云计算环境下 Low-Rate DDoS 攻击检测模型构建

陈 静

（义乌工商职业技术学院，浙江 义乌 322000）

摘要：作为一种新型的分布式拒绝服务 Low-Rate（低速率）DDoS，是另一种破坏云服务的分布式拒绝服务攻击方式。DDoS 攻击通常具有较高的攻击队列，而 LDoS 采用较低的攻击率，此外这种攻击是周期性的，具有攻击速率低、隐蔽性强的特点。LDoS 攻击流量的行为与正常流量的行为非常类似，很容易避开 DDoS 攻击检测系统，很难被检测出来。因此，LDDoS 攻击可以持续很长时间，从而危及受害者。LDoS 攻击在很长一段时间内欺骗性地消耗云资源，导致云计算提供商成本大幅增加。现提出一种基于机器学习的检测方法，它能够有效地检测出云计算环境下的 LDDoS 攻击流。

关键词：Low-Rate DDoS；LDoS；攻击检测；云计算；机器学习

中图分类号：TP393 **文献标志码：**B **文章编号：**1673-4270(2020)04-0112-03

一、引言

随着互联网的快速兴起，云计算成为一种全新的网络应用服务，它是一种为用户提供资源的网络，是一种分布式计算网络。云计算平台将其优势扩展到云客户和云服务提供商。云计算使获得各种服务变得方便和划算[1]，而不需要花费大量的费用来建立自己的计算基础设施。云的几个特性有助于服务提供商降低操作成本，实现更好的吞吐量。

DDoS 是一种分布式拒绝服务，它主要以消耗网络资源（TCP 带宽等）为攻击目的，通过连续发送攻击流量促成网络阻塞，从而降低网络性能，这种攻击不会造成大面积网络链路瘫痪，但是会严重影响客户端和服务器端的链接质量，破坏服务器的正常工作，DDoS 攻击机制见图 1 所示。Low-Rate DDoS 是近几年新出现的一种攻击力更强的针对网络攻击的拒绝服务，它利用 TCP 协议拥塞控制机制的弱点，低速率周期性地发动恶意攻击流量，并利用超时重传机制降低网络吞吐量。与传统的 DDoS 拒绝服务相比，LDDoS 攻击速率低，与正常流量相似，隐蔽性强，很难被传统的 DDoS 攻击防御系统发现，LDDoS 攻击能够持续更长的时间，从而造成网络链接质量急速下降。因此，在云计算环境中，破坏者可以通过长时间欺骗性地消耗云资源来实施 LDDoS 攻击，增加受害者的经济负担。

文中首先对云计算服务中 LDDoS 攻击特性进行分析，通过采用核主成分分析方法提取 LDDoS 攻击流量的特征，作为神经网络的输入，然后利用 SVM 支持向量机模型进行识别分类，判断攻击流量和非攻击流量，从而达到检测的目的。

二、相关的工作

近几年来研究者们针对 LDoS 攻击特点做了大量的研究，对 LDoS 攻击流量检测主要提出了两种方法：基于频域和时域的方法。基于频域的方法主要通过小波变换分析，从小波中提取 LDoS 的特征。基于时域的方法主要是针对网络流量时间序列来预测。吴志军[2]等早期采用队列占有率统计的方法，通过 NS2 虚拟网络平台进行模拟 LDDoS 攻击，提取出 LDDoS 在脉冲流量上的两个特征。吴志军[3]等在

作者简介：陈 静（1981—），女，湖南湘潭人，义乌工商职业技术学院机电信息学院副教授。

基金项目：本文系 2019 年国家公派高级研究学者、访问学者、博士后资助项目“低速率拒绝服务检测关键技术及协同防御系统的应用研究”（项目编号：201908330247）的部分研究成果。

