

面向链路洪泛攻击的多维检测与动态防御方法

王洋, 汤光明, 雷程, 韩冬

(信息工程大学, 河南 郑州 450001)

摘要: 针对现有链路洪泛攻击检测存在的不足, 提出了多维指标检测算法, 通过会话连接时长、数据分组低速比例、数据分组距离均匀性、平均低速率数据分组占比、低速数据分组占比变化率 5 维要素对存在异常的转发链路进行多维检测, 改善了现有方法误报率高的情况。进一步, 提出基于染色理论的“控制器-交换机”动态部署方法, 解决了现有防御缓解机制存在的“难以实际部署在交换机变体类型受限的实际环境中”问题。最后, 实验验证所提方法的有效性。

关键词: 链路洪泛攻击; 多维检测; 动态部署; 软件定义网络

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019040

Multidimensional detection and dynamic defense method for link flooding attack

WANG Yang, TANG Guangming, LEI Cheng, HAN Dong

Information Engineering University, Zhengzhou 450001, China

Abstract: Aiming at the shortcomings of the existing link flooding attack defense methods, a multi-dimensional index detection algorithm is proposed, which performs multi-dimensional detection on the abnormal forwarding links through the five-dimensional elements of connection length, low-speed ratio of data packets, uniformity of data packet distance, average low-speed ratio of data packets, and change rate of low-speed ratio of data packets, thus effectively solving the problem of high false alarm rate of the existing detection methods. Furthermore, a controller-switch dynamic deployment method based on coloring theory is proposed, which solves the problem of difficult to be actually deployed in the actual environment with limited switch variant types existing in the existing defense mitigation mechanisms. Experimental analysis show the feasibility of the proposed method.

Key words: link flood attack, multidimensional detection, dynamic deployment, software defined network

收稿日期: 2019-03-15; 修回日期: 2019-04-28

通信作者: 王洋, 1046149075@qq.com

基金项目: 国家自然科学基金资助项目 (No.61601517)

Foundation Item: The National Natural Science Foundation of China (No.61601517)

论文引用格式: 王洋, 汤光明, 雷程, 等. 面向链路洪泛攻击的多维检测与动态防御方法[J]. 网络与信息安全学报, 2019, 5(4): 80-90.

WANG Y, TANG G M, LEI C, et al. Multidimensional detection and dynamic defense method for link flooding attack[J]. Chinese Journal of Network and Information Security, 2019, 5(4): 80-90.

1 引言

在信息时代,网络应用与服务日渐渗入人们生活的方方面面,如电子政务、在线金融、网络购物等。互联网规模的迅速扩张、网络应用的急剧增加,要求网络架构有更高的可靠性、扩展性、开放性、灵活性和管控性。软件定义网络(SDN, software defined network)应运而生,是满足上述互联网需求的新型网络架构^[1]。其核心思想在于通过数据与控制平面的分离,借助统一、厂商无关的控制与数据平面开放接口构建和呈现逻辑的全网视图,完成网络分片和底层网络的虚拟化,从而为形式各异的网络应用提供灵活的承载服务。

在人们对网络的依赖不断增强的同时,黑客能从中获取的利益也越来越大,他们在利益驱使下不断进行网络渗透、信息窃取及捣毁等各类网络攻击,对军队、企业乃至国家造成严重威胁。随着攻击技术不断更新,链路洪泛攻击(LFA, link flooding attack)作为一种新型的间接式DDoS(distributed denial of service)攻击,一经提出就引起了社会各界的广泛关注。不同于传统DDoS攻击以消耗目标服务器资源为目的,链路洪泛攻击旨在泛洪特定网络链路,阻止用户访问某个重要网络服务,间接破坏依赖这些链路的网络服务。链路洪泛攻击的实施策略相比普通DDoS攻击更加复杂且隐蔽性更高,其使用合法流量或低速流量对目标链路实施攻击,使网络防御机制无法进行有效应对。该种攻击可阻断SDN数据层中关键服务节点与其他端节点的连通关系,从而造成关键服务节点无法提供服务的结果,从而间接达到破坏数据层服务的目的。

为了有效检测链路洪泛攻击并缓解它所带来的影响,本文提出了一种面向链路洪泛攻击的多维检测与基于染色理论的“控制器-交换机”动态

部署方法。通过多维指标实现对链路洪泛攻击的敏感发现与准确定位,从而提高检测链路洪泛攻击的准确性;同时,利用染色理论实现对异构交换机的高效部署,在异构交换机类型有限的条件下最大限度提高SDN网络的不确定性,以此提高链路防洪攻击的难度。

