基于 SDN 架构缓解 DDoS 攻击的方案设计

谢 康 唐宾徽

四川大学锦城学院 计算机与软件学院 四川 成都 610000

【摘 要】SDN 是一种新型的网络架构，将网络分离成管理平面和转发平面，简化了网络配置并减少了维护成本。DDoS 攻击是一种实施简单、攻击性强的网络攻击手段，在 SDN 环境下尚缺乏有效的应对措施。本文提出一种基于 SDN 架构的 DDoS 攻击的缓解方案。首先简述了相关概念与技术，然后提出利用熵值检测和 K-Means 算法分类流量，最后处理攻击流量，达到缓解 DDoS 攻击对 SDN 环境的影响。

【关键词】SDN; DDoS 攻击; K-Means

引言

如今，遭到 DDoS 攻击的网络环境愈加广泛，由于其发起简单且难以被精准检测，常作为侵入者的攻击手段。有 DDoS 攻击出现时，使得 OpenFlow 交换机的流表区溢出，耗尽控制器资源，最终就会使得网络崩溃。

软件定义网络（SDN），独立出控制器收集和管理网络状态信息，实现了网络集中管理和控制，但如果 SDN 控制器受到 DDoS 攻击，会导致控制器和底层交换机通信失败，致使整个网络瘫痪。本文提供了基于 SDN 架构的 DDoS 攻击的缓解方案，使用广义熵值检测异常流量和 K-Means 算法进行流量聚类，最后 SDN 控制器下发指令，处理攻击流量。提高了对攻击流量的检测率和 SDN 的防御能力。

1 相关工作

1.1 DDoS 攻击简介

拒绝服务攻击（DoS）的集群攻击形式就是 DDoS 攻击。将众多分散的主机组成僵尸网络，集中向某一特定目标发起拒绝服务攻击，导致链路拥塞、业务中断等影响。它的目的就是控制用户主机，使其受到损失或威胁他人。

1.2DDoS 攻击的原理及危害

1. 网络层的 DDoS 攻击特点：

利用 TCP/IP 协议的某些特征，通过控制众多的低性能主机形成僵尸网络，向服务器恶意发送大量的数据包，使得服务器资源饱和，正常的业务申请不可应答。

2. 应用层的 DDoS 攻击特点：

模拟正常数据包的格式和真实的 IP 地址，规避了基于匹配特征以及回溯源端口的检测方法，攻击者伪装成合法用户向攻击目标发送大量合理请求，例如下载大型文件，要求对复杂数据进行处理等，使得资源损耗。

当出现 DDoS 攻击时，往往会出现以下特征：

受害主机上有许多的处于半连接的 TCP 请求；伪造源 IP，发出无效的大流量数据，造成网络过载，阻隔正常的网络通信；利用受害主机上存在弊端的传输协议，迅速发出重复的服务申请，使得正常连接请求无法得到处理。

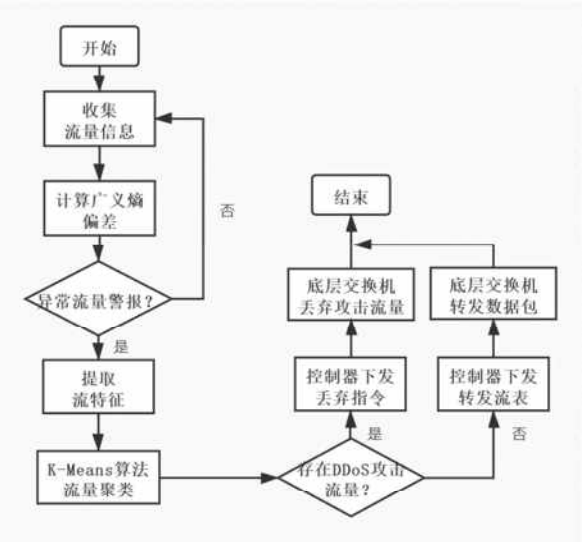
1.3 已知的防御方法

在 SDN 网络架构下，DDoS 攻击的检测方案已有相当成熟的研究成果。例如：

1. 通过信息熵判断攻击流量。梅梦喆等人提出多维条件熵的检测方法，通过计算多个流表项的条件熵值，提取多维向量进行攻击判断[1]。Robinson 等人采用连续窗口的方式推算信息熵误差，有效控制了误报率。但通过信息熵监测 DDoS 攻击存在局限，阈值的设定和网络状态相关，出现网络波动时，熵值的变化较大，会影响检测的准确性。

