

(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
2017 年 6 月 29 日 (29.06.2017)



(10) 国际公布号
WO 2017/107804 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2016/109604
- (22) 国际申请日: 2016 年 12 月 13 日 (13.12.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510990022.1 2015 年 12 月 24 日 (24.12.2015) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 及
- (71) 申请人 (仅对美国): 李然 (LI, Ran) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。王海东 (WANG, Haidong) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。宋加生 (SONG, Jiasheng) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。崔一山 (CUI, Yishan) [CN/CN]; 中国

浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。张建飞 (ZHANG, Jianfei) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。梁永喜 (LIANG, Yongxi) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。周晓敏 (ZHOU, Xiaomin) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。叶根深 (YE, Genshen) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, Beijing 100029 (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, DJ, 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, KH, KN, KP, KR, KW, 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,

[见续页]

(54) Title: METHOD AND DEVICE FOR DDOS ATTACK IDENTIFICATION

(54) 发明名称: 发现 DDoS 攻击的方法及装置

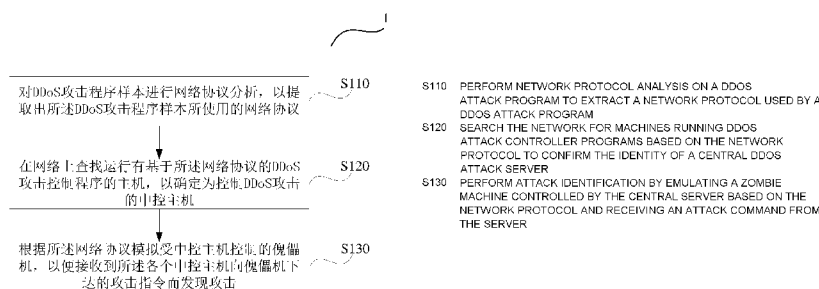


图 1

(57) Abstract: The invention provides a method and device for DDoS attack identification. The method comprises: performing network protocol analysis on a DDoS attack program to extract a network protocol used by the DDoS attack program; searching a network for machines running DDoS attack controller programs based on the network protocol to confirm the identity of a central DDoS attack server; performing attack identification by emulating a zombie machine controlled by the server based on the network protocol and receiving an attack command from the server. On the basis of the technical solution proposed in the present invention, the central server controlling the zombie machines at the source of the DDoS attack can be found, and the real attacker behind the attack can be identified.

(57) 摘要: 本申请提供了一种发现 DDoS 攻击的方法及装置。其方法包括: 对 DDoS 攻击程序样本进行网络协议分析, 以提取出所述 DDoS 攻击程序样本所使用的网络协议; 在网络上查找运行有基于所述网络协议的 DDoS 攻击控制程序的主机, 以确定为中心控制主机的中控制主机; 根据所述网络协议模拟受中控制主机控制的傀儡机, 以便接收到所述各个中控制主机向傀儡机下达的攻击指令而发现攻击。根据本申请的技术方案, 能够获知控制傀儡机发动 DDoS 攻击的中控制主机, 进而可以关联出背后的真正攻击者。



WO 2017/107804 A1



SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW。

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)。

- (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,

本国际公布:

- 包括国际检索报告(条约第 21 条(3))。

发现 DDoS 攻击的方法及装置

技术领域

本申请涉及 DDoS 攻击防御领域，尤其涉及一种发现 DDoS 攻击的方法及装置。

背景技术

DDoS 攻击是指黑客通过控制大量的傀儡机，消耗攻击目标的计算资源阻止目标为合法用户提供服务。现有的 DDoS 防御系统，主要是保护目标免受攻击者的 DDoS 攻击，而攻击者一般是由黑客控制的傀儡机，因此，现有的 DDoS 防御系统，是无法获知背后的真正攻击者到底是谁。最基本的 DDoS 攻击主要是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。现有的 DDoS 防御系统，主要根据流量判断是否受到 DDoS 攻击，然而，在攻击者开始发动 DDoS 攻击时，由于初始流量较小，无法在第一时间准确判断是否要被攻击。

