doi:10.11835/j.issn.1000.582X.2023.07.001

SDN中基于条件熵和决策树的DDoS攻击检测方法

傅　友,邹东升
(重庆大学 计算机学院,重庆 400044)

摘要:软件定义网络(software defined network,SDN)作为一种新型网络架构,其转控分离及集中控制的架构思想为网络带来了显著的灵活性,同时为感知全局网络状态提供了便利。分布式拒绝服务攻击(distributed denial of service,DDoS)是一种典型的网络攻击方式。针对SDN网络中进行DDoS攻击检测的问题,提出了一种基于条件熵和决策树的DDoS攻击检测方法,利用条件熵判断当前网络状态,通过分析SDN中DDoS攻击特点,提取用于流量检测的6项重要特征,使用C4.5决策树算法进行网络流量分类,实现对SDN中的DDoS攻击的检测。实验表明,相比于其它研究方法,文中提出的方法不仅具有较高检测精确率和召回率,而且明显缩短了检测时间。

关键词:软件定义网络;分布式拒绝服务攻击;条件熵;C4.5决策树
中图分类号:TP393　　**文献标志码:**A　　**文章编号:**1000-582X(2023)07-001-08

A DDoS attack detection method based on conditional entropy and decision tree in SDN

FU You, ZOU Dongsheng
(College of Computer Science, Chongqing University, Chongqing 400044, P. R. China)

Abstract: Software defined network (SDN), as a novel network architecture, introduces significant flexibility through the ideas including separation between forwarding and controlling and centralized control. It also facilitates the global awareness of the network status. Distributed denial of service (DDoS) is a typical attack method. This paper focuses on the problem DDoS attack detection in SDN and proposes a DDoS attack detection method based on conditional entropy and decision tree. The proposed method used conditional entropy to evaluate the current network status. It analyzed the characteristics of DDoS attacks in SDN and extracted six key features for traffic detection. The C4.5 decision tree algorithm was utilized to classify network traffic and achieved DDoS attack detection in SDN. Experimental results show that the method presented in this paper exhibits superior detection precision and recall to other research methods. Additionally, it can significantly reduce the detection time.

Keywords: software defined network; distributed denial of service; conditional entropy; C4.5 decision tree

收稿日期:2022-03-12
基金项目:国家自然科学基金资助项目(61309013)。
Supported by National Natural Science Foundation of China (61309013).
作者简介:傅友(1997—),男,硕士研究生,主要从事软件定义网络、网络安全方向研究,(E-mail)2438368267@qq.com。

SDN[1]作为一种新型网络架构,利用转发与控制分离以及集中控制的思想有效解决了传统网络架构下系统封闭、配置繁琐、演化拓展困难等问题。SDN控制器一般通过OpenFlow协议[2]下发流量转发规则至交换机,可获取交换机流表信息,因此,SDN控制器可感知全局网络状态,判断SDN网络中发生DDoS攻击的可能性。DDoS[3]是当前互联网面临的主要安全威胁之一,也是SDN中典型的安全问题。DDoS攻击消耗大量被攻击服务器、数据链路或网络设备等资源,使其无法提供正常网络服务。SDN网络中面临的DDoS攻击除传统攻击方式外,还存在针对SDN架构特定的DDoS攻击方式,包括数据层DDoS攻击[4]和控制层DDoS攻击[5-6]。

目前,SDN网络中DDoS攻击检测主要基于统计分析和机器学习方法。统计分析方法中信息熵、信息距离及相关系数等概念用于计算流量序列的随机性及序列之间的相关程度,配合阈值分析检测当前网络流量。Tao等[7]提出基于香农熵和Sibson距离[8]的两步式DDoS检测方法,该方法能够有效检测和区分DDoS攻击和闪拥事件。Bhatia等[9]提出一套基于广义熵和广义信息距离的信息熵(φ-熵)和信息散度(φ-距离)。在此基础上,Behal等[10]提出运用φ-熵和φ-距离检测DDoS攻击和闪拥事件,该方法具有更优的数据敏感性和算法收敛速度。在基于统计分析的检测方法中,通过分析流量的统计信息并结合阈值判断DDoS攻击行为。研究表明,该类方法通常具有较低的检测时间,但难以保证检测准确率。