2 相关工作

目前,有两类主流的链路洪泛攻击。Studer等^[2]首次提出一种名为“The coremelt attack”的链路洪泛攻击,给出了coremelt攻击的一般原理与过程,更进一步地,Kang等^[3]首次提出一种名为“The crossfire attack”的链路洪泛攻击,给出了crossfire攻击的一般原理与过程。针对链路洪泛攻击的检测与防御,学者做了大量探索,取得了一定成果。Xue等^[4]提出LinkScope架构,该架构由拓扑分析模块、非合作路径测量模块、侦测引擎和定位模块组成。能持续测量目标区域路径的分组丢失率、往返时间(RTT, round trip time)、连接失败率等参数监控是否出现异常,一旦发现路径性能下降,则采用端到端逐跳技术捕获异常链路来检测链路洪泛攻击,并向用户发出攻击告警和诊断信息。Lee等^[5]在自治域层面研究了crossfire攻击,强调了自治域之间的协同合作对最终防御效果的影响,同时使用修改后的路由器,可将低速攻击流从合法流量中检测出来,保护合法流量。Kang等^[6]使用SDN流量工程,临时增加目标链路的逻辑带宽,迫使攻击者增加攻击成本,从而使攻击隐蔽性减弱。Kim等^[7]提出软件定义蜜罐技术,引诱Traceroute数据分组进入蜜网,这样攻击者收集的是通往蜜网的链路,保护真正的网络服务链路不被攻击者探测到。国内学者刘世辉等^[8]提出一种名为LFA Defender的链路洪泛攻击防御架构,利用SDN全局视图、流回溯功能以及网络虚拟化的弹性部署特性检测和缓解

链路洪泛攻击。针对低速链路洪泛攻击流不易从背景流量中识别出来的难题, Misra 等^[9]调查了几种强化学习算法在挖掘攻击行为时空特征方面的性能, 最终发现自编码卷积神经网络和长短期记忆网络在检测处于预热期的链路洪泛攻击时有较好表现。Liaskos 等^[10]提出一种新型架构, 从攻防双方的角度对分布式链路洪泛攻击 Crossfire 和 Coremelt 进行数学建模与分析, 基于深度学习提出一种轻量级的检测程序, 并将其与现有的流量工程模型结合, 最后通过统计学分析指出网络拓扑学能够影响攻击检测的效率。Aydeger 等^[11]提出一种基于 SDN 的移动目标防御技术来缓解链路洪泛攻击, 利用 SDN 控制层拥有网络全局视野的能力分析 traceroute 分组转发行为, 提前锁定潜在目标链路, 并不断变换数据分组传输路径避开潜在的目标链路。Liaskos 等^[12]则将攻防双方交互的行为模型进行描述, 通过严谨的数学证明指出拓扑学的运用能够影响 Crossfire 攻击的检测效率, 分析一个拓扑中潜在的攻击目标并提供全局式的直接检测算法。Crossfire 攻击因其不依赖于僵尸主机所处位置信息, 在攻击发起前可以灵活指定不同的链路集合以达到避免引起警报的目的, 相比于 Coremelt 攻击更具威胁性。因此本文主要研究 Crossfire 型链路洪泛攻击。

针对以上分析可知: 1) 由于链路泛洪具有隐蔽的特性, 现有研究中防御检测的指标较为单一, 造成现有检测方法无法准确分析存在的威胁并定位存在异常的链路, 易出现较高的漏报率或误报率; 2) 由于 SDN 中交换机类型变体的数量有限, 现有研究中防御机制的部署需要丰富的资源, 因此现有防御方法难以实际部署在交换机变体类型受限的真实环境中。

3 整体架构设计

面向链路洪泛攻击的多维检测与动态部署方

法整体架构如图 1 所示, 它由链路监听模块、多维检测模块和动态部署模块 3 部分组成, 具体如下。

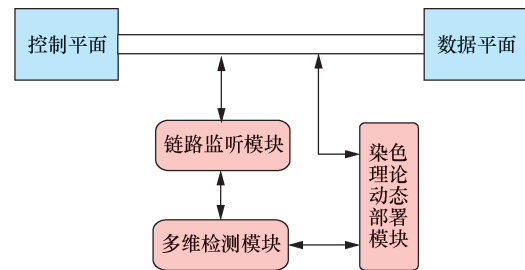


图 1 面向链路洪泛攻击的多维检测与动态部署方法整体架构

1) 链路监听模块直接连接到数据平面与控制平面之间的链路, 它将一直检测链路并感知可能存在的链路拥塞, 一旦发现拥塞出现, 则将预警信息发送给多维检测模块。

2) 多维检测模块在接收到预警信息后, 首先对发生拥塞的链路进行定位和判断, 若发生拥塞的链路存在构成闭合环路的可能, 则对发生拥塞的链路进行检测。由于链路洪泛攻击具有攻击数据速率低、攻击源高度分布式等特性, 因此多维检测模块在利用基于阈值的 ICMP 超时报文检测的基础上, 依据设计的多维指标检测算法, 通过会话连接时长、数据分组低速比例、数据分组距离均匀性、平均低速率数据分组占比、低速数据分组占比变化率 5 维要素对存在异常的转发链路进行多维检测。当多维检测模块检测到链路洪泛攻击后, 将检测信息发送给动态部署模块。

