

(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
2018 年 11 月 8 日 (08.11.2018)



(10) 国际公布号
WO 2018/201581 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2017/088934

(22) 国际申请日: 2017 年 6 月 19 日 (19.06.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710301393.3 2017 年 5 月 2 日 (02.05.2017) CN

(71) 申请人: 深圳大学 (SHENZHEN UNIVERSITY) [CN/CN]; 中国广东省深圳市南山区南海大道 3688 号, Guangdong 518060 (CN)。

(72) 发明人: 闫巧 (YAN, Qiao); 中国广东省深圳市南山区南海大道 3688 号, Guangdong 518060 (CN)。
龚庆祥 (GONG, Qingxiang); 中国广东省深圳市南山区南海大道 3688 号, Guangdong 518060 (CN)。
陈剑勇 (CHEN, Jianyong); 中国广东省深圳市南山区南海大道 3688 号, Guangdong 518060 (CN)。

(74) 代理人: 深圳青年人专利商标代理有限公司 (SHENZHEN YOUTH PATENT AND TRADEMARK AGENCY LTD.); 中国广东省深圳市罗湖区深南东路 5045 号深业中心大厦 2502-2503, Guangdong 518010 (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, JO, 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, 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,

(54) Title: SOFTWARE-DEFINED NETWORK DDOS ATTACK SIMULATION AND ATTACK DETECTION METHOD AND APPARATUS

(54) 发明名称: 一种软件定义网络的DDoS攻击模拟和攻击检测方法及装置

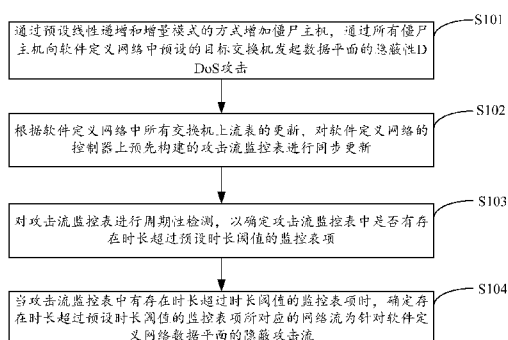


图 1

- S101 ADD ZOMBIE COMPUTERS IN A PRE-DETERMINED LINEARLY INCREASING INCREMENTAL FASHION, AND INITIATE A DATA PLANE CONCEALED DDOS ATTACK ON A PRE-DETERMINED TARGET SWITCH IN A SOFTWARE-DEFINED NETWORK BY MEANS OF SAID ZOMBIE COMPUTERS
- S102 BY MEANS OF UPDATING A FLOW TABLE ON ALL SWITCHES IN A SOFTWARE-DEFINED NETWORK, SYNCHRONIZE AND UPDATE A PRE-CONSTRUCTED ATTACK FLOW MONITORING TABLE ON A CONTROLLER OF THE SOFTWARE-DEFINED NETWORK
- S103 PERIODICALLY CHECK THE ATTACK FLOW MONITORING TABLE, SO AS TO DETERMINE WHETHER THERE IS IN THE ATTACK FLOW MONITORING TABLE A MONITORING TABLE ITEM HAVING A DURATION EXCEEDING A PRE-DETERMINED DURATION
- S104 WHEN THERE IS A MONITORING TABLE ITEM IN THE ATTACK FLOW MONITORING TABLE HAVING A DURATION EXCEEDING A DURATION THRESHOLD, IT IS DETERMINED THAT A NETWORK FLOW CORRESPONDING TO THE MONITORING TABLE ITEM HAVING A DURATION EXCEEDING THE PRE-DETERMINED DURATION THRESHOLD IS A CONCEALED ATTACK FLOW DIRECTED AT THE DATA PLANE OF THE SOFTWARE-DEFINED NETWORK

(57) Abstract: The present invention is used in the technical field of network security. Provided are a software-defined network DDoS attack simulation and attack detection method, and an apparatus, the method comprising: adding zombie computers in a linearly increasing incremental fashion, and initiating a data plane concealed DDoS attack on a pre-determined target switch in a software-defined network by means of said zombie computers; by means of updating a flow table on all switches in a software-defined network, synchronizing and updating a pre-constructed attack flow monitoring table on a controller of the software-defined network; periodically checking the attack flow monitoring table, so as to determine whether there is in the attack flow monitoring table a monitoring table item having a duration exceeding a pre-determined duration; when there is such an item, determining that a network flow corresponding to the monitoring table item is a concealed attack flow directed at the data plane of the software-defined network, thereby effectively increasing efficiency of modeling a concealed DDoS attack on a software-defined network data plane, and effectively increasing efficiency of detecting concealed DDoS attacks on the software-defined network data plane.