发明内容

本申请的一个目的是提供一种发现 DDoS 攻击的方法及装置，能够获知控制傀儡机发动 DDoS 攻击的中控主机以及其攻击的目标主机。

根据本申请的一方面，提供了一种发现 DDoS 攻击的方法，其中，该方法包括以下步骤：

对 DDoS 攻击程序样本进行网络协议分析，以提取出所述 DDoS 攻击程序样本所使用的网络协议；

在网络上查找运行有基于所述网络协议的 DDoS 攻击控制程序的主机，以确定为控制 DDoS 攻击的中控主机；

根据所述网络协议模拟受中控主机控制的傀儡机，以便接收到所述各个中控主机向傀儡机下达的攻击指令而发现攻击。

可选地，对 DDoS 攻击程序样本进行网络协议分析，以提取出所述 DDoS 攻击程序样本所使用的网络协议的步骤包括：

对所述 DDoS 攻击程序样本进行反汇编分析，以还原出所述 DDoS 攻击程序样本所述使用的网络协议。

- 5 可选地，对 DDoS 攻击程序样本进行网络协议分析，以提取出所述 DDoS 攻击程序样本所使用的网络协议的步骤包括：

运行所述 DDoS 攻击程序样本，以通过抓包分析来分析出所述 DDoS 攻击程序样本所使用的网络协议。

- 10 可选地，在网络上查找运行有基于所述网络协议的 DDoS 攻击控制程序的主机，以确定为控制 DDoS 攻击的中控主机的步骤包括：

向网络中的各个主机发送所述网络协议的数据包；

检测接收到的各个主机返回的数据包是否与预期结果匹配；

将返回的数据包与预期结果匹配的主机确定为控制 DDoS 攻击的中控主机。

- 15 可选地，根据所述网络协议模拟受中控主机控制的傀儡机，以便接收到所述各个中控主机向傀儡机下达的攻击指令而发现攻击的步骤包括：

向扫描出的各个中控主机发送所述网络协议中的上线协议，以模拟受中控主机控制的傀儡机；

接收扫描出的各个中控主机中至少一个下达的攻击指令；

- 20 通过解析所述攻击指令，提取出攻击目标的 IP 地址、中控主机的 IP 地址以及攻击类型。

可选地，根据所述网络协议模拟受中控主机控制的傀儡机，以便接收到所述各个中控主机向傀儡机下达的攻击指令而发现攻击的步骤还包括：

- 25 向所述各个中控主机发送所述网络协议的心跳包，以维持与所述各个中控主机的通信连接。

可选地，该方法还包括：将提取出的攻击目标 IP 地址、中控主机的 IP 地址、以及攻击类型进行输出显示。

根据本申请的另一方面，还提供了一种发现 DDoS 攻击的装置，其中，该装置包括：

分析单元，用于对 DDoS 攻击程序样本进行网络协议分析，以提取出所述 DDoS 攻击程序样本所使用的网络协议；

5 查找单元，用于在网络上查找运行有基于所述网络协议的 DDoS 攻击控制程序的主机，以确定为控制 DDoS 攻击的中控主机；

发现单元，用于根据所述网络协议模拟受中控主机控制的傀儡机，以便接收到所述各个中控主机向傀儡机下达的攻击指令而发现攻击。

可选地，所述分析单元进一步用于：

10 对所述 DDoS 攻击程序样本进行反汇编分析，以还原出所述 DDoS 攻击程序样本所述使用的网络协议。

可选地，所述分析单元进一步用于：

运行所述 DDoS 攻击程序样本，以通过抓包分析来分析出所述 DDoS 攻击程序样本所使用的网络协议。

15 可选地，所述查找单元包括：

发送单元，用于向网络中的各个主机发送所述网络协议的数据包；

检测单元，用于检测接收到的各个主机返回的数据包是否与预期结果匹配；

20 确定单元，用于将返回的数据包与预期结果匹配的主机确定为控制 DDoS 攻击的中控主机。

可选地，所述发现单元包括：

模拟单元，用于向扫描出的各个中控主机发送所述网络协议中的上线协议，以模拟受中控主机控制的傀儡机；

25 接收单元，用于接收扫描出的各个中控主机中至少一个下达的攻击指令；

解析单元，用于通过解析所述攻击指令，提取出攻击目标的 IP 地址、中控主机的 IP 地址、以及攻击类型。

可选地，所述发现单元还包括：

心跳包发送单元，用于向所述各个中控主机发送所述网络协议的心跳包，以维持与所述各个中控主机的通信连接。

可选地，该装置还包括：输出单元，用于将提取出的攻击目标的 IP 地址、中控主机的 IP 地址以及攻击类型进行输出显示。

与现有技术相比，本申请的实施例具有以下优点：

1) 现有的 DDoS 防御系统，只能获知被哪些傀儡机所攻击，并不能获知控制傀儡机发起攻击的中控主机，也就很难关联出背后的真正攻击者是谁。与之相比，本申请能够获知控制傀儡机发动 DDoS 攻击的中控主机，进而可以关联出背后的真正攻击者。

2) 本申请对控制傀儡机发动 DDoS 攻击的中控主机进行监控，在攻击发起的初始时刻，就能够获取其要攻击的目标主机以及使用的攻击方式。

附图说明

通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

图 1 为本申请一个实施例提供的方法的流程图；

图 2 为本申请一个实施例的步骤 S120 的流程图；

图 3 为本申请一个实施例的步骤 S130 的一种实施方式的流程图；

图 4 为本申请一个实施例的步骤 S130 的另一种实施方式的流程图；

图 5 为本申请一个实施例提供的装置示意图；

图 6 为本申请实施例提供的装置中查找单元 520 的示意图；

图 7 为本申请实施例提供的装置中发现单元 530 的一种实施方式的示意图；

图 8 为本申请实施例提供的装置中发现单元 530 的另一种实施方式的示意图。

附图中相同或相似的附图标记代表相同或相似的部件。

具体实施方式

在更加详细地讨论示例性实施例之前应当提到的是，一些示例性实
5 施例被描述成作为流程图描绘的处理或方法。虽然流程图将各项操作描
述成顺序的处理，但是其中的许多操作可以被并行地、并发地或者同时
实施。此外，各项操作的顺序可以被重新安排。当其操作完成时所述处
理可以被终止，但是还可以具有未包括在附图中的附加步骤。所述处理
可以对应于方法、函数、规程、子例程、子程序等等。

10 在上下文中所称“计算机设备”，也称为“电脑”，是指可以通过运行
预定程序或指令来执行数值计算和/或逻辑计算等预定处理过程的智能
电子设备，其可以包括处理器与存储器，由处理器执行在存储器中预存
的存续指令来执行预定处理过程，或是由 ASIC、FPGA、DSP 等硬件执
行预定处理过程，或是由上述二者组合来实现。计算机设备包括但不限
15 于服务器、个人电脑、笔记本电脑、平板电脑、智能手机等。

所述计算机设备包括用户设备与网络设备。其中，所述用户设备包
括但不限于电脑、智能手机、PDA 等；所述网络设备包括但不限于单
个网络服务器、多个网络服务器组成的服务器组或基于云计算（Cloud
Computing）的由大量计算机或网络服务器构成的云，其中，云计算是
20 分布式计算的一种，由一群松散耦合的计算机集组成的一个超级虚拟计
算机。其中，所述计算机设备可单独运行来实现本申请，也可接入网络
并通过与网络中的其他计算机设备的交互操作来实现本申请。其中，所
述计算机设备所处的网络包括但不限于互联网、广域网、城域网、局域网、
VPN 网络等。

