基于简单统计特征的 LDoS 攻击检测方法

段雪源[1,2,3]，付钰[1]，王坤[1,4]，李彬[1]

（1. 海军工程大学信息安全系，湖北 武汉 430033；2. 信阳师范学院计算机与信息技术学院，河南 信阳 464000；
3. 信阳师范学院河南省教育大数据分析与应用重点实验室，河南 信阳 464000；
4. 信阳职业技术学院数学与信息工程学院，河南 信阳 464000）

摘 要：传统的低速率拒绝服务（LDoS）攻击检测方法存在特征提取复杂、计算开销大、实验背景单一和攻击场景过时等问题，难以满足现实网络环境对 LDoS 攻击检测的需求。通过研究 LDoS 攻击原理，分析 LDoS 攻击流量的特征，提出一种基于网络流简单统计特征的 LDoS 攻击检测方法。根据网络流量数据包的简单统计特征构造检测数据序列，利用深度学习技术学习输入样本的时间关联性特征，并根据重构序列与原输入序列的差异进行 LDoS 攻击判定。实验结果表明，所提方法能够有效地检测出流量中的 LDoS 攻击流量，且对异构网络流量具有较强的适应性。

关键词：统计特征；深度学习；低速率拒绝服务；攻击检测

中图分类号：TP391

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022216

LDoS attack detection method based on simple statistical features

DUAN Xueyuan[1,2,3], FU Yu[1], WANG Kun[1,4], LI Bin[1]

1. Department of Information Security, Naval University of Engineering, Wuhan 430033, China
2. College of Computer and Information Technology, Xinyang Normal University, Xinyang 464000, China
3. Henan Key Laboratory of Analysis and Applications of Education Big Data, Xinyang Normal University, Xinyang 464000, China
4. School of Mathematics and Information Engineering, Xinyang Vocational and Technical College, Xinyang 464000, China

Abstract: Traditional low-rate denial of service (LDoS) attack detection methods were complex in feature extraction, high in computational cost, single in experimental data background settings, and outdated in attack scenarios, so it was difficult to meet the demand for LDoS attack detection in a real network environment. By studying the principle of LDoS attack and analyzing the features of LDoS attack traffic, a detection method of LDoS attack based on simple statistical features of network traffic was proposed. By using the simple statistical features of network traffic packets, the detection data sequence was constructed, the time correlation features of input samples were extracted by deep learning technology, and the LDoS attack judgment was made according to the difference between the reconstructed sequence and the original input sequence. Experimental results show that the proposed method can effectively detect the LDoS attack traffic in traffic and has strong adaptability to heterogeneous network traffic.

Keywords: statistical features, deep learning, low-rate denial of service, attack detection

0 引言

由于互联网协议和服务的开放性，各种网络入侵攻击行为从未间断，在众多威胁中，低速率拒绝服务（LDoS, low-rate denial of service）攻击由于其巨大的破坏力和良好的隐蔽性，被网络犯罪分子和黑产业链运营商广泛使用。不同于传统的泛洪式拒绝服务攻击，LDoS 攻击主要针对传输层、网络层

收稿日期：2022−08−01；**修回日期：**2022−10−20

通信作者：付钰，fuyu0219@163.com

基金项目：国家重点研发计划基金资助项目（No.2018YFB0804104）

Foundation Item: The National Key Research and Development Program of China (No.2018YFB0804104)

或应用层的协议漏洞，利用较少的攻击流量使系统或网络服务质量下降[1]。例如，针对传输控制协议（TCP, transmission control protocol）超时重传机制的 LDoS 攻击主要通过向瓶颈链路中发送短促高速的攻击脉冲，触发大量数据包丢失，迫使网络启动超时重传机制，造成大量无用数据流耗尽网络带宽。针对应用层的 LDoS 攻击则是利用 HTTP 的连接保持机制，通过向服务器发送多个连接请求，耗尽服务器的可分配资源，使正常请求无法得到响应。可以看出，LDoS 攻击的本质就是利用系统的自适应机制，通过短促的高速脉冲数据流攻击关键链路或端系统，使其因过载而无法对外提供正常服务。

通常，单独 LDoS 攻击流形式上都是合法的网络流量，表现出与正常流量相同的基本特征，且发送的数据包数量少、平均速率低，一般仅为正常数据流的 10%～20%[2]，经常被淹没在正常流量中，能够穿越普通防火墙，传统的针对 DoS 攻击的检测方法并不适用于检测 LDoS 攻击。一直以来，研究人员尝试将小波变换分析、频谱分析、统计分析、信息度量分析等技术引入检测攻击工作中，但提出的检测方法大多依赖特征工程，检测效果受制于研究人员的专业素质和工作经验[3-4]。

深度学习利用神经网络从原始数据中自主地学习数据高层次的特征信息并用于进一步的分类，是解决传统检测方法特征依赖的有效手段。其中，长短期记忆（LSTM, long short-term memory）网络是基于“门”设计的改进型循环神经网络，不仅能捕捉数据序列的时间关联性，还可缓解普通循环神经网络的长时依赖问题，在语音识别、自然语言处理、网络流量异常检测等领域应用广泛。生成式对抗网络（GAN, generative adversarial network）是基于零和博弈思想构建的生成式模型，对异构数据具有较强的适应性，由生成器和判别器 2 个部分组成，其中，生成器通过学习输入样本的分布来生成同分布的相似样本；判别器通过计算判别误差来区分输入样本是真实样本还是生成样本。在序列数据异常检测领域，可利用判别误差来区分输入样本是正常样本还是异常样本。虽然深度学习有着强大的表征能力，但需要足够的样本进行训练才能完成建模[5-6]。当前的检测方法大多是流级别的，需要跟踪分析流内的多个数据包，会消耗大量的计算资源。另外，实验数据大多来源于公开数据集或仿真平台，存在攻击场景过时、通信量不完整、流量背景单一等缺陷。

针对上述问题，本文提出一种基于简单统计特征的 LDoS 攻击检测方法。利用流量采集工具，从真实网络环境中获取流量数据，以流量中数据包大小和到达时间间隔为特征构造检测数据序列，利用神经网络学习正常流量数据的特征分布，能够对正常数据序列进行较好的重构；当待检测数据序列为攻击流时，重构数据与输入数据将会出现较大重构误差，当重构误差超过阈值时则判定为攻击，并输出判定结果，实现从原始流量输入到检测结果输出的端到端检测模式。

1 相关工作

2001 年，ASTA Network 公司在 Internet 2 的主干网上首次发现 LDoS 攻击流量；2005 年，Kuzmanovic 等[7]展示了一种恶意利用 TCP 超时重传机制的低速率 TCP 定向 DoS 攻击，人们才对 LDoS 攻击有了更加清晰的认识。自此，研究人员开始研究检测 LDoS 攻击的有效方法，根据攻击流的脉冲周期性特征以及被攻击网络的波动性表现，这些检测方法可归纳为基于流量特征、基于信号分析、基于机器学习和基于深度学习这 4 类，如图 1 所示。

