不同的时间窗口中, 伪造的域名解析请求行为具有高度自相似性, 而正常的域名解析请求行为呈现不可预测性, 根据相关系数, 即可知晓待检测请求对象在不同时间窗口内发起的域名解析请求行为是否具有相似性, 当具有相似性时, 即可表征待检测请求对象发起了域名反射攻击。

30 本公开实施例中, 在不同的时间窗口中, 伪造的域名解析请求行为具有高度自相似性, 而正常的域名解析请求行为呈现不可预测性。本公开实施例依据待检测请求对象在多个时间窗口发起域名解析请求的请求数量构建请求序列, 请求序列能够表征待检测请求对象在多个时间窗口内的行为特征, 根据请求序列计算相

关系数，进而依据相关系数能够准确确定待检测请求对象是否发起域名反射攻击，本公开提供的域名发射攻击检测方法在接收域名解析请求的过程中检测是否有发起域名反射攻击，能够及时、准确的确定出是否发起域名反射攻击。

在本公开的一示例性实施例中，请参阅图 10，在步骤 S240 中根据至少两个请求序列之间的相关系数，确定待检测请求对象是否发起域名反射攻击，包括步骤 S1010 至步骤 S1030，详细介绍如下：

步骤 S1010，检测至少两个请求序列的相关系数与预设阈值的关系，得到检测结果。

本公开实施例中，检测相关系数与预设阈值的关系，即将相关系数与预设阈值进行比较，得到检测结果，预设阈值可设置为 0.5。

步骤 S1020，若检测结果表征相关系数大于等于预设阈值，则确定待检测请求对象发起域名反射攻击。

本公开实施例中，若相关系数大于等于预设阈值，则确定待检测请求对象发起域名反射攻击，生成预设告警信息，并将预设告警信息发送给受害者网络 Victim130，即向攻击者通过僵尸网络 Zombie110 伪造的源 IP 发送预设告警信息，以此提醒受害者网络 Victim130。

步骤 S1030，若检测结果表征相关系数小于预设阈值，则确定待检测请求对象未发起域名反射攻击。

本公开实施例中，若检测结果表征相关系数小于预设阈值，则表明待检测请求对象在不同时间窗口内发起的域名解析请求行为不具有相似性，即待检测请求对象未发起域名反射攻击。

在本公开的一示例性实施例中，请参阅图 11，图 11 是根据一示例性实施例示出的一种域名反射攻击检测方法，包括步骤 S1110 至步骤 S1180，详细介绍如下：

步骤 S1110，获取系统日志，并对系统日志进行解析，得到多个请求对象，以及多个请求对象发起域名解析请求的时间戳。

本公开实施例中，对系统日志进行解析，得到即可得到多个请求对象，以及各个请求对象发送域名解析请求的时间戳。

步骤 S1120，根据时间戳，获取指定时间窗口内发起域名解析请求的请求对象，并统计请求对象在指定时间窗口内发起域名解析请求的请求数量。

本公开实施例中，预先配置有时间窗口 t 和缓存时间 T ，根据时间戳，能够确定指定时间窗口下发起域名解析请求的请求对象，一般一个时间窗口内，相对应的请求对象包括多个，统计各个请求对象的请求数量。

步骤 S1130，根据请求数量和预设数量阈值的关系，从请求对象中确定待检测请求对象。

本公开实施例中，预先设置有预设数量阈值，将指定时间窗口内，请求数量低于预设数量阈值的请求对象进行过滤，留下的请求对象即可作为待检测请求对象，此时，待检测请求对象可包括多个。

步骤 S1140，获取与指定时间窗口相邻的多个时间窗口，并在多个时间窗口内，确定指定数量个连续的时间窗口作为多个第一时间窗口，以及通过 Shuffle 算法在除第一时间窗口的其他时间窗口中，随机确定指定数量个时间窗口作为多个第二时间窗口；多个第一时间窗口中最晚的第一时间窗口早于多个第二时间窗口中最早的第二时间窗口。

本公开实施例中，获取指定时间窗口的相邻的前一个缓存时间内的 n 个时间窗口，或指定时间窗口的相邻的后一个缓存时间内的 n 个时间窗口，指定数量为 k ，从 n 个时间窗口内确定 k 个连续的时间窗口作为第一时间窗口，再从剩余的时间窗口内通过 Shuffle 算法随机确定 k 个时间窗口作为第二时间窗口。具体的，在确定第一时间窗口时，选择 n 个时间窗口中，第 1 至第 k 个时间窗口作为第一时间窗口，在确定第二时间窗口时，只考虑第 $k+1$ 至第 n 个时间窗口，通过 Shuffle 算法从第 $k+1$ 至第 n 个时间窗口随机获取 k 个时间窗口作为第二时间窗口。

待检测请求对象具有多个时，各个待检测请求对象所对应的第一时间窗口相同，同时第二时间窗口也相同，无需单独确定各个待检测请求对象的第一时间窗口和第二时间窗口，减少计算量。这种基于 Shuffle 算法选取 k 个时间窗口作为第二时间窗口，能够尽可能抓住攻击者在一个相对长的时间范围内，具有高度类似的行为特征，而正常的 DNS 请求，呈现较大的随机性。通过 Shuffle 算法，可以极大提升后续相关系数判断的计算速度。

步骤 S1150，根据指定数量个第一时间窗口构建待检测请求对象的第一请求序列，以及根据指定数量个第二时间窗口构建待检测请求对象的第二请求序列。

本公开实施例中，根据各个待检测请求对象在第一时间窗口内的请求数量构建对应的第一请求序列，以及根据各个待检测请求对象在第二时间窗口内的请求数量构建对应的第二请求序列。

