文章编号：2095-2163(2020)07-0257-04 中图分类号：TP393 文献标志码：A

基于 SOINN 的 DDoS 攻击检测方法研究

李慧敏
（福建船政交通职业学院 信息工程系，福州 350007）

摘 要： 分布式拒绝服务(DDoS)攻击是一种分布式、协作式的大规模网络攻击方式。目前很多 DDoS 攻击检测方法虽然对已知类型攻击具有较高的检测率，但在攻击形式快速变化时，缺乏对新攻击类型的有效检测。因此，本文提出了一种基于 SOINN 的 DDoS 攻击检测方法。在对攻击流量进行分析的基础上，抽取出 5 个重要特征，以此建立 SOINN 检测模型，通过实验验证表明，该方法对已知攻击流量的检测率高、误判率低，而且 SOINN 的增量式学习特性有助于发现新的攻击类型。

关键词： DDoS 攻击；SOINN；攻击检测；增量学习

Research on DDoS attack detection methods based on SOINN

LI Huimin
（Department of Information Engineering, Fujian Chuanzheng Communications College, Fuzhou 350007, China）

【Abstract】 Distributed denial of service (DDoS) attack is a distributed and cooperative large-scale network attack. Although many DDoS attack detection methods have high detection rate for known types of attacks, they lack of effective detection of new attack types when the attack forms change rapidly. A DDoS attack detection method based on SOINN is proposed. Based on the analysis of attack traffic, five important features are extracted to establish the SOINN detection model. Finally, the effectiveness of the detection method is verified by experiments. Experimental results show that this method has high detection rate and low misjudgment rate for known attack traffic, and the incremental learning feature of SOINN is helpful to detect new attack types.

【Key words】 DDoS attack; SOINN; attack detection; incremental learning

0 引 言

根据卡巴斯基实验室发布的研究报告[1]与相关调查[2]显示，在 2020 年第一季度，DDoS 攻击的数量和质量均呈现出显著增加的趋势。与上一个报告周期相比，攻击次数增长了一倍；与 2019 年第一季度相比，攻击次数增长了 80 %。与此同时，攻击的持续时间也变得更长，这些数据表明 DDoS 攻击长期处于总体上升趋势，而且已经对系统和网络形成了严重的安全威胁。分布式拒绝服务攻击(DDoS)是一种分布的、协同的大规模攻击方式，多个攻击者从多方向同时向受害者发动攻击，或者一个攻击者可以利用僵尸网络对目标同时实施攻击，最终导致被攻击目标的系统资源耗尽甚至崩溃，而影响正常用户使用。

在 DDoS 防御中，攻击检测是主要采用的方法之一。然而在实际网络环境中，攻击流量和合法流量相似度极高，使得 DDoS 攻击自动检测很难实现。目前 DDoS 攻击检测算法很多，如基于统计分析的检测方法[3]、基于熵值的检测方法[4]和基于机器学习的检测方法[5]等。自组织增量式神经网络(SOINN)[6]，是一种无监督聚类算法。其可以在线增量式学习；动态更新神经网络；而且不影响之前的学习结果；存储和运算开销小。因此，本文提出了一种基于 SOINN 的 DDoS 攻击检测方法。在对攻击流量进行分析的基础上，综合借鉴国内外专家学者的观点，抽取出网络流量的 5 个重要特征，采用 SOINN 算法进行 DDoS 攻击流量的检测。实验结果表明，该方法对已知攻击流量的检测率高、误判率低，而且后续通过在线增量式学习，可以动态更新检测模型，有助于发现新的攻击类型。

1 相关研究

如今，DDoS 攻击已经是主要的网络安全威胁之一。目前主要的解决方案是实施实时网络监控，当检测到攻击发生时，启动相关安全设备屏蔽攻击源，从而避免后续侵害。为了快速、准确地检测出 DDoS 攻击，已有很多学者在这方面做了大量工作。Mousavi 等[7]以数据包目的 IP 地址熵值作为特征值来检测攻击流量，该方法实现简单，检测率较高，但因其只有一个特征值，表达能力有限，无法覆盖种类繁多的攻击类型。因此，在不同的网络环境下，该

