D4C 循环神经网络
基于深度学习的 DDoS 攻击识别

1st 张亦弛

浙江大学
信息与电子工程学院
杭州, 中国
3210103159@zju.edu.cn

摘要—今年来，分布式拒绝服务（DDoS）攻击的数量增长速度相当之快，已经逐渐成为互联网上最致命的威胁之一。为了防御这种攻击，防御者需要自动检测 DDoS 攻击数据包。传统的防御策略是监视网络流量，并基于统计差异从合法流量中识别攻击活动。机器学习是另一种基于统计特征提高识别性能的方法。然而，传统的机器学习技术受到浅层表示模型的限制，通常只能识别一种或几种类型的 DDoS 攻击。在本文中，我们提出了一种基于深度学习的 DDoS 攻击检测方法。深度学习方法可以自动从低级特征中提取高级特征，并获得强大的表示和推理能力。为此，我们设计了一种循环深度神经网络，从网络流量序列中学习模式并跟踪网络攻击活动，实现对 DDoS 攻击的检测。我们将其命名为 D4C 循环神经网络 (Directional Deep DDoS Detection Convolutional Recurrent Network).

I. 介绍

拒绝服务（DoS）攻击会阻止合法用户访问共享服务和资源 [?]。分布式拒绝服务（DDoS）是指攻击者使用多个分布式计算资源对一个或多个目标发起协调的 DoS 攻击 [?]。这种攻击主要针对系统资源和网络带宽，涵盖了从网络层到应用层的多个层次。自 1999 年第一次 DDoS 攻击浪潮以来 [?]，DDoS 已经成为全球范围内重要、普遍和快速发展的安全威胁。目前，DDoS 的主要攻击向量包括 UDP 洪泛、HTTP 洪泛、SYN 洪泛、ICMP、DNS 等 [?]，对系统和网络构成严重威胁。

DDoS 检测是 DDoS 防御机制中的主要组成部分。然而，DDoS 攻击很难自动检测，因为在大多数情况下，攻击流量与合法流量非常相似。在早期阶段，攻击流量不足、攻击频率低的攻击甚至被认为是合法流量 [?]。许多研究人员尝试使用统计和机器学习方法，或两者的组合来识别 DDoS 攻击。然而，它们仍然存在以下缺点：（1）适当的统计特征需要对网络安全有广泛而深入的了解，并需要大量的 DDoS 攻击实验来确定。（2）防御对象仅限于一种或少数几种 DDoS 向量。（3）它需要经常更新其模型和阈值，以跟上系统和攻击向量的变化。（4）它很难检测慢速 DDoS 攻击。

在本文中，我们提出了一种基于深度学习的方法，用于在受害者接受的合法网络流量中检测 DDoS 攻击，并基于这种方法设计出一种基于循环神经网络的模型。我们将其命名为 **D4C**（**D**irectional **D**eep **D**DoS **D**etection **C**onvolutional Recurrent Network）。我们使用大规模数据集 UNB ISCX Intrusion Detection Evaluation 2012 DataSet（本文中简称 ISCX2012）[?] 来训练 **D4C** 循环神经网络，以解决复杂的 DDoS 攻击识别问题。

本文的其余部分组织如下。第 II 节解释相关工作。在第 III 节中，我们提出了 **D4C** 循环神经网络、数据预处理方法和整体架构。第 IV 节描述了在 ISCX2012 数据集上进行的实验，比较了我们的模型及其变种与传统模型的差异。最后，在第 V 节中总结了我们的工作。

II. 相关工作

A. DDoS 攻击与传统反制措施

主机资源和网络带宽是 DDoS 攻击的两个主要目标。大多数攻击针对协议和应用程序的漏洞，例如 SYN 洪泛、UDP 洪泛、ICMP 洪泛、SIP 洪泛等。一些攻击，如 UDP 洪泛和 ICMP 洪泛，消耗网络带宽，而其

他攻击，如 SYN 洪泛和 SIP 洪泛，还消耗受害者系统资源（如 CPU 和内存）[?]。不仅如此，DDoS 攻击还会利用 IP 欺骗、网络放大器/反射器等技术，结合攻击方法并避免检测，从而造成更大的危害 [?]。

为了防御 DDoS 攻击，一些解决方案使用预防性和响应性机制来减轻 DDoS 攻击对受害网络、中间网络和源网络的影响 [?]。最常用的机制包括攻击预防、攻击检测和攻击响应。攻击预防试图在攻击造成损害之前过滤入站和出站流量，攻击响应旨在最小化 DDoS 攻击造成的损失。本次我们专注的主题在于攻击检测。

