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

姚琳元 董 平* 张宏科
(北京交通大学电子信息工程学院 北京 100044)

摘 要：软件定义网络(SDN)受到分布式拒绝服务(DDoS)攻击时，攻击方会发送大量数据包，产生大量新的终端标识占用网络连接资源，影响网络正常运转。为准确发现受攻击对象，检测被占用资源，利用 GHSOM 技术，该文提出基于对象特征的 DDoS 攻击检测方法。首先，结合 SDN 网络及攻击特点，提出基于目的地址的检测 7 元组，并以此作为判断目标地址是否受到 DDoS 攻击的检测元素；然后，采用模块化设计，将 GHSOM 算法应用于 SDN 网络 DDoS 攻击的分析检测中，并在 OpenDayLight 的仿真平台上完成了仿真实验。实验结果显示，该文提出的检测 7 元组可有效检测目标对象是否受到 DDoS 攻击。

关键词：软件定义网络；7 元组；自组织映射；分布式拒绝服务
中图分类号：TP393 **文献标识码**：A **文章编号**：1009-5896(2017)02-0381-08
DOI: 10.11999/JEIT160370

Distributed Denial of Service Attack Detection Based on Object Character in Software Defined Network

YAO Linyuan DONG Ping ZHANG Hongke
(*School of Electronic and Information Engineering*, *Beijing Jiaotong University*, *Beijing* 100044, *China*)

Abstract: During the Distributed Denial of Service (DDoS) attack happening in Software Defined Network (SDN) network, the attackers send a large number of data packets. Large quantities of new terminal identifiers are generated. Accordingly, the network connection resources are occupied, obstructing the normal operation of the network. To detect the attacked target accurately, and release the occupied resources, a DDoS attack detection method based on object features with the GHSOM technology is provided. First, the seven-tuple is proposed for detection to determine whether the target address is under attack by DDoS. Then, a simulation platform is built, which is based on the OpenDayLight controller. GHSOM algorithm is applied to the network. Simulation experiments are performed to validate the feasibility of the detection method. The results show that the seven-tuple for detection can effectively confirm whether the target object is under a DDoS attack.

Key words: Software Defined Network (SDN); Seven-tuple; Self-organization mapping; Distributed Denial of Service (DDoS)

1 引言

互联网的快速发展，网络用户规模的爆发式增长，传统网络架构随之面临各种各样的问题。为满足时延、负载等网络基本要求，许多网络协议、网络策略在设计之初被预先定义，造成传统 IP (Internet Protocol)网络难于更新，网络结构越发复杂，网络管理更加困难[1]。传统网络控制域与数据域相绑定，是造成网络难以管理的主要因素[2]。为从根本上解决网络痼疾，新型网络架构被相继提出。其中控制域与转发域相分离的思想受到业界的广泛关注，具有代表性的网络结构之一是近年来不断被寄予厚望的软件定义网络(Software Defined Networking, SDN)[3,4]。

传统网络中，控制逻辑分布在各个网络设备。这种分布式的网络结构在一定程度上降低了网络因遭受 Distributed Denial of Service (DDoS) 攻击全面瘫痪的风险。而在 SDN 网络中，控制器集中管理网络设备，增大了网络安全风险[5]。当 SDN 网络受到 DDoS(Distributed Denial of Service)攻击时，攻击方会发送大量数据包，这些数据包含有不同源地址、

收稿日期：2016-04-18；改回日期：2016-10-19；网络出版：2016-12-20
*通信作者：董平 pdong@bjtu.edu.cn
基金项目：国家 973 重点基础研究发展计划(2013CB329100)，国家 863 高技术研究发展计划(2015AA016103)，国家自然科学基金(61301081)，国家电网公司科技项目([2016]377)
Foundation Items: The National Key Basic Research Program of China (2013CB329100), The National High Technology Research and Development Program 863 (2015AA016103), The National Natural Science Foundation of China (61301081), SGRIXTJSFW ([2016]377)

目的地址等信息。为获取转发规则，交换机需要不断向控制器发送请求，以获得新的转发规则；控制器也需要不断响应交换机的请求，制定、下发相应规则，以至于控制器的存储资源、计算资源大量消耗，控制器与交换机的连接资源大量占用。文献[5]将 OpenFlow 下的 SDN 网络 DDoS 攻击归纳为两种，即控制域带宽攻击和交换机流表攻击。文献[6]也将控制域与数据域之间接口造成的固有通信瓶颈视为 SDN 网络的主要安全挑战之一。

冲突检测是一种有效探测 DDoS 攻击的方法。文献[7]对冲突探测进行了说明，并总结为签名探测技术和异常探测技术。统计分析和机器学习是两种主要的异常探测技术。该文阐述了机器学习的 6 种方法，即 Neural Networks, Support Vector Machine, Genetic Algorithms, Fuzzy Logic, Bayesian Networks, Decision Tree，并对 6 种方法的优缺点进行了总结。但是，文章缺乏与 SDN 的关联，没有给出解决 SDN 中控制器受到 DDoS 攻击的具体方法。