25 需要说明的是，所述用户设备、网络设备和网络等仅为举例，其他
现有的或今后可能出现的计算机设备或网络如可适用于本申请，也应包
含在本申请保护范围以内，并以引用方式包含于此。

后面所讨论的方法（其中一些通过流程图示出）可以通过硬件、软
件、固件、中间件、微代码、硬件描述语言或者其任意组合来实施。当

用软件、固件、中间件或微代码来实施时，用以实施必要任务的程序代码或代码段可以被存储在机器或计算机可读介质（比如存储介质）中。（一个或多个）处理器可以实施必要的任务。

这里所公开的具体结构和功能细节仅仅是代表性的，并且是用于描述本申请的示例性实施例的目的。但是本申请可以通过许多替换形式来具体实现，并且不应当被解释成仅仅受限于这里所阐述的实施例。

应当理解的是，虽然在这里可能使用了术语“第一”、“第二”等等来描述各个单元，但是这些单元不应当受这些术语限制。使用这些术语仅仅是为了将一个单元与另一个单元进行区分。举例来说，在不背离示例性实施例的范围的情况下，第一单元可以被称为第二单元，并且类似地第二单元可以被称为第一单元。这里所使用的术语“和/或”包括其中一个或更多所列出的相关联项目的任意和所有组合。

这里所使用的术语仅仅是为了描述具体实施例而不意图限制示例性实施例。除非上下文明确地另有所指，否则这里所使用的单数形式“一个”、“一项”还意图包括复数。还应当理解的是，这里所使用的术语“包括”和/或“包含”规定所陈述的特征、整数、步骤、操作、单元和/或组件的存在，而不排除存在或添加一个或更多其他特征、整数、步骤、操作、单元、组件和/或其组合。

还应当提到的是，在一些替换实现方式中，所提到的功能/动作可以按照不同于附图中标示的顺序发生。举例来说，取决于所涉及的功能/动作，相继示出的两幅图实际上可以基本上同时执行或者有时可以按照相反的顺序来执行。

下面结合附图对本申请作进一步详细描述。

图 1 为本申请一个实施例的发现 DDoS 攻击方法流程图。根据本申请的方法 1 至少包括步骤 110、步骤 120 和步骤 130。本申请能够基于目前能够获取到的 DDoS 攻击程序样本，查找控制该中类型的 DDoS 攻击的中控主机以及被攻击的目标主机。

参考图 1，在步骤 110 中，对 DDoS 攻击程序样本进行网络通信协议分析，以提取出所述 DDoS 攻击程序样本所使用的网络协议。

黑客入侵有安全漏洞的主机获取控制权，并在每台被入侵的主机中安装 DDoS 攻击程序，其中，被黑客入侵并控制的主机为傀儡机。发动 DDoS 攻击时，黑客通过中控主机控制这些傀儡机向目标主机发动 DDoS 攻击。中控主机上被黑客事先安装了 DDoS 攻击控制程序，该

5 DDoS 攻击控制程序用于与傀儡机上安装的 DDoS 攻击程序进行通信，以控制傀儡机向目标主机发起 DDoS 攻击。中控主机（DDoS 攻击控制程序）通过预先约定的网络协议与多个傀儡机（DDoS 攻击程序）进行网络通信，以便向傀儡机下达 DDoS 攻击指令。因此，根据 DDoS 攻击程序样本可以分析出中控主机与傀儡机进行通信的网络协议。所述网络

10 协议包括但不限于：上线协议、心跳包、发动攻击时的指令协议和停止攻击时的指令协议。

步骤 S110 的具体实现方式包括但不限于以下两种：

（1）对所述 DDoS 攻击程序样本进行反汇编分析，以还原出所述 DDoS 样本的网络协议。

15 具体地，将所述 DDoS 攻击程序样本的机器代码翻译成汇编代码，根据翻译成的汇编代码分析出所述 DDoS 攻击程序样本处理网络协议的代码实现逻辑，从而还原出所述 DDoS 攻击程序样本所使用的网络协议。

（2）运行所述 DDoS 攻击程序样本，以通过抓包分析来分析出所述 DDoS 攻击程序样本所使用的网络协议。

20 具体而言，在任意一台主机上运行所述 DDoS 攻击程序样本，并在运行所述 DDoS 攻击程序样本的主机上进行抓包分析，通过抓包分析即可分析出所述 DDoS 攻击程序样本所使用的网络协议。进行抓包分析时，可以使用现有的抓包软件。

参考图 1，在步骤 120 中，在网络上查找运行有基于所述网络协议的

25 DDoS 攻击控制程序的主机，以确定为控制 DDoS 攻击的中控主机。

中控主机通过预先约定的网络协议与多个傀儡机进行网络通信，以便下达 DDoS 攻击指令。因此，向网络上的各个主机发送所述网络协议的数据包，并检测各个主机返回的数据包是否与协议期望的数据包相同，能查找到运行所述网络协议的 DDoS 攻击控制程序的主机，并可以确

定为控制 DDoS 攻击的中控主机。

具体地，可以将所述网络协议输入到基于网络协议探测的扫描器程序，由该扫描器程序根据所述网络协议进行全网扫描，以扫描出控制 DDoS 攻击的中控主机。利用扫描器程序可以通过执行以下的步骤 S121~S123 扫描出控制 DDoS 攻击的中控主机，并输出扫描出的中控主机的 IP 地址列表，以备下一个步骤（步骤 S130）中使用。