机器学习方法对数据具有更强的表征能力,通过机器学习算法构建流量分类或聚类模型实现DDoS攻击检测。Santos等[11]详细讨论了在SDN网络中各类机器学习算法的DDoS检测能力。Braga等[12]利用SDN控制器集中管控的特点,提出基于六项特征的自组织神经网络(self-organizing maps , SOM)算法,但由于SOM网络神经元的排列方式较为固定,对检测实时性造成了影响。Yang等[13]提出利用支持向量机(support vector machine , SVM)对网络流量进行分类,并通过设定的八项特征进行DDoS攻击检测。实验表明,该检测方法具有较高准确率,由于SVM中复杂矩阵运算,同样带来较高的时间开销。Liu等[14]提出基于熵和BP神经网络的DDoS检测方法,通过边缘交换机上的熵值检测算法进行预检测,控制器提取六项特征作为神经网络的输入,利用粒子群算法优化BP神经网络的参数,最后进行DDoS攻击检测。在基于机器学习的检测方法中,通过分析DDoS攻击特点,提取相应流量特征并结合机器学习算法进行DDoS检测。在流量特征合适的情况下,该类方法能够保证较高的检测准确率,但复杂的算法也带来较高的时间开销。文中提出一种SDN网络中基于条件熵和决策树的DDoS检测方法。利用条件熵分析判断当前网络状态,提取DDoS攻击特征,使用决策树分类模型实现DDoS攻击检测。

1 背景介绍

1.1 条件熵

信息熵用于度量随机变量的不确定性,在数学领域中,信息熵定义为信息量的期望。随机变量的不确定性越强,熵值越大。

假定,随机变量X,取值集合为$X=\{x_1,x_2,...,x_n\}$,每个取值概率分布为$P=\{p_1,p_2,...,p_n\}$,其中,$\sum_{i=1}^{n}p_i=1$,$0\leqslant p_i\leqslant 1, i\in(1,...,n)$,随机变量$X$的信息熵为

$$H(X)=-\sum_{i=1}^{n}p_i\log_2 p_i\text{。} \tag{1}$$

对于随机变量X和Y,则X关于Y的条件熵表示为

$$H(X|Y)=\sum_y p(y)H(X|Y=y)=-\sum_y p(y)\sum_x p(x|y)\log_x p(x|y)\text{。} \tag{2}$$

条件熵表示在已知随机变量下,另一随机变量的不确定性。当DDoS攻击发生时,攻击流量中源IP地址和目的IP地址会存在明显多对一的映射关系,源IP地址关于目的IP地址的条件熵会发生明显变化。因此,条件熵变化可用于分析发生DDoS攻击的可能性。

1.2 C4.5决策树

C4.5是机器学习和数据挖掘中经典的分类算法。对于给定数据集,C4.5学习过程即是通过信息增益率构建决策树的过程。信息增益率表示为

$$\mathrm{GainRatio}(D,\alpha)=\frac{\mathrm{Gain}(D,\alpha)}{\mathrm{SpiltInfo}(\alpha)},\tag{3}$$

式中：$\mathrm{Gain}(D,\alpha)=H(D)-H(D|\alpha)$；$\mathrm{SpiltInfo}(\alpha)=-\sum_{v=1}\frac{|D^v|}{|D|}\log_2\frac{|D^v|}{|D|}$；$D$ 为训练集；α 为划分属性；Gain 为信息增益；H 为信息熵；SpiltInfo 为分裂信息。C4.5 每轮选择具有最大信息增益率的属性作为分裂属性构建决策树。

C4.5 作为简单轻量的机器学习分类算法，能够生成易于解释的分类规则并且保证较高的分类准确率。利用 C4.5 构建用于流量检测的决策树分类模型，决策树叶子节点即为相应的流量类别，实现了在 SDN 网络中 DDoS 流量检测。

2　基于条件熵和决策树的检测方法

针对 SDN 网络中 DDoS 攻击检测，笔者提出基于条件熵和决策树的 DDoS 检测方法，主要包括 3 部分：

1）网络监控：控制器通过收集和分析 Packet-in 报文，监控当前网络状态，判断数据平面中发生 DDoS 攻击的可能性；

2）特征计算：通过分析 SDN 网络中 DDoS 流量及正常流量典型特点，提取用于机器学习算法的 6 项重要特征；

3）流量检测：利用 C4.5 流量分类模型，实现 DDoS 攻击流量检测。

2.1　网络监控

DDoS 攻击通常会伪造网络数据包，导致控制器会在短时间内接收大量 Packet-in 报文。并且 DDoS 攻击具有分布式的特点，当攻击行为发生时，针对被攻击目标源 IP 地址的条件熵值会显著增加。因此，Packet-in 报文速率及条件熵均可作为 DDoS 攻击检测的依据。