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))。

(57) 摘要: 本发明适用网络安全技术领域, 提供了一种软件定义网络的DDoS攻击模拟和攻击检测方法
及装置, 所述方法包括: 通过线性递增和增量模式的方式增加僵尸主机, 通过所有僵尸主机向软件定义网
络中预设的目标交换机发起数据平面的隐蔽性DDoS攻击, 根据软件定义网络中所有交换机上流表的更
新, 对软件定义网络的控制器上预先构建的攻击流监控表进行同步更新, 对攻击流监控表进行周期性检
测, 以确定攻击流监控表中是否有存在时长超过预设时长的监控表项, 当存在时, 确定该监控表项对应
网络流为针对软件定义网络数据平面的隐蔽攻击流, 从而有效地提高了模拟软件定义网络数据平面隐蔽
性DDoS攻击的效率, 有效地提高了软件定义网络数据平面隐蔽性DDoS攻击的检测效率。

一种软件定义网络的DDoS攻击模拟和攻击检测方法及装置

技术领域

[0001] 本发明属于网络安全技术领域，尤其涉及一种软件定义网络的DDoS攻击模拟和攻击检测方法及装置。

背景技术

[0002] 近年来以软件定义网络（SDN）为基础架构的网络蓬勃发展，软件定义网络将传统IP网络的路由控制和数据转发进行分离，实现集中控制和分布转发，并通过提供软件可编程的方式简化了网络的管理和配置，然而这也扩大了网络分布式拒绝服务攻击（DDoS）的攻击面。

[0003] 目前，软件定义网络对DDoS的抑制绝大多数只考虑到控制平面的DDoS攻击的问题。已有研究表明，软件定义网络数据平面的DDoS攻击更容易对软件定义网络造成威胁，并且数据平面DDoS攻击的隐蔽性会刻意地回避多数软件定义网络上的DDoS检测。

[0004] 在模拟软件定义网络数据平面的DDoS攻击时，相关算法提出的基于流表项超时的隐蔽性DDoS攻击，该算法使用增量模式（Incremental mode）周期性地增加僵尸主机的个数直到目标交换机流表趋近饱和状态，僵尸主机以小于流表项超时的攻击间隔周期性地发送攻击包，从而保持攻击包的流表项常在目标交换机的流表内，使得合法流表项无法安装处理。然而，增量模式无法使得僵尸主机的攻击速率快速地达到“最小攻击速率”（以最小化的攻击速度使目标交换机的流表项保持趋近于流表总大小的饱和状态）。

[0005] 现有软件定义网络数据平面DDoS攻击的检测算法提出周期性地从目标交换机中获取流表项并检查获取的流表项，通过检查结果判断是否存在隐蔽攻击流当该算法布置在控制器上时，会为软件定义网络的控制平面和数据平面之间的安全通道增加大量的流量负载，当该算法部署在每个目标交换机上时，不符合软件定义网络逻辑集中控制的思想，类似检测算法的升级、网络需要根据检测结

果采取缓解措施（如黑名单等的实现）都是复杂的。

技术问题

- [0006] 本发明的目的在于提供一种软件定义网络的DDoS攻击模拟和攻击检测方法及其装置，旨在解决由于现有技术中软件定义网络的数据平面隐蔽性DDoS攻击模拟、以及软件定义网络的数据平面DDoS攻击检测的效率较低，软件定义网络的数据平面DDoS攻击检测的实现较为复杂的问题。

问题的解决方案

技术解决方案

- [0007] 一方面，本发明提供了一种软件定义网络的DDoS攻击模拟和攻击检测方法，所述方法包括下述步骤：
- [0008] 通过预设线性递增和增量模式的方式增加僵尸主机，通过所有僵尸主机向软件定义网络中预设的目标交换机发起数据平面的隐蔽性DDoS攻击；
- [0009] 根据所述软件定义网络中所有交换机上流表的更新，对所述软件定义网络的控制器上预先构建的攻击流监控表进行同步更新；
- [0010] 对所述攻击流监控表进行周期性检测，以确定所述攻击流监控表中是否有存在时长超过预设时长阈值的监控表项；
- [0011] 当所述攻击流监控表中有存在时长超过所述时长阈值的监控表项时，确定所述存在时长超过所述预设时长阈值的监控表项所对应的网络流为针对所述软件定义网络数据平面的隐蔽攻击流。
- [0012] 另一方面，本发明提供了一种软件定义网络的DDoS攻击模拟和攻击检测装置，所述装置包括：
- [0013] 攻击模拟模块，用于通过预设线性递增和增量模式的方式增加僵尸主机，通过所有僵尸主机向软件定义网络中预设的目标交换机发起数据平面的隐蔽性DDoS攻击；
- [0014] 表更新模块，用于根据所述软件定义网络中所有交换机上流表的更新，对所述软件定义网络的控制器上预先构建的攻击流监控表进行同步更新；
- [0015] 超时检测模块，用于对所述攻击流监控表进行周期性检测，以确定所述攻击流监控表中是否有存在时长超过预设时长阈值的监控表项；以及

[0016] 攻击流确定模块，用于当确定所述攻击流监控表中有存在时长超过所述时长阈值的监控表项时，确定所述存在时长超过所述预设时长阈值的监控表项所对应的网络流为针对所述软件定义网络数据平面的隐蔽攻击流。