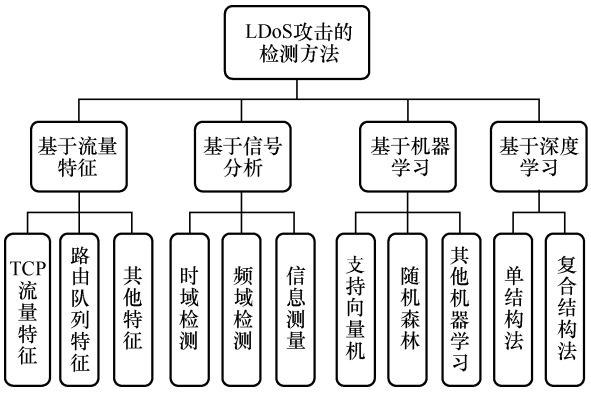


图 1 LDoS 攻击的检测方法

基于流量特征的检测方法通常是利用被攻击网络中流量的异常波动性特征进行检测，这些特征包括从网络流中提取的队列长度、连接持续时间、数据包编号、数据包间隔、数据包大小和 ACK 序列号等信息[8]。流是指具有相同五元组（源 IP、目标 IP、源端口、目标端口以及传统层协议）的所有报文[9]。吴志军等[10]将网络中的实际网络带宽占用率、小分组比例、分组丢失率这 3 个特征组成联合特征输入反向传播神经网络分类器进行 LDoS 攻击检测，在仿真平台和试验网络中验证了方法的有效性。Wu 等[11]提出基于 LDoS 攻击流量的多重分形特

征[12]的检测算法，利用 HÖlder 指数估计 LDoS 攻击下流量的奇异性和突发性，取得的实验结果与理论预测相符。Zhang 等[13]根据网络拥塞期间正常 TCP 流发送的数据包少，而攻击流发送的数据包多的现象，提出基于正常数据包数量与数据包总量比的 LDoS 攻击检测与过滤方法，通过分析路由器中的数据，验证了方法的可行性。然而，这些基于流量特征的检测方法普遍存在 2 个不足，一是研究所用数据大多是在模拟环境中生成的，缺乏真实网络背景；二是网络流特征的设计需要人工完成，提取时需要非常大的计算开销，且时间消耗较长，适合处理离线数据，很难实现在线的 LDoS 攻击检测[14]。

相关实验说明了利用信号分析方法检测网络中 LDoS 攻击流的可行性。杜臻等[15]使用小波分析提取流量数据的多样性特征，利用支持向量机（SVM, support vector machine）完成混合流量中的异常分离。Agrawal 等[16]使用功率谱密度方法识别云环境中的低速 LDoS 攻击，通过傅里叶变换，将持续收集到的流量数据变换为频谱序列，并计算功率谱密度值，将功率谱密度集中在低频段的部分判定为攻击。Brynielsson 等[17]根据 HTTP 中的持续连接特性，实现了利用谱分析方法检测针对应用层 HTTP 服务的 LDoS 攻击。虽然这些频域分析法对 LDoS 攻击的检测是有效的，但信号转换会引起巨大的额外开销，并且可能会产生较高的误警率和漏检率。在时域方面，Wu 等[18]结合 Hilbert 谱和 Pearson 相关系数，利用小尺度检测窗口实现对 LDoS 攻击包的检测。Swami 等[19]提出一种基于高级熵的自适应检测方法，实现了对未知攻击的检测。尽管这些方法简单且检测精度较高，但要求被检测数据在时域上的波动不能过大，否则检测性能严重下降，这显然与真实网络情况不符。

基于机器学习的检测方法通常与其他算法结合使用，Zhang 等[20]将主成分分析（PCA, principal component analysis）与 SVM 模型相结合，利用 PCA 过滤掉噪声干扰并提取 TCP 流的主要特征，作为 SVM 模型的输入来检测 LDoS 攻击。Yan 等[21]提取 TCP 流量的平均值、方差和熵等特征来训练改进的逻辑回归模型，以检测 LDoS 攻击。Pérez-Díaz 等[22]提出了用于检测软件定义网络（SDN, software defined network）环境中 LDoS 攻击的框架，该框架有助于实现各种机器学习模型，如决策树、代表树、随机树、随机森林、多层感知器（MLP, multilayer perceptron）和 SVM 等对 LDoS 攻击的检测，但是该方法的误报率较高。Tang 等[23]提出了将网络流量特征集构建技术与改进的自适应增强（Adaboost, adaptive boosting）分类算法相结合的多特征自适应增强（MF-Adaboost, multi-feature Adaboost）算法，通过提取网络流量数据中最有用的信息，减小数据规模；采取最优特征选择策略，用 28 个特征完成对分类器的训练；改进的 Adaboost 算法可缓解样本权值不平衡问题。然而，以上基于机器学习的检测方法在特征提取上需要消耗较多的计算资源，特征设计依赖人工经验，并且对未知特征的攻击缺乏有效的检测能力。

基于深度学习的检测方法通常以原始流量为输入，经简单预处理后，利用深度学习的强大表征能力，提取样本数据的特征信息，进而完成流量的分类，实现端到端的检测模式。按照所用的神经网络结构类型，可分为单结构模型检测方法和复合结构模型检测方法。单结构模型检测方法是一种以神经网络结构为模型基本架构的检测方法，例如，Ilango 等[24]提出基于前馈卷积神经网络（FF-CNN, feedforward-convolutional neural network）的异常检测方法，用于检测物联网 SDN 中的 LDoS 攻击，在公开数据集上取得了不错的检测效果。Tang 等[25]提出的多特征融合卷积神经网络（MF-CNN, multi-feature fusion-convolutional neural network）检测模型也是利用卷积神经网络区分网络特征映射之间的差别，以检测出哪些特征映射包含 LDoS 攻击。Agarwal 等[26]利用 LSTM 网络模型定期学习 Web 服务器日志并对网站的访问情况进行预测，实现对欺诈型 LDoS 攻击的检测。单结构模型虽然可以检测出 LDoS 攻击，但是存在 2 个不足，一是需要大量样本进行训练，且模型缺少指导，在训练初期较困难；二是对异构数据适应能力较差，模型的泛化能力弱。因此，研究人员更多地使用复合结构模型，即由 2 种以上神经网络构建的检测模型，合理的组合设计可以发挥不同结构神经网络的优势，克服单结构模型自身的不足。Xu 等[27]提出将一维卷积神经网络与双向循环神经网络结合的 LDoS 攻击检测模型，先用卷积模块提取归一化预处理后的信号特征，再用双向循环神经网络估计信号中包含 LDoS 攻击的概率值，实现对 LDoS 攻击的检测。Chen 等[28]设计的 DAEMON 在线检测模型是将变分自编码网络与 GAN 相结合，利用变分自编码网络对异构数据的

适应性，同时作为 GAN 的生成器指导训练，克服 GAN 在训练初期难以收敛的不足。然而当前基于深度学习的检测方法大多是“流级别”的，即以整个网络流为检测对象，需要对流内的每个数据包进行跟踪与分析，计算开销大、时延较长，并且难以完成实时在线检测。另外，检测时需要分析出完整数据流的相关信息才能得到最终的检测结果，不具备对 LDoS 攻击的早期发现能力。

2　网络流量获取

2.1　正常流量的采集

为获得真实流量数据，本文使用支持 Wireshark 软件的高性能流量数据采集系统平台，抓取流经 Web 服务器的所有流量。为获得大量普通用户访问服务器产生的流量，本文选择某校园的 Web 站点作为正常流量的来源。图 2 是经过简化后的正常流量采集网络拓扑结构，交换机设置校园网络 Web 服务器端口的镜像端口，流量采集系统从该镜像端口抓取服务器对外交互的所有上下行流量数据。

