计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(8):354−360 [doi: 10.15888/j.cnki.csa.008673]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

SDN 环境下基于改进 D-S 理论的 DDoS 攻击检测①

王　聪, 崔允贺, 高鸿峰

(贵州大学 计算机科学与技术学院, 贵阳 550025)
通信作者: 高鸿峰, E-mail: hfgao@gzu.edu.cn

摘　要: 软件定义网络 (software-defined networking, SDN) 实现了控制层和转发层设备的分离, 但控制转发的解耦使得 SDN 网络中不同层次设备面临新型的 DDoS 攻击风险. 为了解决上述问题, 本文提出了一种 SDN 环境下基于改进 D-S 理论的 DDoS 攻击检测方法, 用于检测以 SDN 控制器和交换机为目标的 DDoS 攻击. 在改进的算法中, 本文使用离散因子和纯度因子衡量 D-S 证据源之间的冲突. 同时, 结合纯度因子和离散因子调整 D-S 证据理论的证据源, 调整后的证据源将通过 Dempster 规则融合得到 DDoS 攻击检测结果. 实验结果表明本文提出的方法具有较高的精度.

关键词: 软件定义网络 (SDN); 分布式拒绝服务攻击 (DDoS); OpenFlow; D-S 证据理论; 异常检测

引用格式: 王聪,崔允贺,高鸿峰.SDN 环境下基于改进 D-S 理论的 DDoS 攻击检测.计算机系统应用,2022,31(8):354–360. http://www.c-s-a.org.cn/1003-3254/8673.html

DDoS Attack Detection Based on Improved D-S Theory in SDN

WANG Cong, CUI Yun-He, GAO Hong-Feng

(School of Computer Science and Technology, Guizhou University, Guiyang 550025, China)

Abstract: Although the separation of the devices in the control layer and the forwarding layer can be achieved by software-defined networking (SDN), the decoupling of the two layers exposes the devices in different layers of the network to new types of distributed denial of service (DDoS) attacks. To solve the above problem, this study proposes a DDoS attack detection method based on the improved Dempster-Shafer (D-S) theory for detecting DDoS attacks aimed at SDN controllers and switches in an SDN environment. In the improved algorithm, the discrete factor and the purity factor are used to measure the conflicts among D-S evidence sources. Meanwhile, the evidence sources of the D-S evidence theory are adjusted according to the two factors, and the DDoS attack detection result is obtained with the adjusted evidence sources in light of Dempster's rule of combination. Experimental results show that the proposed method achieves high detection precision.

Key words: software-defined networking (SDN); distributed denial of service (DDoS); OpenFlow; Dempster-Shafer (D-S) evidence theory; anomaly detection

作为一种新型的网络架构, SDN 实现了集中式控制和可编程的特点, 解耦了控制层面和转发层面, 使得大型网络管理更为便捷[1−4]. 但是, SDN 的转发与控制分离的特点可能使得交换机和控制器易成为高速和低速分布式拒绝服务攻击的目标[5].

在 SDN 环境中, 针对交换机和控制器的高速和低速 DDoS 攻击是多分类的问题. 在 SDN 环境下, 如何准确地识别多种不同攻击类型仍是一个较为严峻的问

① 基金项目: 国家自然科学基金 (62102111); 贵州省科技计划 (黔科合基础 [2020]1Y267); 赛尔网络下一代互联网技术创新项目 (NGII20161007)
收稿时间: 2021-11-15; 修改时间: 2021-12-13; 采用时间: 2022-01-20; csa 在线出版时间: 2022-05-30

题. 现如今, 针对低速率和高速率 DDoS 攻击问题, 研究者提出了一些方法, 用于检测低速 DDoS 和高速 DDoS 攻击[6–8]. 文献 [9] 提出了基于粒子群优化卷积神经的模型, 并将其用于检测高速率 DDoS 攻击. 文献 [10] 提出了一种基于信息距离度量检测低速率 DDoS 攻击. 信息距离度量指标可以量化网络流量在不同概率分布下的偏差, 基于 SDN 网络流的特性, 该文献使用广义熵的度量方法用于检测控制层的低速率 DDoS 攻击.