3) 染色理论动态部署模块在接收到多维检测模块发送的检测信息后对控制器-交换机的连接关系进行迁移。与此同时, 为提高 SDN 的安全性, 动态部署模块充分发挥异构控制器的优势, 利用基于染色原理的动态部署算法最大化防御的有效性。首先根据染色分布模型推导出染色分布算法, 然后利用染色分布算法对交换机的多变体进行节点“着色”, 最后将变体分发至 SDN 转发节点。

4 多维指标检测方法

Crossfire 攻击被认为是目前最具技巧的 DDoS 攻击，因为它利用数以千计的僵尸节点，且每个僵尸节点都发送低速率攻击流以模仿正常用户。然而，尽管这些攻击流可以绕过各种基于行为的检测方法，但正是由于攻击者从数以千计的僵尸节点向目标节点或者诱骗主机发起了数百万的追踪探测器，导致其独一无二的网络空间探测行为。在侦测阶段，攻击者通过每个僵尸主机向目的节点（目标节点或者诱骗服务器）发送多个追踪探测报文。每个僵尸主机通过向所有目标节点发送探测报文来获取其可以利用的目标节点和诱骗服务器间的共享链路。这个过程有 2 个鲜明特征的行为：

1) 数以千计的探测报文在某个时间段从相同的源节点发送出来；

2) 每个目的节点将在一段时间内被数以千计的端用户（僵尸节点）探测。

由于正常用户同样会追踪服务器，并且网络空间管理员也将追踪作为诊断工具，因此，区分正常用户与恶意敌手的关键在于：正常用户不会发送大量的探测报文给目的节点，并且不会发送大量的探测报文。管理员所用的源节点可以被剔除，因为其发送的探测报文是源于可信的 IP 地址。

令 R 是所有从源节点收集的探测报文，其中每个从源节点 $o_j \in O$ 到目的节点 $c_k \in C_{dst}$ 的探测报文表示为 $r_m \in R$ 。由于这个探测报文会被源节点组件 $c_l \in C_{src}$ 接收，所以总可以追踪源-目标节点对 $u_i = \langle c_l, c_k \rangle$ 的路径 p_i 。此外， R_{oj} 表示所有从僵尸源节点 o_j 发出的探测报文， R_{ck} 则表示所有到达目标节点 $c_k \in C_{dst}$ 的探测报文。相似地， $|R'_{oj}|$ 和 $|R'_{ck}|$ 表示在时间窗口为 t 的源探测报文频率和目的报文频率。设定一个可改变的探测时间

窗口，用 $|R_{oj}|$ 和 $|R_{ck}|$ 表示频率。

由此可知，可计算获得僵尸探测目的节点的报文为 O_{ck} ， $|O_{ck}|$ 则表示其数量。目标组件 c_k 的数量可通过下式计算。

$$O_{ck} = \{\forall o_j \in O, R_{oj} \cap R_{ck} \neq \emptyset\}$$

假设总有一个正常周期，该周期内只有正常用户的探测行为。在这个时间内，网络空间管理员可以计算正常探测的频率，从而作为以上参数的阈值。在本文的探测技术中，正常阈值计算如下。

1) 源探测频率阈值：计算最大和最小源探测频率，并将两者在多日内的偏差作为平均标准探测偏差，记作 T^{diff} 。

2) 目的探测频率阈值：计算每个小时内目的节点收到的最大探测数量，并将该值在连续多日内的平均值作为阈值，记作 T_{dest} 。

如果在任意一个小时内，其平均值超过了 T^{diff} 的两倍，则可以判定该探测行为是不正常的，且它可能是一个侦测攻击。下一个阈值用来判断哪个目标节点被攻击者探测。所有被判定进行侦测的僵尸节点用户将在现有情况或者未来检测中被 SDN 控制器认定是僵尸。

在此基础上，利用前文所述方法，通过会话长度（CL, connection length）、数据分组低速比例（LPR, low packet rate）、数据分组距离均匀性（PDU, packet distance uniformity）、平均低速率数据分组占比（LMPR, low mean packet rate）、低速数据分组占比变化率（LPRV, low packet rate variance）5 维要素对存在异常的转发链路进行多维检测，从而提高检测的准确性，具体如下。

1) 会话长度：在链路洪泛攻击中，恶意敌手通过增加会话的持续时间，从而达到占用链路带宽的目的，因此会话长度是测量会话持续时间的最基本方法。

2) 数据分组低速比例：数据分组速率是指第

一个数据分组到达目标服务器的时间间隔。由于链路洪泛攻击为了增加隐蔽性，其发送的数据分组具有低速率的特性。另外，正常用户为了提高服务质量，通常保持一定的传输速率。因此，数据分组中的低速比率可以作为衡量该会话是否为链路洪泛攻击的关键。

3) 数据分组距离均匀性：数据分组距离是指数据分组之间的时间间隔。由于实际网络中网络资源的利用率不同，正常用户数据分组的距离各不相同；然而链路洪泛攻击的数据分组由于是通过攻击脚本刻意发出的，因此数据分组的距离是相同的。为了减少检测所需的负载，检测过程中仅考虑连续 3 个数据分组的距离，即 2 个连续分组之间的分组距离。