作为机器学习中的一种，神经网络的无监督学习可以在网络目标输出未知的情况下，通过自训练，聚类分析输入样本[8]，达到自动监测的目的。文献[9]利用神经网络中的自组织映射(Self-Organizing Map, SOM)技术实现对 SDN 网络的数据检测。该文提出了一种基于 SOM 技术的 DDoS 攻击检测方法，并在 SDN 网络控制器中实现了此方法。作者采用模块化的方法完成“数据流采集”、“特性提取”以及“攻击探测(数据包分类)”等功能。然而，该文献中的统计元素沿用传统网络的参考元素，并没有对 SDN 网络的数据特点进行分析。另外，SOM 要求预先确定神经元的数量和排列，致使神经元排列固定、单一，这在一定程度上限制了攻击检测的准确性。

文献[10]以目的 IP 地址作为参考要素，采用信息熵与阈值相结合的方法完成检测。虽然信息熵较 SOM 灵活、方便，但在阈值确定和多元素权重分配等方面仍需与其他技术结合。文献[11]提出了 Openflow 与 sFlow 相结合的数据采集方法，这在一定程度上提高了检测带宽。但文献[11]同文献[10]，使用了信息熵检测方法。文献[12]提出了 FortNOX 内核，优化了 SDN 网络中 NOX 控制器的安全性能，但并没有给出具体的 DDoS 攻击检测方法。文献[13]利用基于神经网络和生物威胁理论的计算机防御系统完成风险评估，实现对 DDoS 攻击的防御，但缺乏详尽的实现方案和效果对比。

通过上述分析可知，面向 SDN 网络的 DDoS 攻击检测方法主要包括 SOM 技术和信息熵。但是，SOM 技术要求训练前完成神经元数量和排列的预先确定，而信息熵通常与相应参数的阈值共同使用，难以独立完成对多维数据的分析与检测。而一种基于 SOM 技术的 GHSOM(Growing Hierarchical SOM)[14]技术更加灵活，且可以独立完成对多维数据的分析与检测。该技术已应用于传统网络的攻击检测中，如文献[8], 文献[15]，但在 SDN 网络上却缺乏相应的应用研究。鉴于此，利用 GHSOM 技术，本文提出了基于对象特征的 DDoS 攻击检测方法。

本文的创新性在于：(1)结合 SDN 网络及攻击特点，提出了基于目的地址的检测 7 元组，判断目标地址是否受到 DDoS 攻击；(2)采用模块化设计，将 GHSOM 应用于 SDN 网络 DDoS 攻击的分析检测中，并在 OpenDayLight 的仿真平台上完成了仿真实验。

本文内容如下：第 2 节介绍了 GHSOM 算法的原理与使用方法；第 3 节详细说明了基于对象特征的 DDoS 攻击检测方法；第 4 节完成检测方法的可行性分析，并进行了实验验证；第 5 节总结全文。

2 GHSOM 介绍

本节对 GHSOM 算法进行简单介绍。较 SOM 固定的神经元结构，GHSOM 具有生长、分层的特性，结构更加灵活，数据处理效率更高。GHSOM 算法总结如下[16]：

初始化：GHSOM 从第 0 层开始，该层只包括一个神经元 $\boldsymbol{e}_0$，其权重向量为 $\boldsymbol{m}_0=[\mu_{0_1},\mu_{0_2},\cdots,\mu_{0n}]^{\mathrm{T}}$，$\boldsymbol{m}_0$ 为输入数据的平均值；计算平均量化误差 $\boldsymbol{mqe}_0=(1/d)\|\boldsymbol{m}_0-\boldsymbol{x}\|$，其中 $\boldsymbol{x}$ 表示输入数据，d 表示输入数据的个数。

第 1 次映射：GHSOM 映射过程从第 1 层开始，如图 1，首先从第 0 层的神经元 $\boldsymbol{e}_0$ 扩展到第 1 层的 4 个神经元 A, B, C, D，然后从输入数据中取样执行 SOM 过程，完成输入数据的第 1 次映射。

SOM 过程：(1)相似性匹配：$\boldsymbol{e}_i(\boldsymbol{x})=\arg\min_j\cdot\|\boldsymbol{e}_j-\boldsymbol{x}\|$，$\boldsymbol{e}_i$ 表示获胜神经元，$\boldsymbol{e}_i$ 为 $\boldsymbol{e}_j$ 中的某一个；(2)更新：$\boldsymbol{e}_i(\boldsymbol{t}+1)=\boldsymbol{e}_i(\boldsymbol{t})+\alpha(t)h_{ci}(t)[\boldsymbol{x}(\boldsymbol{t})-\boldsymbol{e}_i(\boldsymbol{t})]$，$t$ 表示迭代次数，α 表示学习率参数，h_{ci} 表示获胜神