D-S 证据理论是一种处理不确定信息并且实现多分类器融合的有力工具, 被广泛地用在模式识别、图像处理、风险评估、目标分类等领域[11]. 文献 [12] 中, 作者结合了云模型和改进 D-S 证据理论, 提出了一种新的冲突参数并用于改进 D-S 证据理论算法, 该算法通过对探测器的证据进行修正实现多个证据最终融合. 文献 [13] 中, 研究者提出了一种基于不一致测量的冲突证据组合方法, 该方法引入了新的冲突系数对冲突证据进行修正, 并通过改进的组合规则获得最终的融合结果. 文献 [14] 中, 作者结合了希尔伯特-黄变换和传统 D-S 理论用于检测传统网络中 DDoS 攻击. 文献 [15] 中, 研究者使用传统的 D-S 证据理论算法用于检测传统网络中 DDoS 攻击. 文献 [16] 中, 研究者使用证据间距离改进 D-S 证据理论, 并使用 SVM 模型结合改进 D-S 证据理论算法用于检测网络中 DDoS 攻击.

在处理多分类器融合的过程中, 使用 D-S 证据理论可能会使得的融合的结果不够充分. 为了解决这一问题, 一些研究者提出修改 Dempster 规则方法, 主要用于解决冲突分配和管理的问题[17–19]. 另外, 一些研究者则是通过改进基本信念分配解决上述问题, 具体改进方法是通过对不可靠的证据源进行预处理, 将经过预处理后的证据与 Dempster 规则进行最终的融合. 本文更倾向于第 2 类研究者改进 D-S 证据理论算法的思想. 目前, 部分研究者提出的基于 D-S 证据理论的 DDoS 攻击检测方法大多数只适用于解决传统网络下 DDoS 攻击安全问题. 本质上讲, 该问题属于二分类问题. 此外, 一些研究者只使用分类器的结果作为 D-S 基本信念分配函数 (basic probability assignment, BPA), 且只使用简单的统计学方法直接对分类器结果进行权重的重新分配, 这种方式容易导致 DDoS 检测精度降低.

基于上述分析, 为防范 SDN 中高速和低速 DDoS 攻击, 本文提出一种 SDN 环境下针对控制器和交换机的多目标 DDoS 攻击检测方法. 首先, 为了更精确的检测 SDN 环境下多种不同种类的 DDoS 攻击, 本文使用 OVO 策略融合多种不同类型的二分类器构建多分类器. 其次, 为了使 BPA 有效的代表网络流量的初始概率分布, 代替多数研究者使用分类器的结果直接作为 BPA, 本文使用 OVO 策略融合多个二分类器至多分类器, 结合得到二分类器的支持度与信息熵方法构建 BPA. 最后, 为了更全面的衡量 D-S 证据间的冲突, 本文提出两种新的冲突因子包含离散因子和纯度因子用于衡量 D-S 证据源之间的冲突. 其中, 离散因子是通过使用 OVO 策略融合多个二分类器至多分类器时支持相同类别的非零概率值之间的熵值计算得到. 纯度因子是指计算使用 OVO 策略融合多个二分类器至多分类器后, 该多分类器内部之间支持度的 Gini 指数得到. 之后, 结合离散因子和纯度因子计算多个证据源的权重. 最后, 利用 D-S 证据理论对调整权重后的证据进行最终的融合. 综上, 本文的主要贡献如下.

(1) 为了更精确的检测 SDN 网络中 DDoS 攻击, 本文提出一种 SDN 环境下针对控制器和交换机的多目标 DDoS 攻击检测方法.

(2) 本文使用 OVO 策略融合多种不同类型的二分类器构建多分类器, 且二分类器的支持度与信息熵方法结合计算得到 BPA.

(3) 为了更好地衡量证据内部和证据之间的冲突, 本文提出两种新的冲突因子包含离散因子和纯度因子, 用于修正 D-S 证据理论的证据.

本论文的结构组织如下. 第 1 节介绍了相关背景技术知识. 第 2 节介绍了本文提出的基于改进 D-S 理论的 DDoS 攻击检测方法. 第 3 节通过实验分析和结果证实本文提出的方法具有较好的效果. 第 4 节对本文提出方法进行了总结.

1 背景

本小节分为两个部分: 第 1 部分讲述了 DDoS 攻击相关背景知识, 第 2 部分讲述了 D-S 证据理论算法相关知识.