参考图 2，步骤 S120 具体包括以下步骤：

步骤 S121，向网络中的各个主机发送所述网络协议的数据包。

步骤 S122，检测接收到的各个主机返回的数据包是否与预定结果匹配。

步骤 S123，将返回的数据包与预期结果匹配的主机确定为控制 DDoS 攻击的中控主机。

所述预定结果就是协议期望的使用所述网络协议的主机在接收到所述网络协议的数据包时回复的应答结果。如果一个主机返回的数据包与预期结果匹配，则表示该主机上运行着基于该网络协议进行通信的 DDoS 中控程序，则可以将该主机确定为控制 DDoS 攻击的中控主机。例如，发送数据包“aaabbbccc”，期望的回复是“haha”，如果某个主机回复的是“haha”，则认为是运行该 DDoS 攻击控制程序的中控主机，反之，则认为不是运行该 DDoS 攻击控制程序的中控主机。

参考图 1，在步骤 130 中，根据所述网络协议模拟受中控主机控制的傀儡机，以便接收到所述各个中控主机向傀儡机下达的攻击指令而发现攻击。

参考图 3，在一个具体实施方式中，步骤 S130 具体包括以下步骤：

步骤 S131，向扫描出的各个中控主机发送所述网络协议中的上线协议，以模拟傀儡机。

中控主机在发动 DDoS 攻击时，通过预先约定的网络协议与其控制的多台傀儡机进行通信，因此，根据分析出的该 DDoS 攻击程序样本的网络协议与扫描出的各个中控主机进行通信能够模拟成傀儡机，以便对各个中

控主机进行监控。具体而言，向扫描出的各个中控主机发送所述网络协议中的上线协议，以表明可以接收其指令，从而伪装成傀儡机。

步骤 S132，接收扫描出的各个中控主机中的至少一个发送的攻击指令；

- 5 当中控主机准备发动攻击时，会向各个傀儡机下达攻击指令，因此，模拟成的傀儡机会接收到发动攻击的中控主机下达的攻击指令。

步骤 S133，通过解析所述攻击指令，提取出攻击目标的 IP 地址、中控主机的 IP 地址以及攻击类型。

- 10 接收到攻击指令后，对指令数据进行解析，能够提取出攻击目标（目标主机）的 IP 地址、发动攻击的中控主机的 IP 地址以及攻击类型。所述攻击类型例如，TCP SYN 攻击、UDP flood 攻击（UDP 洪水攻击）、CC 攻击、DNS 反射等。

参考图 4，在上述实施方式的基础上，步骤 S130 还包括步骤 S134。

- 15 步骤 S134，向各个中控主机发送所述网络协议的心跳包，以维持与各个中控主机的通信连接。

- 心跳包是在客户端和服务端间按照一定的时间间隔发送的、用于通知对方自己状态的一个自定义的结构体。在某些网络协议中，要求按一定的时间间隔发送心跳包，报告自己的状态，因此，如果分析出的所述 DDoS 的网络协议中包含心跳包，则需要向各个中控主机发送所述网络协议中的心跳包，以便在维持与各个中控主机的通信连接。步骤 S134，可以在没有接收到中控主机下达的攻击指令时执行，以维持与各个中控主机的连接。
- 20

应注意，上述步骤 S110、步骤 S120 和步骤 S130 可以在同一设备中执行，亦可在不同设备中执行，例如，为提高各个步骤执行的性能可以分别在不同的计算机上执行。

- 25 基于上述实施例，本申请的方法还可以包括将提取出的攻击目标的 IP 地址、中控主机的 IP 地址以及攻击类型进行输出显示的步骤。还可以将提取的攻击目标的 IP 地址（目标主机的 IP 地址）、中控主机的 IP 地址以及攻击类型发送给攻击目标，以便受到攻击的主机采取 DDoS 防御措施。

现有的 DDoS 防御系统，只能获知被哪些傀儡机所攻击，并不能获知控制傀儡机发起攻击的中控主机，也就很难关联出背后的真正攻击者是谁。与之相比，本申请能够获知控制傀儡机发起攻击的中控主机，进而可以关联出背后的真正攻击者。本申请对控制傀儡机发动攻击的中控主机进行监控，在攻击发起的初始时刻，就能够获取其要攻击的目标主机，以及使用的攻击方式。