Packet-in 报文速率定义为

$$V_{ij}=\frac{\mathrm{NUM}(\mathrm{PKI}_{ij})}{\Delta T},\tag{4}$$

式中：ΔT 为时间窗口；PKI_{ij} 为第 i 个时间窗口内交换机 S_j 发送至控制器的 Packet-in 报文集合；$\mathrm{NUM}(\mathrm{PKI}_{ij})$ 为集合内 Packet-in 报文数量。

源 IP 地址关于目的 IP 地址的条件熵定义为

$$H_{ij}(\mathrm{sip}|\mathrm{dip})=-\sum_{\mathrm{dip}}p(\mathrm{dip})\sum_{\mathrm{sip}}p(\mathrm{sip}|\mathrm{dip})\log_{\mathrm{sip}}p(\mathrm{sip}|\mathrm{dip}),\tag{5}$$

式中，$p(\mathrm{sip}|\mathrm{dip})$ 为源 IP 地址对于目的 IP 地址的条件概率。

为减少误判可能性，要求当式（6）满足时，初步判断交换机 S_j 可能遭受 DDoS 攻击。文中将时间窗口 ΔT 等于流表项中预设置的空闲超时时间，通常为 5 s。

$$(V_{ij}\geqslant R_{\mathrm{v}})\ \mathrm{or}\ (H_{ij}(\mathrm{sip}|\mathrm{dip})\geqslant R_{\mathrm{e}})==\mathrm{True},\tag{6}$$

式中：R_{v} 为报文速率阈值；R_{e} 为条件熵阈值。

上述 2 项指标的有效性以及阈值的确定方法，将在后续实验部分详细讨论。

2.2　特征计算

上述阶段结束后，控制器通过发送 Flow-status-request 消息至可能遭受攻击的交换机，收集交换机内流表项信息。结论不能作为判断 DDoS 攻击发生的准确依据，需要利用机器学习方法进一步鉴别区分 DDoS 攻击流量。虽然，DDoS 攻击者可能采用多种攻击手段发起不同类型的网络攻击，但攻击流量依然存在相似的特征。在文献[12,14]讨论的攻击流量特征的基础上，针对 SDN 网络架构特点，提出如下 6 项重要特征。

1) 流平均包数（average packets per flow，APF）：与正常流量不同的是，典型的 DDoS 攻击往往采用短流攻击方式，导致 APF 明显下降。文中计算 APF 的方式为：根据目的 IP 进行流表项聚合，再计算流包数的中位数作为特征值 APF。APF 定义为

$$\mathrm{APF}=\begin{cases}\mathrm{packet\_nums}((\mathrm{FE\_nums}+1)/2), \text{if FE\_nums is odd;}\\ \dfrac{\mathrm{packet\_nums}(\mathrm{FE\_nums}/2)+\mathrm{packet\_nums}((\mathrm{FE\_nums}+1)/2)}{2}, \text{otherwise.}\end{cases} \tag{7}$$

式中：FE_nums为流数量；packet_nums为流中数据包个数。

2) 流平均字节数（average bytes per flow，ABF）：攻击者通常为提高DDoS攻击效率选择较小字节数的数据包。选择流字节数的中位数作为特征值ABF，ABF定义为

$$\mathrm{ABF}=\begin{cases}\mathrm{Bytes\_nums}((\mathrm{FE\_nums}+1)/2), \text{if FE\_nums is odd;}\\ \dfrac{\mathrm{Bytes\_nums}(\mathrm{FE\_nums}/2)+\mathrm{Bytes\_nums}((\mathrm{FE\_nums}+1)/2)}{2}, \text{otherwise.}\end{cases} \tag{8}$$