基金项目： 福建省教育厅中青年教师教育科研项目(JAT191194)。

作者简介： 李慧敏(1985-)，女，硕士，讲师，主要研究方向：网络与智能信息技术。

收稿日期： 2020-04-28

方法的检测率不够稳定。Feng 等[8]提出了基于遗传算法的检测方法,该方法抽取了流量的 5 个重要统计特征,组成特征向量; Braga 等[9]以流量六元组作为基础,引入 SOM 算法。但 SOM 算法的神经网络结构比较固定,对检测率有所影响。刘纪伟等[10]提取出流量八元组联合特征,并将增量式 GHSOM 算法引入攻击检测,解决了 SOM 算法存在的问题。

综上所述,已有多种类型的 DDoS 攻击检测方法,但还存在较多问题:检测时延长;检测精度低;误报率较高;对新型 DDoS 攻击检测能力较弱等。本文针对上述问题,提出了一种基于 SOINN 的 DDoS 攻击检测方法,该方法有较高的检测精度、误报率低,而且对新出现的 DDoS 攻击类型检测率高。

2 基于 SOINN 的 DDoS 攻击检测方法

2.1 DDoS 攻击流量特征提取

基于 DDoS 攻击流量的主要特征,本文提出流量的 5 个特征,见表 1,以此作为攻击流量检测的基础。

表 1 流量特征

Tab. 1 Flow Characteristics

特征名称	特征含义
$R(sip,dip)$	上下行流量速率差
$AP(dip)$	平均数据分组量
$AB(dip)$	平均比特数
$H(sip \mid dip)$	源 IP 地址 sip 关于目的 IP 地址 dip 的条件熵
$H(dport \mid dip)$	目的端口 dport 关于目的 IP 地址 dip 的条件熵

表 1 中, sip 表示源 IP 地址, dip 表示目的 IP 地址, $dport$ 为目的端口。令 $pcount(sip,dip)$、$bcount(sip,dip)$ 分别表示源 IP 地址到目的 IP 地址的数据包数和字节数, N 表示目的地址对应的源 IP 地址数量; $p(sip \mid dip)$、$p(dport \mid dip)$ 分别表示源 IP 地址和目的端口关于目的 IP 地址的条件概率。在检测过程中,先对网络流量进行采样处理,提取出检测样本集:

$$M = \{(m_i, n_i), i = 1, 2, \cdots, K\}。$$

其中, $m_i = \{R(sip,dip), AP(sip), AB(sip), H(sip \mid dip), H(dport \mid dip)\}_i$; n_i为分类标签,即该样本属于攻击流量或正常流量; K 为样本数目。

在对攻击流量进行分析的基础上,综合借鉴国内外专家学者的观点,发现 DDoS 攻击流量的主要特征体现在以下几个方面:

(1)双向流量差。一般情况下,对目标系统的访问流量会大于其返回给源系统的流量。而当发生 DDoS 攻击时,大量系统资源被占用,情况则发生反转。所以,当双向流量出现反向速率差时,很大概率表明发生了 DDoS 攻击。上下行流量速率差的计算如(1)所示。

$$R(sip,dip) = \frac{bcount(sip,dip)}{pcount(sip,dip)} - \frac{bcount(dip,sip)}{pcount(dip,sip)}. \tag{1}$$

