SDN 环境中基于交叉熵的分阶段 DDoS 攻击检测与识别

刘 涛 尹 胜
(西安科技大学通信与信息工程学院 陕西 西安 710054)

摘 要 针对软件定义网络易遭受 DDoS 攻击、监控负荷重等问题,提出一种分阶段多层次、基于交叉熵的 DDoS 攻击识别模型。采用监控 SDN 交换机 CPU 使用率的初检方法预判异常状态;引入交叉熵理论对异常交换机的目的 IP 交叉熵和 PACKET_IN 数据包联合检测,对正常与异常流量的特征分布相似性进行定量分析;通过选取的基于交叉熵的特征对流量进行检测识别。实验表明,在使用 Mininet 模拟 SDN 网络环境中,该检测方法可高效定位出异常网络设备,减轻了常态化监控时的设备负荷,同时相比信息熵检测方法及其他方法,拥有更高的灵敏度,降低了 DDOS 检测中的漏报率和误报率。

关键词 软件定义网络 异常检测 交叉熵 DDoS 攻击

中图分类号 TP393 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2021.02.053

DETECTION AND IDENTIFICATION OF DDOS ATTACKS BASED ON CROSS ENTROPY IN SDN ENVIRONMENT

Liu Tao Yin Sheng
(*College of Communication and Information Engineering, Xi'an University of Science and Technology, Xi'an 710054, Shaanxi, China*)

Abstract Aiming at the problems that software defined network are vulnerable to DDoS attacks and heavy monitoring load, a hierarchical multi-level and cross-entropy-based DDoS attack recognition model is proposed. The initial detection method of monitoring the CPU usage of SDN switches was used to predict the abnormal state. The cross entropy theory was introduced to jointly detect the destination IP cross entropy and PACKET_IN data packet of the abnormal switch, and the similarity of the feature distribution of normal and abnormal flow was quantitatively analyzed. The selected traffic feature based on cross entropy was used to detect and identify the traffic. The experiments show that in the Mininet analog SDN network environment, this detection method can efficiently locate abnormal network equipment, and it reduces the equipment load during normalization monitoring. Compared with the information entropy detection method and other methods, it has higher sensitivity, and reduces the false negative rate and false positive rate in DDoS detection.

Keywords Software defined network Anomaly detection Cross entropy DDoS detection

0 引 言

移动设备数量激增导致网络规模不断壮大,研究学者们提出软件定义网络(Software Define Network, SDN)解决方案缓解网络压力[1]。尽管 SDN 有很多优点,但仍有一些问题需要解决。在 SDN 网络中,控制器遭受故障可能对整个网络造成恶劣影响,但 SDN 网络易被攻击的控制节点数要比传统网络少两个数量级[2-3],因此可以将抵御攻击的目标放在重要的节点上,从而把恶意攻击阻止在网络外。

针对 SDN 中的 DDoS 攻击,本文提出一种分阶段多层次的 DDoS 攻击识别模型。包含基于 CPU 使用率触发检测模块、目的 IP 交叉熵值、PACKET_IN 数据包的预警检测模块和流量特征识别模块。引入交换机 CPU 使用率的初检方法,期望在降低常态化监控负荷的同时,能够及时发现异常;引入交叉熵值的知识,对正常与异常流量特征分布上的相似性进行定量分析,

收稿日期:2019-08-27。国家重点研发计划项目(2018YFC0808301)。**刘涛**,副教授,主研领域:矿山信息化,物联网系统,网络安全。**尹胜**,硕士生。