式中，Bytes_nums为流中字节数。

3) 流平均持续时间（average duration of per flow，ADF）：攻击者随机生成DDoS攻击数据包，大多数流表项规则生成后将被闲置，从而触发流表项硬超时规则。而正常的流表项一般持续时间会更长。ADF定义为

$$\mathrm{ADF}=\begin{cases}\mathrm{Duration\_time}((\mathrm{FE\_nums}+1)/2), \text{if FE\_nums is odd;}\\ \dfrac{\mathrm{Duration\_time}(\mathrm{FE\_nums}/2)+\mathrm{Duration\_time}((\mathrm{FE\_nums}+1)/2)}{2}, \text{otherwise.}\end{cases}, \tag{9}$$

式中，Duration_time为流持续时间。

4) 流表项增长速率(rate of flow entries，RFE)：当DDoS攻击发生时，大量访问数据包发送至目标主机，导致网络中交换机的流请求显著增加，流表项增长率明显高于正常网络访问。RFE定义为

$$\mathrm{RFE}=\frac{\mathrm{FE\_nums_T}-\mathrm{FE\_nums_t}}{T-t}, \tag{10}$$

式中：$\mathrm{FE_nums_T}$为T时刻流表项数量；$\mathrm{FE_nums_t}$为t时刻流表项数量。

5) 对流比例 (percentage of pair flow，PPF)：由于DDoS攻击具有伪造源地址的特点，当攻击发生时，网络中单向流量数量会显著增加，导致对称流量比例明显下降。PPF定义为

$$\mathrm{PPF}=\frac{2*\mathrm{PF\_nums}}{\mathrm{FE\_nums}}, \tag{11}$$

式中，PF_nums为对称流数量。

6) 源地址φ-熵（source address entropy，SRE）：DDoS攻击往往导致交换机中流表记录的源IP地址分散程度增加，源IP地址信息熵值高于正常流量中熵值。在DDoS检测中，φ-熵相比于香农熵有更好的检测效果。SRE定义为

$$\mathrm{SRE}=-\frac{1}{\sinh\varphi}\sum\nolimits_{\mathrm{sip}}p(\mathrm{sip})\sinh(\varphi\log_2 p(\mathrm{sip})), \tag{12}$$

式中：sip为源IP地址；φ为超参数。

2.3 流量检测

特征计算阶段提取了用于区分DDoS流量及正常流量的6项重要特征。考虑到DDoS检测对于实时性的要求，文中选择轻量级的C4.5决策树算法。在C4.5进行流量检测之前，需要收集训练样本进行决策树的迭代训练，用于构建流量分类模型，最终检测算法的输出对应DDoS攻击流量或正常流量。

3 实验结果与数据分析

3.1 实验环境

在Ubuntu环境下使用Mininet进行SDN网络仿真，SDN控制器及交换机分别选择Ryu控制器及OpenVSwitch交换机。实验网络拓扑如图1所示。其中，S3交换机所连接主机Attacker1至Attacker5模拟发送DDoS攻击流量，攻击目标为位于S1交换机的主机H1和位于S2交换机的主机H6。

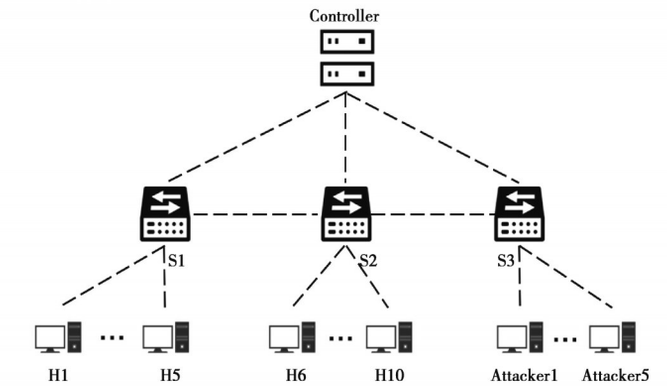

图 1　实验网络拓扑图

Fig. 1　Experimental network topology

3.2　实验数据集

通过 TFN2K 工具生成 DDoS 攻击流量,DDoS 攻击类型包括 TCP_SYN Flood、UDP Flood 和 ICMP Flood。利用林肯实验室提供的真实入侵检测数据集 LLS_DDOS_2.0.2 中合法流量作为实验正常流量,正常流量中包含 85% 的 TCP 流量,10% 的 UDP 流量,5% 的 ICMP 流量[15]。实验的训练阶段使用 10 000 条流量样本确定实验阈值并构建用于流量分类的 C4.5 模型,测试阶段使用 3 000 条样本进行实验方法评估。