步骤 S1160，根据第一请求序列和第二请求序列计算待检测请求对象的相关系数。

本公开实施例中，根据每个待检测请求对象对应的第一请求序列和第二请求序列，计算对应的相关系数，计算相关系数的方案在前述已进行说明，在此不进行赘述。

步骤 S1170，检测待检测请求对象的相关系数与预设阈值的关系，得到待检测请求对象的检测结果。

本公开实施例中，将各个待检测请求对象的相关系数分别与预设阈值进行比

较，得到对应的检测结果。

步骤 S1180，若待检测请求对象的检测结果表征相关系数大于等于预设阈值，则确定待检测请求对象发起域名反射攻击，并向待检测请求对象发送预设告警信息。

本公开实施例中，若待检测请求对象的检测结果表征相关系数大于等于预设阈值，则标定待检测请求对象发起了域名反射攻击，在多个待检测请求对象中，存在多个待检测请求对象发起了域名反射攻击时，向多个待检测请求对象发送预设告警信息。

本公开实施例中，在不同的时间窗口中，伪造的域名解析请求行为具有高度自相似性，而正常的域名解析请求行为呈现不可预测性。本公开实施例根据系统日志得到请求对象，根据请求对象发起域名解析请求的请求数量确定待检测请求对象，从多个时间窗口中确定待检测请求对象的第一时间窗口和第二时间窗口，各个待检测请求对象的第一时间窗口相同，同时第二时间窗口也相同，在一定程度上减少计算量，依据各个待检测请求对象在第一时间窗口和第二时间窗口的请求数量，构建对象的请求序列，请求序列能够表征待检测请求对象在多个时间窗口内的行为特征，根据请求序列计算相关系数，进而依据相关系数能够准确确定待检测请求对象是否发起域名反射攻击，同时，还生成预设告警信息，并将预设告警信息发送给待检测请求对象，即向攻击者通过僵尸网络 Zombie110 伪造的源 IP 发送预设告警信息，以此提醒受害者网络 Victim130。本公开提供的域名发射攻击检测方法在接收域名解析请求的过程中检测是否有发起域名反射攻击，能够及时、准确的确定出是否发起域名反射攻击。

在本公开的一个示例性实施例中，请参阅图 12，图 12 是根据一示例性实施例示出的一种域名反射攻击检测装置，包括：

获取模块 1210，配置为获取待检测请求对象在多个时间窗口内发起域名解析请求的请求数量；

构建模块 1220，配置为根据预设时间关系对多个时间窗口的请求数量进行构建，得到至少两个请求序列；

计算模块 1230，配置为计算至少两个请求序列之间的相关系数；

确定模块 1240，配置为根据至少两个请求序列之间的相关系数，确定待检测请求对象是否发起域名反射攻击。

在本公开一示例性实施例中，构建模块 1220 包括：

划分子模块，配置为根据预设时间关系，将多个时间窗口划分为多个第一时间窗口和多个第二时间窗口；

构建子模块，配置为根据多个第一时间窗口的请求数量构建得到第一请求序列，以及根据多个第二时间窗口的请求数量构建得到第二请求序列。

在本公开一示例性实施例中，多个时间窗口是连续的时间窗口；划分子模块，包括：

第一确定单元，配置为在多个连续的时间窗口中，确定指定数量个连续的时间窗口作为多个第一时间窗口；

- 5 第二确定单元，配置为在除第一时间窗口之外的其他时间窗口中，确定指定数量个时间窗口作为多个第二时间窗口；其中，多个第一时间窗口中最晚的第一时间窗口早于多个第二时间窗口中最早的第二时间窗口。

在本公开一示例性实施例中，至少两个请求序列包括第一请求序列和第二请求序列；计算模块 1230，包括：

- 10 运算子模块，配置为对第一请求序列中含有的各个请求数量进行求平均值运算，得到第一均值，以及对第二请求序列中含有的各个请求数量进行求平均值运算，得到第二均值；

计算子模块，配置为根据第一均值、第二均值、第一请求序列，以及第二请求序列，计算第一请求序列和第二请求序列之间的相关系数。

- 15 在本公开一示例性实施例中，计算子模块，包括：

求差运算单元，配置为将第一请求序列中含有的各个请求数量分别与第一均值进行求差值运算，得到多个第一差值，以及将第二请求序列中含有的各个请求数量分别与第二均值进行求差值运算，得到多个第二差值；

- 20 计算单元，配置为根据多个第一差值和多个第二差值，计算第一请求序列和第二请求序列之间的相关系数。

在本公开一示例性实施例中，域名反射攻击检测装置还包括：

获取单元，配置为获取指定时间窗口内发起域名解析请求的请求对象，并统计请求对象在指定时间窗口内发起域名解析请求的请求数量；

- 25 待检测请求对象确定单元，配置为根据请求数量和预设数量阈值的关系，从请求对象中确定待检测请求对象。

在本公开一示例性实施例中，确定模块 1240，包括：

检测子模块，配置为检测至少两个请求序列的相关系数与预设阈值的关系，得到检测结果；

- 30 第一确定子模块，配置为若检测结果表征相关系数大于等于预设阈值，则确定待检测请求对象发起域名反射攻击；

第二确定子模块，配置为若检测结果表征相关系数小于预设阈值，则确定待检测请求对象未发起域名反射攻击。

需要说明的是，上述实施例所提供的装置与上述实施例所提供的方法属于同一构思，其中各个模块、子模块和单元执行操作的具体方式已经在方法实施例中

进行了详细描述，此处不再赘述。

本公开的实施例还提供了一种电子设备，包括：一个或多个处理器；存储装置，用于存储一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行时，使得所述电子设备实现上述各个实施例中提供的域名反射攻击检测方法。

图 13 示出了适于用来实现本公开实施例的电子设备的计算机系统的结构示意图。

需要说明的是，图 13 示出的电子设备的计算机系统 1300 仅是一个示例，不应对本公开实施例的功能和使用范围带来任何限制。

如图 13 所示，计算机系统 1300 包括中央处理单元 (Central Processing Unit, CPU) 1301，其可以根据存储在只读存储器 (Read-Only Memory, ROM) 1302 中的程序或者从储存部分 1308 加载到随机访问存储器 (Random Access Memory, RAM) 1303 中的程序而执行各种适当的动作和处理，例如执行上述实施例中所述的方法。在 RAM 1303 中，还存储有系统操作所需的各种程序和数据。CPU 1301、ROM 1302 以及 RAM 1303 通过总线 1304 彼此相连。输入/输出 (Input /Output, I/O) 接口 1305 也连接至总线 1304。