基于与方法同样的发明构思，本申请还提供一种发现 DDoS 攻击的装置。图 5 所示为发现 DDoS 的装置 5 示意图，该装置包括：

分析单元 510，用于对 DDoS 攻击程序样本进行网络协议分析，以提取出所述 DDoS 攻击程序样本所使用的网络协议；

查找单元 520，用于在网络上查找运行有基于所述网络协议的 DDoS 攻击控制程序的主机，以确定为控制 DDoS 攻击的中控主机；

发现单元 530，用于根据所述网络协议模拟受中控主机控制的傀儡机，以便接收到所述各个中控主机向傀儡机下达的攻击指令而发现攻击。

可选地，所述分析单元 510 进一步用于：

对所述 DDoS 攻击程序样本进行反汇编分析，以还原出所述 DDoS 攻击程序样本所述使用的网络协议。

可选地，所述分析单元 510 进一步用于：

运行所述 DDoS 攻击程序样本，以通过抓包分析来分析出所述 DDoS 攻击程序样本所使用的网络协议。

图 6 为根据本申请一个实施例的查找单元 520 的结构示意图。参考图 6，可选地，所述查找单元 520 包括：

发送单元 521，用于向网络中的各个主机发送所述网络协议的数据包；

检测单元 522，用于检测接收到的各个主机返回的数据包是否与预期结果匹配；

确定单元 523，用于将返回的数据包与预期结果匹配的主机确定为控

制 DDoS 攻击的中控主机。

图 7 为根据本申请一个实施例的发现单元 530 的结构示意图。参考图 7，所述发现单元 530 包括：

5 模拟单元 531，用于向扫描出的各个中控主机发送所述网络协议中的上线协议，以模拟受中控主机控制的傀儡机；

接收单元 532，用于接收扫描出的各个中控主机中至少一个下达的攻击指令；

解析单元 533，用于通过解析所述攻击指令，提取出攻击目标的 IP 地址、中控主机的 IP 地址、以及攻击类型。

10 图 8 为根据本申请另一个实施例的发现单元 530 的结构示意图。参考图 8，基于上述图 7 所示的实施例，所述发现单元 530 还包括：

心跳包发送单元 534，用于向所述各个中控主机发送所述网络协议的心跳包，以维持与所述各个中控主机的通信连接。

15 可选地，该装置 5 还包括：输出单元，用于将提取出的攻击目标的 IP 地址、中控主机的 IP 地址以及攻击类型进行输出显示。

20 需要注意的是，本申请可在软件和/或软件与硬件的组合体中被实施，例如，本申请的各个装置可采用专用集成电路（ASIC）或任何其他类似硬件设备来实现。在一个实施例中，本申请的软件程序可以通过处理器执行以实现上文所述步骤或功能。同样地，本申请的软件程序（包括相关的数据结构）可以被存储到计算机可读记录介质中，例如，RAM 存储器，磁或光驱动器或软磁盘及类似设备。另外，本申请的一些步骤或功能可采用硬件来实现，例如，作为与处理器配合从而执行各个步骤或功能的电路。

25 对于本领域技术人员而言，显然本申请不限于上述示范性实施例的细节，而且在不背离本申请的精神或基本特征的情况下，能够以其他的具体形式实现本申请。因此，无论从哪一点来看，均应将实施例看作是示范性的，而且是非限制性的，本申请的范围由所附权利要求而不是上

述说明限定，因此旨在将落在权利要求的等同要件的含义和范围内的所有变化涵括在本申请内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。此外，显然“包括”一词不排除其他单元或步骤，单数不排除复数。系统权利要求中陈述的多个单元或装置也可以由一个单元或装置通过软件或者硬件来实现。第一，第二等词语用来表示名称，而并不表示任何特定的顺序。

虽然前面特别示出并且描述了示例性实施例，但是本领域技术人员将会理解的是，在不背离权利要求书的精神和范围的情况下，在其形式和细节方面可以有所变化。

权 利 要 求 书

1. 一种发现 DDoS 攻击的方法，其特征在于，该方法包括以下步骤：

对 DDoS 攻击程序样本进行网络协议分析，以提取出所述 DDoS 攻击程序样本所使用的网络协议；

5 在网络上查找运行有基于所述网络协议的 DDoS 攻击控制程序的主机，以确定为控制 DDoS 攻击的中控主机；

根据所述网络协议模拟受中控主机控制的傀儡机，以便接收到所述各个中控主机向傀儡机下达的攻击指令而发现攻击。

2. 根据权利要求 1 所述的方法，其特征在于，对 DDoS 攻击程序样本
10 进行网络协议分析，以提取出所述 DDoS 攻击程序样本所使用的网络协议的步骤包括：

对所述 DDoS 攻击程序样本进行反汇编分析，以还原出所述 DDoS 攻击程序样本所述使用的网络协议。

3. 根据权利要求 1 所述的方法，其特征在于，对 DDoS 攻击程序样本
15 进行网络协议分析，以提取出所述 DDoS 攻击程序样本所使用的网络协议的步骤包括：

运行所述 DDoS 攻击程序样本，以通过抓包分析来分析出所述 DDoS 攻击程序样本所使用的网络协议。

4. 根据权利要求 1 所述的方法，其特征在于，在网络上查找运行有基
20 于所述网络协议的 DDoS 攻击控制程序的主机，以确定为控制 DDoS 攻击的中控主机的步骤包括：

向网络中的各个主机发送所述网络协议的数据包；

检测接收到的各个主机返回的数据包是否与预期结果匹配；

将返回的数据包与预期结果匹配的主机确定为控制 DDoS 攻击的中控
25 主机。

5. 根据权利要求 1 所述的方法，其特征在于，根据所述网络协议模拟受中控主机控制的傀儡机，以便接收到所述各个中控主机向傀儡机下达的

攻击指令而发现攻击的步骤包括:

向扫描出的各个中控主机发送所述网络协议中的上线协议,以模拟受中控主机控制的傀儡机;

接收扫描出的各个中控主机中至少一个下达的攻击指令;

5 通过解析所述攻击指令,提取出攻击目标的 IP 地址、中控主机的 IP 地址以及攻击类型。

6. 根据权利要求 5 所述的方法,其特征在于,根据所述网络协议模拟受中控主机控制的傀儡机,以便接收到所述各个中控主机向傀儡机下达的攻击指令而发现攻击的步骤还包括:

10 向所述各个中控主机发送所述网络协议的心跳包,以维持与所述各个中控主机的通信连接。

7. 根据权利要求 5 所述的方法,其特征在于,还包括:将提取出的攻击目标 IP 地址、中控主机的 IP 地址、以及攻击类型进行输出显示。

8. 一种发现 DDoS 攻击的装置,其特征在于,该装置包括:

15 分析单元,用于对 DDoS 攻击程序样本进行网络协议分析,以提取出所述 DDoS 攻击程序样本所使用的网络协议;

查找单元,用于在网络上查找运行有基于所述网络协议的 DDoS 攻击控制程序的主机,以确定控制 DDoS 攻击的中控主机;

20 发现单元,用于根据所述网络协议模拟受中控主机控制的傀儡机,以便接收到所述各个中控主机向傀儡机下达的攻击指令而发现攻击。

9. 根据权利要求 8 所述的装置,其特征在于,所述分析单元进一步用于:

对所述 DDoS 攻击程序样本进行反汇编分析,以还原出所述 DDoS 攻击程序样本所述使用的网络协议。

25 10. 根据权利要求 8 所述的装置,其特征在于,所述分析单元进一步用于:

运行所述 DDoS 攻击程序样本,以通过抓包分析来分析出所述 DDoS

攻击程序样本所使用的网络协议。

11. 根据权利要求 8 所述的装置，其特征在于，所述查找单元包括：

发送单元，用于向网络中的各个主机发送所述网络协议的数据包；

检测单元，用于检测接收到的各个主机返回的数据包是否与预期结果

5 匹配；

确定单元，用于将返回的数据包与预期结果匹配的主机确定为控制 DDoS 攻击的中控主机。

12. 根据权利要求 8 所述的装置，其特征在于，所述发现单元包括：

模拟单元，用于向扫描出的各个中控主机发送所述网络协议中的上线

10 协议，以模拟受中控主机控制的傀儡机；

接收单元，用于接收扫描出的各个中控主机中至少一个下达的攻击指令；

解析单元，用于通过解析所述攻击指令，提取出攻击目标的 IP 地址、中控主机的 IP 地址、以及攻击类型。

15 13. 根据权利要求 12 所述的装置，其特征在于，所述发现单元还包括：

心跳包发送单元，用于向所述各个中控主机发送所述网络协议的心跳包，以维持与所述各个中控主机的通信连接。

14. 根据权利要求 12 所述的装置，其特征在于，还包括：输出单元，用于将提取出的攻击目标的 IP 地址、中控主机的 IP 地址以及攻击类型进
20 行输出显示。