3.3　实验结果分析

3.3.1　阈值选择

该阶段是为确定网络监控阶段中 Packet-in 报文速率的阈值 R_v 及条件熵阈值 R_e。实验中,通过调整攻击数据包比例 $R = N_a/(N_a + N_b)$,模拟不同强度的 DDoS 攻击,N_a 和 N_b 分别为攻击数据包和正常数据包数量。

实验中,Packet-in 报文采样周期为 5 s,在 20~35 s 期间发起 DDoS 攻击,Packet-in 报文速率及条件熵变化情况如图 2~图 3 所示。

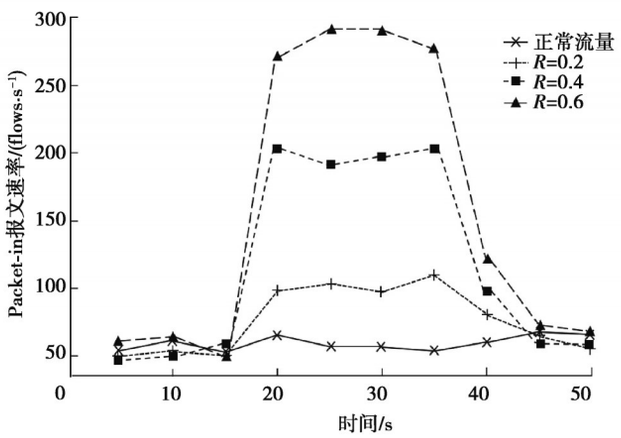

图 2　Packet-in 报文速率随时间变化趋势

Fig. 2　Trend of Packet-in rate changes over time

图 2 和图 3 分别表示 Packet-in 报文速率及条件熵值随时间的变化曲线。可以看到,在 20~35 s 这段时间中,由于发生 DDoS 攻击,导致 Packet-in 报文速率及条件熵值显著上升,DDoS 的强度越大,所达到的峰值越大。

当 DDoS 攻击行为发生时,Packet-in 报文速率及条件熵相比于正常网络访问时已具有显著的差异性。阈值选择如表 1 和表 2 所示,正常网络流量中 Packet-in 报文速率最大值为 70 flows/s,条件熵为 1.51。为降低误判率,笔者选择 75 flows/s 作为 Packet-in 报文速率阈值及 1.6 作为条件熵阈值。

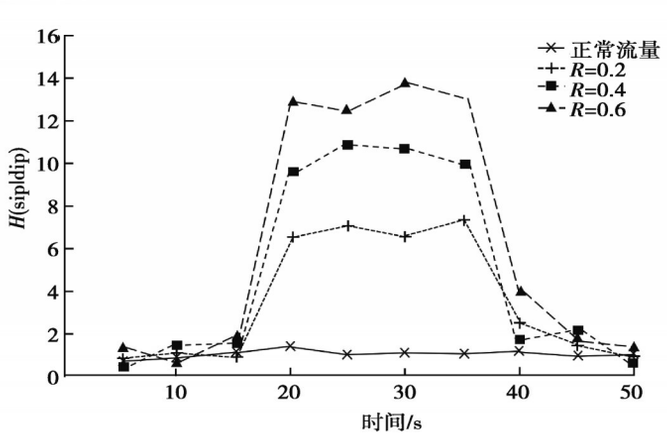

图3 H(sip|dip)随时间变化趋势

Fig. 3 Trend of H(sip|dip) changes over time

表1 Packet-in报文速率阈值选择

Table 1 Packet-in rate threshold selection

参 数	正常流量/(flows·s^{-1})
均 值	59.2
标准差	5.90
最小值	52.0
最大值	70.0
阈 值	75.0

表2 条件熵阈值选择

Table 2 Conditional entropy threshold selection

参 数	正常流量/(flows·s^{-1})
均 值	1.14
标准差	0.23
最小值	0.78
最大值	1.51
阈 值	1.60

3.3.2 性能比较

为验证基于C4.5检测方法的有效性,使用相同实验数据集,在3种不同攻击强度的流量环境中分别与文献[14]中基于PSO-BP的检测方法、文献[12]中基于SOM的检测方法以及文献[16]中基于GHSOM的检测方法进行对比。评价指标包括:精确率(precision)、召回率(recall) 和检测时间(time)。其中,Precision、Recall指标定义为

$$\text{Precision}=\frac{\text{TP}}{(\text{TP}+\text{FP})},\tag{13}$$

$$\text{Recall}=\frac{\text{TP}}{(\text{TP}+\text{FN})},\tag{14}$$

式中:TP表示攻击数据包中被正确预测的数据包数量;FP表示正常数据包中被错误预测的数据包数量;FN表示攻击数据包中被错误预测的数据包数量。精确率和召回率是二分类模型中重要的评价指标,相比于准确率,精确率和召回率更有效地应用于样本不平衡的分类场景。