2. 通过机器学习算法进行攻击检测。N.Meti 等人通过比较在 SDN 控制器上采用 SVM、贝叶斯以及神经网络方法检测 DDoS 攻击，验证了机器学习算法可以在 SDN 架构下进行攻击流量判别。肖甫等人提出基于 KNN 算法通过模块化分布以细化检测流程、提升检测精度，但在样本数高的情况下会增加误报率[2]。以上文献中的方法利用了 SDN 控制器的集中管控功能，但控制器上处理过多数据，在大型网络中，会明显增加控制器的资源开销和攻击检测的延迟，甚至可能还未检测出攻击流量，SDN 控制器便已经不堪重负。

2 SDN 环境下 DDoS 攻击缓解方案设计



2.1DDoS 攻击流量检测流程

SDN 控制器定期从底层交换机收集流量信息，计算熵值，若发生异常流量警报时，先提取流特征，进而调用 K-means 算法对流量进行分类，判断是否存在攻击流量。最后对攻击流量进行处理，达到缓解 SDN 环境中 DDoS 攻击的目的。

2.2 基于熵值检测

熵，泛指某些物质系统状态的度量和可能出现的程度。在信息论中，信息熵作为系统随机程度的一种度量，信息变量的确定性越高，熵值越低；系统的信息分布越发散，熵值越高。

发生 DDoS 攻击时，攻击者会向受害主机发出大量数据包，导致网络系统的随机性下降，使得熵值减小，所以，可利用熵值检测是否存在 DDoS 攻击，信息熵的计算公式可表示为：

$$H = -K\sum_{i=1}^{w} p_i \log_2 p_i$$

其中，表示为概率空间的全部样本，为单窗口中的样本量，为相关单位的常数， 表示某样本出现概率。

相对于信息熵，信息熵的广义形式，在高概率事件的情况下，产生的影响更明显，有利于确定合适的阈值，提高检测的准确率[3]。所以，本文选取广义熵来进行流量监测，其计算公式为：

$$H_a = \frac{1}{1-a}\log_2\left(\sum_{i=1}^{w} p_i^a\right)$$

2.2.1 熵值检测思想

SDN 环境中，底层交换机用流表存储转发规则。从流表项中提取源 IP、目的 IP、数据包数量以及 IP 协议作为一个信息组。

1. 设定每收集 n 个数据包，对信息组进行一次熵值计算。根据网络状态，选择适当的阈值 Y。

2. 设定检测相连的 5 个窗口，单窗口的数据包为 40 个，计算每次的熵值，当熵值 H 均小于阈值 Y 时，说明网络中可能存在攻击流量。

虽然通过熵值可判断网络中是否存在异常流量，但是在正常情况下仍存在造成网络随机性降低的事件。因此，当系统出现熵值异常警报时，进一步调用 K-Means 算法进行流量分类，准确筛选攻击流量。

2.3 流特征提取

将流特征提取模块布署于 SDN 控制器上。设定时间间隔为 4s，收集底层交换设备的流量信息。

由于 DDoS 攻击通常只包含一个数据包，字节长度比正常流量大，且数据包抵达的间隙非常短。因此，选取 4 个流特征作为攻击流量检测模块的输入：数据包数量、数据包抵达的时间间隙、字节长度和数据包平均尺寸[4]。

2.4 基于 K-Means 的 DDoS 攻击流量检测

K-Means 算法是一种无监督学习中的聚类处理算法，主要通过迭代求解，进一步聚类所有样本点，结束条件：簇划分的样本点都向所在簇的质心向量收敛，误差和平方局部最小。直到各簇的中心点稳定时，得到收敛的正常流量和攻击流量的簇。

2.4.1K-Means 算法聚类过程

2.4.1、K-Means 算法聚类过程

设定处理的样本集 $D=\{x_1,x_2,\ldots,x_m\}$，迭代次数上限为 N，簇树个数为 K。聚类后的簇数 $C=\{C_1,C_2,\ldots,C_k\}$。