验证是否能提高灵敏度,降低漏报率和误报率,以期提升攻击识别检测效果。

1　相关研究

近年来,学者们对 SDN 中的 DDoS 攻击识别展开了相关研究。Giotis 等[4]提出在 SDN 中提取流特征信息,采用信息熵的算法进行检测。Basicevic 等[5]引入广义熵值区分异常攻击,但计算负荷也随之上升。Mousavi 等[6]对目的 IP 信息熵值进行计算,并与指定阈值对比判断网络是否正在遭受攻击。Ma 等[7]采用源 IP 和目的 IP 的信息熵来检测攻击流量,Jun 等[8]在此基础上添加了对数据包速度的监控检测 DDoS 攻击。但单一的属性检测对攻击的覆盖面不够广,且信息熵值只能表明两种分布分散程度的差异性,无法体现相似性。

武泽慧等[9]提出在 SDN 中对交换机进行吞吐率检测,当大于指定阈值时报警,触发交换机洗牌算法筛选正常流量,但监控负荷重。姚琳元等[10]使用基于神经网络的检测方法,对流量的七元组特征进行提取,通过对特征进行分类处理来检测 DDoS 攻击。Yan 等[11]将流表项的部分特征进行收集,利用模糊综合评判方法进行模糊评价,但该方法初始最优权重确定困难,且自适应能力较差。

2　常用熵值分析

2.1　信息熵

1948 年,香农在信息论中引入信息熵(Information Entropy),定量地表征一个随机变量 X 的随机性及取值的分散程度。变量的分散程度越高、随机性越大,则信息熵值越大。其计算公式定义为:

$$H(X) = -\sum_{i=1}^{n} p(x_i)\log(p(x_i)) \tag{1}$$

式中:X 表示随机变量,其取值集合域为 $\{x_1, x_2, \cdots, x_n\}$;取值 x_i 的概率(或频率)为 $p(x_i)$,$i = 1, 2, \cdots, n$。

2.2　相对熵(KL 散度)

根据式(1)的相关定义,可进一步给出相对熵的概念,计算公式定义如下:

$$D_{\mathrm{KL}}(p \parallel q) = \sum_{i=1}^{n} p(x_i)\log\left(\frac{p(x_i)}{q(x_i)}\right) \tag{2}$$

相对熵又被称为 KL 散度,可体现不同概率分布 p 和 q 的差异性,定量分析相似程度。当差别大时,相对熵值增加;如果两个分布相同,则相对熵为零。

2.3　交叉熵

为了简化计算,对式(2)变形可得:

$$D_{\mathrm{KL}}(p \parallel q) = -H(p(x)) + \left[-\sum_{i=1}^{n} p(x_i)\log(q(x_i))\right] \tag{3}$$

式(3)第一项为分布 $p(x)$ 信息熵的相反数,定义式(3)的第二项为交叉熵:

$$H(p,q) = -\sum_{i=1}^{n} p(x_i)\log(q(x_i)) \tag{4}$$

当 $H(p(x))$ 为常量时(即 $p(x)$ 为给定的真实分布),交叉熵的值等于相对熵的值与给定的真实分布的信息熵值相加。交叉熵 $H(p,q)$ 等价于 KL 散度 $D_{\mathrm{KL}}(p \parallel q)$。

在攻击识别过程中,需区分待检异常流量和正常流量的差异。KL 散度值 $D_{\mathrm{KL}}(p(\text{正常}) \parallel p(\text{待检异常}))$ 可衡量正常流量分布 p(正常)与待检异常流量分布 p(待检异常)的相似性,相比信息熵值得出分布分散程度的差异,其精准度更高,可更好地识别异常攻击流量。因为交叉熵等价于 KL 散度,为了简化计算量,本文采用交叉熵。

3　SDN 中 DDoS 检测模型

3.1　DDoS 攻击特点分析

在 SDN 网络中,攻击者制造大量网络设备流表项无法匹配的高流量伪造数据,设备缓存未匹配分组机制,严重消耗设备的 CPU 资源及带宽;同时大量的 PACKET_IN 数据包导致控制器计算资源紧张。攻击者不需知道控制器的位置就可发动攻击,任何可产生 PACKET_IN 数据包的方式都可作为攻击控制器的手段。攻击特点分析如下:

