# SDN 环境下基于机器学习算法的 DDoS 攻击检测模型

马乐乐 ，束永安
（安徽大学 计算机科学与技术学院，安徽 合肥 230601）

摘要： 软件定义网络（SDN）是一种新兴的网络架构,将控制逻辑和转发逻辑分离.SDN 网络中，控制器拥有对网络的全局控制能力.正是由于控制器的这一特性，使得它成为分布式拒绝服务（DDoS）攻击的主要目标.针对这个问题，提出了一种基于机器学习的方法来检测 DDoS 攻击的模型，首先使用熵值检测流是否异常，发出异常警告后提取网络流特征，依次调用 SVM 与 K-means 两种机器学习算法来检测 DDoS 攻击.实验结果表明，所提出的算法能够降低误报率，并且对 DDoS 攻击的检测率和准确率高于原始的 SVM 和 K-means 算法.此外，还通过实验验证了所提出的模型的 CPU 平均利用率低于无熵值检测的 SVM+K-means 算法.

关键词： 软件定义网络；分布式拒绝服务；熵；支持向量机；K 均值

# A DDoS Attack Detection Model Based on Machine Learning Algorithm in SDN Environment

MA Le-le， SHU Yon-gan
(School of Computer Science and Technology, Anhui University, Hefei 230601, China)

Abstract： The Software Defined Network (SDN) is an emerging network architecture that separates control logic from forwarding logic. In SDN, the controller has a global control of the network. Because of this feature of the controller, making it becomes the main goal of the distributed denial of service (DDoS) attack. Aiming at this problem, this paper proposes a method based on machine learning to detect the DDoS attack model. Firstly, it uses the entropy to check whether the traffic is abnormal. After extracting the abnormal alarm, the network flow feature is extracted, and SVM and K-means are called to detect the DDoS attacks. The experimental results show that the proposed algorithm can reduce the false alarm rate, and the detection rate and accuracy of DDoS attacks are higher than those of the original SVM and K-means. In addition, the experimental results show that the average CPU utilization rate of the proposed model is lower than that of SVM + K-means without entropy detection

Key words： software defined network (SDN); distributed denial of service (DDoS); entropy; support vector machine(SVM); k-means

作者简介：
马乐乐女，(1994-)，硕士研究生.研究方向为软件定义网络. E-mail: 1790879656@qq.com.
束永安男，(1964-)，博士，教授.研究方向为无线网络、软件定义网络.