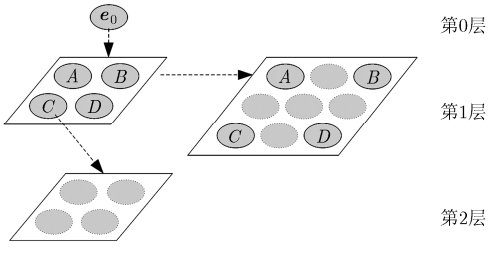


图 1 GHSOM 扩展说明

经元 i 周围的邻域函数。当在映射结果中看不到明显变化时，SOM 过程结束。

横向拓展：当映射神经元满足 $\boldsymbol{MQE}_m \geq \tau_m \boldsymbol{mqe}_0$ 时，进行横向拓展，找出映射神经元中最大量化误差的神经元 $\boldsymbol{e}_e$ 以及 $\boldsymbol{e}_e$ 临近神经元中最不同的神经元 $\boldsymbol{e}_d$，在二者间增加 1 列(行)神经元，然后完成 SOM 过程，并判断上述条件；当不满足上述条件时，进行纵向拓展。其中，$\boldsymbol{MQE}_m = \frac{1}{u}\sum_i \boldsymbol{mqe}_i$，$u$ 表示该映射中获胜神经元的个数；τ_m 为横向拓展参数。

纵向拓展：当映射神经元满足 $\boldsymbol{mqe}_i > \tau_u \boldsymbol{mqe}_0$ 时，进行纵向拓展，产生新的映射层，完成 SOM 过程，并重新进行横向拓展条件检验；当不满足上述条件时，映射结束。其中，τ_u 为纵向拓展参数。

3　基于对象特征的 DDoS 攻击检测方法

DDoS 攻击的目的主要在于资源占用和资源消耗[17]。对 SDN 网络而言，DDoS 攻击主要包括控制域带宽、流表条目两个方面[5]。当网络中的设备受到攻击时，交换机会接收到大量不同包头数据，流表条目会大幅增长，数据带宽会被大量消耗，严重时攻击会直接造成网络瘫痪。为准确检测网络是否遭受攻击，及时遏制攻击规模。当攻击者通过 DDoS 方式攻击网络目标时，其数据包目的地址、长度变化幅度单一，源地址、源端口、目的端口变化多样。根据这一特点，本文提出了基于对象特征的 DDoS 攻击检测方法。

该方法充分利用了 SDN 网络的可编程性以及控制器对网络的综合管理性，包括流信息采集、7 元组提取、数据训练与分析、命令下发 4 个部分，如图 2。

(1)流信息采集：　该部分负责向控制器数据库周期性发送信息请求，获取最新的网络流表信息，请求周期为 τ。

(2)7 元组提取：　SDN 网络遭受到 DDoS 攻击主要包括流表溢出和控制器带宽[5]。因此从层级角度分析，SDN 网络受到的网络攻击主要位于 OSI (Open System Interconnection)参考模型中的网络层和传输层。虽然 SDN 网络改变了传统网络路由设备的转发方式，但并没有改变数据包的封装结构，因此，目的 IP 地址仍然是数据包到达目的地的最终依据。如文献[11]中，作者便使用目的地址作为信息熵的参考对象。相对于受攻击对象的目的 IP 地址唯一性，为躲避安全防护系统，DDoS 攻击方会制造大量不同的源 IP 地址、端口数据包。针对这一特性，我们提出了基于被攻击对象目的地址的检测 7 元组，如表 1。接收到网络流表信息后，通过对特别要素的提取与检测，得到相应流表数据。

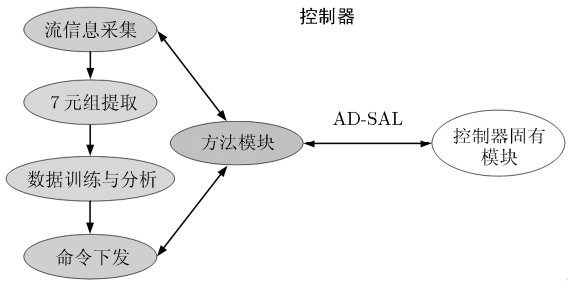


图 2 检测方法说明图

表 1 检测 7 元组

缩写	元素名称
S_{ip}_Num	一个目的 IP 地址对应源 IP 地址数量
$S_{\text{ip}}\_\text{Rate}$	一个目的 IP 地址对应源 IP 地址的变化速率
$S_{\text{port}}\_\text{Num}$	一个目的 IP 地址对应源端口数量
$S_{\text{port}}\_\text{Rate}$	一个目的 IP 地址对应源端口的变化速率
$D_{\text{port}}\_\text{Num}$	一个目的 IP 地址对应目的端口数量
$D_{\text{port}}\_\text{Rate}$	一个目的 IP 地址对应目的端口的变化速率
St_D	一个目的 IP 地址对应数据包长度的标准差

$S_{\text{ip}_i}\_\text{Num}$，$S_{\text{port}_i}\_\text{Num}$ 和 $D_{\text{port}_i}\_\text{Num}$ 表示在某次采样后对应的元素数目；$S_{\text{ip}_i}\_\text{Rate}$，$S_{\text{port}_i}\_\text{Rate}$，$D_{\text{port}_i}\_\text{Rate}$ 表示相邻两个周期对应元素前后两次取样数目差，用公式表示为

$$S_{\text{ip}_i}\_\text{Rate} = S_{\text{ip}_i}\_\text{Num}(T_1+\tau) - S_{\text{ip}_i}\_\text{Num}(T_1)$$

$$S_{\text{port}_i}\_\text{Rate} = S_{\text{port}_i}\_\text{Num}(T_1+\tau) - S_{\text{port}_i}\_\text{Num}(T_1)$$

$$D_{\text{port}_i}\_\text{Rate} = D_{\text{port}_i}\_\text{Num}(T_1+\tau) - D_{\text{port}_i}\_\text{Num}(T_1)$$