1) 分布式:发起的攻击流量的来源由大量的主机组成,同时还伪造源 IP 地址、随机伪造源端口等参数构成无用的数据包,所以攻击流量分组中的来源是分散的。

2) 无规律:在进行攻击时使用常见的协议和服务,导致从协议和服务的类型上很难对攻击进行区分。且攻击数据包的一些信息都是经过伪造的,对攻击地址确定困难。

3) 多样性:不论是利用协议漏洞、伪造数据流量等,任何产生 PACKET_IN 数据包的形式都可发动攻击,从而对目标所处的网络造成拥堵直至瘫痪。攻击形式可能是一对一映射、一对多映射、多对一映射、多对多映射等。

3.2 检测特征

3.2.1 触发及预警阶段检测特征

1）SDN 交换机 CPU 使用率：攻击者伪造攻击流量或占用带宽的 DDoS 攻击，网络设备的 CPU 使用率会有变化。与传统网络不同，SDN 交换机只负责转发功能，因此具有丰富的计算能力用于 CPU 使用率监控。

2）PACKET_IN 生成速率：对异常交换机 PACKET_IN 数据包监控可确定目标交换机是否遭受攻击，在遭受攻击时，设备中 PACKET_IN 数据包生成速度会上升。

3）目的 IP 交叉熵值：如 3.1 节分析，若发生了 DDoS 攻击，攻击者产生的异常流量的特征分布情况与正常流量会有一些差异，根据第 2 节可知，交叉熵可以灵敏地检测到正常流量分布及异常待检分布的相似性，区分异常流量。

3.2.2 攻击识别阶段特征

1）流数据包平均长度：攻击者发出的流量数据，是为了耗尽攻击目标的资源处理能力，而不是请求服务，所以攻击流量的数据包平均长度较短。而针对带宽的攻击，数据包的平均长度较长。

2）流数据包数量均值：与数据包平均长度特征类似，单流数据包的数量较少。若是针对流量带宽的攻击，则每个流中数据包数量将会增加。

3）双向流的比例：流量传输是为获取或提供服务，数据流的交互请求是双向的。而攻击流量不具备交互性，攻击者的地址 A 和攻击目标的地址 B 之间的流量传输呈现单向性。

4）协议的交叉熵值：当攻击者注入攻击流量时，很难兼顾到攻击目标网络中不同协议的数据包比例，所以协议的交叉熵值可体现正常流量协议分布与异常流量协议分布的相似性。

5）目的端口的交叉熵值：与协议的交叉熵值类似的表现，目的端口的交叉熵值可作为检测两种流量分布的相似性的一个特征。

6）目的 IP 的交叉熵值：如 3.2.1 节介绍，目的 IP 的交叉熵值可作为识别攻击流量的一个特征。

3.3 攻击预警及识别机制

本文提出常态化监测交换机设备的 CPU 使用率，与传统网络不同，SDN 交换机只负责转发功能，因此具有丰富的计算能力可用于监控；当发现异常，通过进一步对 PACKET_IN 数据包及目的 IP 交叉熵值进行分析，对网络中是否遭受攻击进行预警；最后通过对流量中的特征进行分析，判断当前是否遭受 DDoS 攻击。攻击检测方案如图 1 所示。