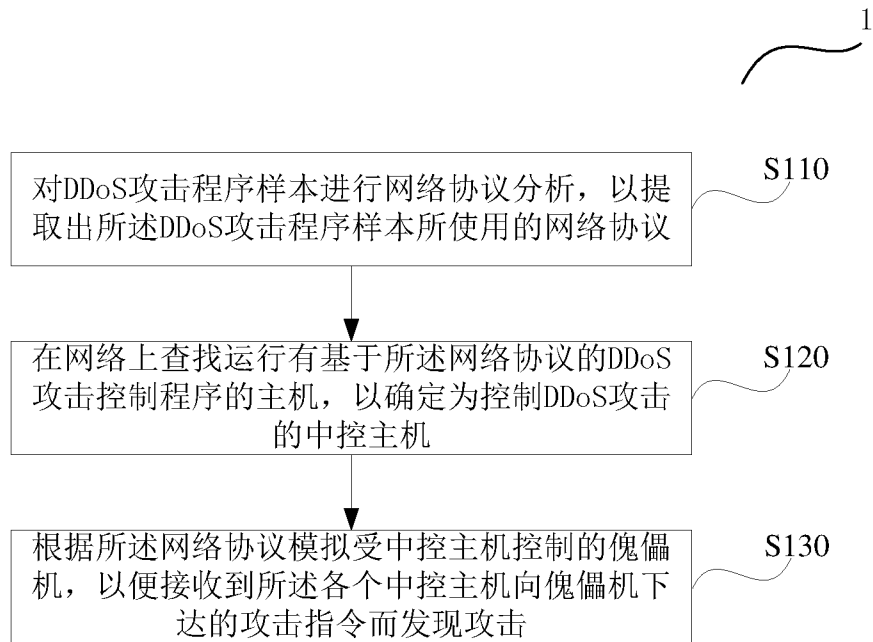


图 1

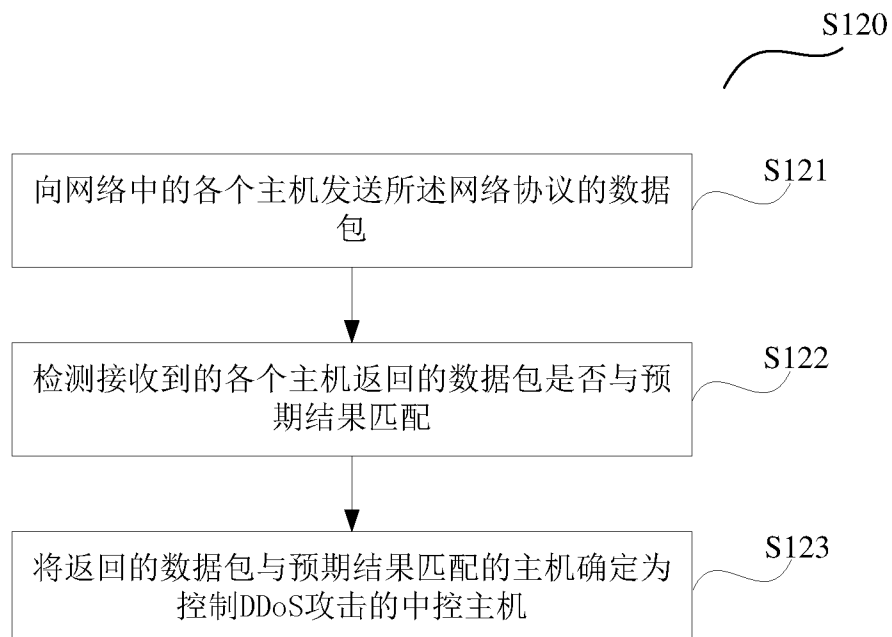


图 2

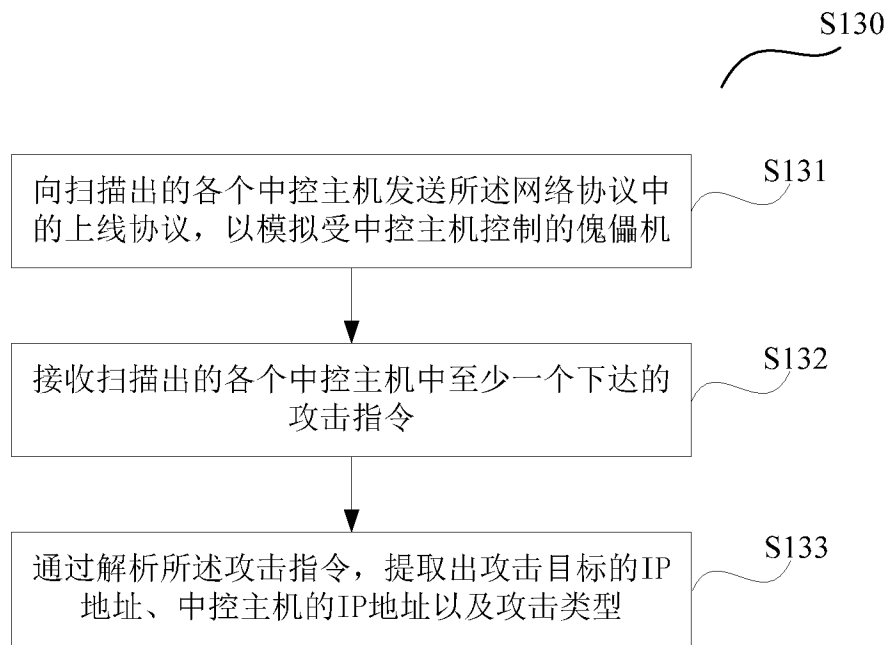


图 3

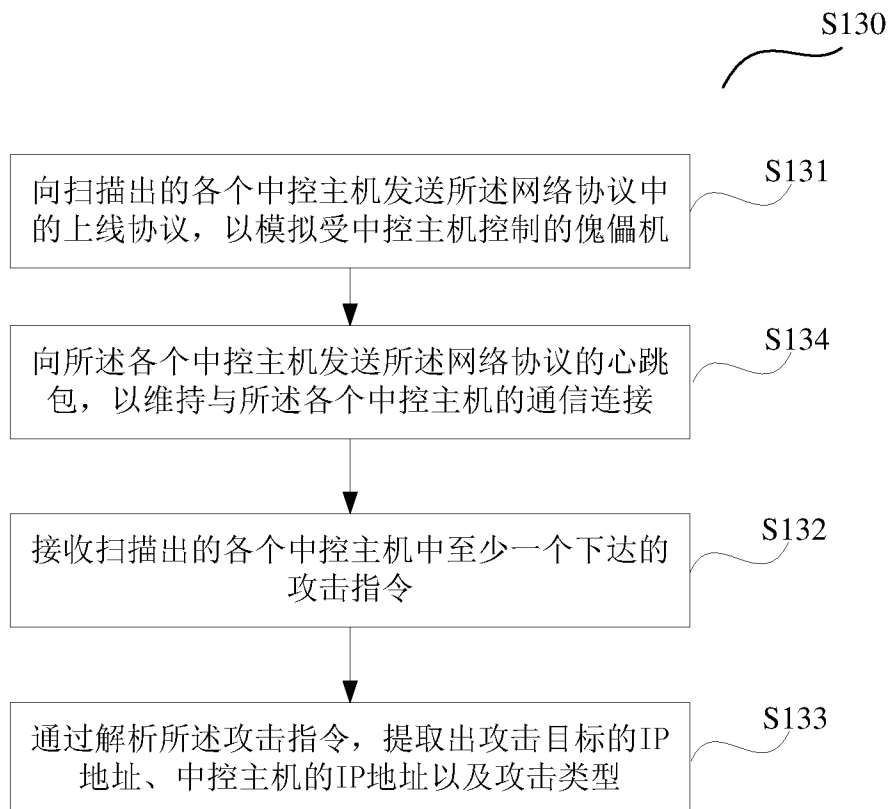


图 4

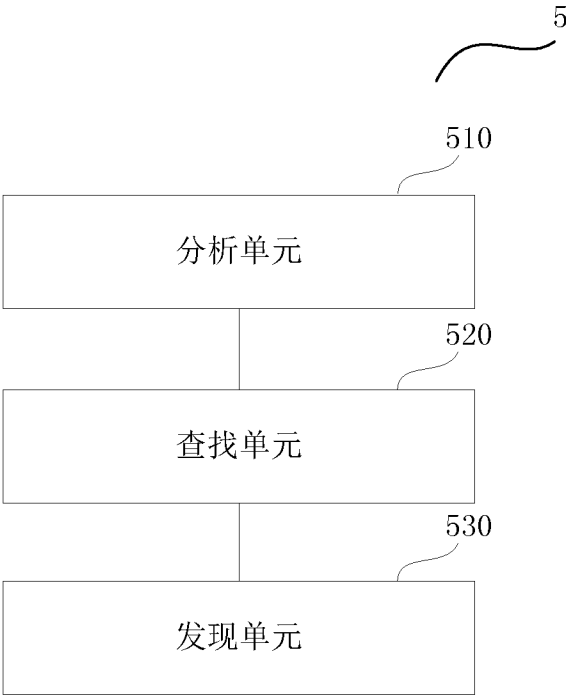


图 5

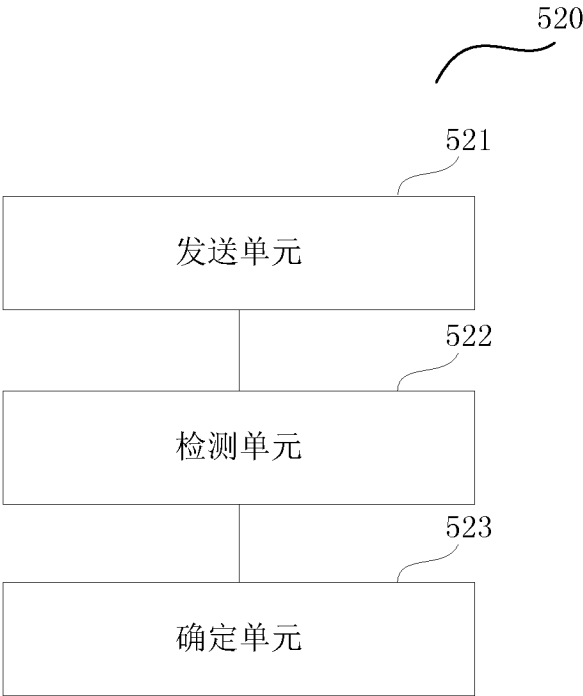


图 6

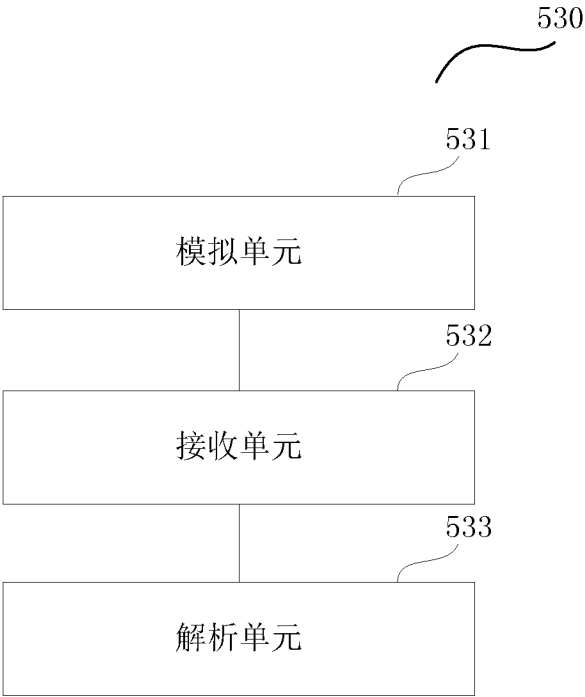


图 7

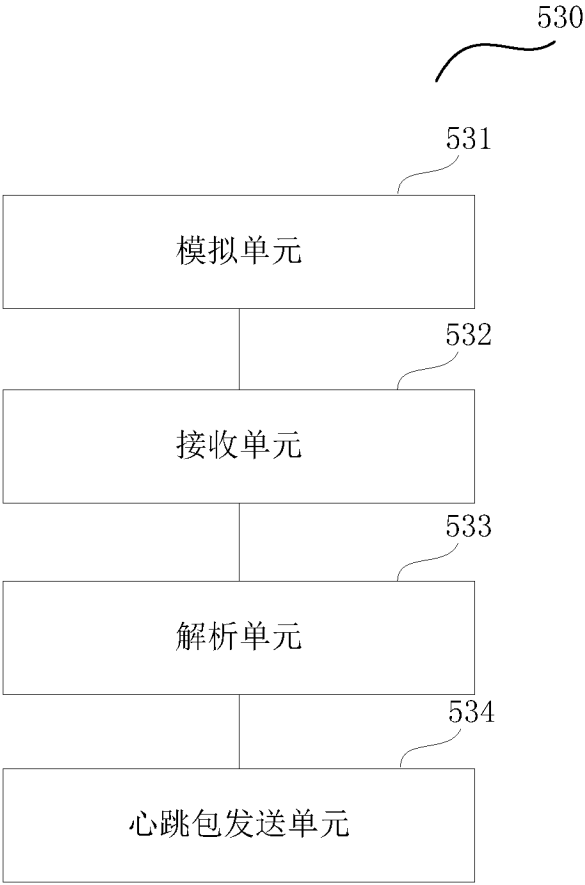


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/109604

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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; G06F

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)

CNPAT, WPI, EPODOC, CNKI: distributed denial of service, puppet, broiler, zombie, DDOS, DOS, bot+, host, machin+, protocol, heart+, command, instruction, attack+, simulat+, fals+, forge+, detect

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101360019 A (HUAWEI TECHNOLOGIES CO., LTD.), 04 February 2009 (04.02.2009), description, page 4, line 16 to page 9, line 19	1-14
X	CN 102546298 A (PEKING UNIVERSITY), 04 July 2012 (04.07.2012), description, paragraphs [0035]-[0055]	1-14
A	CN 101321171 A (BEIJING RUN TECHNOLOGY CO., LTD.), 10 December 2008 (10.12.2008), the whole document	1-14
A	US 2013074183 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE), 21 March 2013 (21.03.2013), the whole document	1-14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 13 February 2017 (13.02.2017)	Date of mailing of the international search report 03 March 2017 (03.03.2017)