以下部件连接至 I/O 接口 1305：包括键盘、鼠标等的输入部分 1306；包括诸如阴极射线管 (Cathode Ray Tube, CRT)、液晶显示器 (Liquid Crystal Display, LCD) 等以及扬声器等的输出部分 1307；包括硬盘等的储存部分 1308；以及包括诸如 LAN (Local Area Network, 局域网) 卡、调制解调器等的网络接口卡的通信部分 1309。通信部分 1309 经由诸如因特网的网络执行通信处理。驱动器 1310 也根据需要连接至 I/O 接口 1305。可拆卸介质 1311，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器 1310 上，以便于从其上读出的计算机程序根据需要被安装入储存部分 1308。

特别地，根据本公开的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本公开的实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的计算机程序。在这样的实施例中，该计算机程序可以通过通信部分 1309 从网络上被下载和安装，和/或从可拆卸介质 1311 被安装。在该计算机程序被中央处理单元 (CPU) 1301 执行时，执行本公开的系统中限定的各种功能。

需要说明的是，本公开实施例所示的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器 (RAM)、只读存储器 (ROM)、

可擦式可编程只读存储器 (Erasable Programmable Read Only Memory, EPROM)、闪存、光纤、便携式紧凑磁盘只读存储器 (Compact Disc Read-Only Memory, CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本公开中, 计算机可读存储介质可以是任何包含或存储程序的有形介质, 该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本公开中, 计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号, 其中承载了计算机可读的计算机程序。这种传播的数据信号可以采用多种形式, 包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质, 该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的计算机程序可以用任何适当的介质传输, 包括但不限于: 无线、有线等等, 或者上述的任意合适的组合。

附图中的流程图和框图, 图示了按照本公开各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。其中, 流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分, 上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意, 在有些作为替换的实现中, 方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如, 两个接连地表示的方框实际上可以基本并行地执行, 它们有时也可以按相反的顺序执行, 这依所涉及的功能而定。也要注意的, 框图或流程图中的每个方框、以及框图或流程图中的方框的组合, 可以用执行规定的功能或操作的专用的基于硬件的系统来实现, 或者可以用专用硬件与计算机指令的组合来实现。

描述于本公开实施例中所涉及到的单元可以通过软件的方式实现, 也可以通过硬件的方式来实现, 所描述的单元也可以设置在处理器中。其中, 这些单元的名称在某种情况下并不构成对该单元本身的限定。

本公开的另一方面还提供了一种计算机可读存储介质, 其上存储有计算机程序, 该计算机程序被处理器执行时实现如前所述的方法。该计算机可读存储介质可以是上述实施例中描述的设备中所包含的, 也可以是单独存在, 而未装配入该设备中。

本公开的另一方面还提供了一种计算机程序产品或计算机程序, 该计算机程序产品或计算机程序包括计算机指令, 该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令, 处理器执行该计算机指令, 使得该计算机设备执行上述各个实施例中提供的方法。

上述内容，仅为本公开的较佳示例性实施例，并非用于限制本公开的实施方案，本领域普通技术人员根据本公开的主要构思和精神，可以十分方便地进行相应的变通或修改，故本公开的保护范围应以权利要求书所要求的保护范围为准。

权 利 要 求

1.一种域名反射攻击检测方法，包括：

获取待检测请求对象在多个时间窗口内发起域名解析请求的请求数量；

5 根据预设时间关系对所述多个时间窗口的请求数量进行构建，得到至少两个请求序列；

计算所述至少两个请求序列之间的相关系数；

根据所述至少两个请求序列之间的相关系数，确定所述待检测请求对象是否发起域名反射攻击。

10 2.如权利要求1所述的方法，其中，所述根据预设时间关系对所述多个时间窗口的请求数量进行构建，得到至少两个请求序列，包括：

根据预设时间关系，将所述多个时间窗口划分为多个第一时间窗口和多个第二时间窗口；

15 根据所述多个第一时间窗口的请求数量构建得到第一请求序列，以及根据所述多个第二时间窗口的请求数量构建得到第二请求序列。

3.如权利要求2所述的方法，其中，所述多个时间窗口是连续的时间窗口；所述根据预设时间关系，将所述多个时间窗口划分为多个第一时间窗口和多个第二时间窗口，包括：

20 在多个连续的时间窗口中，确定指定数量个连续的时间窗口作为所述多个第一时间窗口；

在除所述第一时间窗口之外的其他时间窗口中，确定所述指定数量个时间窗口作为所述多个第二时间窗口；其中，所述多个第一时间窗口中最晚的第一时间窗口早于所述多个第二时间窗口中最早的第二时间窗口。

25 4.如权利要求1所述的方法，其中，所述至少两个请求序列包括第一请求序列和第二请求序列；所述计算所述至少两个请求序列之间的相关系数，包括：

对所述第一请求序列中含有的各个请求数量进行求平均值运算，得到第一均值，以及对所述第二请求序列中含有的各个请求数量进行求平均值运算，得到第二均值；

根据所述第一均值、所述第二均值、所述第一请求序列，以及所述第二请求序列，计算所述第一请求序列和所述第二请求序列之间的相关系数。

30 5.如权利要求4所述的方法，其中，所述根据所述第一均值、所述第二均值、所述第一请求序列，以及所述第二请求序列，计算所述第一请求序列和所述第二请求序列的相关系数，包括：