其中，T_1 表示某采样时刻。

St_i_D 表示在某次采样后目的 IP_i 的数据包长度标准差，用公式表示为

$$St_i\_D = \sqrt{\frac{1}{N_i}\sum_{j=1}^{N_i}\left(\text{Len}_{ij} - E\left(\text{Len}_i\right)\right)^2}\, E(\text{Len}_i) = \frac{1}{N_i}\sum_{j=1}^{N_i}\text{Len}_{ij}$$

N_i 表示目的 IP_i 在采样后数据包个数，Len_{ij} 表示目的 IP_i 在采样后的数据包 j 的长度，$E(\text{Len}_i)$ 表示目的 IP_i 在采样后数据包 j 长度的期望。

(3)数据训练与分析：　该部分采用 GHSOM 算法，对获取到的元素进行训练和检测。

训练过程主要包括 4 个部分：(a)初始化：按照

输入数据，计算第 0 层神经元权重向量，并计算出平均量化误差；(b)第 1 次映射：将第 0 层的独立神经元扩展为第 1 层的 4 个神经元，执行 SOM 过程，完成数据的第 1 次映射；(c)横向拓展：计算最新层获胜神经元的平均量化误差，并将其与第 0 层神经元的平均量化误差进行比较，确定是否进行横向拓展；如果满足横向拓展条件，在映射神经元中寻找最大量化误差的神经元以及与该神经元临近的最不同神经元，在二者间增加新列或行，继续 SOM 过程，并继续判定是否满足横向拓展条件；(d)纵向拓展：完成横向拓展后，判断映射神经元是否满足纵向拓展条件，如果需要纵向拓展，产生新的映射层，对新映射层重新进行 SOM 过程、横向拓展和纵向拓展。

检测过程将采样数据放入训练结果中进行比对，判断目标对象是否遭受到 DDoS 攻击。

(4)命令下发： 对发现异常目的地址，该部分负责向控制器数据库发送安全指令，修改流表内容，使交换机停止接收发向受攻击目的地址的数据包。

4 可行性分析与仿真验证

本节包括可行性分析与仿真验证两个部分。在可行性分析中，本文对 SOM 与信息熵的特点进行了总结，并对选取的 GHSOM 算法是否适合于 SDN 网络下的 DDoS 攻击进行了说明；另外，对本文提出的 7 元组是否可以充分体现 SDN 网络下的 DDoS 攻击数据特点进行了实验验证。在仿真验证中，本文搭建了网络环境，在 OpenDayLight 控制器下完成了检测方法，通过模拟实际数据，对所提方法的效果进行了分析。

4.1 可行性分析

(1)GHSOM 可行性分析： 针对 SDN 网络的 DDoS 攻击，信息熵和 SOM 是两种主要的探测方法。信息熵通常与相应参数的阈值共同使用，如文献[10]。该方法较 SOM 更加方便、灵活，对系统资源的占用更少。但是，阈值的设定过程会消耗一定的计算资源，而且，当需要分别计算并考虑多个参数的信息熵时，衡量各参数的权值也需要额外的算法实现。因此，信息熵灵活、方便的特点并不适用于对多维数据的分析与检测。

使用 SOM，首先对数据完成训练，得到合法数据与攻击数据的排列规律，依此规律完成对录入数据的检测。然而，SOM 要求在训练前完成神经元数量和排列的预先确定，相对 DDoS 攻击数据量大且多变、数据特征不明等特点，SOM 难以准确完成 SOM 神经元的数量和排列。此外，SOM 中神经元分布在同一映射层，而类型繁多的 DDoS 攻击数据加重了数据映射后的处理难度。

GHSOM 算法具有生长、分层的特性，可根据处理数据的复杂程度自动调整神经元层级和数量。其更加灵活的结构、更高的数据处理效率，更适用于 DDoS 攻击的数据检测。在传统的无中心网络中，GHSOM 算法已被广泛使用，如文献[8]，文献[15]。在 SDN 网络环境下，控制与数据相分离，控制器可以掌控全网数据，更有利于 GHSOM 算法的实现。因此，从算法的灵活性、完整度，以及自身的可实现性等角度考虑，GHSOM 算法较 SOM 算法和信息熵具有明显优势。

(2)检测 7 元组的可行性： 本文首次提出了基于目的地址的检测 7 元组，并以此作为判定 SDN 网络下 DDoS 攻击的参考要素。为验证所提 7 元组的可行性，本节对 7 元组进行了数据分析与说明。