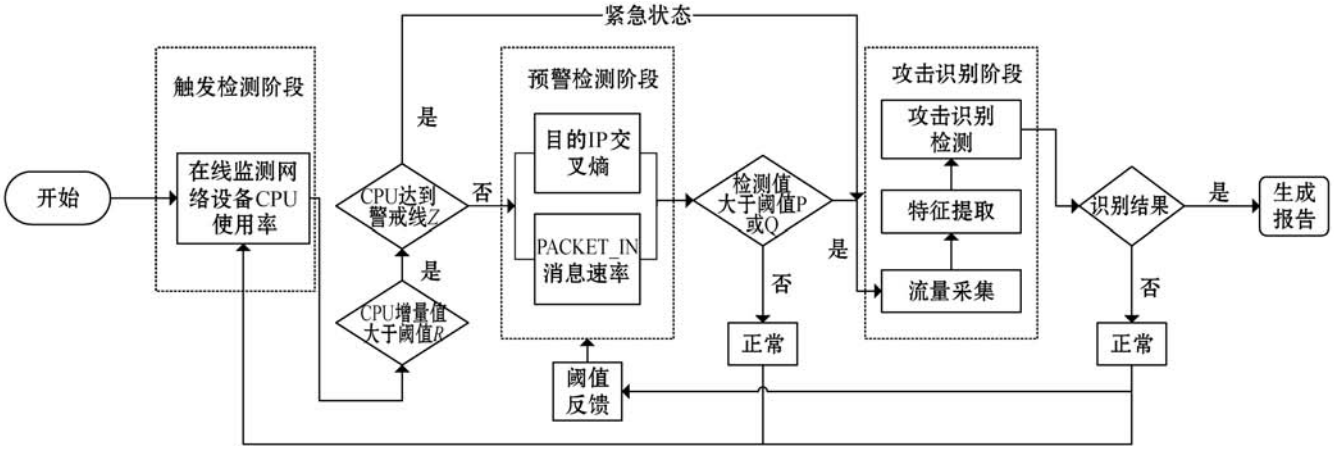

图 1 DDoS 攻击检测方案

3.3.1 触发检测阶段

SDN 设备的 CPU 使用率可反映转发进程负载情况。当网络正常，CPU 使用率处于稳定的值；当受到攻击行为，则 CPU 使用率将上升。设定阈值 R，当 CPU 增量值高于 R，满足触发条件。

若长时间处于满负荷情况，转发进程则无法及时处理流量请求而造成丢包现象。设定警戒线 Z，CPU 使用率达到警戒线 Z 时，触发紧急状态，直接进入攻击识别模块，预防高流量攻击。阈值 R 及警戒线 Z 根据具体的网络情况进行相应的调整。

本文将 SDN 交换机转发进程的 CPU 使用率作为触发特征，不需要过多的计算负荷，且能有效检测到异常情况，以较低的监控成本来监测网络。

3.3.2 预警检测阶段

引起 CPU 使用率变化的不都是攻击行为，误警率较高，所以需进一步对 PACKET_IN 数据包及网络流量中目的 IP 的交叉熵进行检测分析。

对触发异常交换机的 PACKET_IN 数据包进行统计，计算每秒钟发出的 PACKET_IN 数据包数。若单位时间数据包数变化值达到阈值 Q，则发出预警。

同时收集异常交换机的流量数据,设置检测窗口 n,计算流量中目的 IP 交叉熵值,当其变化差值大于阈值 P,进行攻击预警。由第 2 节可知,待检流量与正常流量的相似性越低,其交叉熵值越大。若后期检测结果为正常,则对阈值 P、Q 进行反馈调整,提升检测灵敏度。

3.3.3　攻击识别阶段

当攻击预警之后,启动攻击识别模块。本阶段通过收集异常交换机的数据分组信息及流表项信息,对流量进行特征提取,得到攻击识别所需要的 6 元组特征,进行攻击流量识别,如果发现攻击行为,生成检测报告。

4　实　验

4.1　实验环境

实验在基于 i5 CPU,4 GB 内存计算机的 Ubuntu 16.04 系统上进行,使用 Mininet 仿真软件搭建 SDN 实验网络拓扑,用 OpenDaylight 控制器作为 SDN 网络的控制器,使用 Open vSwitch 交换机作为 SDN 网络转发设备。网络拓扑如图 2 所示。