图4表示在相同场景下,随着攻击强度提高,4种检测方法Precision的比较结果。整体来看,4种检测方法精确率差异较小,随着攻击强度提高,对精确率都存在一定的影响。攻击强度R=0.2时,基于C4.5检测方法的精确率为0.985,略低于基于PSO-BP、SOM及GHSOM的检测方法。但当攻击强度提高至0.6时,检测方

法精确率为 0.974,与基于 GHSOM 的检测方法相等,高于另外 2 种检测方法。

实验结果中 Recall 对比结果如图 5 所示,4 种检测方法召回率都随着攻击强度提高小幅度下降,但基于 C4.5 检测方法召回率始终高于另外 3 种检测方法。在 3 种不同攻击强度的实验环境下,文中检测方法召回率均值为 0.913,基于 PSO-BP、SOM 及 GHSOM 的检测方法召回率均值分别为 0.908、0.903 及 0.909。

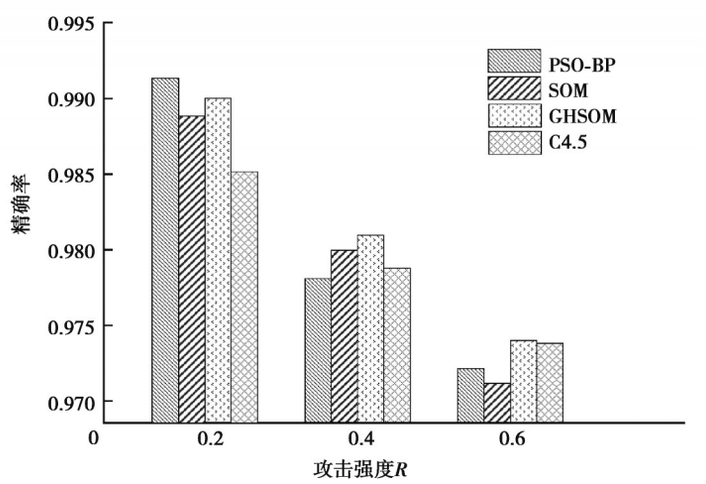

图 4　检测精确率比较

Fig. 4　Comparison of detection precision

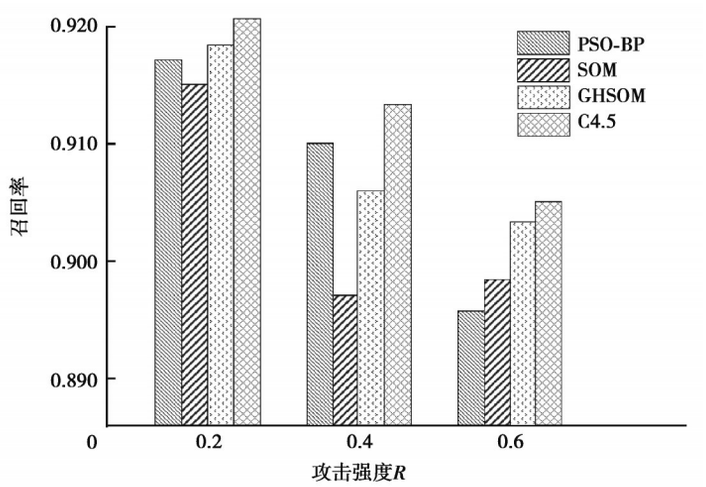

图 5　检测召回率比较

Fig. 5　Comparison of detection recall

表 3 表示 4 种检测方法的检测时间对比结果。文中检测方法具有明显优势,在 3 种不同攻击强度的实验环境下,检测时间均值为 6.83 s,而基于 PSO-BP、SOM 及 GHSOM 检测方法的检测时间均值分别为 14.7 s、11.22 s 及 13.18 s。这是由于 C4.5 决策树模型在构建时仅使用概率分布信息,相比于另外的 3 种检测方法,计算复杂度较低。