网络拓扑如图 3 所示，控制器为 OpenDayLight (ODL)，连接 3 个 Openflow 交换机。Openflow 交换机 1，交换机 3 与普通交换机相连，主要为模拟数据的接入口；同时，与未被攻击的虚拟主机相连，虚拟主机用来模拟真实网络中的各种设备。3 台目标主机目标 1，目标 2，目标 3 作为被攻击对象，与 Openflow 交换机 2 连接。依据文献[18]中 3 种常见协议 ICMP, TCP, UDP 数据包的比例(5:85:10)，仿照 WIDE 项目[19]的数据流量，本文模拟了常规通信的数据流量，同时通过 tfn2k 攻击软件获得了攻击数据。

在数据采集中，为了能够保证每次取样的数据是在该时间间隔内正在通信的条目，取样周期 τ 为 5 s，并在每次取样后清空控制器流表，重新计时，重新取样。在取样过程中，我们选取了时长为 16τ 连续合法数据，4τ 攻击数据，攻击数据发生时间在合法数据的 T8~T11 之间(如图 4 所示)，攻击对象为图 3 中目标 1，目标 2，目标 3。通过对数据的采集分析，我们得到了图 4，图 5，图 6 的对比图。

图 4 中横坐标表示 16 个不同时段的目的 IP 地址，纵坐标分别表示不同时段不同目的 IP 对应的源 IP 数量(图 4(a))、源端口数量(图 4(b))和目的端口数量(图 4(c))。从 3 个子图中可以看出，每个图可分上下两部分。上半部分包括 3 条折线，对应的是图 3 中 3 个受攻击目标 1，目标 2，目标 3 在遭受 DDoS 攻击时对应的源 IP、源端口和目的端口数量；下半部分表示未遭受到攻击的目的 IP 地址对应的纵坐标数量。

从图 4 可以看出，本文选取的 S_{ip}_Num，$S_{\text{port}}\_\text{Num}$ 和 $D_{\text{port}}\_\text{Num}$ 3 个参考元素在被攻击对

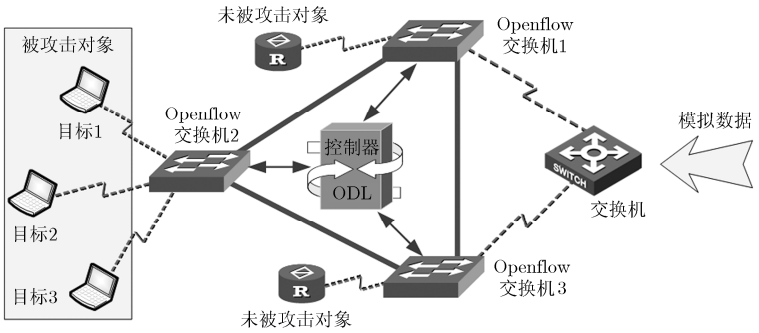
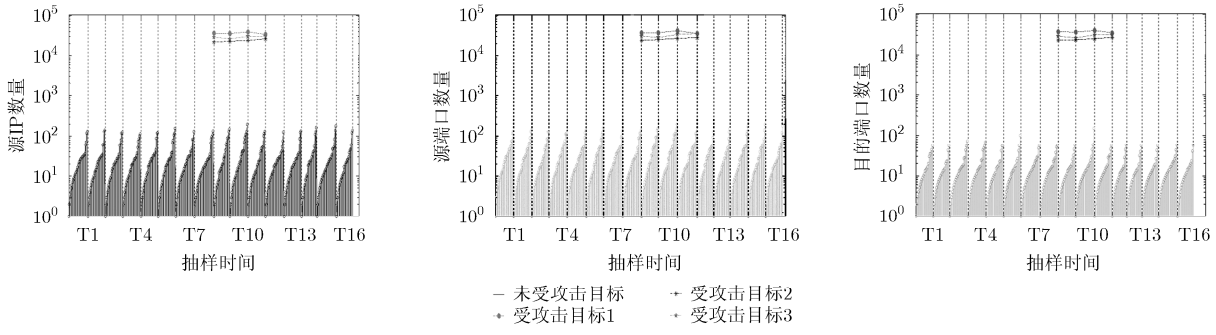
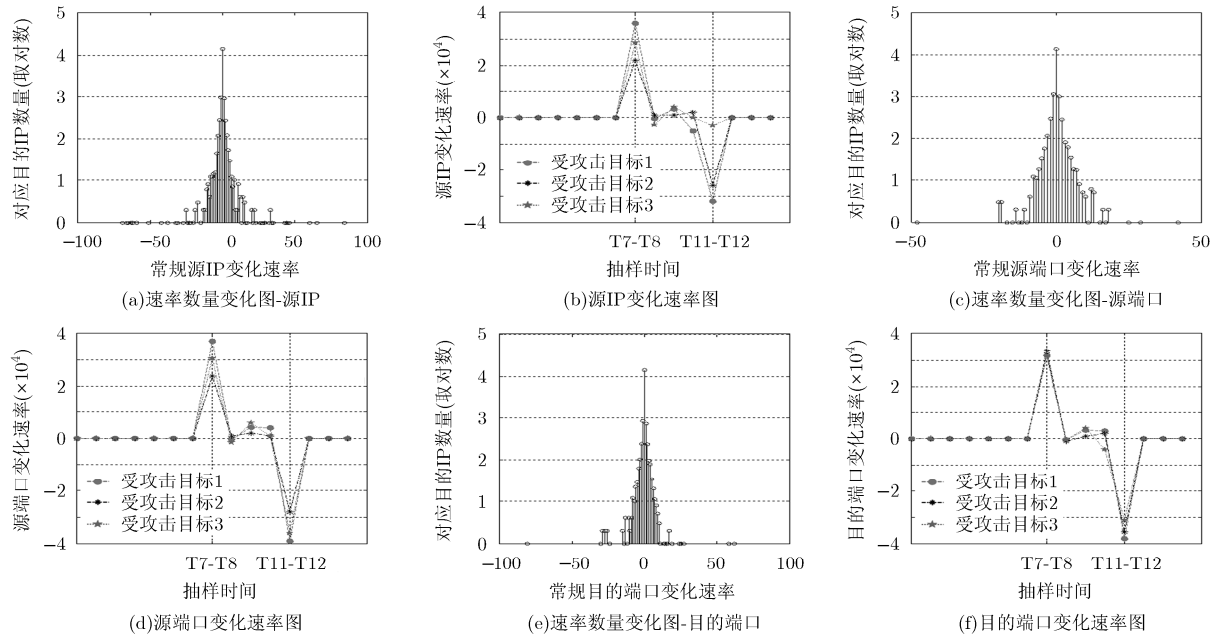