将所述第一请求序列中含有的各个请求数量分别与所述第一均值进行求差值运算，得到多个第一差值，以及将所述第二请求序列中含有的各个请求数量分别与所述第二均

值进行求差值运算，得到多个第二差值；

根据所述多个第一差值和所述多个第二差值，计算所述第一请求序列和所述第二请求序列之间的相关系数。

- 5 6.如权利要求1至5中任一项所述的方法，其中，在获取待检测请求对象在多个时间窗口内发起域名解析请求的请求数量之前，所述方法还包括：

获取指定时间窗口内发起域名解析请求的请求对象，并统计所述请求对象在所述指定时间窗口内发起域名解析请求的请求数量；

根据所述请求数量和预设数量阈值的关系，从所述请求对象中确定所述待检测请求对象。

- 10 7.如权利要求1至5中任一项所述的方法，其中，所述根据所述至少两个请求序列之间的相关系数，确定所述待检测请求对象是否发起域名反射攻击，包括：

检测所述至少两个请求序列的相关系数与预设阈值的关系，得到检测结果；

若所述检测结果表征所述相关系数大于等于所述预设阈值，则确定所述待检测请求对象发起域名反射攻击；

- 15 若所述检测结果表征所述相关系数小于所述预设阈值，则确定所述待检测请求对象未发起域名反射攻击。

8.一种域名反射攻击检测装置，包括：

获取模块，配置为获取待检测请求对象在多个时间窗口内发起域名解析请求的请求数量；

- 20 构建模块，配置为根据预设时间关系对所述多个时间窗口的请求数量进行构建，得到至少两个请求序列；

计算模块，配置为计算所述至少两个请求序列之间的相关系数；

确定模块，配置为根据所述至少两个请求序列之间的相关系数，确定所述待检测请求对象是否发起域名反射攻击。

- 25 9.一种电子设备，包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行时，使得所述电子设备实现如权利要求1至7中任一项所述的域名反射攻击检测方法。

- 30 10.一种计算机可读存储介质，其上存储有计算机可读指令，当所述计算机可读指令被计算机的处理器执行时，使计算机执行权利要求1至7中任一项所述的域名反射攻击检测方法。