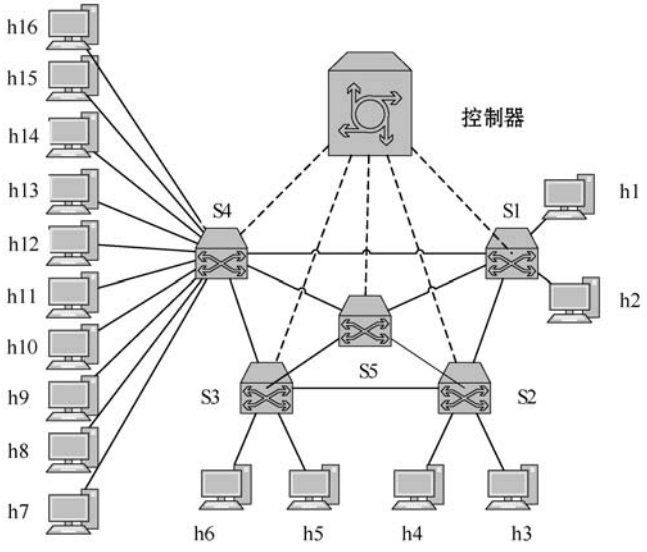

图 2　网络拓扑结构图

拓扑中共有 5 台 OVS 交换机和 16 台主机,s4 交换机中连接 10 台主机。为了尽可能模拟真实的网络流量,使用 Mininet 中的 iperf 工具编程以随机流量模型生成正常流量,各主机向另一任意主机以随机的方式建立连接,连接带宽设置为 0.5 MB。

实验时选择主机 h16 作为受害主机,采用 hping3 作为产生异常流量的攻击工具,其可生成 SYNflood、UDPflood、ICMPflood 等一系列攻击流量。使用 wireshark 工具统计收集流量,并用 tshark 做相应的数据处理后,使用开源软件 weka 对统计流量进行处理分析。

4.2　实验结果与分析

4.2.1　SDN 交换机 CPU 使用率分析

为了测试交换机 CPU 使用率检测的有效性,本文进行了一些实验。使用 top 命令行工具对 CPU 使用率进行监测。Top 命令通过在规定周期 t 秒内测量进程使用的 CPU 时间 $t1$,将 $t1$ 与 t 的比值作为该进程的 CPU 使用率。因设备实现转发功能的是 ovs-vswitch 进程,所以以该进程的 CPU 使用率作为转发进程的 CPU 使用率。

根据攻击强度进行 2 组实验,第一组为低强度攻击实验,攻击强度分别为 30%、40%、50%,攻击强度为攻击分组流量占总流量中的比例。第二组为高强度攻击实验,攻击强度分别为 60%、70%、80%、90%。前 30 s 为正常状态,然后进行 60 s 的流量攻击,同时测量攻击结束后 30 s 内的 CPU 使用率。实验结果如图 3 和图 4 所示。