D-WARD 是一种部署在源端网络中的 DDoS 防御系统，它监视双向流量。D-WARD 提出了基于不同协议的合法流量和 DDoS 流量之间的统计比较来检测 DDoS 攻击的能力 [?]。Bhuyan 和 Kalita 比较了四个重要的信息熵度量（即 Hartley 熵、Shannon 熵、Renyin++s 熵和 Renyin++s 广义熵）在 DDoS 检测中的应用 [?]。基于这四种信息熵方法，他们计算网络流量中的信息距离并分别检测低速率和高速率的 DDoS 攻击。Chen 通过对 SYN 到达率和 SYN 和 ACK 数据包数量进行两个统计 t 检验来识别 DDoS 攻击 [?]。大多数统计方法在特定的 DDoS 攻击方法中表现良好，但需要大量时间和专业知识对流量进行的特征筛选以及根据所需指标进行预处理。

B. 基于机器学习的 DDoS 攻击防御

事实上，如今机器学习算法已经广泛应用于 DDoS 防御中，特别是在异常检测阶段。最常用的算法包括朴素贝叶斯、神经网络、支持向量机、决策树和 K 最近邻。图 1 描述了基于机器学习 DDoS 攻击检测系统的一般架构。网络流量通过过滤规则进行过滤并存储在数据库中。然后从流量中提取特征，例如数据包速率和协议类型，并进行归一化以加速训练过程。然后使用训练数据来训练机器学习算法，将实时网络流量中的每个数据包分类为 DDoS 攻击或合法流量。最后，系统丢弃机器学习算法检测到的 DDoS 数据包并更新其过滤规则。

Xu、Sun 和 Huang 基于观察到的源 IP 广告使用隐马尔可夫模型（HMM）和强化学习来区分基本流量和 DDoS 攻击，[?]。他们将检测代理放置在中间网络节点或靠近 DDoS 攻击源处。提出了 HMM 来计算新 IP 地址的特定观察序列的概率。和他们所做的工作类似，Berral 等人从中间网络收集流量信息，让每个节点

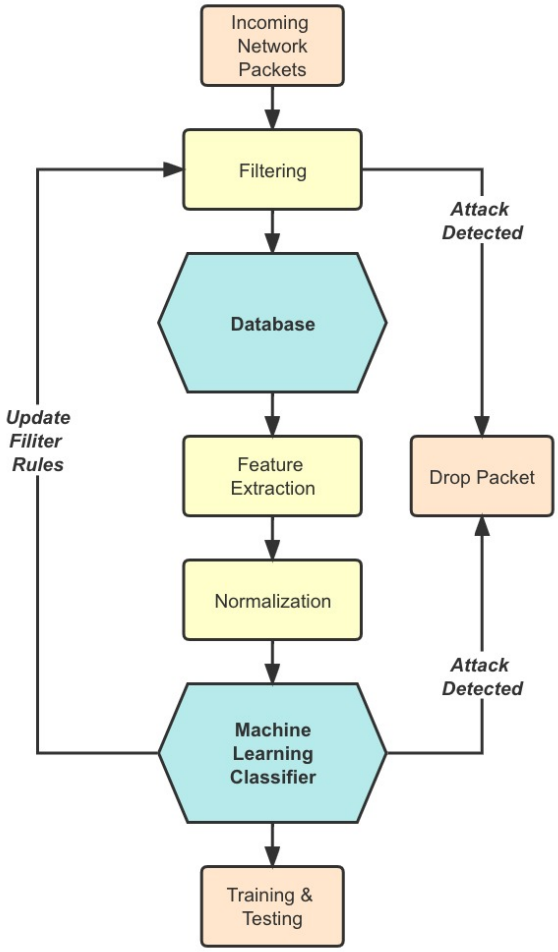

图 1. 基于机器学习 DDoS 攻击检测系统的一般架构

独立学习并共享信息 [?]。每个节点配备了朴素贝叶斯算法，根据源和目的地址检测 DDoS 攻击，并共享信息。这一方法减少了反应时间并减轻了 DDoS 攻击的影响。Shon 等人提出了一种遗传算法（GA）和支持向量机（SVM）[?]。他们使用基于 GA 的特征选择来包括更多的网络流量域。然后使用 SVM 对数据包进行分类以检测 DDoS 攻击。