(2)数据分组数量、大小特征。DDoS 攻击流量一般是用工具生成的,大小固定,并经常进行 IP 伪装或利用僵尸网络发送,而正常流量一般是无规律的。平均数据分组量的计算如(2)所示。

$$AP(dip) = \frac{\sum_j pcount(sip_j, dip)}{N}. \tag{2}$$

另外,在 DDoS 攻击中,攻击者经常会对攻击目标发送大量比特数较小的数据分组。例如,在 TCP 泛洪攻击中发现大量的 120B 的数据分组。因此,以平均比特数作为检测攻击流量的重要特征之一,其计算如(3)所示。

$$AB(dip) = \frac{\sum_j bcount(sip_j, dip)}{N}. \tag{3}$$

(3)多对一映射。确定攻击目标(唯一)后,攻击者出于最大化获利或逃避追责等目的,采用僵尸网络、跳板等手段,尽可能伪装源 IP 地址。与正常流量相比,攻击流量的源 IP 地址数量多、变化快;同时,对同一个攻击目标,攻击者会尽可能地对目标所提供的所有服务发起连接,涉及多个目的端口。当某一随机变量为定值时,另一变量的随机性分布可以通过条件熵表示出来。因此,本文通过条件熵来表示源 IP 地址、目的端口与目的 IP 地址之间的多对一映射关系。根据条件熵的定义,可以得到:

$$H(sip \mid dip_k) = -\sum_j p(sip_j \mid dip_k) \log p(sip_j \mid dip_k), \tag{4}$$

$$H(dport \mid dip_k) = -\sum_j p(dport_j \mid dip_k) \log p(dport_j \mid dip_k). \tag{5}$$

2.2 SOINN 算法

SOINN 是一种增量式竞争型神经网络[6],可以在线学习,动态更新神经网络,并且不影响之前的学习成果,这种机制可以降低学习过程中的存储和运算开销。同时,其网络去噪机制使得其具有较强的鲁棒性。算法主要步骤如下:

(1)在每个竞争学习周期内,初始化神经元集

合 $M=\{s_1,s_2\}$。其中，s_1、s_2 是随机的两个初始数据样本，初始化神经元连接关系集合 $C \subseteq M \times M$ 为空集。

(2) 输入新样本 ξ，基于 L_2 范数，找出 M 中与 ξ 最相似的神经元 s_1 和 s_2(获胜神经元)。即：

$$s_1 = argmin \| \xi - W_\tau \|, \tau \in M, \quad (6)$$

$$s_2 = argmin \| \xi - W_\tau \|, \tau \in M \backslash \{S_1\}. \quad (7)$$

其中，$W\tau$ 表示神经元 τ 的权重。

(3)计算相似度阈值 T_{s1} 和 T_{s2}。相似度阈值的计算方法如(8)：

$$\begin{cases} T\tau = \max \| W_\tau - W_j \|, j \in M_\tau, \\ T\tau = \min \| W_\tau - W_j \|, j \in M \backslash \{\tau\}. \end{cases} \quad (8)$$

其中，M_τ 为 τ 的邻居神经元集合。

若 $\| \xi - W_{s1} \| > T_{s1}$ 或 $\| \xi - W_{s2} \| > T_{s2}$ 成立，则 $M = M \cup \{\xi\}$。ξ 作为新生成神经元加入集合，并返回步骤 (2)，否则继续执行。

(4) 若 s_1 和 s_2 不存在连接关系，则为其增加新连接，即 $C = C \cup \{(s_1,s_2)\}$。

(5) 更新获胜节点 s_1 所有边的年龄参数，即 $age(s_1,i) = age(s_1,i) + 1, i \in M_{s_1}$，$M_{s_1}$ 为 s_1 的所有邻居神经元。

(6) 更新获胜神经元权重。

$$W_{s_1} = W_{s_1} + \epsilon(t)(\xi - W_{s_1}), \quad (9)$$

$$W_{s_2} = W_{s_2} + \epsilon'(t)(\xi - W_{s_2}). \quad (10)$$

其中，$\epsilon(t)$ 和 $\epsilon'(t)$ 为学习率；$\epsilon(t) = \frac{1}{t}$；$\epsilon'(t) = \frac{t}{100}$；$t$ 代表获胜次数。