1.1 SDN 环境下 DDoS 和 LDDoS 攻击

SDN 实现了控制层与转发层的解耦, 具有集中式控制和可编程性等特点, 然而 SDN 的控制层和转发层也都面临着一些安全问题, 例如 DDoS 攻击等[20].

在 SDN 中, 以控制器为目标的攻击者通过持续向目标主机发送新的数据包对控制器发起攻击. 攻击者发送的数据包将与交换机中的流表进行匹配, 如果数

据包匹配成功, 则流表相应动作将会被执行. 否则, 交换机将向控制器发送 *packet_in* 消息. 在这种攻击方式中, 攻击者将发送大量无法与流表匹配的数据包, 使控制器处理大量 *packet_in* 消息, 导致控制器单点故障.

此外, 以交换机为目标的攻击者将向交换机发送新的数据包. 同时在 *idle_time* 时间内将持续发送与第一个数据包头部相同的数据包, 保持相关流表项一直存在交换机中. 通过持续重复这个过程, 交换机的流表项空间将被恶意无用的流表项占满, 导致正常的流表项在到达交换机时被丢弃.

以交换机和控制器为攻击目标, 其攻击发起方式主要分为两种类型, 即 DDoS 攻击以及 LDDoS 攻击. DDoS 攻击是通过伪造 IP 地址持续不断地向攻击目标发送大量攻击流量, 而 LDDoS 攻击则是通过调整发送攻击的周期、攻击流量持续的时间和发送攻击流量的速率达到降低控制器和交换机服务质量的目的.

1.2 D-S 证据理论

在多源数据融合中, 具有不精确推理特点的 D-S 证据理论是一种较有优势的技术. 目前, D-S 证据理论已被广泛运用在模式识别、图像处理、多类目标分类和模式分类等领域.

D-S 证据理论建立在集合框架ϑ基础之上, 框架ϑ包括了对应问题的所有结果的集合.

定义 1. 假设$\vartheta=\{A_1,A_2,\cdots,A_N\}$是包含所有结果的集合框架, 基本信度分配函数 m 被定义为从集合框架ϑ中的幂集2^{ϑ}到概率区间 [0, 1] 的映射函数, $m(A)$ 为 A 的 BPA, A 为框架2^{ϑ}的任一子集, $m(A)>0$ 的集合则为焦元, 反映了在该证据下命题 A 的可信程度, 具体计算如式 (1) 所示.

$$\begin{cases} m(\varnothing)=0 \\ \sum\limits_{A\in 2^{\vartheta}} m(A)=1 \end{cases} \tag{1}$$

定义 2. Dempster 合成法则如式 (2) 所示. 其中, n 为证据数量, j 为第 j 个证据, N 为假设的数量, k 为第 k 个假设, K 为合成公式中 [0, 1] 范围内多个证据之间的冲突系数, $m_1\oplus m_2\oplus\cdots\oplus m_n$为证据之间的内积和.

$$m(A)=m_1\oplus\cdots\oplus m_n$$
$$\begin{cases} \dfrac{1}{1-K}\sum\limits_{\cap_{k=1}^{N}A_k=A,A\subseteq 2^{\vartheta}}\prod\limits_{j=1}^{n}m_j(A_k) A\neq\varnothing \\ K=\sum\limits_{\cap_{k=1}^{N}A_k=A,A\subseteq 2^{\vartheta}}\prod\limits_{j=1}^{n}m_j(A_k) \end{cases} \tag{2}$$

2 SDN 环境下基于改进 D-S 理论算法检测 DDoS 攻击机制

2.1 设计原理

SDN 网络具有转发层和控制层分离的特点使其具备传统网络不能比拟的优势, 同时也可能使得 SDN 中控制层和转发层遭受不同类型的 DDoS 攻击. 针对 SDN 中不同类型的 DDoS 攻击, 本文提出一种 SDN 环境下基于改进 D-S 理论的 DDoS 攻击检测方法. 该方法提出的两个因子包含离散因子和纯度因子, 用于衡量证据内部和证据之间的冲突和关联, 以此修正 D-S 理论算法的证据冲突. 离散因子是指在使用 OVO 策略进行二分类器融合成一个多分类器的过程中, 相同类别的非零支持度之间的熵值. 纯度因子指不纯度与 1 之间的差异绝对值. 不纯度是指每个多分类器内部不同类别的支持度之间的 Gini 指数. 当 Gini 指数越高时, 则表示多分类器内部不同类别之间的支持度分布不纯度越高, 则分类差异越为突出. 本文使用两个因子用于修正多分类器输出的结果, 使用 D-S 证据理论方法融合修正后的输出结果得到最终的分类结果. 检测方法整体架构图具体如图 1 所示.