图 3 网络拓扑图



(a)源IP数量分布　(b)源端口数量分布　(c)目的端口数量分布

图 4　IP 与端口数量对比图



(a)速率数量变化图-源IP　(b)源IP变化速率图　(c)速率数量变化图-源端口

(d)源端口变化速率图　(e)速率数量变化图-目的端口　(f)目的端口变化速率图

图 5 变化速率对比图

象受到攻击前后变化十分明显，这也说明攻击者针对同一攻击对象伪造了大量不同头部的数据包。

图 5(a)，图 5(c)，图 5(e)横坐标分别表示正常通信中源 IP、源端口、目的端口的变化率，纵坐标表示不同变化率对应的目的 IP 地址数量。可以看出，源 IP 和目的端口的变化范围为(−100,100)，源端口的变化范围为(−50,50)，而且分布呈抛物线形式，越靠近中心点(横坐标为 0，即相邻 τ 变化速率为 0)，目的 IP 地址越多。

图 5(b)，图 5(d)，图 5(f)横坐标表示抽样时间，纵坐标表示图 3 中 3 个受攻击目标 1，目标 2，目标 3 在遭受 DDoS 攻击时对应的源 IP、源端口和目的

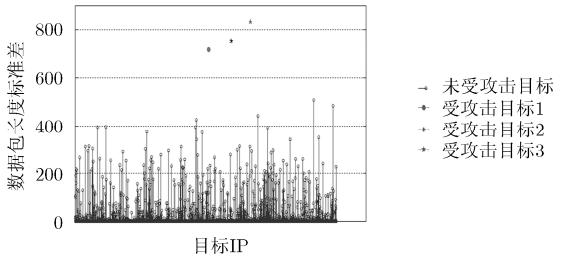


图 6 数据包长度标准差对比图

端口变化速率。在 T8 时刻，3 个目标受到攻击，可以看到其对应的变化速率迅速升高，当攻击结束时(T12 时刻)，变化速率迅速降低，在攻击过程中，各变化速率也在不停抖动。通过左右对比可以看出，合法数据的变化速率远远低于受到攻击时的速率。

图 5 说明本文选取的 $S_{\text{ip}}\_\text{Rate}$，$S_{\text{port}}\_\text{Rate}$ 和 $D_{\text{port}}\_\text{Rate}$ 可以充分体现被攻击对象受到攻击前后的不同特征。

图 6 为数据包长度标准差对比图，横坐标表示目标 IP，纵坐标表示目标 IP 对应的数据包长度标准差。上半部分 3 个点表示 3 个受攻击目标 1，目标 2，目标 3 在遭受 DDoS 攻击时的数据包长度标准差；下半部分为未受攻击下的标准差。从图中可以看出，虽然合法数据包的不同目的 IP 地址对应的数据包长度标准差大小不一，但攻击者发送的攻击数据包其数据包长度的标准差明显大于合法数据包长度的标准差。St_D 充分体现了被攻击对象受到攻击前后的差异性。

通过实际拓扑的搭建、数据的模拟，图 4，图 5，图 6 有力证明了文中所提出基于对象特征的 7 元组可以检测 SDN 网络是否遭受 DDoS 攻击的可行性。

4.2 仿真验证与结果分析

在 OpenDayLight 控制器(Helium 版本)上结合 Openflow1.0 完成了上文所提方法，并利用图 3 所示拓扑完成了数据的模拟、采集、训练和检测。与可行性检测类似，常规通信中训练、检测所用数据完全由 ICMP, TCP, UDP 3 种协议，按 5:85:10 比例构成，数据流量仿照 WIDE 项目；攻击数据通过 tfn2k 攻击软件获得；取样周期 τ 为 5 s。参数设置：$\tau_m = 0.7$，$\tau_u = 0.035$，学习速率 $\alpha(t) = 0.1/(1+0.001t)$。