4) 平均低速率数据分组占比：实践表明，与正常用户相比，链路洪泛攻击发起的会话连接平均速率更高，因此它可以作为评判指标之一。

5) 低速数据分组占比变化率：与正常用户相比，链路洪泛攻击的数据分组是定期生成的，且其平均数据分组速率更为一致，因此它的低速数据分组占比变化率更小。

由于以上的检测指标是在网络层上进行的分析，因此其计算复杂度和存储需求较小，可以实

现在 SDN 中的检测分析。

5 基于染色理论的动态部署算法

为了增加恶意敌手再次发起攻击的难度，在选取重新构建拓扑时，本文试图通过部署异构交换机增加网络的动态性。而染色理论的优势在于，随着时间推移，染色体会发生突变和组合，形成多元染色体，从而提高 SDN 的安全性。

在 SDN 中，控制器通常按照分域结构进行部署，每个域内网络由独立的一个或者一组控制器负责管理，该控制器（组）负责该子网交换机的管理、流表推送等。核心控制器（组）负责管理各个域内的控制器。需要指出的是，当按照控制器组进行管理时，组内仅有一个 Master 控制器，当该控制器出现故障时，组内按照选举算法选取出下一个 Master 控制器接管网络。因此，为了简化描述，后续按照一个域内仅有一个控制器进行描述，如图 2(a)所示。

由于 SDN 具有资源有限的特性，因此首要问题是解决如何利用有限的异构交换机实现最优动态部署，最大化交换机的多样性。以此提高链路洪泛攻击的难度。

若将网络表示为有向图 $G=(V,E)$ ，其中顶点

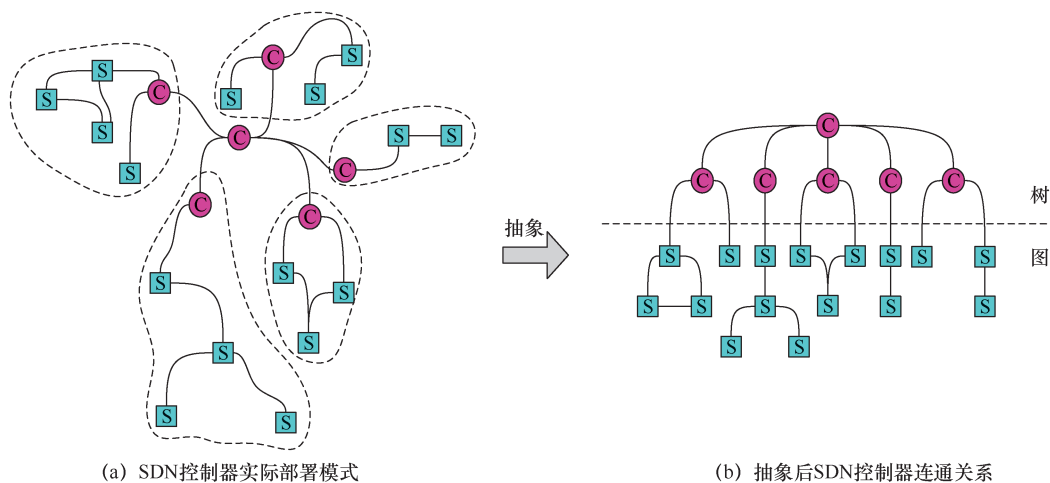


图 2 SDN 网络节点抽象

为 V ，有向边为 E 。图 G 的子图表示为 $G'=(V',E')$ ，其中 $E'=\{(w_1,w_2)|(w_1,w_2)\in E, w_1\in V', w_2\in V'\}$ ，对于图中的节点 $w\in G$ ，用 $d(w)$ 表示该节点的度，即图 G 中与 w 相邻的节点数， $d_{V'}(w)$ 表示子图中与 w 相邻的节点数。

G 的染色分布是一种映射，该映射满足相邻节点分布不同颜色，即 $f:V\rightarrow\{1,2,\dots,k\}$ ，且 $f(u)=f(v)$ 时， $(u,v)\notin E$ 。其中， $\chi(G)$ 表示对图 G 进行染色时需要的颜色种类。

染色分布模型作用于图结构中的节点，因此需要对 SDN 进行图形化抽象。图 2(a)所示为简化 SDN，由控制器 (C) 和交换机 (S) 组成，其中，控制器按照分域结构连接，交换机按照图结构连接。因此，映射到如图 2(b)所示的抽象结果，控

制器则是树形结构，交换机仍然是图结构。本文的染色模型是指交换机染色模型。

由图 2 可知，SDN 中交换机节点连接符合连通图结构，但由于 SDN 中该类型节点数目较大，因此需要提取该连通图的关节点，即满足：在删除顶点 v 以及和 v 相关联的各边之后，将图的一个连通分量分割成 2 个或 2 个以上。本文用图的深度优先遍历算法完成关节点选取。