发明的有益效果

有益效果

[0017] 本发明通过预设的线性递增和增量模式的方式增加僵尸主机，通过所有僵尸主机向软件定义网络中预设的目标交换机发起数据平面的隐蔽性DDoS攻击，根据软件定义网络中所有交换机上流表的更新，对软件定义网络的控制器上预先构建的攻击流监控表进行同步更新，对攻击流监控表进行周期性检测，以确定攻击流监控表中是否有存在时长超过预设时长阈值的监控表项，当确定攻击流监控表中有该监控表项时，确定该监控表项对应的网络流为针对软件定义网络数据平面的隐蔽攻击流，从而通过线性递增与增量模式结合有效地提高了软件定义网络中数据平面隐蔽性DDoS攻击模拟的效率，通过控制器上攻击流监控表的构建、更新和检测实现数据平面隐蔽性DDoS攻击的检测，有效地避免了软件定义网络安全通道额外的通信开销，提高了数据平面隐蔽性DDoS攻击的检测效率。

对附图的简要说明

附图说明

[0018] 图1是本发明实施例一提供的软件定义网络的DDoS攻击模拟和攻击检测方法的实现流程图；

[0019] 图2是本发明实施例二提供的软件定义网络的DDoS攻击模拟和攻击检测装置的结构示意图。以及

[0020] 图3是本发明实施例二提供的软件定义网络的DDoS攻击模拟和攻击检测装置的优选结构示意图。

发明实施例

本发明的实施方式

[0021] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例

，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0022] 以下结合具体实施例对本发明的具体实现进行详细描述：

[0023] 实施例一：

[0024] 图1示出了本发明实施例一提供的软件定义网络的DDoS攻击模拟和攻击检测方法的实现流程，为了便于说明，仅示出了与本发明实施例相关的部分，详述如下：

[0025] 在步骤S101中，通过预设线性递增和增量模式的方式增加僵尸主机，通过所有僵尸主机向软件定义网络中预设的目标交换机发起数据平面的隐蔽性DDoS攻击。

[0026] 本发明实施例适用于软件定义网络数据平面的隐蔽性DDoS攻击的攻击模拟和攻击检测平台或系统，DDoS攻击即分布式拒绝服务攻击。在攻击模拟者向软件定义网络中的目标交换机发起数据平面的隐蔽性DDoS攻击时，先通过预设的线性递增方式多批次地增加僵尸主机的数量。在通过线性递增方式多批次增加僵尸主机的过程中，通过当前已有的僵尸主机按照软件定义网络的正常流速率向目标交换机发起攻击，在预设的攻击时间间隔后，再增加下一批次的僵尸主机。

[0027] 在本发明实施例中，在线性递增的同时检测目标交换机的流安装成功率，当流成功率低于预设的第一成功率阈值时，可认为目标交换机的流表即将达到饱和状态，此时停止僵尸主机的线性递增。接着，通过预设的增量模式方式增加僵尸主机数量（即一个一个地增加僵尸主机数量），同时通过这些僵尸主机按照正常流速率向目标交换机发起攻击，当检测到目标交换机的流安装成功率低于预设的第二成功率阈值时，可以认为目标交换机的流表已经达到饱和状态，即僵尸主机发送的网络流产出的流表项填满了流表，导致目标交换机无法为正常的网络流保存流表项进而无法响应正常的流请求，此时所有僵尸主机向目标交换机发起攻击的速率达到了最小攻击速率。

[0028] 具体地，流安装成功率为目标交换机的流表中成功安装的流表项占有需要安装流表项的比例。第一成功率为目标交换机的流表中流安装成功率的一个较低

阈值，第二成功率为目标交换机流表中流安装成功率的一个最低阈值，第一成功率和第二成功率可根据攻击模拟中对目标交换机流表饱和度的需要进行调整。最小攻击速率为僵尸主机以最小化的攻击速度使目标交换机的流表中的流表项趋近于流表总大小的饱和状态。

[0029] 作为示例地，在采用线性递增方式时，第一次增加一个僵尸主机，总共 $1 \times (1+1)/2$ 个僵尸主机，每个僵尸主机都以软件定义网络的正常流速率向目标交换机发起攻击，在攻击时间间隔过后，第二次增加两个僵尸主机，总共 $2 \times (2+1)/2$ 个僵尸主机。每次增加僵尸主机的数目都以线性递增的个数增加。

[0030] 在本发明实施例中，通过线性递增和增量模式方式有效提高了僵尸主机对目标交换机的攻击速度达到最小攻击速率的效率，满足攻击速度不超过最小攻击速度的DDoS攻击都具有隐蔽性，因此增加僵尸主机时的攻击和僵尸主机增加完毕后的攻击都具有攻击的隐蔽性特征。