(7)每个竞争学习周期完结时，需要执行神经元去噪。即如果神经元的年龄参数大于预定值，即 $age(i,j) > age_{max}$，$C = C\backslash\{(i,j)\}$，则执行删除操作。若竞争学习未结束，则返回步骤(2)。

最后输出神经元集合 M 和连接关系集合 C。

2.3　DDoS 攻击检测方法

DDoS 攻击检测方法的基本思想是：先进行初始训练，得到一个初始模型，然后在初始模型的基础上进行在线增量式学习，动态更新检测模型。具体步骤如下：

(1)根据训练样本，经过 SOINN 算法得到一个成熟的 SOINN 初始模型。

(2)从网络流量中提取出一个竞争学习周期的检测样本集(包含 K 个样本)。

(3)按顺序将检测样本输入检测模块，寻找其的获胜神经元；

(4)对比检测样本与获胜神经元，确定检测样本的类型并进行后续处理(转发或记录)。如果该样本的检测结果与获胜神经元不为同一类型，则有可能发现新攻击类型，将其添加到神经元集中。

(5)更新获胜节点所有边的年龄参数，更新获胜神经元权重。每学习完 K 个样本，表示竞争学习周期结束。此时需要执行神经元去噪，即如果神经元的年龄参数大于预定值，则执行删除操作，得到新模型，增量学习结束。如果竞争学习周期未结束，则返回步骤(3)。

基于 SOINN 的 DDoS 攻击检测流程如图 1 所示。

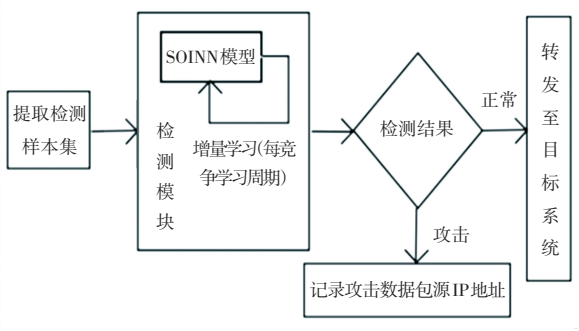

图 1　基于 SOINN 的 DDoS 攻击检测流程

Fig. 1　DDoS attack detection flow based on SOINN

3　实验结果及分析

本文的实验环境配置：CPU 为 Intel(R) Core(TM) i7-6700 @ 3.40GHz、8G 内存、硬盘 1T、操作系统为 Ubuntu16.04，采用 Python 语言实现。本文采用 ISCX 数据集训练检测模型，该数据集收集了 7 天的真实网络环境中的流量信息，其中包含合法的网络流量以及多种类型的恶意 DDoS 攻击流量。

实验包括训练和检测两个阶段，每个阶段分别从数据集中采样计算，生成训练样本集(2 000 个)和检测样本集(1 000 个)。

(1)离线验证本文方法对已知攻击类型的检测效果。选择 KNN、SVM 及 BRAGA[10] 等人提出的 SOM 神经网络算法作为对比对象；实验结果采用检测率和误判率两个指标进行评价。其中，检测率为将攻击流量预测为攻击流量的样本数的概率；误判率为将正常流量预测为攻击流量样本数的概率。实验结果见表 2。

由表 2 数据可以看出，本文检测方法拥有较高的检测率及较低的误判率。

(2)验证本文方法对新增类型 DDoS 攻击的检测效果。初始训练样本集由正常流量样本和 5 种类型 DDoS 攻击流量样本组成。在线检测样本集中增

了 1 种新攻击流量样本,具体组成情况见表 3。

表 2 实验结果

Tab. 2 Experimental results

检测方法	检测率	误判率
SOINN	97.5%	3.2%
KNN	95.6%	4.1%
SVM	96.4%	4.3%
SOM	97.1%	3.5%

表 3 样本集组成

Tab. 3 Composition of sample set

攻击类型	训练样本集	在线检测样本集
正常流量	2 000	1 000
SYN 泛洪	2 000	1 000
ICMP 泛洪	2 000	1 000
UDP 泛洪	2 000	1 000
LAND 攻击	2 000	1 000
XMAS 攻击	2 000	1 000
Smurf 攻击	—	1 000