用 $G_s=(V_s,E_s)$ 表示控制器组成的拓扑图，用 V_s 和 E_s 分别表示 SDN 中交换机节点和交换机之间的连接，定义数组 $dfs[v]$ ($v\in V_s$) 为深度优先搜索遍历连通图时访问顶点 v 的次序号，引入 $low()$ 函数，该函数满足如下条件。

$$low(v) = \text{Min} \left\{ \begin{array}{l} dfs[v], low[w], dfs[k] \end{array} \right\} \left\{ \begin{array}{l} w \text{ 是顶点 } v \text{ 在深度优先生成树上的子节点} \\ k \text{ 是顶点 } v \text{ 在深度优先生成树上由回边连接的父节点} \\ (v,w) \in E_s \\ (v,k) \in E_s \end{array} \right.$$

若某个顶点 v ，存在子节点 w 且 $low[w] \geq dfs[v]$ ，则该顶点 v 必为关节点。通过关节点将交换机组成的子图 E_s 再次划分为 $\{E_{s1}, E_{s2}, E_{s3}, \dots, E_{sn}\}$ ，假设每个子图仅有一个关节点 w_{sk} ($w_{sk} \in Arti(E_{sk}), k \in \{1, 2, 3, \dots, n\}$)，此时由交换机组成的子图的染色原则为

$$\left. \begin{array}{l} w_{sk} \in Arti(E_{sk}) \\ w_{sr} \in \{E_{sk} - Arti(E_{sk})\} \end{array} \right\} \Rightarrow f(w_{sk}) \neq f(w_{sr})$$

即关节点的染色与该子图内的其他节点不同。

在对 SDN 控制器和交换机节点进行染色时，由于控制器和交换机构成的拓扑类型不同，因此算法需要首先从网络拓扑图中提取控制器和交换机的拓扑图，然后采用不同的染色算法。算法 1 为控制器和交换机子图提取算法 Topology Abstract，该算法利用图的广度优先算法遍历网络拓扑图，在遍历过程中分别提取控制器和交换机

子图。

算法 1 控制器和交换机子图提取算法

TopologyAbstract

输入 邻接表 G 表示的网络拓扑结构图

$G=(V,E)$ ，其中， $N=|V|$

输出 存储交换机子图 G_s

Process:

1) initialization

for ($v=0; v<G.vexnum; ++v$) then

visited[v]=FALSE

end for

InitQueue(Q)

InitGraph(G_s)// G_s 存储交换机子图

2) //使用广度优先算法分别构建交换机组成的子图

for ($v=0; v<G.vexnum; ++v$) then

```

if (!visited[v]) then
    visited[v]=TRUE
    TopologyExtract(v)
    EnQueue(Q,v)
    while (!QueueEmpty(Q))
        DeQueue(Q,u)
        for (w=FirstAdjVex(G,u); w ≥ 0;
w=NextAdjVex(G,u,w)) then
            if (!visited[w]) then
                visited[w]=TRUE
                TopologyExtract(v)
                EnQueue(Q,w)
            end if
        end for
    end if
end for
end if
end void

```

算法 2 为染色分布算法, 使用深度优先算法对交换机子图进行遍历, 遍历过程中对关节点进行判定, 按照交换机染色分布模型进行染色。

算法 2 染色分布算法 ColorAssignment

输入 存储交换机子图 G_s

输出 存储控制器染色分布结果的数组 $X[i](0 \leq i \leq N-1)$ 和存储交换机染色结果的数组 $Y[i](0 \leq i \leq N-1)$

Process:

1) initialization

$X[0 \dots N-1] \leftarrow 0$

$Y[0 \dots N-1] \leftarrow 0$

```

 $Z[0 \dots N-1] \leftarrow 0$  // 存储关节点位置
count = 1
visited[0]=1
for (i=1; i <  $G_s.vexnum$ ; ++i) then
    visited[i]=0
end for
2) switchColor( $G_s$ )
3) exit
4) void switchColor( $G_s$ )
     $p = G_s.vertices[0].firstarc$ 
     $v = p \rightarrow adjvex$ 
    DFSArticul( $G_s, v$ ) // 从第 v 个顶点出发深度优先查找关节点
if (count <  $G_s.vexnum$ ) then
         $Z[G_s.vertices[0]] = G_s.color$  // 根节点是关节点
        while ( $p \rightarrow nextarc$ )
             $p = p \rightarrow nextarc$ 
             $v = p \rightarrow adjvex$ 
            if (visited[v] == 0) then
                DFSArticul( $p, v$ )
            end if
        end while
    end if
end void
5) void DFSArticul( $G, v$ )
    visited[v] = min = ++count
    for ( $p = G.vertices[v].firstarc$ ; p;  $p = p \rightarrow nextarc$ )
then
         $w = p \rightarrow adjvex$ 
        if (visited[w] == 0) then
            DFSArticul( $G, w$ );
            if (low[w] < min) then
                min = low[w]
            end if
        end if
    end for