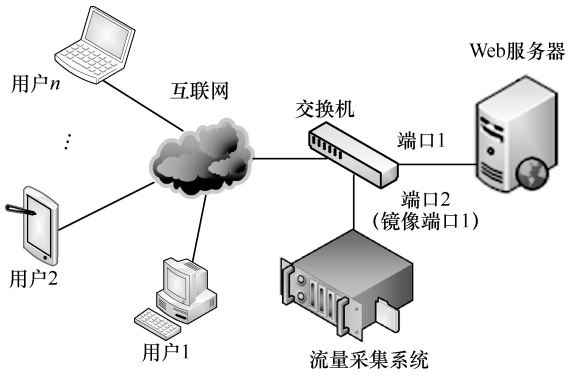


图 2　正常流量采集网络拓扑结构

本文实验从采集的流量数据中选取连续 600 min 没有发生网络异常的数据作为正常流量样本，因为该采集时段网络能够正常提供服务，表明网络中没有明显异常，已经排除拒绝服务攻击的可能，或有少量其他攻击，但对 LDoS 攻击检测影响基本可以忽略。

2.2　异常流量的采集

为了不影响网络的正常运行，攻击流量不能在实际的 Web 服务器网络中传输，只能通过隔离网络生成与采集，因此，本文单独设计了采集攻击流量的局域网。该局域网由一个流量采集系统、5 台计算机主机以及相应的网络连接设备组成，其中 4 台主机安装 Linux 系统，一台主机安装 Windows 系统，其拓扑结构如图 3 所示。其中，一台 Linux 主机运行 OpenSwitch 作为 OpenFlow 交换机，运行 Pox controller 作为 OpenFlow 控制器以创建 SDN 环境；南向接口是带宽为 1 Gbit/s 的 TCP 通道，OpenFlow v1.3 协议用于交换机和控制器之间的通信。一台 Linux 主机作为单独的 Web 服务器，是校园 Web 服务器的镜像网站。一台 Linux 主机作为普通客户端，运行良性程序对 Web 服务器进行正常访问。一台 Linux 主机提供运行低速攻击程序的 Linux 环境、一台 Windows 主机提供运行低速攻击程序的 Windows 环境，它们按计划运行不同的攻击程序对 Web 服务器进行 LDoS 攻击。客户端和服务器通过千兆网卡与 OpenFlow 交换机连接。

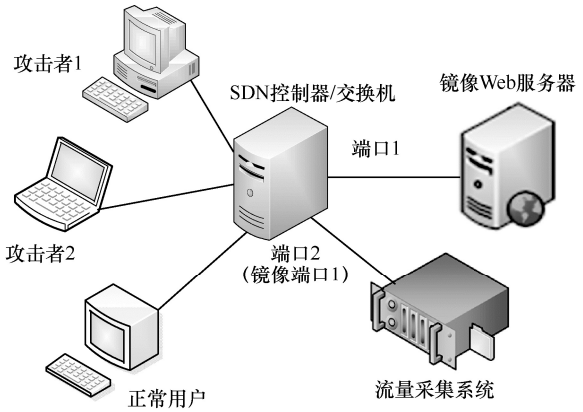


图 3　采集攻击流量的局域网拓扑结构

攻击流量由各攻击主机上运行的攻击程序生成，攻击流量种类包括各种 TCP 同步序列编号（SYN, synchronize sequence number）低速率攻击、HTTP 慢速读取攻击等。为了实现在短时间间隔内的 SYN 低速率攻击，设计了每次攻击 50 s，然后休眠 100 s，且攻击只发生在每秒的前 0.1 s 内的攻击模式。每类攻击程序净运行时间为 60 min（不含休眠时间）。图 4 为攻击程序运行周期示意。

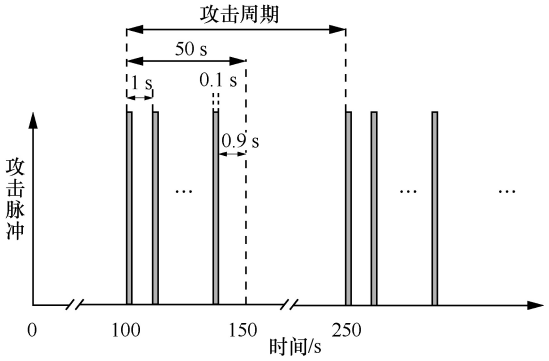


图 4　攻击程序运行周期示意

需要说明的是，Slowhttptest 程序为慢速读取攻击，没有使用脉冲成形攻击。从采集的流量中剔除休眠时间的数据，即可得到 6 种不同的以正常流量为背景的攻击流量，时长均为 60 min 无背景的纯攻击流量，本文设计的攻击流虽然复杂、检测难度大，但更接近真实网络环境中的流量模式。

3　特征选取与数据设计

3.1　特征选取

使用 CICFlowMeter 工具从采集到的流量文件中提取每个 TCP 流或用户数据报协议（UDP, user datagram protocol）流中数据包的特征信息，大约可提取 80 个流量的统计特征，不同协议解析出的结果略有差异。利用 sklearn 中的随机森林回归算法，计算每个特征在该流中的重要性，图 5 和图 6 分别显示了正常流量和攻击流量中 6 个主要特征对其他特征的影响力指数，数值越大，特征越重要。

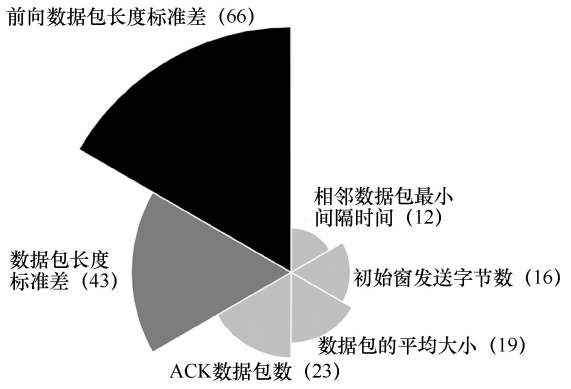


图 5　正常流量主要特征影响力指数

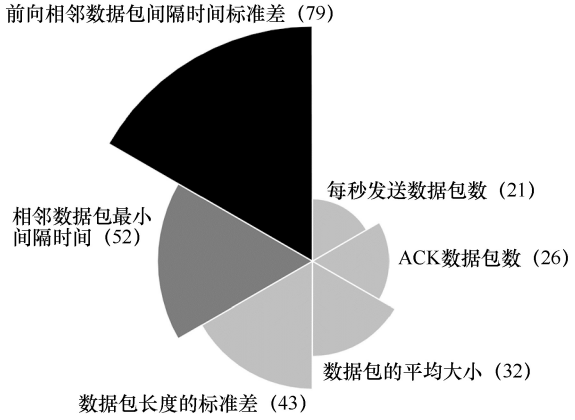


图 6　攻击流量主要特征影响力指数

从图 5 中可以发现，前向数据包长度标准差和数据包长度标准差是正常流量最显著的特征。不同于 LDoS 攻击流，正常流量是由正常的网络用户与服务器交互产生的，由于用户需求的多样性以及访问的随机性，生成的数据包大小是随机的且差异性较大。攻击流的数据包是由程序产生的，通常具有固定大小且小于正常数据包。从图 6 中可以看出，相邻数据包时间间隔的信息，包括前向相邻数据包时间间隔标准差和相邻数据包最小时间间隔在攻击流的特征中较重要，原因是 LDoS 攻击在向被攻击者发送数据包时表现为突发行为，而正常流量通常不具备这种突发性；另外，这种突发行为会影响数据包的到达率和相邻数据包的时间间隔相关特征。