[0031] 在步骤S102中，根据软件定义网络中所有交换机上流表的更新，对软件定义网络的控制器上预先构建的攻击流监控表进行更新同步。

[0032] 在本发明实施例中，为了避免软件定义网络中控制器（控制平面）和交换机（数据平面）之间的安全通道出现大量的流量负载问题，选择在控制器上进行数据平面隐蔽性DDoS攻击的检测，同时也可以充分利用软件定义网络中控制器的全局拓扑信息和动态编程等特点，因此预先在软件定义网络的控制器上构建攻击流监控表，为了便于区别，将攻击流监控表的表项称为监控表项。监控表的结构可包括交换机标识、流表项序列、流表项匹配域、流表项添加时刻以及流表项存在时长等，交换机标识用来标识流表项所在的交换机，流表项序列用来区别每个监控表项以及监控表项对应的流表项，流表项添加时刻为流表项被添加到流表中的时刻，流表项存在时长即流表项在流表中存在的时长，每个监控表项分别用来监控交换机上流表中对应的一个流表项，其中，交换机标识、流表项序列、流表项匹配域、流表项添加时刻都可通过交换机触发的Packet-in事件获得，流表项存在时长可通过当前时刻减去流表项添加时刻得到。

[0033] 优选地，为了在保持每个监控表项的唯一性、每个监控表项对应流表项的唯一性、且通过攻击流监控表可以在控制器上快速地检索到特定的网络流，将流表

项的cookie字段设置为监控流表项中的流表项序列。

[0034] 在本发明实施例中，控制器无法在检测前确定出目标交换机，因此通过攻击流监控表监控软件定义网络所有交换机上流表的更新。当软件定义网络中交换机接收到网络流、且交换机的流表中不存在该网络流对应的流表项时，交换机触发Packet-in事件，即发送Packet-in消息给控制器，由控制器做出决策，当控制器决定在交换机的流表中添加该网络流对应的流表项时，在攻击流监控表中添加该流表项对应的监控表项，即该网络流对应的监控表项。当网络流由于超过定时器时间idle_timeout被交换机删除或者交换机接收到删除命令将网络流删除并将该网络流对应的流表项删除时，触发Flow-removed事件，当控制器接收到Flow-removed消息时，将该流表项（或者该网络流）对应的监控表项删除，从而不需要实时或周期性地查询软件定义网络所有交换机上的所有流表，有效地提高了网络流监控的效率。

[0035] 在步骤S103中，对攻击流监控表进行周期性检测，以确定攻击流监控表中是否有存在时长超过预设时长阈值的监控表项。

[0036] 在本发明实施例中，对控制器上的攻击流监控表进行周期性地检测，确定攻击流监控表中是否存在流表项存在时长超过预设时长阈值的监控表项，即确定攻击流监控表中是否有存在时长超过该时长阈值的监控表项，也即确定流表中是否有存在时长超过该时长阈值的流表项。具体地，时长阈值可根据实验结果进行设置。

[0037] 在步骤S104中，当确定攻击流监控表中有存在时长超过时长阈值的监控表项时，确定存在时长超过时长阈值的监控表项所对应的网络流为针对软件定义网络数据平面的隐蔽攻击流。

[0038] 在本发明实施例中，当确定攻击流监控表中存在超时的监控表项时，可认为该监控表项对应的网络流为针对软件定义网络数据平面的隐蔽攻击流，通过该监控表项查找到该网络流，实现数据平面隐蔽性DDoS攻击的检测。

[0039] 在本发明实施例中，通过线性递增和增量模式方式增加僵尸主机，在成功模拟数据平面隐蔽性DDoS攻击同时，有效地加快了DDoS攻击速率达到最小攻击速度过程。通过在控制器上构建攻击流监控表实现在控制器上进行DDoS攻击检测

，并在攻击检测的过程中通过Packet-in事件和Flow-removed事件更新攻击流监控表，有效地避免攻击检测给交换机和控制器间的安全通道带来额外的通信开销，提高了数据平面隐蔽性DDoS攻击的检测效率。

[0040] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通程序来指令相关的硬件来完成，所述的程序可以存储于一计算机可读取存储介质中，所述的存储介质，如ROM/RAM、磁盘、光盘等。

[0041] 实施例二：

[0042] 图2示出了本发明实施例二提供的软件定义网络的DDoS攻击模拟和攻击检测装置的结构，为了便于说明，仅示出了与本发明实施例相关的部分，其中包括：

[0043] 攻击模拟模块21，用于通过预设线性递增和增量模式的方式增加僵尸主机，通过所有僵尸主机向软件定义网络中预设的目标交换机发起数据平面的隐蔽性DDoS攻击；

[0044] 表更新模块22，用于，根据软件定义网络中所有交换机上流表的更新，对软件定义网络的控制器上预先构建的攻击流监控表进行同步更新；

[0045] 超时检测模块23，用于对攻击流监控表进行周期性检测，以确定攻击流监控表中是否有存在时长超过预设时长阈值的监控表项；以及

[0046] 攻击流确定模块24，用于当攻击流监控表中有存在时长超过时长阈值的监控表项时，确定存在时长超过时长阈值的监控表项所对应的网络流为针对软件定义网络数据平面的隐蔽攻击流。