```

```

if (low[w] ≥ visited[v]) then
    Z[Gs.vertices[v]] = Gs.color // 关
节点染色相同
else then
    Z[Gs.vertices[v]] =
(Gs.color+1)%colors // colors
end if
end if
end for
low[v] = min
end void

```

对于给定的 SDN 拓扑图, 算法 1 和算法 2 首先执行 TopologyAbstract, 该部分主要是完成染色前的预处理过程, 通过图的广度优先遍历算法遍历拓扑中的所有节点。如果是交换机, 则将其加入交换机拓扑图 G_s 中。在此基础上, 执行 ColorAssignment 算法, 该算法完成具体的节点染色过程, 对于交换机拓扑图 G_s , 由于其呈无向图结构, 因此按照图的深度优先遍历算法查找图中所有的关节点, 保证关节点与非关节点染上不同颜色即可满足交换机染色分布模型。此外, 由于交换机拓扑图中可能不存在连通分量为 1 的关节点, 但是必然存在连通分量为 r (r 为大于 1 的自然数) 的关节点, 因此可以修改算法 DFSArticul(), 使其完成查询连通分量为 r 的关节点。

6 实验环境与结果

本文使用交换机多变体仿真和攻击模拟对所提出的面向链路洪泛攻击的多维检测与动态部署方法的防御能力进行测试。其中, 实验测试主要分为链路洪泛攻击检测实验和防御缓解实验。

6.1 实验环境构建

实验环境基于 Mininet 仿真平台, 网络拓扑结构如图 3 所示, 其中, 12 个实心点 (大) 表示 Ryu 控制器, 100 个实心点 (小) 表示 OVS 交换

机, 实线表示控制器之间的连接, 虚线表示交换机与控制器以及交换机之间的连接。交换机使用 OVS v2.5 及其变体, 控制器与交换机均安装在 Ubuntu14.04 虚拟机中。

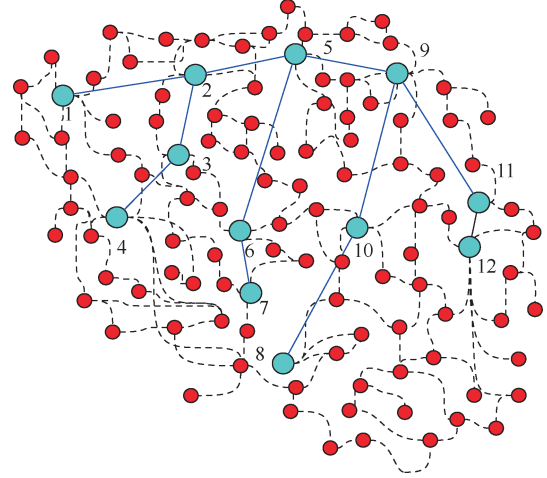


图 3 网络拓扑结构

实验中使用的控制器为 Ryu, 交换机为 Open vSwitch (OVS), 其中, 交换机通过多变体仿真实现多变体异构。选择 Ryu 作为控制器一方面是由于 Ryu 基于 Python 模块化开发, 完全开源并且结构相对简单, 与 ODL (OpenDaylight)、Floodlight 和 ONOS 相比, 更容易获取和进行二次开发; 另一方面是 Ryu 支持北向 REST API 的自定义。选择 OVS 主要是由于其相对容易通过二级映射表的方式实现多变体构造。二级映射表实现多变体的原理如图 4 所示, 对于交换机, 通过映射表完成自定义配置转发命令与 OVS 配置转发命令的映射。由于 SDN 交换机仅根据控制器下发的配置转发命令完成数据分组的转发, 不具备传统交换机路由学习、最小值支撑树计算等能力, 因此构建不同的映射表即可完成交换机多变体的构建。

在实验中, 首先利用本文提出的染色分布模型提取图 3 中的网络拓扑结构, 使用 5 号节点作为整个网络的主控制器, 与该控制器直接相连的控制器组成其子节点, 依次进行。拓扑提取完成

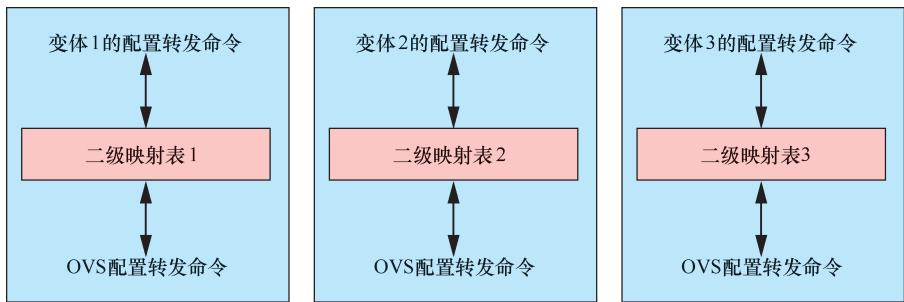


图 4 交换机多变量仿真原理

后按照 ColorAssignment 算法进行节点染色,部署不同交换机变体。交换机节点中预先安装存在缓冲区溢出漏洞的程序,恶意敌手由与 1 号节点相连接的主机 A 发出链路洪泛攻击,然后使用主机 B 探测当前网络的网络时延情况,判断控制器受链路洪泛攻击的影响程度。测试过程执行 50 次,取各次测试的均值作为最终结果,测试结果与分析如下。