2.2 离散因子

当 OVO 策略融合多个二分类器为一个多分类器过程时, 多个二分类器相同类别的非零支持度之间的离散程度影响该多分类器的分类效果. 相同类别非零支持度之间的离散因子越大, 则表示该多分类器效果越好.

本文通过 M 个二分类器使用 OVO 策略融合成一个多分类器. 此处, $M=N\times(N-1)/2$, N 指 N–1 种网络攻击流量和正常网络流量. 其中, 网络攻击流量包含了针对控制器和交换机的高速 DDoS 攻击和低速 DDoS 攻击. 本文通过式 (3)、式 (4) 和式 (5) 计算 O_i 并得到 BPA, 并通过式 (6) 和式 (7) 计算得到离散因子.

$$\varphi=\begin{pmatrix} O_{i,1,2}^{1} & \cdots & O_{i,1,2}^{5} \\ \vdots & \ddots & \vdots \\ O_{i,4,5}^{1} & \cdots & O_{i,4,5}^{5} \end{pmatrix} \tag{3}$$

$$\tau_i^j=\left(O_{i,1,2}^{j},O_{i,1,3}^{j},O_{i,1,4}^{j}\cdots O_{i,3,4}^{j},O_{i,4,5}^{j}\right) \tag{4}$$

$$O_i=\frac{\sum_{i=1}^{10}\tau_i^j}{\sum_{j=1}^{5}\sum_{i=1}^{10}\tau_i^j}=(O_i^1,O_i^2,O_i^3,O_i^4,O_i^5) \tag{5}$$

$$H\left(\tau^j\right)=-\sum_{i=1}^{10}\tau_i^j\log\tau_i^j \tag{6}$$

$$Dis\left(m_i\right)=\frac{H\left(\tau^j\right)}{\sum_{i=1}^{5}H\left(\tau^j\right)} \tag{7}$$

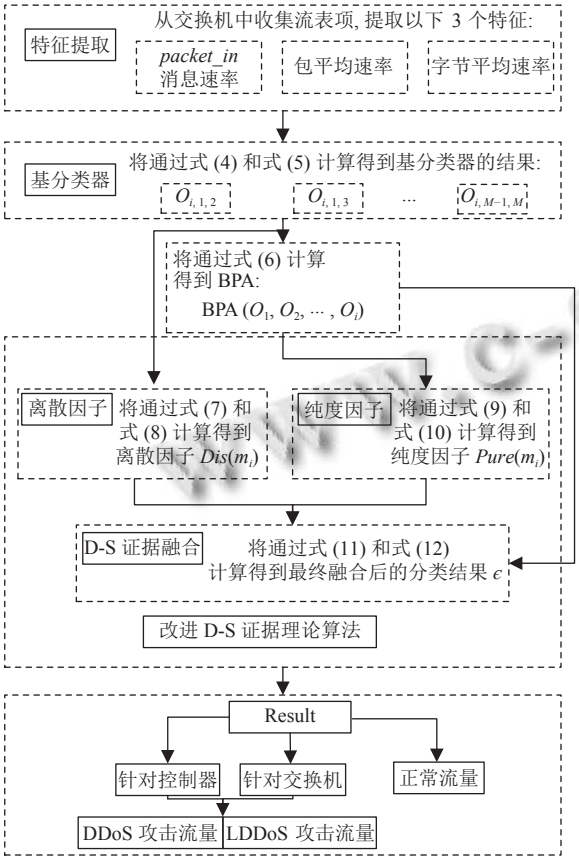

图 1 检测方法整体架构图

2.3 纯度因子

纯度因子通过计算多分类器内部的支持度之间的 Gini 指数得到. 当多分类器内部的之间支持度的纯度越低, 则多分类器的分类效果越为明显. 纯度因子的具体计算过程如式 (8) 和式 (9) 所示:

$$P\left(O_i\right)=\sum_{k=1}^{5}O_i^k\left(1-O_i^k\right)=1-\sum_{k=1}^{5}\left(O_i^k\right)^2 \tag{8}$$

$$Pure\left(m_i\right)=\frac{P\left(O_i\right)}{\sum_{i=1}^{3}P\left(O_i\right)} \tag{9}$$