因此，可以确定前向数据包长度标准差和前向相邻数据包时间间隔标准差是区分正常流量和攻击流量的 2 个重要特征。然而，攻击检测除了关注检测的准确率外，检测的及时性也是需要特别注重的。而前向数据包长度标准差和数据包长度标准差这类特征值需要检测完整的 TCP 流或 UDP 流才能得出，前向相邻数据包时间间隔标准差特征也存在相同情况。因此，要想实现早期检测就不能直接用它们的标准差作为检测的特征。根据文献[8,29]的研究结果可以发现，流内前 2 s 内的数据包大小和到达的时间间隔对检测 DoS 攻击非常重要。因此，本文尝试利用流中前若干个时间步内到达的数据包大小和时间间隔作为特征，构造出由 2 个统计特征组成的检测序列数据集，因此，数据集的单个样本可表示为

$$\boldsymbol{x}_i=\begin{bmatrix} t_i^1,t_i^2,\cdots,t_i^n \\ l_i^1,l_i^2,\cdots,l_i^n \end{bmatrix},\ t_i^j,l_i^j\in\mathbb{R}\left(j\in[1,n]\right) \tag{1}$$

其中，t_i^j 为第 i 个样本中第 j 个数据包与第 j−1 个数据包到达的时间间隔，l_i^j 为第 j 个数据包的大小。每个数据包到达都是一个时间步。

3.2　数据设计

为减少运算开支，将数据流按每 10 s 切分出一个流片段，那么 600 min 的正常流量数据可得到 3 600 段正常流片段，利用 CapAnalysis 网络数据包分析工具提取本文所需要的特征数据，并标注为正常样本。用同样的方法处理各攻击流，每种攻击流量可切分出 360 段流片段，标注为异常样本。另外，为了便于汇总最终的检测结果，将正常样本和异常样本中的每个流片段添加唯一标志符。使用正常流量数据进行训练和验证，因此随机抽取 30%的正常流片段作为训练集，再抽取 30%作为验证集，剩余的

40%作为测试集。为构造不同的测试数据集，每次取一种攻击流片段随机插入正常流片段中，得到 6 种合成流量测试数据集，每种攻击流量的检测集包含时长为 300 min 的 1 800 段流片段，其中，正常流片段为 1 440 段，攻击流片段为 360 段。考虑到现实网络中攻击流量的多样性，需要包含多种攻击流的测试数据检验所提方法对复杂攻击的检测能力。因此，从 6 种攻击流量中各随机抽取 120 段攻击流片段随机插入正常流量中，即可生成一个包含 6 种攻击流量的“All-United”合成流量集，该流量集共包含时长为 360 min 的 2 160 段流片段，其中正常流片段为 1 440 段，攻击流片段为 720 段。表 1 展示了各合成流量测试数据集信息。

表 1　各合成流量测试数据集信息

攻击种类	流量 总时长/min	正常流 片段数/段	攻击流 片段数/段	异常比
Pwnloris	300	1 440	360	0.2
Hping	300	1 440	360	0.2
Torshammer	300	1 440	360	0.2
Slowloris	300	1 440	360	0.2
Httpbog	300	1 440	360	0.2
Slowhttptest	300	1 440	360	0.2
All-United	360	1 440	720	0.33

4　LDoS 攻击检测模型

网络流量作为时间序列数据记录了网络状态的变化情况，循环神经网络适用于处理序列数据，LSTM 网络弥补了普通循环神经网络梯度消失、长期记忆不足等问题，能够挖掘序列数据的时间相关性。GAN 是生成式模型，可以生成与输入数据同分布的更多样本，这一特性能缓解样本数量不足的问题，同时 GAN 对异构数据有较强适应性，能提升模型的泛化能力，但普通 GAN 的生成器经常会遇到因缺少编码指导在初期难以训练的问题。因此，本文设计出以 LSTM 为 GAN 的生成器的流量数据重构器（LSTM-GAN），由 LSTM 作为生成器学习输入样本的空间分布并生成重构样本输入判别器，判别器将重构样本与输入样本之间的差异反馈给生成器，指导生成器更新参数完成训练。

利用正常流量训练出 LSTM-GAN 学习到正常流量的数据特征，能够重构出与输入正常流量类似的流量模式。当输入的待检测数据为攻击流时，LSTM-GAN 则不能对其进行有效的重构，生成的重构样本与输入样本间存在较大的误差，该误差可作为攻击判定的依据。图 7 展示了基于 LSTM-GAN 重构器的 LDoS 攻击检测的整体功能架构，包括数据准备、数据重构、攻击判定 3 个功能模块。当从现实网络中采集网络流量后，经过预处理提取流量的简单统计特征构造为检测数据；待检测数据样本输入训练好的 LSTM-GAN 中，LSTM 自编码器（生成器）对其进行编码和解码后生成重构样本，判别器计算重构样本与检测样本之间的重构误差；攻击判定模块将此重构误差与判定阈值进行比较，如果重构误差超过判定阈值，则判定检测样本对应的网络流量为 LDoS 攻击流。

4.1　数据准备模块

数据准备模块由流量获取和数据预处理 2 模块组成，主要完成从网络接口处抓取流量数据，并按 3.1 节中特征选取的方法进行相应格式转换和特征提取等操作，生成下一步检测所需的数据序列。通过实验发现，16 个时间步足以跨越数据流的前 2 s，因此只需研究网络流片段中前 16 个数据包的信息，即模型的输入数据是一个包含 16 个时间步的包大小和到达时间间隔信息的 2 维数组。

4.2　数据重构模块

数据重构模块主要是以 LSTM 自编码器为生成器的 GAN 构成的 LSTM-GAN 流量数据重构器。LSTM 自编码器（生成器）将输入流量样本映射到潜在特征空间并在该空间中完成样本的重构，为充分学习流数据的特征信息，在编码器与解码器中间设置了信道增强层。判别器用来指导生成器进行训

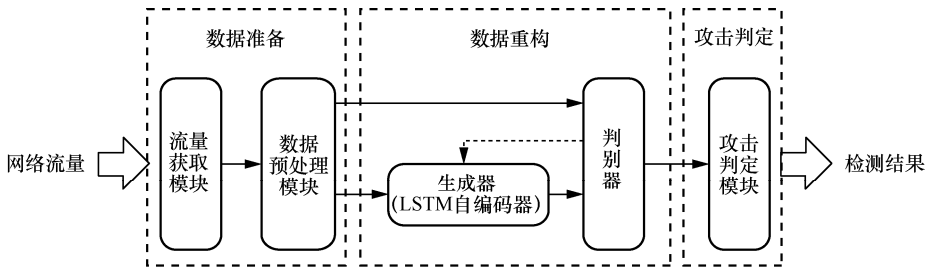


图 7　基于 LSTM-GAN 重构器的 LDoS 攻击检测的整体功能架构

练，计算出重构器在稳态下的重构误差并将其作为检测攻击的门限。

LSTM 自编码器各层的功能如下。

1) 编码器

第 1 层，LSTM（32），读取输入数据并输出 32 个特征，每个特征有 16 个时间步。

第 2 层，LSTM（8），从第 1 层获取 16×32 的输入，并将特征大小减少到 8，输出一个大小为 1×8 的特征矩阵。

第 3 层，信道增强层（16），将 1×8 的特征矩阵复制 15 次，形成 16×8 的 2 维矩阵作为解码器层的输入，可为解码器提供更加丰富的特征表示，是编码器和解码器之间的桥梁。