首先进行初始训练,得到一个初始模型。然后在初始模型基础上进行在线增量式学习,动态更新检测模型。检测结果见表 4。

表 4 SOINN 模型动态更新检测效果

Tab. 4 Detection effect of SOINN model when dynamic update %

攻击类型	初始模型检测率	模型增量后检测率
SYN 泛洪	99.1	100
ICMP 泛洪	93.4	97.6
UDP 泛洪	94.6	96.5
LAND 攻击	90.5	93.7
XMAS 攻击	93.6	96.5
Smurf 攻击	—	98

在此,初始训练模型检测率是利用表 3 初始训练样本集,训练得到初始模型的检测结果,模型增量后检测率是动态更新后的检测结果。从表 4 中数据可见,本文方法的检测率较高,而且可以动态更新,有助于发现新攻击类型,且更新后不影响原学习结果,保证了对原攻击类型的检测率。

以上实验结果验证了本文提出的基于 SOINN 的 DDoS 攻击检测方法的可用性。

4 结束语

DDoS 攻击如今已经是主要的网络安全威胁之一,而且长期处于总体上升趋势。在 DDoS 防御中,攻击检测是重中之重。本文提出了一种基于 SOINN 的 DDoS 攻击检测方法,根据 DDoS 攻击流量的特点提取了流量的 5 个特征,在此基础上采用 SOINN 算法进行 DDoS 攻击流量的检测,并通过实验验证。由于未对大规模 DDoS 攻击网络流量进行验证实验,则今后将针对模型的可扩展性、适应性、高性能等开展进一步的研究。

参考文献

[1] 卡巴斯基. 卡巴斯基实验室: 2019 年 Q1 全球近 60% 的 DDoS 攻击的目标是中国[EB/OL]. [2020-04-20]. http://www.199it.com/archives/882603.html.

[2] 胡义裁. 2020 第 1 季度 DDoS 攻击趋势[J]. 计算机与网络, 2020,10:51-53.

[3] Rup Kumar Deka, Dhruba Kumar Bhattacharyya, Jugal Kumar Kalita. Granger Causatity in Tcp Flooding Attack[J]. International Journal of Network Security, 2019, 21(1):30-39.

[4] 郭伟, 邱菡, 周天阳, 等. 基于 IP 熵变量的 DDoS 攻击溯源模型[J]. 计算机工程与设计, 2019(12):3367-3374.

[5] VINAYAKUMAR R, ALAZAB M, KP S, et al. Deep Learning Approach for Intelligent Intrusion Detection System[J]. IEEE Access, 2019:41525-41550.

[6] 邱天宇,申富饶,赵金熙. 自组织增量学习神经网络综述[J]. 软件学报,2016,27(9): 2230-2247.

[7] MOUSAVI S M, ST-HILAIRE M. Early detection of DDoS attacks against SDN controllers[C]//International Conference on Computing, Networking and Communications (ICNC), 2015: 77-81.

[8] FENG Y F, GUO R, WANG D Q, et al. Research on the active DDoS filtering algorithm based on IP flow[C]//Fifth International Conference on Natural Computation, 2009: 600-607.

[9] BRAGA R, MOTA E, PASSITO A. Lightweight DDoS flooding attack detection using NOX/OpenFlow [C]//IEEE Local Computer Network Conference, 2010: 408-415.

[10] 刘纪伟,李睿楠,张玉,等. 一种增量式 GHSOM 算法在 DDoS 攻击检测中的应用[J]. 南京邮电大学学报(自然科学版), 2020,40(3): 82-88.