作为对比，我们使用相同采样数据，从中提取了文献[9]中引用的 6 个参考元素(平均每个流的包数(APf)、平均每个流的比特数(ABf)、平均每个流的持续时间、对称流比例、独立流增长速度和不同端口增长速度)(后文简称 6 元组)，并进行了基于 GHSOM 算法的实验。实验中，我们对合法数据和攻击数据分别进行了 3600 次和 2160 次训练，并将攻击数据包速率与合法数据包速率之比(后文简称为速率比)设定为 1:6，对攻击数据和合法数进行了 1400 次和 1800 次的检测。

在实际检测中，本文将攻击方式分为 3 种，方式 1 受攻击对象包括目标 1，目标 2，目标 3；方式 2 受攻击对象包括目标 2，目标 3；方式 3 受攻击对象包括目标 1。表 2 给出了速率比为 1:6 时两种检测方法对应的检测率，其中 3 种攻击方式的总攻击次数为 1440 次。从表 2 可以看出，本文所提出的 7 元组的检测率要高于 6 元组对应的检测率。这是因为 6 元组检测项以流为分析对象，而每个流表条目可能会对应诸多信息，比如目的地址、源地址、Vlan 等，提高了检测受攻击目的地址的难度，牺牲了检测率。而本文提出的 7 元组，以目的地址为分析对象，从数目、变化速率等多个角度对同一目标进行分析，提高了检测率。

为验证攻击速率对检测率的影响，本文按不同速率比 $1:n\ (1 \le n \le 10, n \in N^*)$ 分 10 次依照表 2 中攻击方式重新进行了攻击实验，并分别使用 7 元组与 6 元组进行了攻击检测，检测结果如图 7 所示。从图中可以看出，在数据类型不变的情况下，检测率随速率比的增加而上升。同时，不同速率比下 7 元组的检测率要高于 6 元组的检测率。当速率比达到 1:5 时，7 元组首先达到 100%，在速率比达到 1:4 时，6 元组的检测率才接近 100%。

4.3 算法开销讨论

本文方法的开销主要包括训练过程和检测过程两部分。

训练过程是线下过程，可以在其他网络设备中

表 2 攻击与检测

攻击方式	攻击对象			攻击次数	7 元组检测次数	7 元组检测率(%)	加权检测率(%)	6 元组检测次数	6 元组检测率(%)	加权检测率(%)
	目标 1	目标 2	目标 3							
方式 1	√	√	√	1000	956	95.6		944	94.4	
方式 2		√	√	300	291	97.0	95.7	279	93.0	93.4
方式 3	√			140	131	93.6		122	87.1	

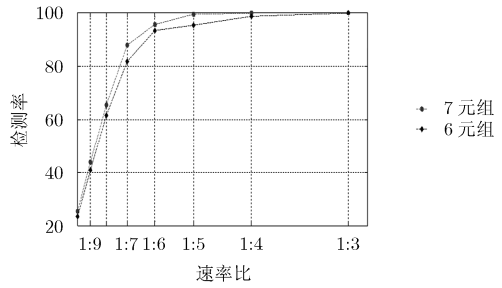


图 7 不同速率比检测率

进行。因此，训练过程对控制器的影响可以忽略。检测过程的计算复杂度主要受检测目标数量和单次检测目标所需计算次数决定。其中检测目标数量由目的 IP 地址的数量决定，在实验过程中以千为单位。单次检测目标所需计算次数受到 7 元组提取和 GHSOM 算法匹配时间影响。7 元组提取主要包括前后两次数据的比较，因此，如果每个周期提取的数据包数目为 N，那么在完成一次 7 元组提取时，数据包处理总量应为 $2N$。GHSOM 算法匹配时间，主要受到神经元匹配过程影响，单位应小于受检测目标数量。

综上，可以看出本文所提方法的计算复杂度为 $O(10^3)$。实验过程中，本文选用 8 G 缓存、3.2 GHz 因特尔 i5 处理器的硬件设备作为控制器的仿真设备。因此，本文方法的计算开销对控制器的影响可忽略。

5　总结

在基于 Openflow 协议的 SDN 网络环境中，控制器利用传输层协议与交换机建立连接，传输指令，交换信息。当网络受到 DDoS 攻击时，攻击方会发送大量数据包，产生大量新的终端标识，造成控制器的存储资源、计算资源大量消耗，并大量占用控制器与交换机的连接资源，影响网络正常运转。为便捷准确地发现受攻击对象，最大限度释放攻击数据占用的网络资源，利用 GHSOM 技术，本文提出了基于对象特征的 DDoS 攻击检测方法。

首先，结合 SDN 网络及攻击特点，提出了基于目的地址的检测 7 元组，并以此作为判断目标地址是否受到 DDoS 攻击的检测元素；然后，采用模块化设计，将 GHSOM 算法应用于 SDN 网络 DDoS 攻击的分析检测中，并在 OpenDayLight 的仿真平台上完成了仿真实验。实验结果表明，本文提出的检测 7 元组可以有效检测目的地址是否受到攻击。

参 考 文 献

[1] BENSON T, AKELLA A, and MALTZ D A. Unraveling the Complexity of Network Management[C]. 6th USENIX Symposium on Networked Systems Design and Implementation, Boston, MA, USA, 2009: 335–348.