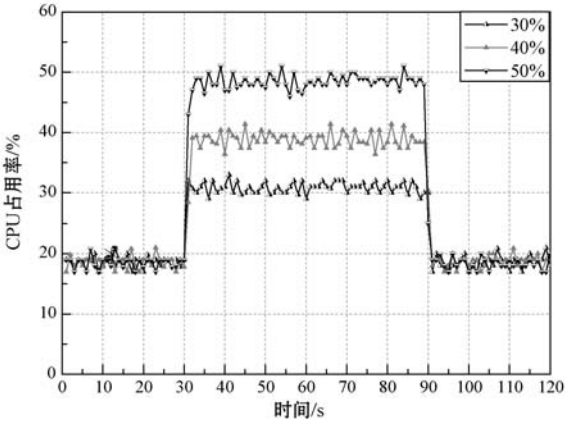

图 3　低速率攻击时 CPU 变化情况

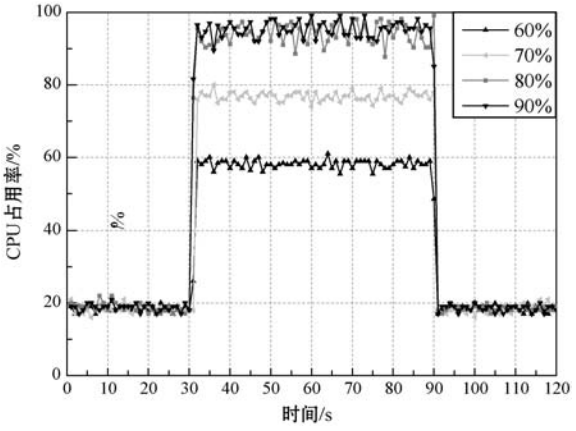

图 4　高速率攻击时 CPU 变化情况图

可以看出,在 0 ~ 30 s,设备的 CPU 使用率处于稳定状态,此时设备 CPU 使用率较低,在 19% 左右。启动攻击后,设备的 CPU 使用率瞬间增长,从图 3 可得不同的攻击强度会引起 CPU 不同程度的稳定增长;从图 4 可看出,当攻击强度为 80% 和 90% 时无更明显的变化,稳定在一个峰值。

根据实验结果可知,设备的 CPU 使用率可作为预警设备是否遭受 DDoS 攻击的特征。CPU 使用率变化值设置阈值 R,当变化值大于阈值时,触发预警检测,若监测到 CPU 使用率达警戒线 Z,则直接跳过预警检测,进入识别检测模块。

4.2.2 PACKET_IN 包与目的 IP 交叉熵值分析

对预警交换机发送 PACKET_IN 数据包进行监测统计。同样做了两组实验,攻击强度、实验环境等与上述实验环境一致。被攻击交换机产生的 PACKET_IN 数据包变化如图 5 和图 6 所示。

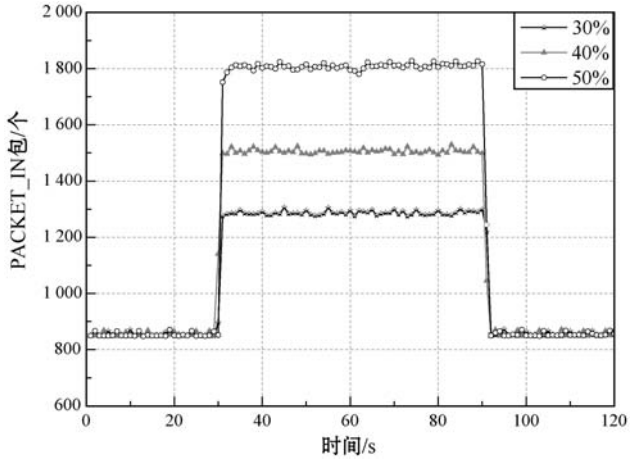

图 5 低速率攻击时 PACKET_IN 数据包

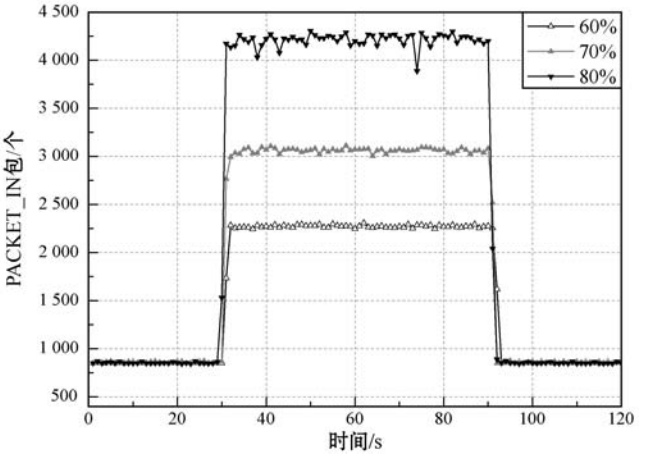

图 6 高速率攻击时 PACKET_IN 数据包数

可以看出,在 0 ~ 30 s,PACKET_IN 数据包处于稳定状态。随着未知流的进入,PACKET_IN 数据包骤升,攻击结束后,PACKET_IN 数据包的速率慢慢恢复至攻击前的正常状态。另外,攻击强度高时,波峰与波谷差距明显,分析发现,当交换机负载过高时,未匹配流数多,此时数据包会携带更多未匹配的流信息。