2.4 D-S 证据理论融合

在计算离散因子和纯度因子后, 结合两个因子将得到证据的权重. 通过式 (10) 和式 (11) 融合两个因子计算得到证据最终的权重, ρ 的区间属于 [0, 1].

$$W\left(O_i\right)=\frac{\rho Dis\left(m_i\right)+\left(1-\rho\right)Pure\left(m_i\right)}{max_{1\leqslant i\leqslant 5}\left\{\rho Dis\left(m_i\right)+\left(1-\rho\right)Pure\left(m_i\right)\right\}} \tag{10}$$

$$\epsilon=\begin{cases}m(\theta)=\dfrac{\sum_{\cap\theta_k=\theta}\prod_{i=1}^{n}W_i^c m_i(\theta_k)}{1-\sum_{\cap\theta_k\neq\varnothing}\prod_{i=1}^{n}W_i^c m_i(\theta_k)},\ \theta\neq\varnothing,\forall\theta_k\in\vartheta\\ m(\theta)=0,\ \theta=\varnothing\end{cases} \tag{11}$$

2.5 算法实现

SDN 环境下基于改进 D-S 理论算法检测 DDoS 攻击算法具体如算法 1 所示.

算法 1 中, 首先调用 RYU 控制器提供的北向接口获取交换机与控制器交互的 *OpenFlow* 消息和流表项. 随后计算 *packert_in rate*, *byte_rate* 和 *paket_rate* 等特征. 将计算后的流表项特征记为 *Feature_x*, 并作为二分类器的输入, 按样本类别顺序依次训练 M 个基分类器, 包含 ($O_{i,1,2}$, $O_{i,1,3}$, ⋯ , $O_{i,3,4}$, $O_{i,4,5}$, i=1, 2, 3). 在本文中, M=10, N=5. 训练完不同的基分类器后, 本文将 10 个基分类器的输出构建成一个 10×5 的矩阵φ; 得到矩阵φ后, 通过式 (4), 式 (5) 和式 (6) 计算得到多分类器O_i, 式 (7) 和式 (8) 计算获得第 i 个多分类器分类类别为 j 的离散因子$Dis(m_i)$; 在得到多分类器O_i后, 式 (9) 和式 (10) 计算多分类器O_i内部之间的纯度因子 $Pure(m_i)$; 使用式 (11) 和式 (12) 结合离散因子和纯度因子得到最终调整权重后的多分类器分类结果, 获得最终的 DDoS 攻击检测结果.

算法 1. 改进 D-S 证据理论检测算法

Feature_x=*packert_in rate*, *byte_rate*, *paket_rate*
M, *N*←5, 10
BPA, ϕ←[], []
For *i* **in** *N* **do**
  O_i=*Binary_base*(*Feature_x*)
  For *j* **in** *M* **do**
    φ.append(O_i)
    $\tau_i^j=\left(O_{i,1,2}^j,O_{i,1,3}^j,O_{i,1,4}^j,\cdots,O_{i,3,4}^j,O_{i,4,5}^j\right)$
    $Dis(m_i)$=*Dis_calculate*($_i^j$)
  $m_i=O_i=\frac{\sum_{i=1}^{10}\tau_i^j}{\sum_{j=1}^{5}\sum_{i=1}^{10}\tau_i^j}=(O_i^1,O_i^2,O_i^3,O_i^4,O_i^5)$
  BPA.append(m_i)
  End
End
For *i* **in** BPA **do**
  $Pure(m_i)$ =*Pure_calculate*(BPA_i)
End
R=*Dempster_fusion*(*Dis*,*Pure*)

3 实验分析

本节对提出的算法进行了实验验证及分析. 在本节中, 所提方法被命名为 DFDoS-DS. 实验评估中, 通过比较精度、准确率、召回率、*F*-score 值和混淆矩阵等指标, 本节对比了文献 [13] 和文献 [17] 的算法. 其中, 文献 [13] 和文献 [17] 的算法分别被命名为 Ensemble-DS 和 SVM-DS.