总之，使用机器学习算法的 DDoS 检测方法可以有效减轻 DDoS 攻击对网络的影响。在选择方法和算法时，必须考虑攻击的类型和特征，才能实现更好的检测性能。

III. D4C 循环神经网络——基于深度学习的 DDoS 攻击检测

通常我们很难检测出低速率的 DDoS 攻击，因为它们从受害者端看起来与合法的网络流量相似。然而我们注意到，基于 DDoS 攻击的原理和特性，对受害者系统的 DDoS 攻击必须持续一段时间，否则它们就不会对网络/系统资源产生明显的恶意影响。这一结论展现了历史模式在 DDoS 检测攻击检测中的重要性。传统的检测方法和学习模型之所以需要大量时间和精力去对数据集进行标注和预处理，是因为其缺乏历史模式的学习，基于数据包本身的检测方法很难突破分类器的性能瓶颈。因此我们提出了一种基于循环神经网络的模型 **D4C** 循环神经网络（**D**irectional **D**eep **D**DoS **D**etection **C**onvolutional Recurrent Network）。

为了实现对历史模式的学习，我们的检测方法利用网络数据包的连续序列，并能够区分攻击流量和合法流量之间的微小差异。历史信息被输入到 RNN 模型中以识别 DDoS 攻击。对历史模式的学习有助于找到代表 DDoS 攻击的重复模式，并在长期流量序列对 DDoS 攻击流量进行定位。循环神经网络的另一个优点是它不依赖于输入窗口大小。先前机器学习方法中使用的窗口大小通常是任务相关的，这限制了它们检测不同类型攻击的能力。此外，传统的机器学习方法很难对长期序列进行训练。然而，循环神经网络（尤其是 LSTM、GRU 等门控 RNN）已经显示出解决这些问题的能力 [**?**]。这也是为什么我们选择循环神经网络作为我们 DDoS 分类器的主要组件。

为了实现我们希望的具有对历史模式拥有学习能力的循环神经网络模型，我们需要对 ISCX2012 数据集进行特征提取以及模式变换以适应模型搭建的需要。

A. 特征提取与数据整形

由于 ISCX2012 是一个相当规模的数据集，我们首先从 ISCX2012 数据集中提取了 28 个网络流量字段。表 I 显示了这些字段的示例和类型。我们将这 28 个网络流量字段用作训练特征，与应用于 DDoS 检测的其他机器学习方法不同，我们不需要在模型中选择统计特征。

我们将字段分类为三种类型：Text、Boolean、Numerical。对于 Text 字段，我们使用 LabelEncoder 方法进行编码。对于 Boolean 字段，我们进行转换将大多数 Boolean 字段转换为 0 和 1。然而，由于计算资源限制，我们只有有限数量的训练样本（50,000），因此攻击和正常流量的大多数 ip.src 和 ip.dst 相似。经过实验测试如果训练这三个 Text 特征极大概率导致模型过拟合。因此在本文中，我们的模型没有训练这三个 Text 字段特征。

表 I
NETWORK TRAFFIC FIELDS

Field	**Field Example**	**Field Type**
frame.len	206	Numerical
ip.hdr_len	20	Numerical
frame.protocols	eth:ethertype:ip:tcp:ssh	Text
ip.len	192	Numerical
ip.flags.rb	0	Boolean
ip.flags.df	1	Boolean
ip.flags.mf	0	Boolean
ip.frag_offset	0	Boolean
ip.ttl	128	Numerical
ip.proto	6	Numerical
ip.src	192.168.1.101	Text
ip.dst	192.168.5.122	Text
tcp.srcport	4175	Numerical
tcp.dstport	22	Numerical
tcp.len	152	Numerical
tcp.ack	1	Numerical
tcp.flags.res	0	Boolean
tcp.flags.ns	0	Boolean
tcp.flags.cwr	0	Boolean
tcp.flags.ecn	0	Boolean
tcp.flags.urg	0	Boolean
tcp.flags.ack	1	Boolean
tcp.flags.push	1	Boolean
tcp.flags.reset	0	Boolean
tcp.flags.syn	0	Boolean
tcp.flags.fin	0	Boolean
tcp.window_size	16697	Numerical
tcp.time_delta	0.000537000	Numerical

为了实现对历史模式的学习，我们还要对数据进行整形。从数据集中以字段为依据提取特征之后，我们获得了一个 $m \times n'$ 矩阵，其中 m 表示网络数据包的数量，n' 表示转换后的新特征数量。为了学习长期和短期模式，我们使用滑动窗口将连续数据包分开，并将数据重新整形为大小为 T 的一系列时间窗口，其中每个窗口中的标签 p 表示最后一个数据包的类别。重新整形后，我们得到一个三维矩阵，形状为 $(m - F) \times T \times n'$。图 2 说明了特征提取、转换和重新整形的工作流程。