6.2 实验结果与分析

(1) 多维指标检测结果与分析

如表 1 所示,现有方法主要采用 Renyi 熵实现对链路洪泛攻击的检测^[13]。由于 Renyi 熵具有较高的敏锐性,因此该方法在正确率达到 94.75% 的同时,误报率达到 7.19%。这说明检测结果中存在“正常用户被误认为是链路洪泛攻击”的概率。本文设计的多维指标检测算法则在正确率达到 98.58% 的同时极大地降低了误报率,相较现有检测方法降低 81.78%。究其原因在于多维指标检测方法通过会话连接时长、数据分组低速比例、数据分组距离均匀性、平均低速率数据分组占比、低速数据分组占比变化率 5 个维度可能被误判的正常用户行为进行过滤,从而有效提高检测的准确率。

(2) 链路洪泛攻击缓解结果与分析

通过对比以下 3 种部署策略下会话访问时延来分析不同方法抵御链路洪泛攻击的能力:
① 采用相同交换机进行部署;② 采用随机分

布算法部署交换机变体;③ 采用染色分布算法部署交换机变体。实验结果如图 5 所示,通过对比分析可知,在采用相同交换机的网络中,网络时延(单位毫秒)在 15 min 后会持续增大,并最终导致全网络出现拒绝服务现象;在采用随机分布算法部署交换机变体的方法中,网络时延在 30 min 后逐渐增加,且当攻击时间持续到 40 min 后,网络时延进一步增加;使用染色分布模型的 SDN 在遭到链路洪泛攻击时增加的网络时延最小,虽然在 30 min 后网络时延逐渐增加,但是相较于传统网络和采用随机分布算法部署变体的方法,网络时延增加较小,且在遭到攻击后仍能够继续提供服务。另外,图 6 所示为 $\chi(G)$ 与抵御链路洪泛攻击的关系,从图中可知,当 $\chi(G) > 2$ 时,继续增大 $\chi(G)$,抵御链路洪泛攻击的能力降低不大。

表 1 链路洪泛攻击检测结果

算法	正确率	漏报率	误报率
现有检测算法	94.75%	3.43%	7.19%
多维指标检测算法	98.58%	0.69%	1.31%

(3) 性能测试

性能测试的目的是确定本文提出的方法对控制器、交换机的 CPU 和内存开销的影响,以及对网络建立和故障恢复所需时长的影响。性能测试结果如表 2 所示。① 使用面向链路洪泛攻击的多维检测与动态部署方法后控制器、交换机的平均

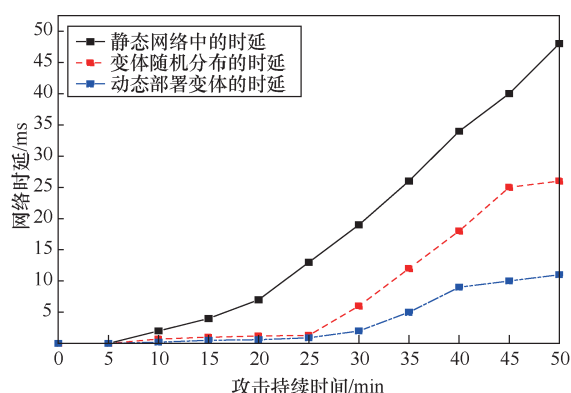


图5 变体分布与抵御链路洪泛攻击的关系

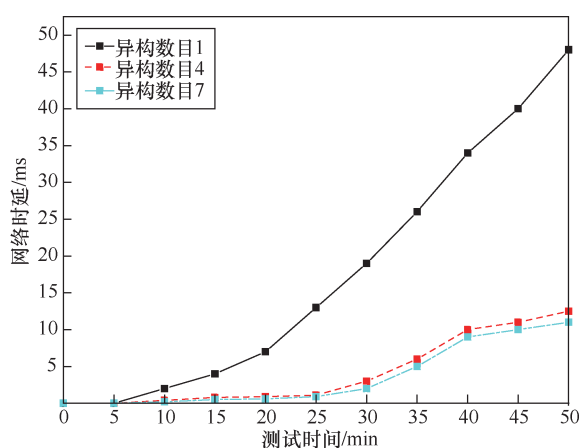


图6 变体数目与链路洪泛攻击的关系

CPU 和内存开销均增大,这主要是由于控制器需要对网络链路进行多维检测、交换机需要实时处理并存储二级映射表的映射关系产生额外开销。由于 SDN 控制器和交换机通常部署在 X86 架构廉价设备中,因此对 CPU 和内存的开销可以相对容易地通过扩容和扩频等方式解决。② 网络建立的平均时长和故障恢复的平均时长增大同样是由于该方法需要检测链路洪泛攻击、生成变体部署结果。但是由于网络建立和故障恢复出现的频率较低,因此对网络的整体性能影响不大。③ 该方