3.1 实验设置

实验中, 本文在配置 i5 的 CPU 的计算机上运行 Mininet 2.2.2 软件用于生成如图 2 所示的网络拓扑. 此外, 本文将 RYU 4.9.1 作为 SDN 中的控制器. 本文通过设置带外模式使用 Mininet 软件搭建网络拓扑并连接 RYU 控制器. 根据相关研究工作[21−24], 本文按如下方式生成该网络中的背景流量: 背景流量由不同协议组成, 其中 TCP 协议占比 80%, UDP 协议占比 15%, ICMP 协议占比 5%. 同时, 背景流量中数据包的大小和速率服从泊松分布. 此外, 本文使用了两种攻击方式: (1) 攻击者将通过泛洪的方式发起高速 DDoS 攻击, (2) 攻击者通过控制 (*T*, *L*, *R*) 参数以周期性的方式发起低速 LDDoS 攻击, 其中, *T* 是发起攻击周期, *L* 是发起攻击持续脉冲长度, *R* 是发起攻击速率[25,26].

3.2 实验评估

本节对比了 DFDoS-DS 算法和 Ensemble-DS 算法以及 SVM-DS 算法的有效性. 在表 1 中, 本文通过混淆矩阵、精度、准确率、召回率以及 *F*-score 值对比 DFDoS-DS 算法、Ensemble-DS 算法和 SVM-DS 算法. 图 3、图 4 和图 5 是 DFDoS-DS 算法, Ensemble-DS 算法和 SVM-DS 算法的混淆矩阵. 在混淆矩阵指标中, 混淆矩阵中的 *y* 轴表示样本的真实分类值, *x* 轴则表示样本的预测分类值.

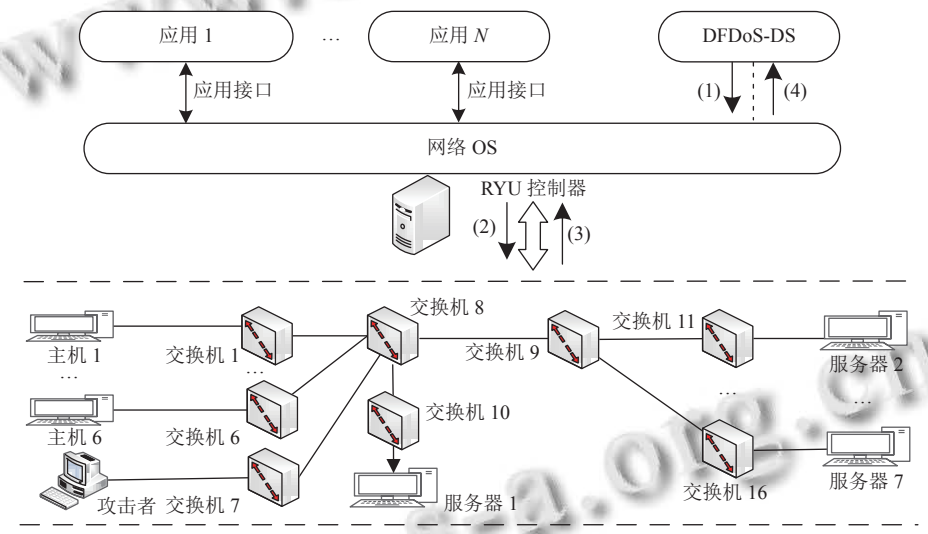

图 2 实验网络拓扑图

表 1 准确率、精度、召回率和 *F*-score 对比 (%)

方法	准确率	精度	召回率	*F*-score值
DFDoS-DS	**97**	**97**	**98**	**98**
Ensemble-DS	95	93	96	95
SVM-DS	62	64	65	57

如表 1 所示, DFDoS-DS 算法的准确率、精度召回率和 *F*-score 达到了 97%、97%、98% 和 98%, 同时, SVM-DS 的精度、准确率、召回率和 *F*-score 是 62%、64%、65% 和 57%. 与 SVM-DS 比较了精度、准确率、召回率和 *F*-score, DFDoS-DS 算法增加了 56%、51%、51% 和 72%. 同时, 相比 Ensemble-DS, DFDoS-DS 算法的上述指标分别增加了 2%、4%、2% 和 3%.