同时,对目的 IP 的交叉熵值与信息熵值进行对比分析,模拟正常流量连接单个主机约每秒发出 1 000 个数据包,设置检测窗口为 2 000,计算目的 IP 的交叉熵值及信息熵值,不同攻击强度下计算 5 次熵值的平均值,实验结果如表 1 所示。

表 1 不同攻击强度下的信息熵及交叉熵

熵值	强度					
	30%	40%	50%	60%	70%	80%
正常信息熵值	1.114 3	1.114 2	1.110 5	1.120 4	1.125 5	1.116 7
异常信息熵值	0.930 8	0.868 2	0.760 5	0.673 3	0.626 7	0.393 8
正常交叉熵值	1.120 7	1.121 0	1.121 2	1.120 6	1.120 2	1.120 7
异常交叉熵值	1.433 3	1.510 9	1.612 5	1.667 4	1.712 6	1.832 1
信息熵值差	0.183 5	0.246 0	0.350 0	0.447 1	0.498 8	0.722 9
交叉熵值差	0.312 6	0.389 9	0.491 3	0.546 8	0.592 4	0.711 3

可以看出,针对攻击流量温和变化的情况,本文引入的交叉熵值度量标准与使用信息熵值相比,增大了正常流量与攻击流量间的信息敏感距离。对于攻击的前期以及攻速较慢的 DDoS 攻击,可放大攻击特征信息,提升区分准确度,降低误警率,更快地发出预警。

4.2.3 攻击识别实验与分析

实验收集 8 500 个样本,训练集中正常样本 3 000 个,攻击样本 2 000 个,测试集中正常样本 2 000 个,攻击流量样本 1 500 个。为了比较引入交叉熵分类特征的效果,与文献[12]中所提出的 8 元组和文献[13]的 4 元组进行了对比实验,同时对 C4.5 决策树、KNN 算法及 BayesNet 算法进行了实验,结果如表 2 所示。

表 2 检测率对比 %

检测特征	本文 6 元组	文献[12] 8 元组	文献[13] 4 元组
决策树	98.2	96.9	97.1
KNN	97.3	96.4	95.8
BayesNet	96.5	95.9	95.7

实验结果显示本文引入交叉熵的 6 元组特征具有最高检测率 98.2%,因为交叉熵值可体现正常流量分布与异常流量分布的相似性,而信息熵值只体现出分散程度的差异,但不能体现相似性,所以本文基于交叉熵值的特征区分度好。

从表 3 检测时间来看,虽然本文 6 元组比文献[13]中的 4 元组检测时长,但检测效果好,耗费时长属于可接收的范围。综上,本文在检测特征上引入交叉熵值,对正常流量与待检异常流量分布的相似性量化体现,取得了更好的检测效果。

表 3　检测时间对比　　ms

检测特征	本文 6 元组	文献[12] 8 元组	文献[13] 4 元组
决策树	468	527	430
KNN	441	467	414
BayesNet	235	257	218

5　结　语

本文提出一种在 SDN 网络环境中的基于交叉熵的分阶段多层次 DDoS 攻击检测模型,采用基于交换机设备 CPU 使用率的初检方法,检测转发进程 CPU 的使用率,减轻计算资源使用率,又可快速定位异常交换机;引入交叉熵值的理论,将正常与攻击流量在特征分布上的相似性定量分析,有效增加数据间的信息距离,提升检测准确度;预警检测模块使用目的 IP 交叉熵值及 PACKET_IN 数据包联合检测,降低了漏报率。实验结果验证了检测特征的良好表现。

后期的工作将对特征筛选进行研究,使用优化算法选取最优特征集,同时考虑对比更多的特征,根据攻击报告进行攻击溯源研究。

参　考　文　献

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

[2] Dayal N, Srivastava S. Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN[C]//2017 9th International Conference on Communication Systems and Networks(COMSNETS), 2017: 274 – 281.