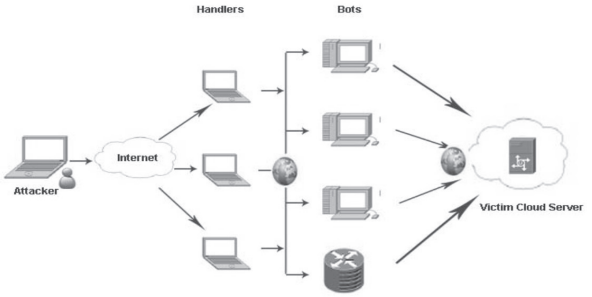


图 1　DDoS 攻击图

早期研究的基础上，进一步改进了特征提取方法，采用 KPCA（核主成分分析）方法对采集的攻击流量进行降维处理，提取出 LDoS 脉冲流量的特征，作为神经网络的输入值，利用神经网络进行了分类检测。通过实验表明提出的算法复杂度较低，实时性较强。Kriti[4] 等通过分析云计算环境下 DDoS 的攻击特点，提出了一种 t-statistic 假设检验方法来识别 LDoS 攻击流。Naiji[5] 等采用时间域检测方法，利用基于 Entropy 的 PSD 算法来提取 LDoS 脉冲流的主要成分特征，采用 SVM 支持向量机网络进行分类检测，这种方法平衡了检测率和效率。

三、Low-Rate DDoS 特性

LDoS 低速率拒绝服务攻击中，攻击者利用 TCP 拥塞控制的漏洞，周期性地发送短时脉冲流量包，利用超时重传机制降低网络的吞吐量，导致服务器拒绝正常服务，从而降低网络性能 [6]。LDoS 攻击模式可以用图 2 表示，主要包含 3 个参数：F，L，R。

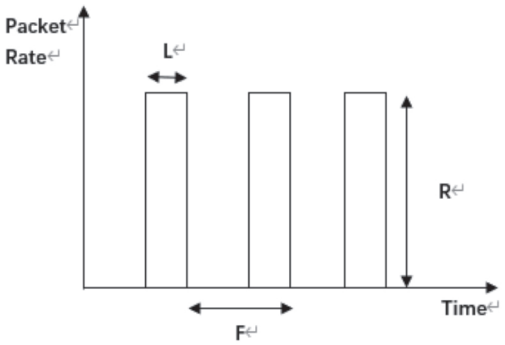


图 2　LDoS 攻击模式

F：LDoS 的攻击频率。LDoS 攻击通常根据超时重传设置 F 的值，以获得最佳的攻击效果。当拥塞控制机制被触发时，拥塞窗口将等待 RTO 超时，然后再尝试重新传输。如果攻击者可以获得 RTO 的确切值，那么当 TCP 源重新发送 TCP 包时，攻击者会将攻击包发送给受害者，这样将会导致每次传输失败，拥塞窗口的容量总是 1，吞吐量总是 0。

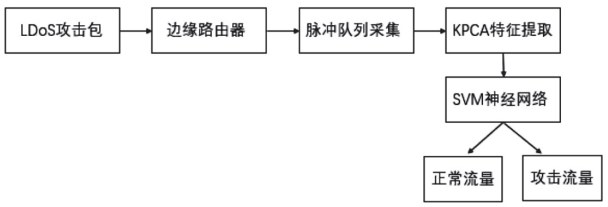
L：LDoS 的攻击爆发的时间。由于在一个 LDoS 攻击周期中只有一个短期的高强度攻击流，所以 L 的值远远小于 F。只要确保 L 大于最大的往返时间值 RTT，LDoS 攻击就会触发拥塞控制机制。在攻击过程中，L 的值可以通过 RTT 来确定。

R：LDoS 的攻击爆发时流量包的速率。当 LDoS 攻击发生时，R 越高，所造成的带宽损失越大，然而，LDoS 攻击的隐蔽性就越小。

四、模型搭建

通过对相关研究的分析表明，利用数学方法或机器学习方法都可以对 LDoS 进行建模和检测。一些数学方法具有较好的性能和较低的检测率，而机器学习方法能够准确地检测出具有较高时间复杂度的 LDoS。LDoS 攻击相对稳定且速率较低，而正常的流量由于缺乏周期性而跨越所有频率。当 LDoS 攻击与正常流量混合时，流量速度没有显著差异，但流量中的流量变化有助于区分正常流量与攻击流量 [7]。

LDoS 攻击的目的是降低网络服务质量，而 FRC（Fraudulent Resource Consumption）攻击是在云环境下进行的，其目的是对基于云的服务提供商施加经济上的关注。传入流量的采样是在网络的边缘路由器上完成的。云服务提供商确保了云计算环境中所有边缘路由器之间的协调，因此，可以在云平台上有效地实现该方法。使用基于 SVM 的机器学习模型来学习流量模式，并为检测算法选择合适的特征。设计基于机器学习的检测系统的重要一步是识别出最相关的特征，从而提高检测效率。在数据准备过程中，采用了主成分分析 (KPCA) 技术。检测模型如下图 3 所示：