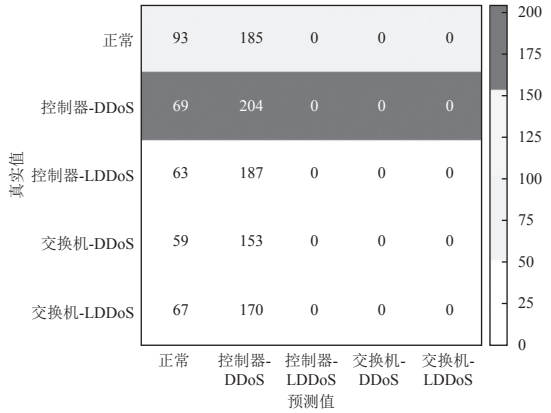

图 3 SVM-DS 算法混淆矩阵

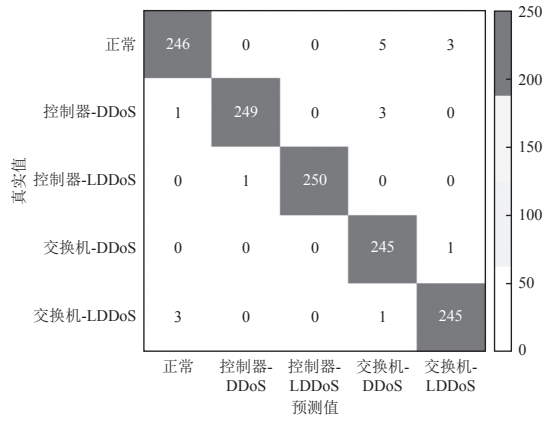

图 4 DFDoS-DS 算法混淆矩阵

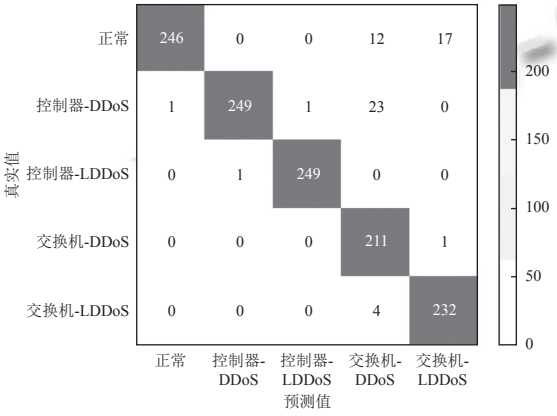

图 5 Ensemble-DS 算法混淆矩阵

4 结论

本文提出了一种 SDN 环境下基于改进 D-S 理论的 DDoS 攻击检测方法. 在改进 D-S 证据理论算法中, 本文设计了离散因子和纯度因子, 用于衡量 D-S 证据理论中证据源之间的冲突: 离散因子通过支持相同类别的支持度之间的熵值计算得到; 纯度因子是指多分类器内部的不同类别之间的支持度的 Gini 指数. 最后, 本文结合两种因子调整 D-S 证据源, 并通过 Dempster 规则融合得到最终的分类结果. 本文对别了 DFDoS-DS 算法和 Ensemble-DS 算法以及 SVM-DS 算法, 实验结果证明本文提出的方法取得较为优异的结果.

参考文献

1 Rawat DB, Reddy SR. Software defined networking architecture, security and energy efficiency: A survey. IEEE Communications Surveys & Tutorials, 2017, 19(1): 325–346.

2 Xie RJ, Xu MW, Cao JH, *et al*. SoftGuard: Defend against the low-rate TCP attack in SDN. Proceedings of 2019 IEEE International Conference on Communications. Shanghai: IEEE, 2019. 1–6.

3 龙霏, 余铮, 刘芬, 等. 改进 PSO-LSSVM 算法的 SDN 网络流量预测模型. 计算机系统应用, 2021, 30(7): 283–289. [doi: 10.15888/j.cnki.csa.008039]

4 李佟, 韩春静, 李俊. SDN 网络虚拟化中规则映射研究. 计算机系统应用, 2017, 26(9): 238–245. [doi: 10.15888/j.cnki.csa.005970]

5 王全民, 韩晓芳. 基于 Netflow 的网络安全大数据可视化分析. 计算机系统应用, 2019, 28(4): 1–8. [doi: 10.15888/j.cnki.csa.006836]

6 Kuzmanovic A, Knightly EW. Low-rate TCP-targeted denial of service attacks: The shrew vs. the mice and elephants. Proceedings of 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. Karlsruhe: ACM, 2003. 75–86.

