基于软件定义网络的粗粒度 DDoS 攻击检测方案

汪　哲
中国移动通信集团重庆有限公司 重庆 401120

【摘　要】DDoS 攻击是现代网络架构上的一种常见攻击方式，其威胁不断加剧，并且攻击手段不断演变和复杂化，因此需要研究更加有效的检测和防御方案。随着软件定义网络技术的发展和应用，软件定义网络已经成为网络架构的主流趋势之一，同时也为网络安全提供了新的思路和解决方案。传统的 DDoS 防御方案主要基于硬件设备和静态规则，无法及时响应攻击变化，并且需要大量的人工干预和管理，因此需要研究更加智能和灵活的防御方案。本文通过实验证明了在使用 Mininet 模拟 SDN 网络的环境中，使用条件熵粗粒度检测方案可准确检测出 DDoS 攻击。

【关键词】软件定义网络；DDoS 攻击；检测方案

1.DDoS 攻击流量的识别和防御

控制器通过 SDN 架构中的协议，实时获取所有交换机上的流量信息，对流量进行监测和统计分析。控制器将分析获取的流量进行分类，例如区分正常的流量和异常的 DDoS 攻击流量。控制器识别出攻击流量后，在硬件交换机上进行转发规则的安装，从而仅将正常的流量发送到网络云。控制器会设定一种或多种与流量有关的阈值，例如交换机端口的带宽使用率、接收/发送速率等等，当这些阀值被超过时抛出警戒，触发对攻击流量的拦截措施。控制器可以向 SDN 交换机发送控制指令，对流量进行处理和控制。

2.条件熵粗粒度检测方法

DDoS 攻击主要以占用有限资源而导致目标主机或网络拒绝服务。此类资源可以是硬件资源，例如有限的存储器和网络带宽。当 DDoS 攻击发生时，可导致计算机系统崩溃、带宽耗尽、硬盘被填满等，从而导致拒绝服务。DDoS 攻击也可以是数据资源，例如服务器的 TCP 最大连接数。当服务器与正常客户端维持的 TCP 连接数达到最大值时，将不再接收新的客户请求，以保证当前所有连接的服务质量。粗粒度检测-条件熵检测模块的主要优点是可以在短时间内对网络流量进行初步筛选，同时对攻击流量和正常流量的准确率都有较高的保证。本文使用 WIDE 实验室数据集作为正常流量，使用林肯实验室 DARPA1999 数据集、CIC- DDoS2019 数据集作为攻击流量。但因为该模块只考虑了简单而较为直接的特征值，难以对高度复杂的攻击流量进行较为精确的检测，因此它通常被用作 DDoS 攻击检测系统中的辅助模块。在本次实验中经过研究发现当 W＝200 能体现出所使用数据集的变化情况。

3.选择有效的流量特征

在软件定义网络的 DDoS 攻击检测中，H(Sip|Dip)用于选择有效的流量特征来区分正常流量和 DDoS 攻击流量。H(Sip|Dip)表示在已知目的 IP 地址（Dip）的情况下，源 IP 地址（Sip）的熵值，即在 Dip 条件下 Sip 的不确定性。在 SDN 的 DDoS 攻击检测中，使用 H(Sip|Dip)的原因是因为攻击者通常使用伪造的源 IP 地址进行攻击，H(Sip|Dip)可以很好地衡量 DDoS 攻击流量的熵值，从而更好地区分正常流量和 DDoS 攻击流量。H(Sip|Dport)用于选择有效的流量特征来区分正常流量和 DDoS 攻击流量。在 SDN 的 DDoS 攻击检测中，攻击者通常会将攻击流量发送到目标 IP 地址上的某些特定端口，而在这些端口上接收到大量的目标 IP 地址的数据流，其数据如下图所示。计算 H(Sip|Dport)可以衡量流量数据中 Sip 在 Dport 条件下的变化程度，因此可以帮助 SDN 系统检测和区分 DDoS 攻击流量。H(Dport|Dip)的计算可以帮助 SDN 系统判断攻击流量是否使用了随机的端口号，如果攻击者使用的端口随机，那么 Dport 值将会是相对均匀的分布，即熵值较高。如果攻击者使用的是固定的端口号，那么对于特定的目标 IP 地址，Dport 值的分布将会是不均匀的，即熵值较低。

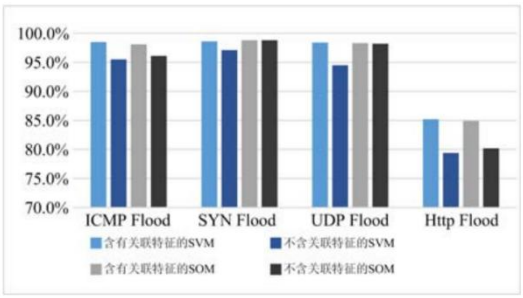

图 1 攻击检测率

4.阈值的选择方式

在 SDN 的 DDoS 攻击检测中，我们通常使用某些特征作为指标来区分正常流量和攻击流量。然而，由于网络环境的复杂性和攻击者的多样性，这些特征在不同场

景和情境下的表现可能会有所不同。因此在确定特征阈值时，需要进行一定的统计分析。在 SDN 环境中，控制器在处理 Packet_in 数据帧时，会首先检查这个警告标志 Flag，以确定是否需要采取相应措施。如果警告标志 Flag 被置位，那么说明这个数据包已经在交换机中发生了问题，例如匹配不上流表项或发生了缓存溢出等。此时，控制器需要对这个数据包进行深入的处理。如果警告标志 Flag 未被置位，则说明这个数据包与交换机的流表项匹配成功，或者交换机并没有相关的流表项。此时，控制器可以直接将这个数据包转发给目的主机，或者根据需要新增流表项等。

5.结语

SDN 架构的优点包括动态可控、集中式管理、可编程性强、易于实现自动化管理和智能功能的开发等。在检测方面，为了提高模型的精度，采用软件定义网络进行特征提取，最后利用支持向量机 SVM 作为分类器以检测攻击。该方法可以有效提高攻击检测率，降低误报率，而且通过模拟的监控页面也可以非常方便地观察网络的安全状态。

【参考文献】

[1]张朝昆,崔勇,唐骞祎,等.软件定义网络(SDN)研究进展[J].软件学报,2015,26(1):62-81.

[2]徐玉华,孙知信. 软件定义网络中的异常流量检测研究进展[J].软件学报,2020,31(1):182-207.XUYH.