[3] Dayal N, Maity P, Srivastava S, et al. Research trends in security and DDoS in SDN[J]. Security and Communication Networks, 2016, 9(18): 6386 – 6411.

[4] Giotis K, Argyropoulos C, Androulidakis G, et al. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments [J]. Computer Networks, 2014, 62:122 – 136.

[5] Basicevic I, Ocovaj S, Popovic M. Use of tsallis entropy in detection of SYN flood DoS attacks[J]. Security and Communication Networks, 2015, 8(18):3634 – 3640.

[6] Mousavi S M, St-Hilaire M. Early detection of DDoS attacks against SDN controllers[C]//2015 International Conference on Computing, Networking and Communications (ICNC), 2015:77 – 81.

[7] Ma X, Chen Y. DDoS detection method based on chaos analysis of network traffic entropy[J]. IEEE Communications Letters, 2013, 18(1):114 – 117.

[8] Jun J H, Lee D, Ahn C W, et al. DDoS attack detection using flow entropy and packet sampling on huge networks [C]//The Thirteenth International Conference on Networks, 2014: 185 – 190.

[9] 武泽慧,魏强,任开磊,等. 基于 OpenFlow 交换机洗牌的 DDoS 攻击动态防御方法[J]. 电子与信息学报,2017,39(2):397 – 404.

[10] 姚琳元,董平,张宏科. 基于对象特征的软件定义网络分布式拒绝服务攻击检测方法[J]. 电子与信息学报,2017,39(2):381 – 388.

[11] Yan Q, Gong Q, Deng F A. Detection of DDoS attacks against wireless SDN controllers based on the fuzzy synthetic evaluation decision-making model [J]. Ad Hoc & Sensor Wireless Networks, 2016, 33(1): 275 – 299.

[12] 刘振鹏,贺玉鹏,王文胜,等. SDN 环境下的 DDoS 攻击检测方案[J]. 武汉大学学报(理学版),2019,65(2):178 – 184.

[13] 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.

(上接第 327 页)

[12] 李非非,韩笑,曾琦. 具有隐私保护的固定密文长度分布式属性基加密方案[J]. 计算机应用与软件,2018,35(5):323 – 327.

[13] 范运东,吴晓平. 基于策略隐藏属性加密的云存储访问控制方案[J]. 计算机工程,2018,44(7):139 – 144,149.

[14] Li J, Wang Q, Wang C, et al. Enhancing attribute-based encryption with attribute hierarch[J]. Mobile Networks and Applications, 2011, 16(5):553 – 561.

[15] Wang G J, Liu Q, Wu J, et al. Hierachical attribute-based encryption and scalable user revocation for sharing data in cloud servers[J]. Computers & Security, 2011, 30(5):320 – 331.

[16] Hur J. Improving security and efficiency in attribute-based data sharing[J]. IEEE Transactions on Knowledge and Data Engineering, 2013, 25(10):2271 – 2282.

[17] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts[C]//20th USENIX Conference on Security, 2011.

[18] Lai J, Deng R H, Guan C, et al. Attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(8): 1343 – 1354.

[19] Wang S L, Yu J P, Zhang P, et al. A novel file hierarchy access control scheme using attribute-based encryption[J]. Applied Mechanics and Materials, 2014, 701 – 702:911 – 918.

[20] 雷丽楠,李勇. 基于密文策略属性基加密的多授权中心访问控制方案[J]. 计算机应用研究,2018,35(1):248 – 252,276.

[21] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//2007 IEEE Symposium on Security and Privacy (SP'07), 2007:321 – 334.