从样本集 D 中随机挑选 k 个对象作为初始聚类中心，即质心向量：

$\mu_j=\{\mu_1,\mu_2,\ldots,\mu_k\}$。

对所有的样本点进行 N 次迭代：

1. 先将划分的簇 C 初始化为：$C_j=\varnothing, j=1,2,\ldots,k$。

2. 计算样本 x_i 和各个质心向量 μ_j 之间的距离：$d_{ij}=x_i-\mu_{i2}^2$，

3. 将 x_i 标记为 d_{ij} 最小时所对应的簇 C_{x_i}，$C_{x_i}=C_{x_i}\cup\{x_i\}$，

4. 对 C_j 中的全部数据再次计算每个聚类中心，即更新质心向量：$\mu_j=\frac{1}{|C_j|}\sum_{x\in C_j}x$，

5. 在这 k 个簇中，要求误差平方和足够小，即每个簇的质心和该簇的样本点的距离最近，计算公式为：$SSE=\sum_{i=1}^{k}\sum_{x\in D}x-\mu_j^2$，

6. 当迭代程度符合结束条件或迭代次数达到上限时，输出簇划分 $C=\{C_1,C_2,\ldots,C_k\}$

3 DDoS 攻击流量的处理

通过以上的流分类后，最后进行攻击流量的处理，减小网络受到 DDoS 攻击的危害和概率。

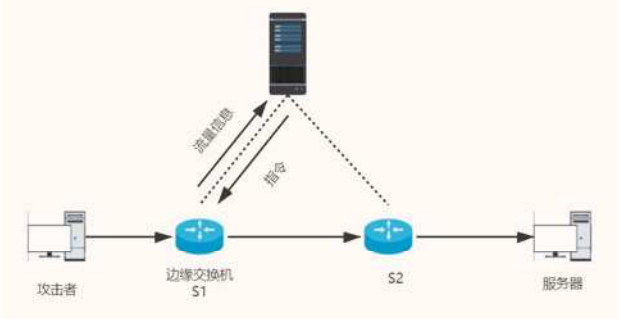
在 SDN 架构中，可以通过 OpenFlow 交换机流表将攻击流量进行引导到安全的虚拟设备或 SDN 控制器下发丢弃指令到交换机，丢弃攻击流量[5]。

攻击流量处理步骤：

1. 当攻击者对服务器发起 DDoS 攻击时，数据包到达该网络中的边界交换机 S1，通过查询是否存在匹配该流标签的流表项，若存在则直接进行转发；

2. 若不存在该流表项，将该流量信息上传至 SDN 控制器，由控制器通过 DDoS 攻击流量检测算法判断是否是 DDoS 攻击流量；

3. 若不是攻击流量，则下发含路由信息的流表，使交换机转发该数据流量；



4. 否则，SDN 控制器发送丢弃指令给底层交换机，交换机将丢弃该攻击流量，同时，可以发送命令到防火墙进行攻击流量的阻隔，例如：修改请求超时参数或者屏蔽该 IP 地址段等，避免 DDoS 攻击流量危害网络环境。

4 结语

DDoS 攻击作为一种低成本、高危害的网络攻击手段，在 SDN 环境下，尚且缺乏有效的应对措施。通过广义熵检测，判断异常流量，利用 K-Means 算法将流量准确分类，可以有效地筛选攻击流量。最后，对攻击流量进行处理，可直接减小 DDoS 攻击对 SDN 环境的危害。但随着网络的发展，DDoS 攻击仍在迅速演化，使得针对于 DDoS 攻击的防御方案逐渐失效。如何阻止 DDoS 攻击的入侵，有效防御 DDoS 攻击，仍需要不断地技术革新，提升网络环境的安全性。

【参考文献】

[1] 梅梦喆. SDN 中基于多维条件熵的 DDoS 攻击检测与防护研究 [D]. 南昌航空大学 ,2016.

[2] 肖甫 , 马俊青 , 黄洵松 , 王汝传 .SDN 环境下基于 KNN 的 DDoS 攻击检测方法 [J]. 南京邮电大学学报 (自然科学版),2015,35(01):84-88.

[3] 刘振鹏 , 贺玉鹏 , 王文胜 , 张彬 .SDN 环境下的 DDoS 攻击检测方案 [J]. 武汉大学学报 (理学版),2019,65(02):178-184.

[4] 马乐乐. SDN 环境下的 DDoS 攻击检测与防御方法研究 [D]. 安徽大学 ,2019.

[5] 王文蔚 , 肖军弼 , 程鹏 , 张悦 . 基于 SDN 的 DDoS 攻击防御系统 [J]. 计算机与现代化 ,2021(02):117-121+126.