4　结束语

传统的基于统计和机器学习方法在解决 SDN 网络中 DDoS 检测时存在精确率低、检测时间长等缺陷,文中提出基于条件熵和决策树的检测方法,在利用条件熵进行预检测的基础上,通过分析 SDN 网络中流量特征并构建决策树分类模型实现 DDoS 攻击检测。为验证方法有效性,通过仿真实验,在真实数据集下,对比了基于 PSO-BP 的检测方法、基于 SOM 的检测方法及基于 GHSOM 的检测方法,结果表明,文中检测方法具

有较高精确率和召回率,明显缩短了检测时间。

表3 检测时间比较

Table 3 Comparison of detection time

检测方法	检测时间均值/s
C4.5	6.83
PSO-BP	14.07
SOM	11.22
GHSOM	13.18

在后续工作中,将尝试把检测方法运用在真实复杂的SDN网络环境中,继续优化检测方法的复杂度,进一步降低控制器负载。

参考文献

[1] Sezer S, Scott-Hayward S, Chouhan P K, et al. Are we ready for SDN? Implementation challenges for software-defined networks[J]. IEEE Communications Magazine, 2013, 51(7): 36-43.

[2] McKeown N, Anderson T, Balakrishnan H, et al. OpenFlow[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 69-74.

[3] Yan Q, Yu F R, Gong Q X, et al. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges[J]. IEEE Communications Surveys & Tutorials, 2016, 18(1): 602-622.

[4] Dhawan M, Poddar R, Mahajan K, et al. SPHINX: detecting security attacks in software-defined networks[C]//Proceedings 2015 Network and Distributed System Security Symposium. San Diego, CA. Reston, VA: Internet Society, 2015.

[5] Noh J, Lee S, Park J, et al. Vulnerabilities of network OS and mitigation with state-based permission system[J]. Security and Communication Networks, 2016, 9(13): 1971-1982.

[6] Yan Q, Yu F R. Distributed denial of service attacks in software-defined networking with cloud computing[J]. IEEE Communications Magazine, 2015, 53(4): 52-59.

[7] Tao Y, Yu S. DDoS attack detection at local area networks using information theoretical metrics[C]//2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. July 16-18, 2013, Melbourne, VIC, Australia. IEEE, 2013: 233-240.

[8] Yu S, Thapngam T, Liu J W, et al. Discriminating DDoS flows from flash crowds using information distance[C]//2009 Third International Conference on Network and System Security. October 19-21, 2009, Gold Coast, QLD, Australia. IEEE, 2009: 351-356.

[9] Bhatia P K, Singh S. On a new csiszar's f-divergence measure[J]. Cybernetics and Information Technologies, 2013, 13(2): 43-57.

[10] Behal S, Kumar K. Detection of DDoS attacks and flash events using novel information theory metrics[J]. Computer Networks, 2017, 116: 96-110.

[11] Santos R, Souza D, Santo W, et al. Machine learning algorithms to detect DDoS attacks in SDN[J]. Concurrency and Computation: Practice and Experience, 2020, 32(16): e5402.

[12] Braga R, Mota E, Passito A. Lightweight DDoS flooding attack detection using NOX/OpenFlow[C]//IEEE Local Computer Network Conference. October 10-14, 2010, Denver, CO, USA. IEEE, 2011: 408-415.

[13] Yang L F, Zhao H. DDoS attack identification and defense using SDN based on machine learning method[C]//2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN). October 16-18, 2018, Yichang, China. IEEE, 2019: 174-178.

[14] Liu Z P, He Y P, Wang W S, et al. DDoS attack detection scheme based on entropy and PSO-BP neural network in SDN[J]. China Communications, 2019, 16(7): 144-155.

[15] Borgnat P, Dewaele G, Fukuda K, et al. Seven years and one day: sketching the evolution of Internet traffic[C]//IEEE INFOCOM. April 19-25, 2009, Rio de Janeiro, Brazil. IEEE, 2009: 711-719.

[16] 田俊峰, 齐鎏岭. SDN中基于条件熵和GHSOM的DDoS攻击检测方法[J]. 通信学报, 2018, 39(8): 140-149.
Tian J F, Qi L L. DDoS attack detection method based on conditional entropy and GHSOM in SDN[J]. Journal on Communications, 2018, 39(8): 140-149.(in Chinese)

(编辑 陈移峰)