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 GUO, Haibo Telephone No.: (86-10) 61648258

International application No.
PCT/CN2016/109604

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2016/109604

A. 主题的分类

H04L 29/06 (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; G06F

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))

CNPAT, WPI, EPODOC, CNKI: 分布式拒绝服务, 傀儡, 肉鸡, 僵尸, 主机, 协议, 心跳, 命令, 指令, 攻击, 模拟, 伪造, 检测, DDOS, DOS, bot+, host, machin+, protocol, heart+, command, instruction, attack+, simulat+, fals+, forge+, detect

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
X	CN 101360019 A (华为技术有限公司) 2009年 2月 4日 (2009 - 02 - 04) 说明书第4页第16行至第9页第19行	1-14
X	CN 102546298 A (北京大学) 2012年 7月 4日 (2012 - 07 - 04) 说明书第[0035]-[0055]段	1-14
A	CN 101321171 A (北京锐安科技有限公司) 2008年 12月 10日 (2008 - 12 - 10) 全文	1-14
A	US 2013074183 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 2013年 3月 21日 (2013 - 03 - 21) 全文	1-14

☐ 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

2017年 2月 13日

国际检索报告邮寄日期

2017年 3月 3日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局 (ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10) 62019451

受权官员

郭海波

电话号码 (86-10) 61648258

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/109604

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	101360019	A	2009年 2月 4日	WO	2010031288	A1	2010年 3月 25日
CN	102546298	A	2012年 7月 4日	无			
CN	101321171	A	2008年 12月 10日	无			
US	2013074183	A1	2013年 3月 21日	KR	20130030086	A	2013年 3月 26日

表 PCT/ISA/210 (同族专利附件) (2009年7月)