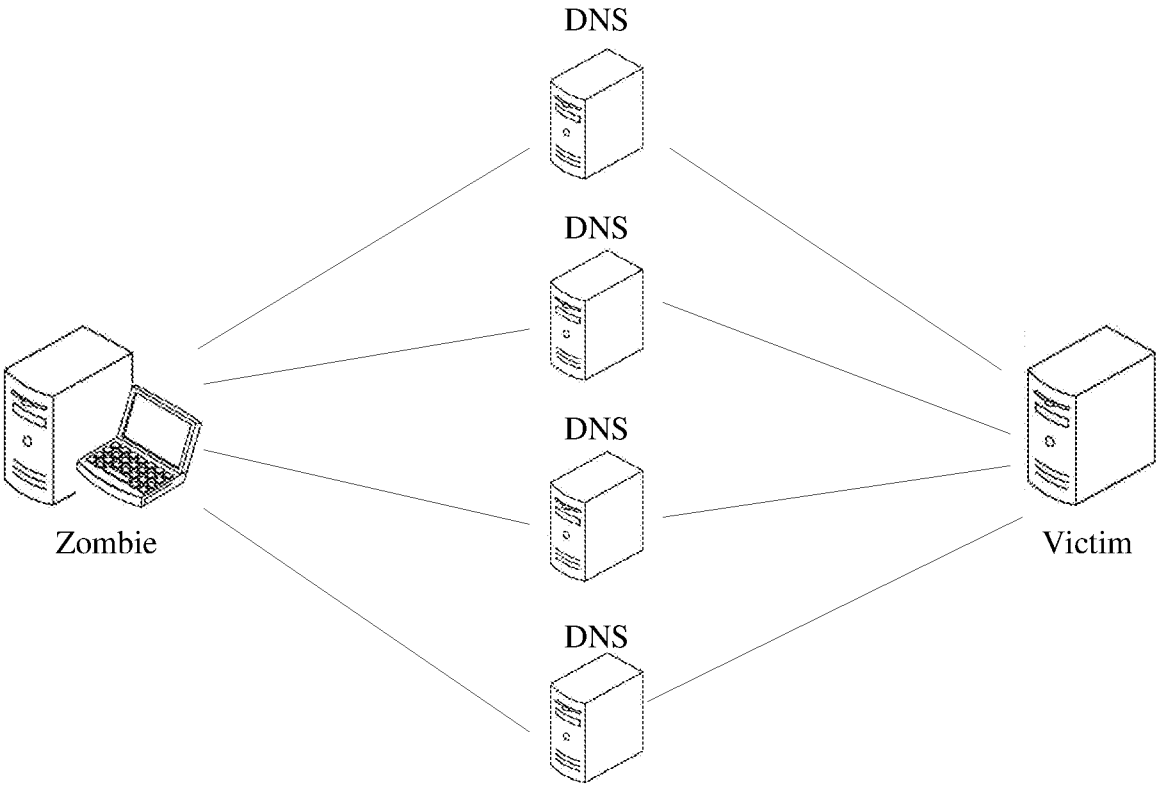


图 1

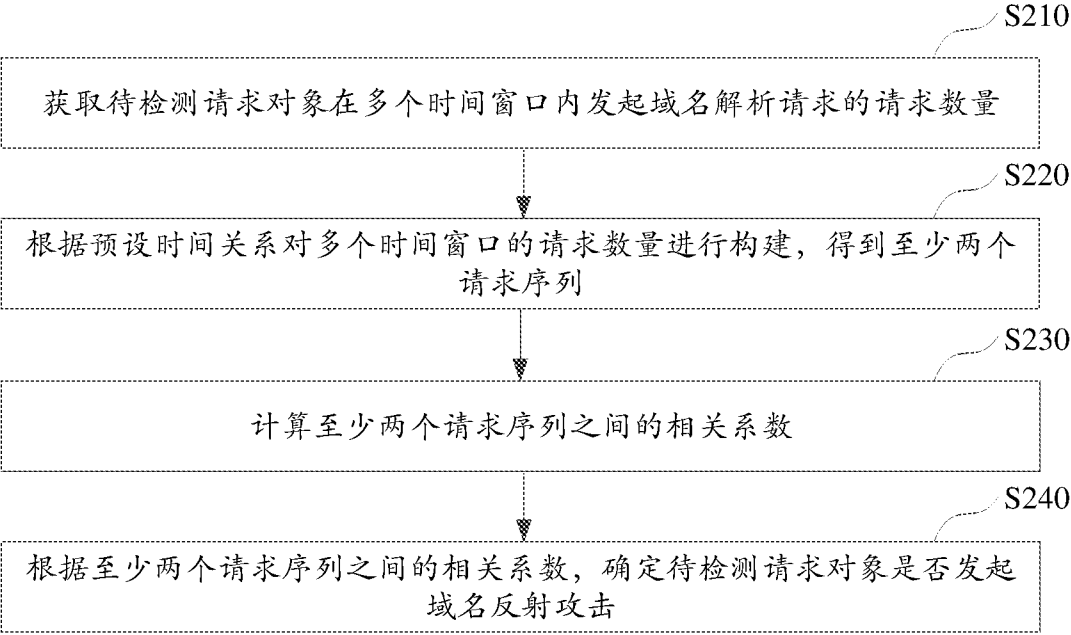


图 2

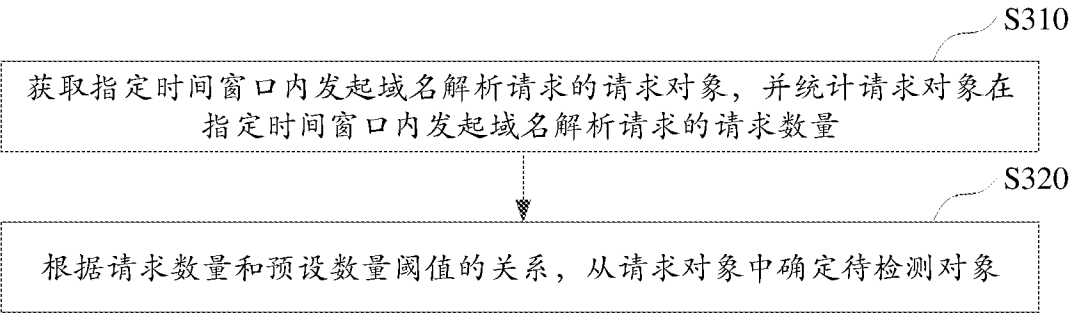


图 3

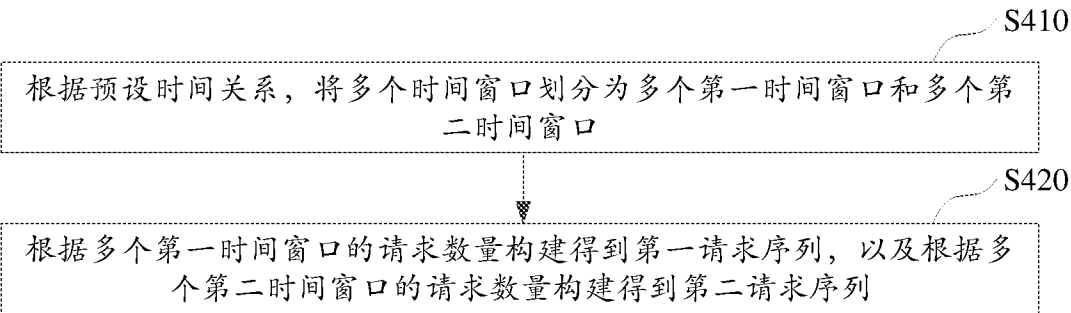


图 4

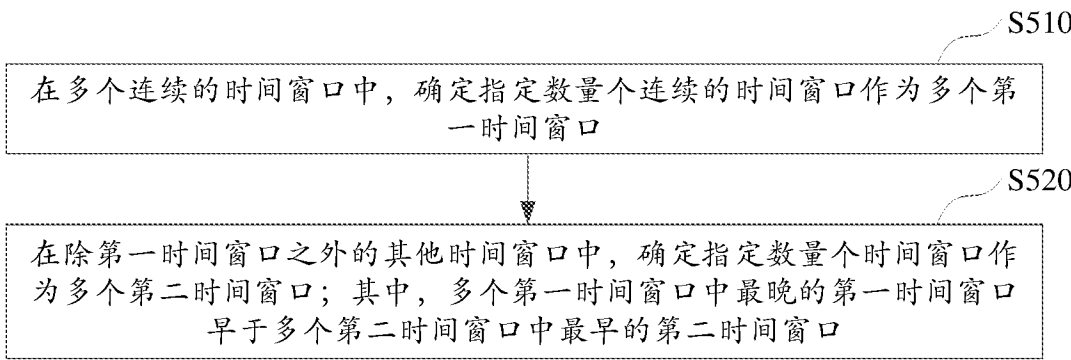


图 5

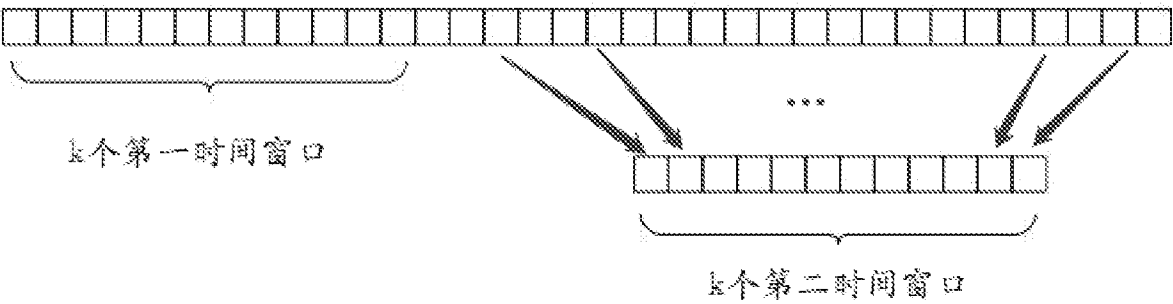


图 6

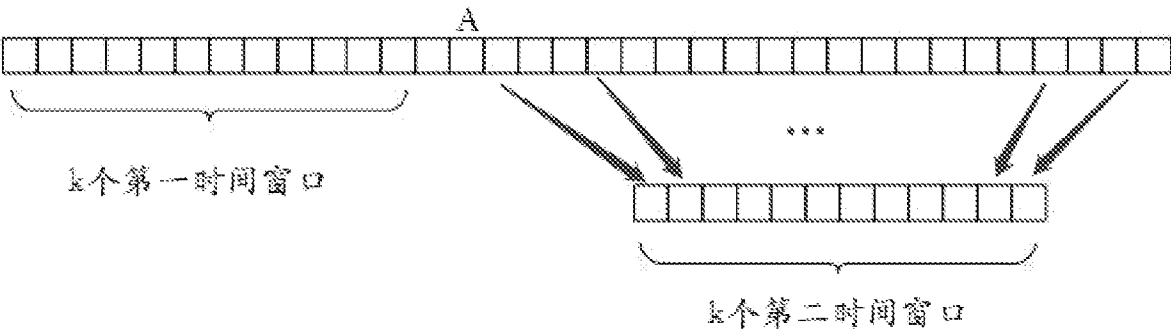


图 7

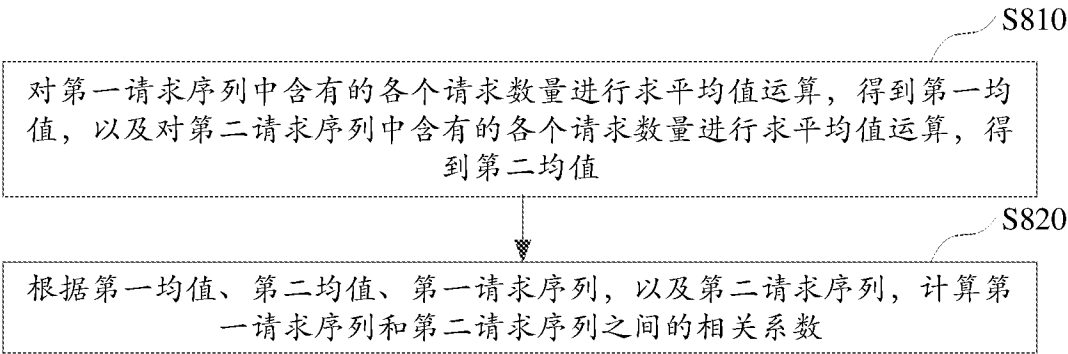


图 8

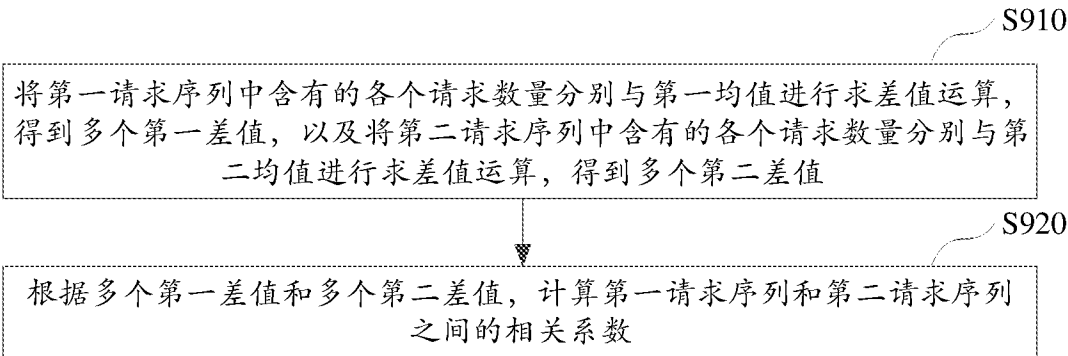


图 9

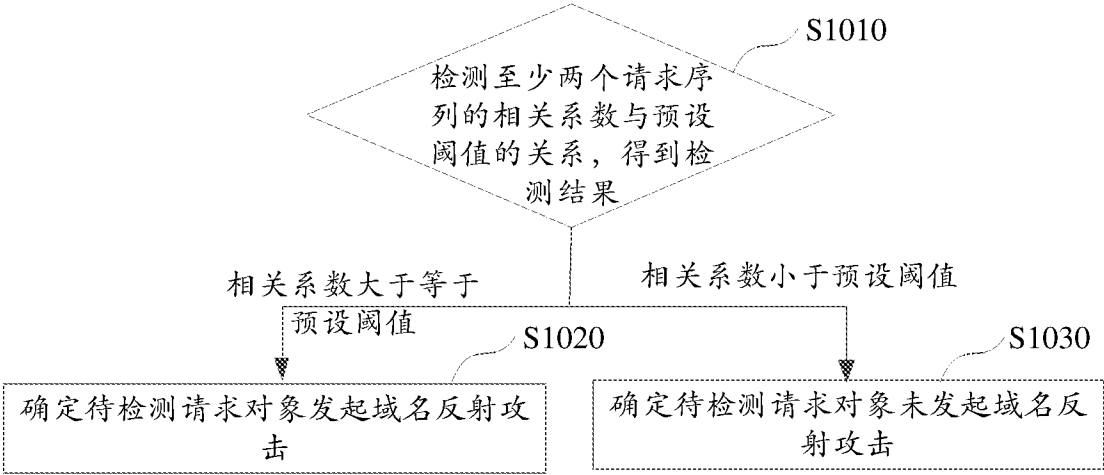


图 10

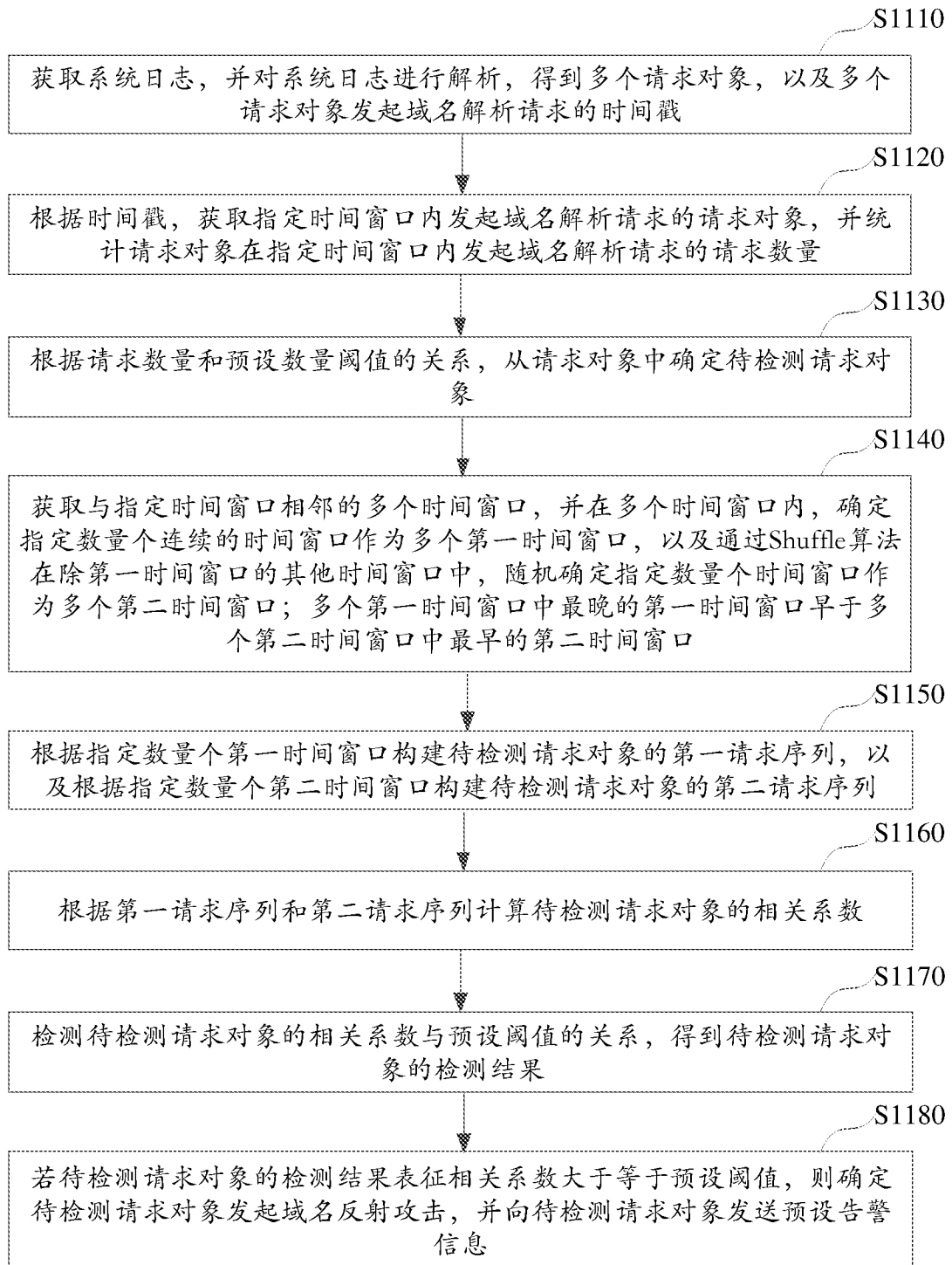


图 11

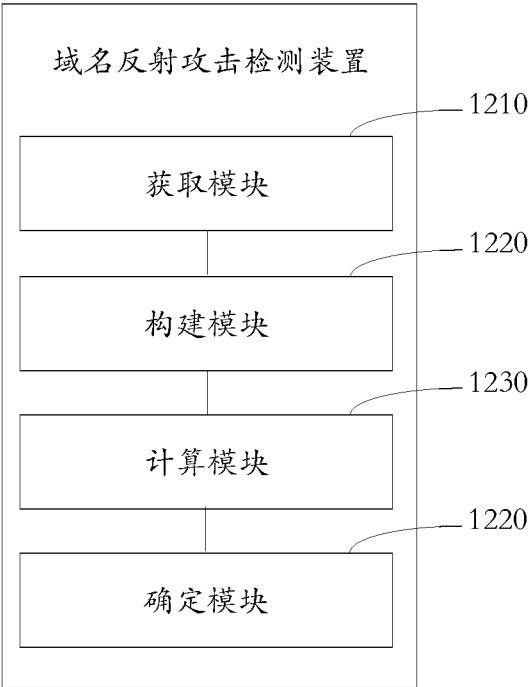


图 12

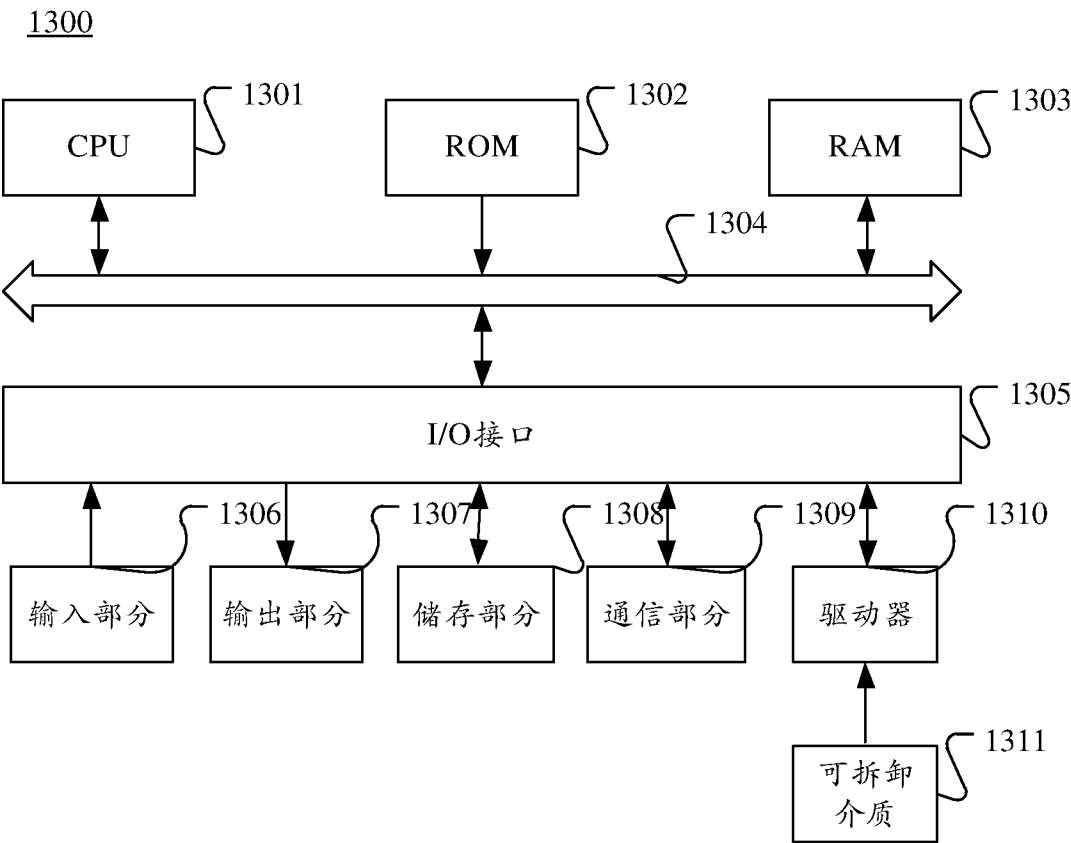


图 13

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/140321

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/40(2022.01)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)

IPC: 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)

CNTXT, ENTXTC, VEN, 3GPP, IEEE: 次数, 共性, 时间窗, 时间段, 时序, 数量, 相关, 相关系数, 相近, 相似, 序列, DDoS, DoS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 115296904 A (CHINA TELECOM CORP., LTD.) 04 November 2022 (2022-11-04) claims 1-10	1-10