使用这种方法，我们将传统的基于数据包的特征转

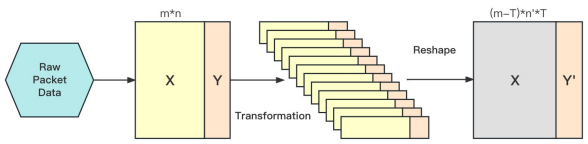

图 2. 特性提取与数据整形

换为基于时间窗口的特征，这使我们能够从先前 $T-1$ 个数据包和当前数据包中学习网络模式。接下来我们尝试设计一个基于循环神经网络的模型来对这个全新的数据集进行训练。

B. *D4C* 循环神经网络

在这个部分中，我们在我们的 **D4C** 模型中设计了一个双向循环神经网络（RNN）。每个方向都由两个序列到序列的循环层组成。循环层帮助我们从以前的网络数据包中追踪历史。为了解决深层 RNN 网络中的梯度爆炸问题，我们在本文中尝试了 LSTM 和 GRU。具体来说，LSTM 旨在克服 RNN 的梯度消失问题，并使用内存单元表示以前的时间戳 [**?**]。GRU 是标准 LSTM 的简化变体，并且由于参数较少，训练速度更快。修改后的 LSTM 目前在每个单元中包括三个门：输入门、遗忘门和输出门。它们计算如下：

$$
\begin{aligned}
i_t &= \sigma(W_{ii}x_t + b_{ii} + W_{hi}h_{t-1} + b_{hi}) \\
f_t &= \sigma(W_{if}x_t + b_{if} + W_{hf}h_{t-1} + b_{hf}) \\
g_t &= \tanh(W_{ig}x_t + b_{ig} + W_{hg}h_{t-1} + b_{hg}) \\
o_t &= \sigma(W_{io}x_t + b_{io} + W_{ho}h_{t-1} + b_{ho}) \\
c_t &= f_t \odot c_{t-1} + i_t \odot g_t \\
h_t &= o_t \odot \tanh(c_t)
\end{aligned}
$$

i_t、f_t 和 o_t 分别表示输入门、遗忘门和输出门的输出。g_t 表示当前时刻的候选细胞状态。$\sigma(\cdot)$ 表示 sigmoid 激活函数，$\odot$ 表示逐元素乘法。W_{ii}、W_{if}、W_{ig}、W_{io}、W_{hi}、W_{hf}、W_{hg} 和 W_{ho} 分别对应于当前时刻的输入特征、以前的隐藏状态和门单元的权重矩阵。b_{ii}、b_{if}、b_{ig}、b_{io}、b_{hi}、b_{hf}、b_{hg} 和 b_{ho} 分别对应于相应门的偏置向量。

基于 LSTM，我们实现了一个双向循环神经网络模型，它是由卷积神经网络（CNN）和双向长短期记忆神经网络（BiLSTM）组成的。其中卷积神网络用于学习输入模式，双向长短期记忆神经网络用于实现对历史模式的学习。该模型的输入数据是经特征提取和整形后的时间序列流量。输入数据首先经过一个卷积神经网络，将数据从一个特征维度转换为多个特征维度，用于提取时间序列数据的局部特征。经过一个归一化层，用于规范卷积层的输出。这样设计的原因主要是为了利用卷积神经网络和批归一化处理输入数据，加快模型的训练速度，同时还能尽量减少梯度消失和过拟合的问题。

卷积神经网络的输出被转换为 BiLSTM 的输入，用于学习时间序列数据的时间依赖性。BiLSTM 是一种能够处理长序列数据的循环神经网络，它可以同时考虑过去和未来的信息，从而更好地捕捉时间序列数据的上下文信息。具体地，该模型包含一个双向的 LSTM 层和一个全连接层，用于输出预测结果。其中，LSTM 层的输出被送入全连接层进行特征的降维和输出的转换，全连接层的输出经过 Sigmoid 函数进行激活，将输出值限制在 0 到 1 之间，方便输出概率值。