2) 解码器

解码器按与编码器相反的顺序搭建第 4 层 LSTM（8）和第 5 层 LSTM（32），它们分别是第 2 层和第 1 层的镜像。

第 6 层是全连接层，对第 5 层的输出与其内部向量进行矩阵乘，最终生成 16×2 的输出向量。

定义编码器每层的功能函数为 $\varphi:\mathcal{X}\to\mathcal{Z}$，可完成输入的 $\boldsymbol{x}\in R^{x}=\mathcal{X}$ 到中间向量 $\boldsymbol{z}\in R^{z}=\mathcal{Z}$ 的映射；解码器层中的功能函数为 $\psi:\mathcal{Z}\to\mathcal{X}'$，能够完成中间向量 $\boldsymbol{z}\in R^{z}=\mathcal{Z}$ 到 $\boldsymbol{x}'\in R^{x}=\mathcal{X}'$ 的映射。LSTM 自编码器的编码和解码过程可表示为

$$\boldsymbol{z}=\varphi^2(\varphi^1(\boldsymbol{x}))=\varphi^2\circ\varphi^1(\boldsymbol{x}) \tag{2}$$

$$\boldsymbol{z}'=C^{16}_{\text{boosted}}(\boldsymbol{z}) \tag{3}$$

$$\boldsymbol{x}'=\psi^1(\psi^2(\boldsymbol{z}'))=\psi^1\circ\psi^2(\boldsymbol{z}') \tag{4}$$

$$G_\theta(\boldsymbol{x})=\boldsymbol{x}'=\psi^1\circ\psi^2\circ C^{16}_{\text{boosted}}\circ\varphi^2\circ\varphi^1(\boldsymbol{x}) \tag{5}$$

其中，$\circ$ 为联合函数，$C^{16}_{\text{boosted}}(\bullet)$ 为信道增强函数，$G_\theta(\boldsymbol{x})$ 为 LSTM 自编码器定义模型的函数，θ 为各神经元待定参数。LSTM 自动编码器（生成器）拟合的目的是使输出尽可能拟合输入，而判别器的训练目标是尽量区分输入的原始数据和经编解码后的重构数据，因此 GAN 的目标函数为

$$\min_G\max_D = D(\boldsymbol{x}_i)-D(G(\boldsymbol{x}_i)) \tag{6}$$

其中，$\boldsymbol{x}_i$ 为输入 LSTM-GAN 的预处理后数据，$G(\boldsymbol{x}_i)$ 为经 LSTM 自编码器编码、解码后输出的重构数据。LSTM-GAN 模型利用随机梯度下降法训练，选用 RMSProp 优化算法，其训练算法如算法 1 所示。

算法 1　LSTM-GAN 重构器训练算法

输入　检测数据 X，完整训练次数 epochs，批大小 batch size，学习率 α

输出　模型参数 θ

初始化　θ

1) 利用 X 训练 D//更新判别器参数
2) for i in range(epochs)
3)　for j in range(len(X))//len(X)为训练数据的数量
4)　$\boldsymbol{x}_j\in X$
5)　$G_\theta\leftarrow\nabla_\theta[\boldsymbol{x}_j-G_\theta(\boldsymbol{x}_j)]$//更新梯度
6)　$\theta\leftarrow\theta+\alpha\text{RMSProp}(\theta,G_\theta)$//更新模型参数
7)　end for
8) end for
9) return θ

重构误差会随着训练次数的增多而减小，LSTM-GAN 重构器最终达到一种稳定状态，额外的训练不会减少重构误差。利用验证集计算 LSTM-GAN 重构器在稳定状态下的重构误差，计算区分正常流量或攻击流量的门限标准，即异常判定的阈值。参照“3σ”准则，将阈值设置为所有验证集样本重构误差均值加 3 个标准差，则异常检测阈值可表示为

$$S_{\text{threshold}}=\mu+3\sigma \tag{7}$$

其中，μ 为训练好的 LSTM-GAN 计算出的验证集中所有样本重构误差的平均值，σ 为标准差。

4.3　攻击判定模块

由于使用正常流量数据建模，LSTM-GAN 重构器可学习到正常流的特征分布，能够很好地完成对正常流的重构。当输入攻击流时，因为攻击流偏离了正常 TCP 流的特征，重构器不能对其有效重构，生成的重构序列与原始输入存在较大的偏差，判别器计算出的重构误差将会偏大。攻击判定模块将每个输入样本的重构误差与阈值比较，如果重构误差大于阈值则判定为攻击，反之则判定为正常流。

5　实验结果及分析

5.1　实验设置

本文实验环境配置的使用的硬件为 Core i9-12900F、128 GB RAM(DDR5)、NVIDIA RTX3090，使用的软件为 Ubuntu 18.04LTS、CUDA11.2、Pytorch1.8。

5.2　LSTM-GAN 模型训练

在进行检测之前，需要利用训练集中的样本数据对 LSTM-GAN 模型进行充分训练，直到达到最

大训练次数或设置的停止训练阈值。图 8 展示了 LSTM-GAN 迭代训练损失函数值。从图 8 可以看出，在前 30 次迭代训练时，损失函数值振荡减小；当迭代 70 次后，损失函数值趋于稳定。为保险起见，在实验中将最大迭代次数设置为 80。

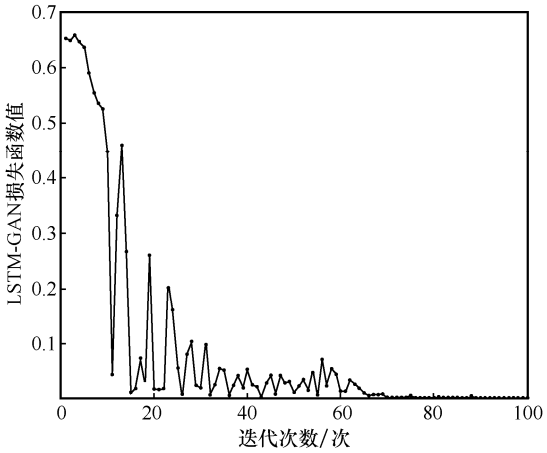


图 8 LSTM-GAN 迭代训练损失函数值

模型的其他超参数根据经验与实验调试设定，表 2 为 LSTM-GAN 模型超参数的取值。

表 2 LSTM-GAN 模型超参数的取值

超参数属性	取值
最大迭代次数/次	80
批大小	16
学习率	0.000 5
停止训练阈值	0.000 1

5.3 评价指标

基于 LSTM-GAN 重构器的 LDoS 攻击检测方法的目的是从待检测流量中发现攻击流量，并不关注攻击发起的阶段和类型，因此，检测的最终目标可转换为二分类问题。将正常流量定义为负样例，攻击流量定义为正样例，使用准确率（Accuracy）、精确率（Precision）、召回率（Recall）、误警率（FPR, false positive rate）以及 F1 值这 5 项指标作为评价模型检测性能的主要依据。