[0047] 优选地，如图3所示，攻击模拟模块21包括线性递增模块311、增量模式模块312和隐蔽性攻击模块313，其中：

[0048] 线性递增模块311，用于对僵尸主机的数目进行线性递增，当检测到目标交换机的流安装成功率低于预设第一成功率阈值时，停止对僵尸主机进行线性递增；

[0049] 增量模式模块312，用于对僵尸主机的数目进行增量递增，当检测到目标交换机的流安装成功率低于预设第二成功率阈值时，停止对僵尸主机进行增量递增；以及

[0050] 隐蔽性攻击模块313，用于根据所有的僵尸主机和软件定义网络的正常流速率

，以最小攻击速率向目标交换机发送网络流。

[0051] 进一步优选地，线性递增模块311包括递增攻击模块和递增停止模块，其中：

[0052] 攻击模块，用于根据线性递增的方式和预设的攻击时间间隔多批次地增加僵尸主机的数目，每批僵尸主机在出现后以正常流速率向目标交换机发起攻击；以及

[0053] 停止模块，用于通过控制器获取目标交换机的流安装成功率，当检测到流安装成功率低于第一成功率阈值时，确定流表趋于饱和，停止线性递增。

[0054] 优选地，表更新模块22包括监控表构建模块321、更新确定模块322和监控表更新模块323，其中：

[0055] 监控表构建模块321，用于预先在控制器上构建攻击流监控表，攻击流监控表的监控表项包括交换机标识、流表项序列、流表项匹配域、流表项添加时刻和流表项存在时长；

[0056] 更新确定模块322，用于根据所有交换机触发的Packet-in事件和Flow-removed事件，分别确定所有交换机的流表中添加的流表项和删除的流表项；以及

[0057] 监控表更新模块323，用于在攻击流检测表中添加该添加的流表项对应的监控表项和删除该删除的流表项对应的监控表项。

[0058] 优选地，超时检测模块23包括检测模块331和超时确定模块332，其中：

[0059] 检测模块331，用于对攻击流监控表进行周期性检测，以检测攻击流监控表中是否存在流表项存在时长超过时长阈值的监控表项；以及

[0060] 超时确定模块332，用于当存在流表项存在时长超过时长阈值的监控表项时，确定攻击流监控表中有存在时长超过时长阈值的监控表项。

[0061] 在本发明实施例中，通过线性递增和增量模式方式增加僵尸主机，在成功模拟数据平面隐蔽性DDoS攻击同时，有效地加快了DDoS攻击速率达到最小攻击速度过程。通过在控制器上构建攻击流监控表实现在控制器上进行DDoS攻击检测，并在攻击检测的过程中通过Packet-in事件和Flow-removed事件更新攻击流监控表，有效地避免攻击检测给交换机和控制器间的安全通道带来额外的通信开销，提高了数据平面隐蔽性DDoS攻击的检测效率。

[0062] 在本发明实施例中，软件定义网络的DDoS攻击模拟和攻击检测装置的各模块

可由相应的硬件或软件模块实现，各模块可以为独立的软、硬件模块，也可以分别集成为软件定义网络的DDoS攻击模拟系统和软件定义网络的系统上的一个软、硬件模块，在此不用以限制本发明。

[0063] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

权利要求书

- [权利要求 1] 一种软件定义网络的DDoS攻击模拟和攻击检测方法，其特征在于，所述方法包括下述步骤：
- 通过预设线性递增和增量模式的方式增加僵尸主机，通过所有僵尸主机向软件定义网络中预设的目标交换机发起数据平面的隐蔽性DDoS攻击；
- 根据所述软件定义网络中所有交换机上流表的更新，对所述软件定义网络的控制器上预先构建的攻击流监控表进行同步更新；
- 对所述攻击流监控表进行周期性检测，以确定所述攻击流监控表中是否有存在时长超过预设时长阈值的监控表项；
- 当所述攻击流监控表中有存在时长超过所述时长阈值的监控表项时，确定所述存在时长超过所述预设时长阈值的监控表项所对应的网络流为针对所述软件定义网络数据平面的隐蔽攻击流。
- [权利要求 2] 如权利要求1所述的方法，其特征在于，通过预设线性递增和增量模式的方式增加僵尸主机，通过所有僵尸主机向软件定义网络中预设的目标交换机发起数据平面的隐蔽性DDoS攻击的步骤，包括：
- 对所述僵尸主机的数目进行线性递增，当检测到所述目标交换机的流安装成功率低于预设第一成功率阈值时，停止对所述僵尸主机进行线性递增；
- 对所述僵尸主机的数目进行增量递增，当检测到所述目标交换机的流安装成功率低于预设第二成功率阈值时，停止对所述僵尸主机进行增量递增；
- 根据所有的僵尸主机和所述软件定义网络的正常流速率，以最小攻击速率向所述目标交换机发送网络流。
- [权利要求 3] 如权利要求2所述的方法，其特征在于，对所述僵尸主机的数目进行线性递增，当检测到所述目标交换机的流安装成功率低于预设第一成功率阈值时，停止对所述僵尸主机进行线性递增的步骤，包括：
- 根据所述线性递增的方式和预设攻击时间间隔多批次地增加所述僵尸