X	US 2019020663 A1 (CISCO TECHNOLOGY INC.) 17 January 2019 (2019-01-17) description, paragraphs [0002], [0016], [0046]-[0048], and [0065]-[0083]	1-10
X	CN 114363062 A (SANGFOR TECHNOLOGIES INC.) 15 April 2022 (2022-04-15) description, paragraphs [0063]-[0075]	1-10
A	CN 109005181 A (SANGFOR TECHNOLOGIES INC.) 14 December 2018 (2018-12-14) entire document	1-10
A	CN 113783892 A (BEIJING TOPSEC NETWORK SECURITY TECHNOLOGY CO., LTD. et al.) 10 December 2021 (2021-12-10) entire document	1-10
A	US 2012174220 A1 (VERISIGN INC.) 05 July 2012 (2012-07-05) entire document	1-10



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

“D” document cited by the applicant in the international application

“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

06 February 2023

Date of mailing of the international search report

13 April 2023

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
China No. 6, Xitucheng Road, Jimenqiao, Haidian District,
Beijing 100088

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2022/140321

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	115296904	A	04 November 2022	None			
US	2019020663	A1	17 January 2019	US	10616267	B2	07 April 2020
CN	114363062	A	15 April 2022	None			
CN	109005181	A	14 December 2018	None			
CN	113783892	A	10 December 2021	None			
US	2012174220	A1	05 July 2012	TW	201242313	A	16 October 2012
				WO	2012091896	A1	05 July 2012
				EP	2659647	A1	06 November 2013

国际检索报告

国际申请号

PCT/CN2022/140321

A. 主题的分类 H04L9/40 (2022.01) 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) IPC: 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)) CNTXT, ENTXTC, VEN, 3GPP, IEEE: 次数, 共性, 时间窗, 时间段, 时序, 数量, 相关, 相关系数, 相近, 相似, 序列, DDoS, DoS		
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 115296904 A (中国电信股份有限公司) 2022年11月4日 (2022 - 11 - 04) 权利要求1-10	1-10
X	US 2019020663 A1 (CISCO TECH INC) 2019年1月17日 (2019 - 01 - 17) 说明书第[0002]、[0016]、[0046]-[0048]、[0065]-[0083]段	1-10
X	CN 114363062 A (深信服科技股份有限公司) 2022年4月15日 (2022 - 04 - 15) 说明书第[0063]-[0075]段	1-10
A	CN 109005181 A (深信服科技股份有限公司) 2018年12月14日 (2018 - 12 - 14) 全文	1-10
A	CN 113783892 A (北京天融信网络安全技术有限公司等) 2021年12月10日 (2021 - 12 - 10) 全文	1-10
A	US 2012174220 A1 (VERISIGN INC) 2012年7月5日 (2012 - 07 - 05) 全文	1-10
☐ 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 “D” 申请人在国际申请中引证的文件 “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 2023年2月6日		国际检索报告邮寄日期 2023年4月13日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		授权官员 徐千慧 电话号码 (+86) 0512-88996259

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/140321

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	115296904	A	2022年11月4日	无			
US	2019020663	A1	2019年1月17日	US	10616267	B2	2020年4月7日
CN	114363062	A	2022年4月15日	无			
CN	109005181	A	2018年12月14日	无			
CN	113783892	A	2021年12月10日	无			
US	2012174220	A1	2012年7月5日	TW	201242313	A	2012年10月16日
				WO	2012091896	A1	2012年7月5日
				EP	2659647	A1	2013年11月6日