7 Xie SX, Xing CY, Zhang GM, *et al*. Research on LDoS attack detection and defense mechanism in software defined networks. Proceedings of the 6th International Symposium on Security and Privacy in Social Networks and Big Data. Tianjin: Springer, 2020. 85–96.

8 Sahoo KS, Puthal D, Tiwary M, *et al*. An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics. Future Generation Computer Systems, 2018, 89: 685–697. [doi: 10.1016/j.future.2018.07.017]

9 奚玉龙. 基于深度学习的 DDoS 攻击检测模型. 计算机系统应用, 2021, 30(4): 216–221. [doi: 10.15888/j.cnki.csa.007649]

10 Wang WT, Ke X, Wang LX. A HMM-R approach to detect L-DDoS attack adaptively on SDN controller. Future Internet, 2018, 10(9): 83. [doi: 10.3390/fi10090083]

11 Zhao YX, Jia RF, Shi P. A novel combination method for conflicting evidence based on inconsistent measurements. Information Sciences, 2016, 367: 125–142. [doi: 10.1016/j.ins.2016.05.039]

12 尹东亮, 黄晓颖, 吴艳杰, 等. 基于云模型和改进 D-S 证据理论的目标识别决策方法. 航空学报, 2021, 42(12): 299–310.

13 Wang Z, Wang RX, Gao JM, *et al*. Fault recognition using an ensemble classifier based on Dempster-Shafer theory. Pattern Recognition, 2020, 99: 107079. [doi: 10.1016/j.patcog.2019.107079]

14 陈鸿昶, 程国振, 伊鹏. 基于多尺度特征融合的异常流量检

测方法. 计算机科学, 2012, 39(2): 42–46. [doi: 10.3969/j.issn.1002-137X.2012.02.010]

15 诸葛建伟, 王大为, 陈昱, 等. 基于 D-S 证据理论的网络异常检测方法. 软件学报, 2006, 17(3): 463–471.

16 李佳, 范巍. 基于改进 D-S 证据理论的网络入侵检测. 控制工程, 2017, 24(11): 2362–2367.

17 Pan Y, Zhang LM, Wu XG, *et al*. Multi-classifier information fusion in risk analysis. Information Fusion, 2020, 60: 121–136. [doi: 10.1016/j.inffus.2020.02.003]

18 Xiao FY. Evidence combination based on prospect theory for multi-sensor data fusion. ISA transactions, 2020, 106: 253–261. [doi: 10.1016/j.isatra.2020.06.024]

19 Li SB, Liu GK, Tang XH, *et al*. An ensemble deep convolutional neural network model with improved D-S evidence fusion for bearing fault diagnosis. Sensors, 2017, 17(8): 1729. [doi: 10.3390/s17081729]

20 Lukaseder T, Maile L, Erb B, *et al*. SDN-assisted network-based mitigation of slow DDoS attacks. Proceedings of the 14th International Conference on Security and Privacy in Communication Systems. Singapore: Springer, 2018. 102–121.

21 Braga R, Mota E, Passito A. Lightweight DDoS flooding attack detection using NOX/OpenFlow. Proceedings of IEEE Local Computer Network Conference. Denver: IEEE, 2010. 408–415.

22 Borgnat P, Dewaele G, Fukuda K, *et al*. Seven years and one day: Sketching the evolution of Internet traffic. Proceedings of IEEE INFOCOM 2009. Rio de Janeiro: IEEE, 2009. 711–719.

23 Cui YH, Yan LS, Li SF, *et al*. SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks. Journal of Network and Computer Applications, 2016, 68: 65–79. [doi: 10.1016/j.jnca.2016.04.005]

24 Singh J, Behal S. Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. Computer Science Review, 2020, 37: 100279. [doi: 10.1016/j.cosrev.2020.100279]

25 Pascoal TA, Fonseca IE, Nigam V. Slow denial-of-service attacks on software defined networks. Computer Networks, 2020, 173: 107223. [doi: 10.1016/j.comnet.2020.107223]

26 Yue M, Liu L, Wu ZJ, *et al*. Identifying LDoS attack traffic based on wavelet energy spectrum and combined neural network. International Journal of Communication Systems, 2018, 31(2): e3449. [doi: 10.1002/dac.3449]

(校对责编: 孙君艳)