5.4 实验结果与分析

5.4.1 本文数据集的实验结果

本文数据集上的检测实验分为 2 个阶段，第一阶段是单独对各攻击流量进行检测，得到 LSTM-GAN 模型对每种 LDoS 攻击的检测能力；第二阶段是对由多种攻击流量组成的 All-United 数据集进行测试，测试模型对复杂攻击的检测性能。另外，为评估模型检测能力，本文将其与经典 LDoS 攻击检测方法的检测结果进行比较。

1) 单一攻击检测实验

第一阶段中，利用验证集数据求出训练好的模型在稳态下所有样本重构误差的均值，并加上 3 个标准差作为误差判定的阈值。由于随机划分的验证集可能出现类别失衡，从而导致计算出的阈值出现偏差，因此采用 5 折交叉计算的方式，将验证集划分为 5 份，每次取其中 4 份进行计算，将 5 次计算得到的阈值的平均值作为攻击检测的最终阈值。另外，为排除运算时可能出现的偶然性因素，模型对每种 LDoS 攻击的测试集进行 5 次检测，以评价指标的平均值作为最终检测结果。表 3 展示了 LSTM-GAN 模型对单一攻击的检测性能。从表 3 可以看出，LSTM-GAN 对各攻击流量检测的召回率均达到 93%以上。对 Pwnloris 攻击的检测指标最好，可能是由于 Pwnloris 是 Slowloris 的升级版，低速率攻击的特征更加明显。其次对 Hping 攻击的检测性能也很好，原因是 Hping 程序本来是用于泛洪式的 DDoS 攻击，在本文实验中，为了低速攻击的效果，Hping 被设置为仅在每秒的前 0.1 s 的时间间隔内生成攻击，且数据包大小为定值，这使 Hping 攻击流具有显著的周期性和突发性特征，因此更加容易被检测出。Slowhttptest 攻击的检测效果相对略差的原因是 Slowhttptest 程序生成的是慢速读取攻击流量，时间跨度比较大，而本文选择的数据为每 10 s 流片段中前 16 个时间步的特征，可能出现了选取的某些数据刚好处理 Slowhttptest 攻击流量的“静默期”，从而没有形成明显的数据特征，对检测造成不利影响。虽然最高误警率达到 4.86%，但平均误警率为 2.93%，这在以安全告警为目标的检测设计中是可以接受的。

表 3 LSTM-GAN 模型对单一攻击的检测性能

攻击种类	准确率	召回率	精确率	误警率	F1 值
Pwnloris	0.979 4	0.961 1	0.937 7	0.016 0	0.949 2
Hping	0.969 4	0.947 2	0.904 5	0.025 0	0.925 4
Torshammer	0.968 9	0.955 6	0.895 8	0.027 8	0.924 7
Slowloris	0.962 2	0.936 1	0.882 2	0.031 3	0.908 4
Httpbog	0.964 4	0.930 6	0.895 7	0.027 1	0.912 8
Slowhttptest	0.951 7	0.952 8	0.830 5	0.048 6	0.887 5
平均值	0.966 0	0.947 2	0.891 1	0.029 3	0.918 0

2) 复杂攻击检测实验

第一阶段的实验表明 LSTM-GAN 模型对单一攻击流量的检测性能表现良好，为了测试模型应对复杂攻击的能力，第二阶段将在包含多种复杂攻击流量的 All-United 数据集中进行实验。因为整体数据量不大，采用“留一法”进行检测，将测试集数据随机分成 10 份，每次选取 9 份参与运算，最终结果取 10 次运算结果的平均值，如图 9 所示，平均准确率为 0.949 9、平均召回率为 0.942 8、平均精确率为 0.910 3、平均误警率为 0.046 6、平均 F1 值为 0.926 2。对比单独攻击流检测的整体性能，准确率和召回率略有下降，精确率提升明显，F1 值有所提升，误警率也有所上升。原因可能是 All-United 数据集中异常样本比单一攻击数据集中异常样本的占比高，数据集中正负样本数量更加趋于均衡，使检测结果也更加合理平稳，这从 F1 值的提升可以看出。

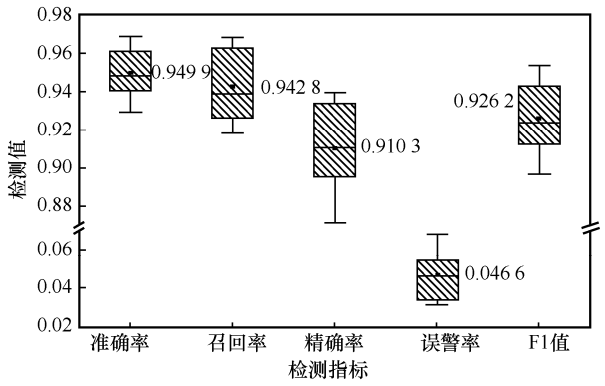


图 9　LSTM-GAN 对复杂攻击的检测指标

在攻击检测任务中，研究人员更加关注攻击的召回率，LSTM-GAN 对单一攻击的召回率均超过了 93%，对复杂攻击的召回率也达到了 94.28%，因此 LSTM-GAN 模型无论是对单一种类的攻击还是复杂攻击的检测都能取得较好的检测效果。

由于检测中只需用到流片段中的前 16 个数据包的 2 项统计特征，即每个检测样本只需经过 16 个时间步就能得到，而本文的设备每分钟可以从原始的.pcap 文件中解析出数千条网络流信息，即检测所需的特征数据能够实时生成。另外，特征提取和攻击检测分属 2 个模块，可以并行处理，因此相对于传统需要分析流内大量数据包信息的检测方法，本文所提的检测方法具有早期检测的能力。

表 4 为 LSTM-GAN 完成每种攻击检测的时间消耗。从表 4 可以看出，对每个数据集检测一次的时间消耗约为 1 s，对单样本的检测时间达到毫秒级，这样的检测速率可以满足在线检测的时间需求。

表 4　LSTM-GAN 完成每种攻击检测的时间消耗

攻击种类	检测时间/s	单轮检测时间/s	单样本检测时间/ ms
Pwnloris	5.67	1.134	0.63
Hping	4.72	0.944	0.52
Torshammer	6.32	1.264	0.70
Slowloris	6.67	1.334	0.74
Httpbog	4.98	0.996	0.55
Slowhttptest	3.39	0.678	0.38
All-United	12.58	1.258	0.58

3) 与其他检测方法的比较

本节将本文方法与几种不同类型的典型检测方法进行了比较，包括基于联合特征的检测方法[10]，PCA 与 SVM 相结合的方法 PCA-SVM [20]，SDN 框架下的多层感知器方法 SDN-MLP [22]，基于多特征自适应增强方法 MF-Adaboost [23]，以及前馈卷积神经网络方法 FF-CNN[24]共 5 种检测方法。表 5 展示了各检测方法的实验数据、数据来源及检测性能指标等信息。