法对网络平均时延影响较小。

7 结束语

本文提出了一种面向链路洪泛攻击的多维检测到与动态防御部署方法,针对现有检测方法检测维度单一导致的误报率高的问题,提出了一种多维指标检测算法,通过会话连接时长、数据分组低速比例、数据分组距离均匀性、平均低速率数据分组占比、低速数据分组占比变化率 5 维要素对存在异常的转发链路进行多维检测,从而提高检测的准确性。针对现有防御缓解机制存在的“难以实际部署在交换机变体类型受限的真实环境中”问题,运用染色理论在异构交换机类型有限的前提下最大化网络的异构多样性,从而有效提高对链路洪泛攻击的抵御能力。实验结果表明,该方法可以在少量增加网络负载的前提下有效降低链路洪泛攻击的成功率。

参考文献:

- [1] 谭磊,张红旗,雷程,等.面向SDN的移动目标防御技术研究进展[J].网络与信息安全学报,2018,4(7):5-16.
TAN J L, ZHANG H Q, LEI C, et al. Research progress on moving target defense or SDN[J]. Chinese journal of Network and Information Security, 2018, 4(7): 5-16.
- [2] STUDER A, PERRIG A. The coremlt attack[C]//European Symposium on Research in Computer Security (ESORICS). 2009: 37-52.
- [3] KANG M S, LEE S B. The crossfire attack[C]//IEEE Security and Privacy symposium (SP). 2013: 127-141.
- [4] XUE L, LUO Z, CHAN W, et al. Towards detecting target link flooding attack[C]//USENIX Conference. 2014: 81-96.
- [5] LEE S B, KANG M S, GLIGOR V D. CoDef: collaborative defense against large-scale link-flooding attacks[C]//ACM CoNEXT.

表2

性能测试结果

方法	控制器 CPU 平均开销	控制器内存 平均开销	交换机 CPU 平均开销	交换机内存 平均开销	网络建立 平均时长/s	网络平均 延迟/ms	故障恢复 平均时长/s
使用本文方法	29.9%	38.2%	38.2%	40.3%	131	754	247
未使用本文方法	25.3%	30.7%	22.7%	31.6%	9	681	169

2013: 417-428.

- [6] KANG M S, GLIGOR V D, SEKAR V, et al. SPIFFY: inducing cost-detectability tradeoffs for persistent link-flooding attacks[C]// Network and Distributed System Security Symposium. 2016.
- [7] KIM J, SHIN S. Software-defined honeynet: towards mitigating link flooding attacks[C]//IEEE/IFIP International Conference on Dependable Systems and Networks Workshop, IEEE Computer Society. 2017:99-100.
- [8] 刘世辉. 基于 SDN 和 NFV 的链路洪泛攻击检测与防御[D]. 武汉: 武汉大学, 2017.
LIU S H. Detecting and mitigating target link-flooding attacks using SDN and NFV[D]. Wuhan: Wuhan University, 2017.
- [9] MISRA S, TAN M, REZAZAD M, et al. Early detection of cross-fire attacks using deep learning[C]//2017 Deep Learning Security Workshop. 2017.
- [10] LIASKOS C, KOTRONIS V, DIMITROPOULOS X. A novel framework for modeling and mitigating distributed link flooding attacks[C]//IEEE International Conference on Computer Communications. 2016.
- [11] AYDEGER A, SAPUTRO N, AKKAYA K, et al. Mitigating cross-fire attacks using SDN-based moving target defense[C]//IEEE Local Computer Networks. 2016: 627-630.
- [12] LIASKOS C, IOANNIDIS S. Network topology effects on the detectability of crossfire attacks[J]. IEEE Transactions on Information Forensics & Security, 2018, (99): 1-1.
- [13] 蔡佳晔, 张红旗, 宋佳良. 基于 Renyi 熵的 Openflow 信道链路洪泛攻击主动防御方法[J]. 计算机应用研究, 2019, 36(6): 1767-1770.
CAI J Y, ZHANG H Q, SONG J L. Active defense method of OpenFlow channel link flooding attack based on Renyi entropy[J]. Application Research of Computers, 2019, 36(6):1767-1770.

[作者简介]



王洋（1985—），女，陕西西安人，信息工程大学博士生，主要研究方向为网络与信息安全。



汤光明（1963—），女，湖南常德人，信息工程大学教授、博士生导师，主要研究方向为网络与信息安全、信息安全管理、信息隐藏。



雷程（1989—），男，北京人，信息工程大学博士生，主要研究方向为移动目标防御、网络流安全交换。



韩冬（1983—），男，陕西蒲城人，信息工程大学讲师，主要研究方向为网络与信息安全。