主机的数目，每批僵尸主机在出现后以所述正常流速率向所述目标交换机发起攻击；

通过所述控制器获取所述目标交换机的流安装成功率，当检测到所述流安装成功率低于所述第一成功率阈值时，确定所述流表趋于饱和，停止所述线性递增。

[权利要求 4] 如权利要求1所述的方法，其特征在于，根据所述软件定义网络中所有交换机上流表的更新，对所述软件定义网络的控制器上预先构建的攻击流监控表进行同步更新的步骤，包括：

预先在所述控制器上构建所述攻击流监控表，所述攻击流监控表的监控表项包括交换机标识、流表项序列、流表项匹配域、流表项添加时刻和流表项存在时长：

根据所述所有交换机触发的Packet-in事件和Flow-removed事件，分别确定所述所有交换机的流表中添加的流表项和删除的流表项；

在所述攻击流检测表中添加所述添加的流表项对应的监控表项和删除所述删除的流表项对应的监控表项。

[权利要求 5] 如权利要求1所述的方法，其特征在于，对所述攻击流监控表进行周期性检测，以确定所述攻击流监控表中是否有存在时长超过预设时长阈值的监控表项的步骤，包括：

对所述攻击流监控表进行周期性检测，以检测所述攻击流监控表中是否存在所述流表项存在时长超过所述时长阈值的监控表项；

当存在所述流表项存在时长超过所述时长阈值的监控表项时，确定所述攻击流监控表中有存在时长超过所述时长阈值的监控表项。

[权利要求 6] 一种软件定义网络的DDoS攻击模拟和攻击检测装置，其特征在于，所述装置包括：

攻击模拟模块，用于通过预设线性递增和增量模式的方式增加僵尸主机，通过所有僵尸主机向软件定义网络中预设的目标交换机发起数据平面的隐蔽性DDoS攻击；

表更新模块，用于根据所述软件定义网络中所有交换机上流表的更新

，对所述软件定义网络的控制器上预先构建的攻击流监控表进行同步更新；

超时检测模块，用于对所述攻击流监控表进行周期性检测，以确定所述攻击流监控表中是否有存在时长超过预设时长阈值的监控表项；以及

攻击流确定模块，用于当确定所述攻击流监控表中有存在时长超过所述时长阈值的监控表项时，确定所述存在时长超过所述预设时长阈值的监控表项所对应的网络流为针对所述软件定义网络数据平面的隐蔽攻击流。

[权利要求 7]

如权利要求6所述的装置，其特征在于，所述攻击模拟模块包括：

线性递增模块，用于对所述僵尸主机的数目进行线性递增，当检测到所述目标交换机的流安装成功率低于预设第一成功率阈值时，停止对所述僵尸主机进行线性递增；

增量模式模块，用于对所述僵尸主机的数目进行增量递增，当检测到所述目标交换机的流安装成功率低于预设第二成功率阈值时，停止对所述僵尸主机进行增量递增；以及

隐蔽性攻击模块，用于根据所有的僵尸主机和所述软件定义网络的正常流速率，以最小攻击速率向所述目标交换机发送网络流。

[权利要求 8]

如权利要求7所述的装置，其特征在于，所述线性递增模块包括：

递增攻击模块，用于根据所述线性递增的方式和预设的攻击时间间隔多批次地增加所述僵尸主机的数目，每批僵尸主机在出现后以所述正常流速率向所述目标交换机发起攻击；以及

递增停止模块，用于通过所述控制器获取所述目标交换机的流安装成功率，当检测到所述流安装成功率低于所述第一成功率阈值时，确定所述流表趋于饱和，停止所述线性递增。

[权利要求 9]

如权利要求6所述的装置，其特征在于，所述表更新模块包括：

监控表构建模块，用于预先在所述控制器上构建所述攻击流监控表，所述攻击流监控表的监控表项包括交换机标识、流表项序列、流表项

匹配域、流表项添加时刻和流表项存在时长；

更新确定模块，用于根据所述所有交换机触发的Packet-in事件和Flow-removed事件，分别确定所述所有交换机的流表中添加的流表项和删除的流表项；以及

监控表更新模块，用于在所述攻击流检测表中添加所述添加的流表项对应的监控表项和删除所述删除的流表项对应的监控表项。

[权利要求 10]