表 5　各检测方法的实验数据、数据来源及检测性能指标

检测方法	实验数据	数据来源	准确率	召回率	精确率	误警率	F1 值	消耗时间/ms
联合特征	自采集数据	实际网络环境中搭建的 Test-bed 实验平台	—	0.966 8	—	0.038 9	—	—
PCA-SVM	自采集数据	NS-2 试验平台	0.924 7	0.951 6	—	0.068 8	—	—
SDN-MLP	CICDoS2017	公开数据集	0.950 1	0.945 1	0.954 6	0.005 2	0.949 8	—
MF-Adaboost	自采集数据	NS-2 试验平台	—	0.970 6	—	0.003 3	—	—
FF-CNN	CICDoS2017	公开数据集	0.990 0	0.963 0	0.975 0	—	0.969 0	0.003 8
LSTM-GAN	自采集数据	实际网络环境及模拟攻击平台	0.949 9	0.942 8	0.910 3	0.046 6	0.926 2	0.580 0

由表 5 可知，虽然 LSTM-GAN 方法的召回率最低，但是本文设计的攻击模式为每次攻击持续 50 s、休眠 100 s，然后按此周期进行攻击和休眠，即每次攻击流的持续时间为 50 s。实验中以每 10 s 划分 1 个流片段，每个攻击流可划分为 5 个流片段，这 5 个流片段中只要有 1 个流片段被检测出来，就可认为这次的攻击被检测出，因此 LSTM-GAN 对攻击流的召回率是大于 0.999 9 的。另外，LSTM-GAN 取得 0.046 6 的误报率。在攻击检测任务中，人们更加关注对攻击的召回率，对误报率会有一定的容忍度，因此，LSTM-GAN 的检测性能总体上优于其他几种方法。

5.4.2　其他数据集的实验结果

为了验证本文所提方法对异构网络流量数据的泛化能力，分别在 ISCX2016、CICIDS2018、CICDDoS2019、DARPA2000、UTSA2021 这 5 个公开数据集上进行检验。

由于本文方法用于检测传输层和应用层的 LDoS 攻击，因此在进行实验前，需要对各数据集进行处理，提取 DoS 攻击流数据，再用分析工具提取检测所需的数据信息。需要说明的是，对于已经被 CICFlowMeter 处理过的数据集，如 CICDDoS2019 数据集的 80 维特征属性值是不能直接使用的，需要进行一定的等价变换。用流的统计信息代替数据包的统计信息，即用流中前向数据包的平均值代替数据包大小，用前向数据包时间间隔的平均值代替数据包时间间隔，这样将连续 16 个流的特征数据构造为一个数据样本，正常流量集和攻击流量集均按此方法构造。例如，利用 CICDDoS2019 数据集构造的攻击流量样本和正常流量样本形式分别为

$$\begin{bmatrix} 322.5, & 577, & 288.5, & 457, & 251, & 465, & 265.5, \cdots, 259 \\ 108.6, & 16, & 108.6, & 23, & 108.6, & 7, & 108.6, \cdots, 108.6 \end{bmatrix}$$

$$\begin{bmatrix} 322.5, & 281, & 27972.8, & 132, & 76, & 68899, & \cdots, 505217 \\ 108.6, & 19, & 98.7, & 0, & 10.3, & 58, & \cdots, 35.7 \end{bmatrix}$$

由于各数据集网络配置环境具有较大的差异性，因此在进行检测前，先使用各数据集中的部分正常样本对模型 LSTM-GAN 进行训练。并计算出异常判定的阈值，再使用测试数据进行实验。LSTM-GAN 模型在各数据集中的检测性能如图 10 所示。

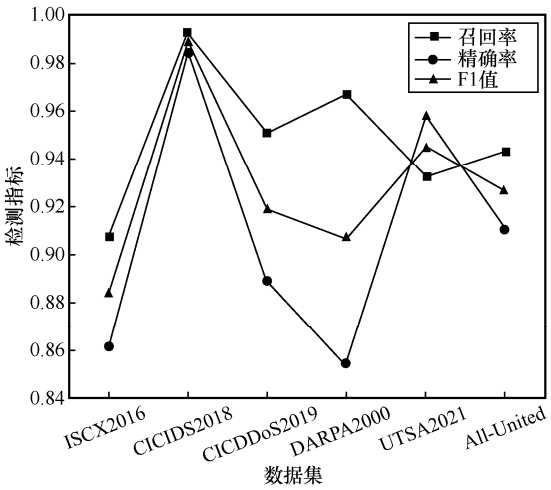


图 10　LSTM-GAN 模型在各数据集中的检测性能

从图 10 可以看出，LSTM-GAN 方法在几个数据集上的检测召回率都大于 90%，其中，在 CICIDS2018、CICDDoS2019、DARPA2000 数据集上的召回率超过 95%，其原因可能是 CICDDoS2019，DARPA2000 这 2 个数据集中的攻击流量为 DoS 或者 DDoS 攻击，比 LDoS 的包间隔和包大小具有更加明显的统计特征，构造出的检测数据可以被轻松识别。而 CICIDS2018 构造出的攻击样本中包大小和时间间隔都几乎完全相同，所以攻击样本更容易被检测出。在 UTSA2021 数据集中，本文选用的是攻击峰值为 50 rad/s 的子数据集 Syn50，相比从更高攻击速率的数据集中检测攻击特征更加具有挑战性，然而 93.27%的召回率也是个不错的成绩。在 ISCX2016 数据集的召回率相对较低（90.73%），这是由于攻击样本与正常样本的生成网络环境不同，因此在利用正常样本训练出的 LSTM-GAN 模型更加粗犷，难以发现统计特征中微小的变化。LSTM-GAN 模型在 ISCX2016、CICDDoS2019、DARPA2000 数据集上的精确率没有取得召回率那样优异的成绩，原因是本文选用的特征向量相对较少，需要训练的参数相对于大型深度网络模型要少得多，在训练样本相对充足的情况下，模型出现了过拟合的问题。这使模型在判定正常流量时标准更加“苛刻”，以至于部分正常样本被误认为攻击样本。但总体来说，LSTM-GAN 能够在 6 个数据集上表现出较强的泛化能力，即便是在 ISCX2016 数据集上召回率也超过了 90%，说明本文设计的 LSTM-GAN 方法可以很好地发现异构网络环境中的攻击行为。

6　结束语

针对传统的 LDoS 攻击流量检测方法需要跟踪提取网络中大量数据包特征，消耗资源大，难以满足实时在线检测需求，以及实验环境与现实网络环境差异过大的问题，本文提出以真实网络流量为背景，基于网络流量简单统计特征的 LDoS 攻击检测方法（LSTM-GAN），只选用网络流量片段中前 16 个数据包的大小及到达时间间隔作为特征数据，利用正常流量特征数据对 LSTM-GAN 模型建模，使 LSTM-GAN 学习到正常流量特征的空间分布，根据重构序列与输入数据的重构误差进行攻击判定。

实验结果表明，所提方法能够对真实网络环境中获取的流量数据进行简单统计特征提取，并准确地检测出流片段中包含的多种 LDoS 攻击行为产生的异常流；以流片段为检测对象，比以整个数据流为目标的检测方法更加具备早期发现攻击的优势。另外，实验环境虽然是以校园网的 Web 服务器为背景，由于特征数据只需网络流量中部分数据包的大小和到达时间间隔的统计信息，不需要人工刻意设计复杂特征，更不用分析流量具体内容，因此，本文方法原则上也可以用于其他针对 HTTP 服务器或 HTTPS 服务器的 LDoS 攻击的检测。

参考文献：

[1] WU Z J, LI W J, LIU L, et al. Low-rate DoS attacks, detection, defense, and challenges: a survey[J]. IEEE Access, 2020, 8: 43920-43943.