（一）LDoS 攻击流特征提取

PCA 方法能够消除原始数据流中可能存在的噪声，大大减少数据量和检测过程的复杂度。它是一

种采用多变量统计的算法，是最常用的用于数据处理初期实现数据降维的方法之一。它通过正交变换方法将可能存在相关性的一组变量转换为一组线性不相关的数据，达到降维的目的。PCA 是一种线性映射方法，如果特征之间的关系是非线性的或多维的数据，则无法完成较优的分类。TCP 流量脉冲队列具有较强的非线性特征，因此采用 KPCA（核主成分分析），它是对 PCA 算法的非线性扩展。它利用核化（核函数 Kernel）的思想，将样本空间映射到更高维的空间，再利用更高维的空间进行线性降维，这种方法能够更好地提取队列特征。实现 KPCA 方法如下：

1. 输入脉冲队列数据；

2. 利用核函数计算核矩阵 K。这里采用高斯核函数；

3. 计算核矩阵特征向量 {v1,v2,v3……vn}；

4. 将特征向量按对应特征值大小从上到下按行排列成矩阵，取前 k 行组成矩阵 P；

5.P 即为降维后的数据，也就是新的特征序列。

（二）LDoS 攻击流检测

SVM（Support Vector Machines，支持向量机）是一种机器学习算法，它在高维或无限维空间中构造超平面或超平面集合，可用于分类、回归或其他任务。它的基本模型是定义在特征空间上的间隔最大的线性分类器，具有良好的分类性能和处理非线性问题的能力[8]。在设计基于机器学习算法的检测系统时很重要的一步是识别最相关的特征能够提高检测效率。然而，随着处理样本数据的增加，所要求的计算时间和存储空间也会大幅度增加，通过 KPCA 算法降低数据的维度，提取出网络 TCP 流量的特征向量（正常流、LDoS 攻击流），SVM 算法对处理后的流量数据进行模型训练，得到相应的最优超平面。

通过对 KPCA 算法降维后的训练集数据和数据处理后生成的训练集标签进行训练，得到支持向量机算法的模型。使用的参数是 fitcsvm 函数的默认值。利用支持向量机算法的模型对特征选择后的测试集数据进行分类和预测，达到检测 TCP 合法流量和 LDoS 攻击流量的目的。

五、总结

LDoS 攻击流量低速率高隐蔽性，与正常合法流量的特征非常相似，如何在低假阳性率的情况下实时检测出 LDoS 攻击包是一项非常有挑战的课题。文中提出了一种在云计算环境下 Low-Rate DDoS 攻击检测机制，在边缘路由器上进行架构，利用 KPCA 方法提取出攻击流特征，结合机器学习算法 SVM 对输入流数据进行分类，检测识别出正常流量和异常攻击流量。

参考文献

[1] Idziorek, J.,Tannian,M.,& Jacobson,D. Detecting fraudulent use of cloud resources [J]. Proceedings of the 3rd ACM workshop on Cloud computing security workshop, 2011(10):61-72.

[2] 吴志军 , 张东 . 低速率 DDoS 攻击的仿真和特征提取 [J]. 通信学报 ,2008,29(1):71-76.

[3] 吴志军 , 刘亮 , 岳猛 . 基于 ANN 与 KPCA 的 LDoS 攻击检测方法 [J]. 通信学报 ,2018,39(5):11-22.

[4] Kriti Bhushana, B. B. Guptaa.Hypothesis Test for Low-rate DDoS Attack Detection in Cloud Computing Environment[J]. Procedia Computer Science, 2018(132) :947-955.

[5] Naiji Zhang,Femhi Jaafar,Yasir Malik.Low-Rate DoS Attack Detection Using PSD based Entropy and Machine Learning[J].2019 6th IEEE International Conference on Cyber Security and Cloud Computing, 2019(6):59-62.

[6] 陈静 . 基于改进神经网络的 LDoS 攻击感知 [J]. 信息通信 , 2017(7):1-2.

[7] 陈静 . 基于拟态安全防御的 LDoS 攻击防御研究 [J]. 福建电脑 , 2017(2):6-7.

[8] Xiang, Y.,Li, K., & Zhou,W.Low-rate DDoS attacks detection and traceback by using new information metrics[J]. IEEE transactions on info. forensics and sec,2011(2): 426-437.

（责任编辑：汝艳红）