如权利要求6所述的装置，其特征在于，所述超时检测模块包括：

检测模块，用于对所述攻击流监控表进行周期性检测，以检测所述攻击流监控表中是否存在所述流表项存在时长超过所述时长阈值的监控表项；以及

超时确定模块，用于当存在所述流表项存在时长超过所述时长阈值的监控表项时，确定所述攻击流监控表中有存在时长超过所述时长阈值的监控表项。

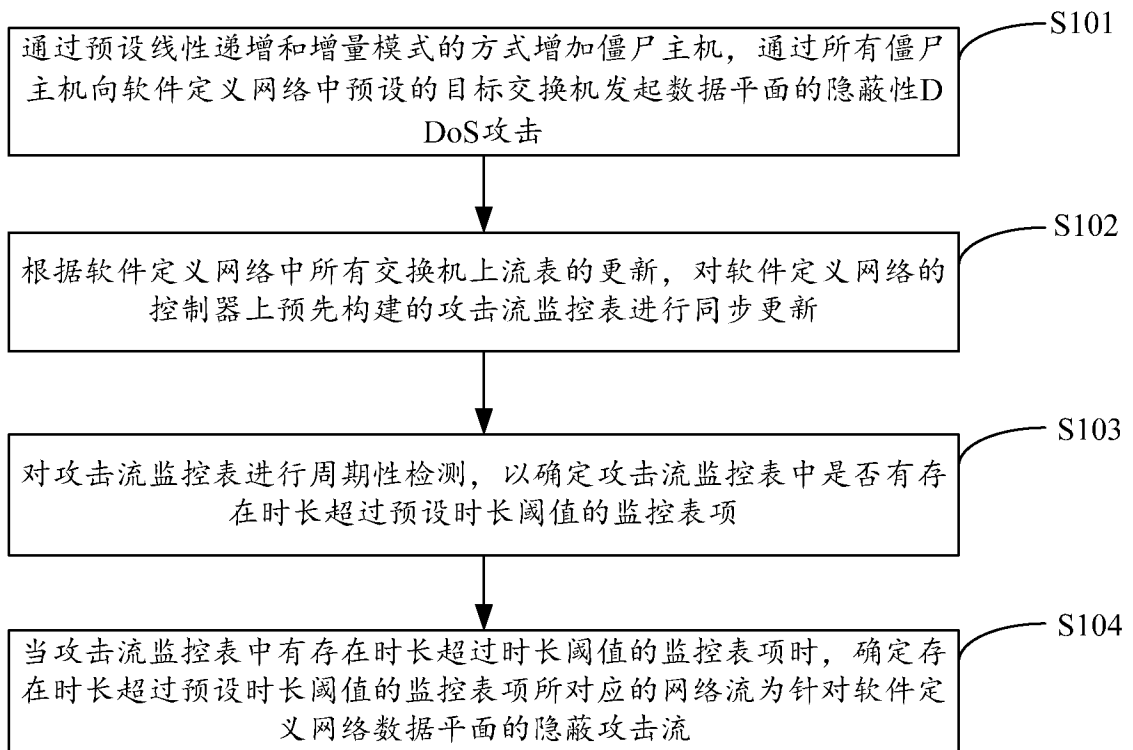


图 1

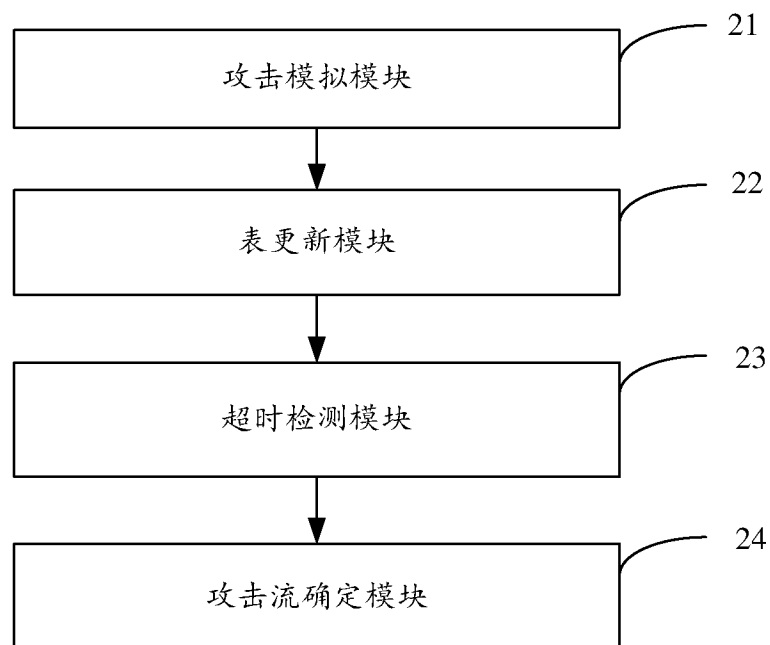


图 2

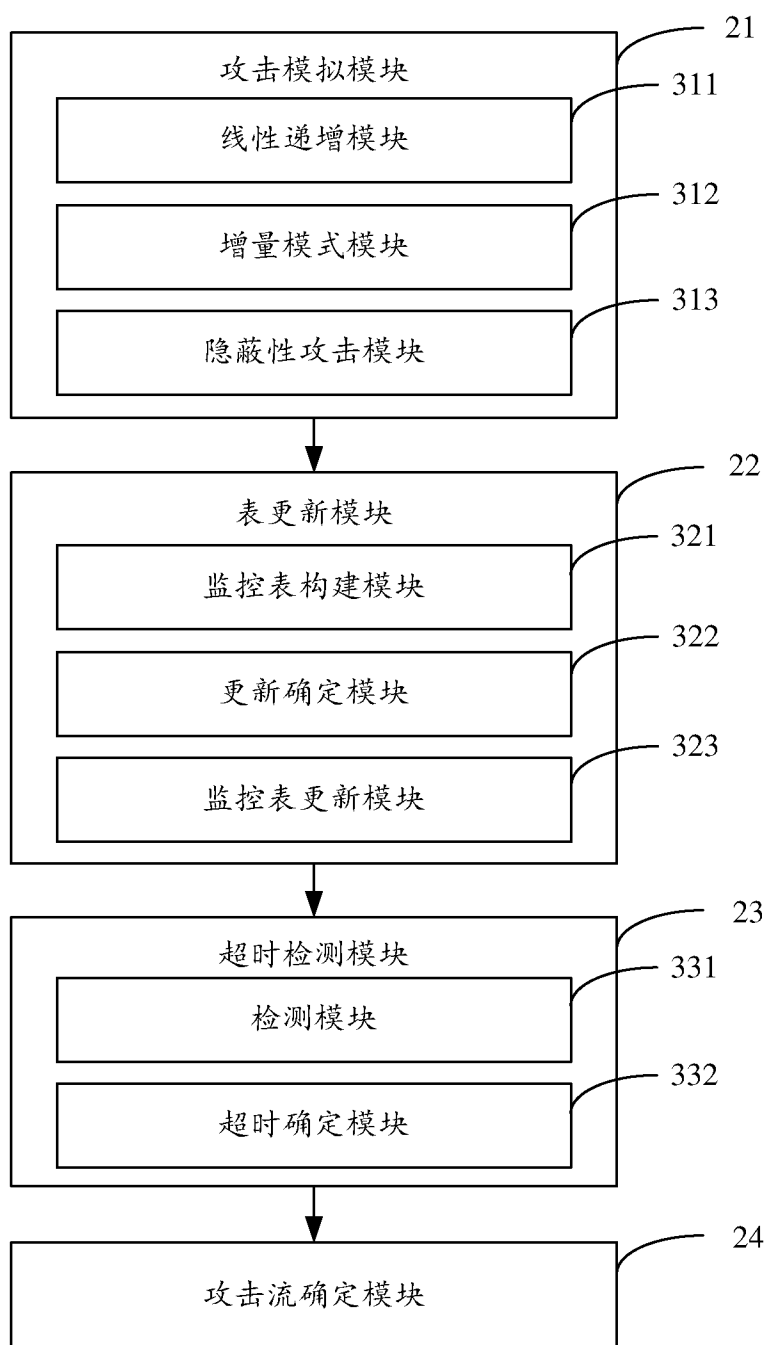


图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/088934

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

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: 软件定义网络, 僵尸, 傀儡, 分布式拒绝服务, 攻击, 模拟, 仿真, 检测, 线性, 增长, 增加, 递增, 增量, software defined network+, SDN, bot?, botnet?, distributed denial of service, DDoS, attack+, simulat+, detect+, linear+, increas+, grow+, incremental

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 105554041 A (JIANGSU SANLENG ZHIHUWULIAN DEVELOPMENT CO., LTD. et al.), 04 May 2016 (04.05.2016), description, paragraphs [0031]-[0044]	1-10
Y	CN 105791220 A (CHINA TELECOM CORPORATION LIMITED), 20 July 2016 (20.07.2016), description, paragraphs [0061]-[0080]	1-10
A	WO 2015030977 A1 (A10 NETWORKS, INC.), 05 March 2015 (05.03.2015), entire document	1-10

☐ 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 08 January 2018	Date of mailing of the international search report 26 January 2018
Name and mailing address of the ISA 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 CHENG, Jiali Telephone No. (86-10) 53961625