[2] ADI E, BAIG Z, LAM C P, et al. Low-rate denial-of-service attacks against HTTP/2 services[C]//Proceedings of 2015 5th International Conference on IT Convergence and Security (ICITCS). Piscataway: IEEE Press, 2015: 1-5.

[3] 李洪成，吴晓平,姜洪海.基于改进聚类分析的网络流量异常检测方法[J].网络与信息安全学报, 2015, 1(1): 66-71.
LI H C, WU X P, JIANG H H. Traffic anomaly detection method in networks based on improved clustering algorithm[J]. Chinese Journal of Network and Information Security, 2015, 1(1): 66-71.

[4] MANIMURUGAN S, ALMUTAIRI S. A user-based video recommendation approach using CAC filtering, PCA with LDOS-CoMoDa[J]. The Journal of Supercomputing, 2022, 78(7): 9377-9391.

[5] 李佳, 云晓春, 李书豪, 等. 基于混合结构深度神经网络的 HTTP 恶意流量检测方法[J]. 通信学报, 2019, 40(1): 24-33.
LI J, YUN X C, LI S H, et al. HTTP malicious traffic detection method based on hybrid structure deep neural network[J]. Journal on Communications, 2019, 40(1): 24-33.

[6] SHI W, TANG D, ZHAN S J, et al. An approach for detecting LDoS attack based on cloud model[J]. Frontiers of Computer Science, 2022, 16(6): 1-12.

[7] KUZMANOVIC A, KNIGHTLY E W. Low-rate TCP-targeted denial of service attacks and counter strategies[C]//Proceedings of IEEE/ACM Transactions on Networking. Piscataway: IEEE Press, 2005: 683-696.

[8] LIU L, WANG H Y, WU Z J, et al. The detection method of low-rate DoS attack based on multi-feature fusion[J]. Digital Communications and Networks, 2020, 6(4): 504-513.

[9] SHARAFALDIN I, GHARIB A, LASHKARI A H, et al. Towards a reliable intrusion detection benchmark dataset[J]. Software Networking, 2017, 2017(1): 177-200.

[10] 吴志军, 张景安, 岳猛, 等. 基于联合特征的 LDoS 攻击检测方法[J]. 通信学报, 2017, 38(5): 19-30.
WU Z J, ZHANG J G, YUE M, et al. Approach of detecting low-rate DoS attack based on combined features[J]. Journal on Communications, 2017, 38(5): 19-30.

[11] WU Z J, ZHANG L Y, YUE M. Low-rate DoS attacks detection based on network multifractal[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(5): 559-567.

[12] LIU D L, SHUAI D X. Multifractal characteristic quantities of network traffic models[C]//Grid and Cooperative Computing. Berlin: Springer, 2004: 413-417.

[13] ZHANG C W, CAI Z P, CHEN W F, et al. Flow level detection and filtering of low-rate DDoS[J]. Computer Networks, 2012, 56(15): 3417-3431.

[14] WU Z J, WANG M X, YAN C C, et al. Low-rate DoS attack flows filtering based on frequency spectral analysis[J]. China Communications, 2017, 14(6): 98-112.

[15] 杜臻, 马立鹏, 孙国梓. 一种基于小波分析的网络流量异常检测方法[J]. 计算机科学, 2019, 46(8): 178-182.
DU Z, MA L P, SUN G Z. Network traffic anomaly detection based on wavelet analysis[J]. Computer Science, 2019, 46(8): 178-182.

[16] AGRAWAL N, TAPASWI S. Low rate cloud DDoS attack defense method based on power spectral density analysis[J]. Information Processing Letters, 2018, 138: 44-50.

[17] BRYNIELSSON J, SHARMA R. Detectability of low-rate HTTP server DoS attacks using spectral analysis[C]//Proceedings of 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). Piscataway: IEEE Press, 2015: 954-961.

[18] WU X X, TANG D, TANG L, et al. A low-rate DoS attack detection method based on Hilbert spectrum and correlation[C]//Proceedings of 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). Piscataway: IEEE Press, 2018: 1358-1363.

[19] SWAMI R, DAVE M, RANGA V. Defending DDoS against software defined networks using entropy[C]//Proceedings of 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). Piscataway: IEEE Press, 2019: 1-5.

[20] ZHANG D S, TANG D, TANG L, et al. PCA-SVM-based approach of detecting low-rate DoS attack[C]//Proceedings of 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems. Piscataway: IEEE Press, 2019: 1163-1170.

[21] YAN Y D, TANG D, ZHAN S J, et al. Low-rate DoS attack detection based on improved logistic regression[C]//Proceedings of 2019 IEEE 21st International Conference on High Performance Computing and

Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems. Piscataway: IEEE Press, 2019: 468-476.

[22] PÉREZ-DÍAZ J A, VALDOVINOS I A, CHOO K K R, et al. A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning[J]. IEEE Access, 2020, 8: 155859-155872.

[23] TANG D, TANG L, DAI R, et al. MF-Adaboost: LDoS attack detection based on multi-features and improved Adaboost[J]. Future Generation Computer Systems, 2020, 106: 347-359.

[24] ILANGO H S, MA M D, SU R. A FeedForward-convolutional neural network to detect low-rate DoS in IoT[J]. Engineering Applications of Artificial Intelligence, 2022, 114: 105059.

[25] TANG D, TANG L, SHI W, et al. MF-CNN: a new approach for LDoS attack detection based on multi-feature fusion and CNN[J]. Mobile Networks and Applications, 2021, 26(4): 1705-1722.

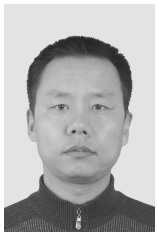
[26] AGARWAL A, PRASAD A, RUSTOGI R, et al. Detection and mitigation of fraudulent resource consumption attacks in cloud using deep learning approach[J]. Journal of Information Security and Applications, 2021, 56: 102672.

[27] XU C Y, SHEN J Z, DU X. Low-rate DoS attack detection method based on hybrid deep neural networks[J]. Journal of Information Security and Applications, 2021, 60: 102879.

[28] CHEN X H, DENG L W, HUANG F T, et al. DAEMON: unsupervised anomaly detection and interpretation for multivariate time series[C]//Proceedings of 2021 IEEE 37th International Conference on Data Engineering. Piscataway: IEEE Press, 2021: 2225-2230.

[29] ANDREAS V, MICHAEL W, SERGE B. Residual networks behave like ensembles of relatively shallow networks[C]//Advances in Neural Information Processing Systems. Massachusetts: MIT Press, 2016: 550-558.

[作者简介]



段雪源（1981− ），男，河南开封人，海军工程大学博士生，主要研究方向为人工智能、信息处理、网络安全。

付钰（1982− ），女，湖北武汉人，博士，海军工程大学教授、博士生导师，主要研究方向为信息安全、人工智能。

王坤（1981− ），女，河南信阳人，海军工程大学博士生，主要研究方向为信息安全。

李彬（1998− ），男，湖南娄底人，海军工程大学硕士生，主要研究方向为信息安全、人工智能。