[2] KREUTZ D, RAMOS F M V, ESTEVES VERISSIMO P, *et al.* Software-defined networking: A comprehensive survey[J]. *Proceedings of the IEEE*, 2015, 103(1): 14–76. doi: 10.1109/jproc.2014.2371999.

[3] MCKEOWN N. How SDN will shape networking[C]. Open Networking Summit, Palo Alto, CA, USA, 2011: 56–61.

[4] SHENKER S, CASADO M, KOPONEN T, *et al.* The future of networking, and the past of protocols[C]. Open Networking Summit, Palo Alto, CA, USA, 2011: 24–29.

[5] KANDOI R and ANTIKAINEN M. Denial-of-service attacks in OpenFlow SDN networks[C]. 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, BC, Canada, 2015: 1322–1326. doi: 10.1109/inm.2015.7140489.

[6] SHIN S, YEGNESWARAN V, PORRAS P, *et al.* Avant-guard: Scalable and vigilant switch flow management in software-defined networks[C]. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 2013: 413–424. doi: 10.1145/2508859.2516684.

[7] ASHRAF J and LATIF S. Handling intrusion and DDoS attacks in software defined networks using machine learning techniques[C]. IEEE 2014 National Software Engineering Conference (NSEC), Event-Karachi, Pakistan, 2014: 55–60. doi: 10. 1109/nsec.2014.6998241.

[8] 杨雅辉, 姜电波, 沈晴霓, 等. 基于改进的 GHSOM 的入侵检测研究[J]. 通信学报, 2011, 32(1): 121–126. doi: 10.3969/j.issn.1000-436X.2011.01.016.

YANG Yahui, JIANG Dianbo, SHEN Qingni, *et al.* Research on intrusion detection based on an improved GHSOM[J]. *Journal on Communications*, 2011, 32(1): 121–126. doi: 10.3969/j.issn.1000-436X.2011.01.016.

[9] BRAGA R, MOTA E, and PASSITO A. Lightweight DDoS flooding attack detection using NOX/OpenFlow[C]. IEEE 2010 35th Conference on Local Computer Networks (LCN), Denver, Colorado, USA, 2010: 408–415. doi: 10.1109/lcn.2010.5735752.

[10] MOUSAVI S M and ST-HILAIRE M. Early detection of DDoS attacks against SDN controllers[C]. IEEE 2015 International Conference on Computing, Networking and Communications (ICNC), Anaheim, California, USA, 2015: 77–81. doi: 10.1109/iccnc.2015.7069319.

[11] 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, 6(2):

122–136. doi: 10.1016/j.bjp.2013.10.014.

[12] PORRAS P, SHIN S, YEGNESWARAN V, *et al.* A security enforcement kernel for OpenFlow networks[C]. Proceedings of the First Workshop on Hot Topics in Software Defined Networks, Helsinki, Finland, 2012: 121–126. doi: 10.1145/2342441.2342466.

[13] MIHAI-GABRIEL I and VICTOR-VALERIU P. Achieving DDoS resiliency in a software defined network by intelligent risk assessment based on neural networks and danger theory[C]. IEEE 2014 15th International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, Hungary, 2014: 319–324. doi: 10.1109/CINTI.2014.7028696.

[14] RAUBER A, MERKL D, and DITTENBACH M. The growing hierarchical self-organizing map: exploratory analysis of high-dimensional data[J]. *IEEE Transactions on Neural Networks*, 2002, 13(6): 1331–1341. doi: 10.1109/tnn.2002.804221.

[15] HUANG S Y and HUANG Y. Network forensic analysis using growing hierarchical SOM[C]. IEEE 2013 13th International Conference on Data Mining Workshops (ICDMW), Brisbane, Australia, 2013: 536–543. doi: 10.1109/icdmw.2013.66.

[16] RAUBER. The GHSOM Architecture and Training Process [OL]. http://www.ifs.tuwien.ac.at/~andi/ghsom/description.html, 2016.

[17] 鲍旭华, 洪海, 曹志华. 破坏之王: DDoS 攻击与防范深度剖析[M]. 北京: 机械工业出版社, 2014: 20–76.
BAO Xuhua, HONG Hai, AND CAO Zhihua. The King of Destruction: DDoS Attact and Defense Depth Analysis[M]. Beijing: China Machine Press, 2014: 20–76.

[18] BORGNAT P, DEWAELE G, FUKUDA K, *et al.* Seven years and one day: Sketching the evolution of internet traffic[C]. IEEE 2009 INFOCOM, Rio de Janeiro, Brazil, 2009: 711–719. doi: 10.1109/infcom.2009.5061979.

[19] KENJIRO Cho. MAWI working group traffic archive[OL]. http://mawi.wide.ad.jp/mawi/, 2016.

姚琳元： 男，1988 年生，博士生，研究方向为下一代互联网网络层关键技术.

董 平： 男，1979 年生，副教授，研究方向为新一代互联网、移动、安全.

张宏科： 男，1957 年生，教授，博士生导师，研究方向为下一代互联网架构、协议理论与技术、移动互联网络路由、传感器网络技术等.