International application No.
PCT/CN2017/088934

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

国际检索报告

国际申请号

PCT/CN2017/088934

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

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: 软件定义网络, 僵尸, 傀儡, 分布式拒绝服务, 攻击, 模拟, 仿真, 检测, 线性, 增长, 增加, 递增, 增量, software defined network+, SDN, bot?, botnet?, distributed denial of service, DDoS, attack+, simulat+, detect+, linear+, increas+, grow+, incremental

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
Y	CN 105554041 A (江苏三棱智慧物联发展股份有限公司等) 2016年 5月 4日 (2016 - 05 - 04) 说明书第[0031]-[0044]段	1-10
Y	CN 105791220 A (中国电信股份有限公司) 2016年 7月 20日 (2016 - 07 - 20) 说明书第[0061]-[0080]段	1-10
A	WO 2015030977 A1 (A10 NETWORKS, INC.) 2015年 3月 5日 (2015 - 03 - 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

“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

2018年 1月 8日

国际检索报告邮寄日期

2018年 1月 26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

授权官员

程佳丽

电话号码 (86-10) 53961625

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/088934

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	105554041	A	2016年 5月 4日	无			
CN	105791220	A	2016年 7月 20日	无			
WO	2015030977	A1	2015年 3月 5日	US	2015058977	A1	2015年 2月 26日
				US	2016134655	A1	2016年 5月 12日