具体的模型设计图如图 3 所示。

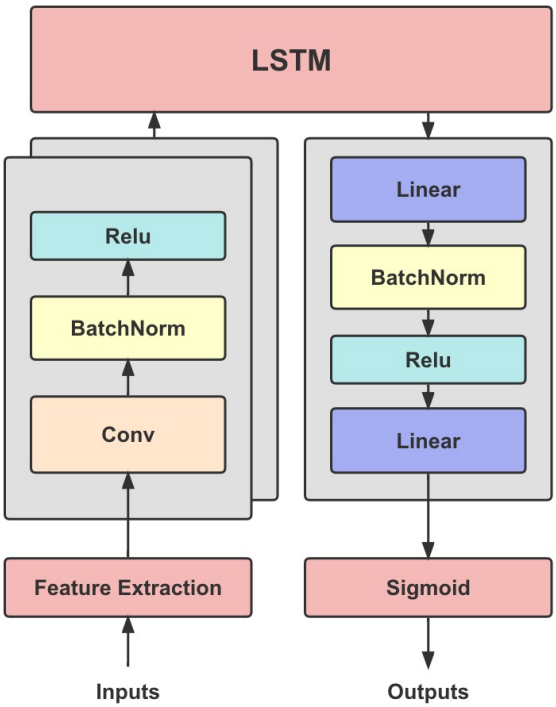

图 3. **D4C** 循环神经网络架构

IV. 实验

A. 数据集介绍与处理

ISCX2012 数据集是一个用于网络入侵检测的数据集，包含大量的网络流量数据和与之相关的攻击标签。评估模型在该数据集上的性能，可以帮助我们了解他们的模型在网络入侵检测任务中的表现，并为未来的研究提供借鉴。然而计算资源的限制，我们只能选择 50,000 条数据记录进行训练和测试。这种限制可能会影响模型的性能，因为模型没有足够的数据来学习网络流量数据的多样性和复杂性。但我们相信尽管只是在小范围的数据上进行训练和验证我们的模型也足以表示出学习历史模式的优越性。

B. 实验设置与结果分析

在本节中，我们主要设计了两种测试。首先是我们进行横向比较，经过相同训练后，LSTM 模型、GRU-**D4C** 模型（使用 GRU 替代 LSTM）、Bi-**D4C** 模型（使用双向 LSTM，基准模型）和 Uni-**D4C** 模型（使用单向 LSTM）的预测准确性. 其次我们还设置了实验纵向比较了在不同滑动窗口大小下，Bi-**D4C** 模型的训练性能和预测准确性。

为了确保实验的可信度，我们从初始参数 $learning\_rate = 0.001$、$num\_epoch = 40$、$batch\_size = 128$、Adam 优化器和使用 BCELoss 开始实验。我们还将数据集分成训练集和测试集方便我们分别进行测试和验证，比例为 4:1。为了确保实验的可靠性，每个数据都是经过十次相同实验取平均值获得的。

循环神经网络性能对比实验: 本次实验中，我们将滑动窗口大小设为 25 以进行统一训练。在训练后，具体的测试数据如表 II 所示。

表 II
D4C 模型比较

模型	误差率	准确率
LSTM	7.86%	92.14%
Bi-D4C	0.79%	99.21%
GRU-D4C	1.96%	95.04%
Uni-D4C	2.36%	97.64%

该表格展示了在相同数据集上测试不同循环神经网络模型（LSTM 模型、GRU-**D4C** 模型、Bi-**D4C** 模型和 Uni-**D4C** 模型）的结果。通过比较这些模型的误差率和准确率，可以得出以下结论：在这个数据集上，Bi-**D4C** 模型表现最好，误差率最低，准确率最高，分别为 0.26% 和 99.74%，优于其他所有模型。LSTM 模型表现最差，误差率为 7.86%，准确率为 92.14%。GRU-**D4C** 和 Uni-**D4C** 模型的性能相对较差，但它们仍然达到了相对较高的准确率，分别为 95.04% 和 97.64%。总体而言，如果选择一种模型来实现 DDoS 攻击检测，Bi-**D4C** 模型是最好的选择，因为它具有最低的误差率和最高的准确率。

*Bi-**D4C** 滑动窗口性能实验:* 本次实验中，我们使用不同大小的滑动窗口训练了我们的模型，并在训练后得到了具体的测试数据，如表 III 所示。

表 III
不同滑动窗口大小下的 Bi-**D4C**

窗口大小	误差率	准确率	训练时间
5	6.32%	93.68%	5min37s
10	3.39%	96.61%	12min6s
20	1.24%	98.76%	22min58s
25	0.79%	99.21%	28min37s
50	0.01%	99.99%	1h2min12s

从表格中我们可以看出在数据集上使用不同滑动窗口大小的 Bi-**D4C** 模型的性能。列出了五个滑动窗口大小：5、10、20、25 和 50。对于每个窗口大小，表格列出了三个指标：误差率、准确率和训练时间。误差率和准确率以百分比表示，训练时间以分钟和秒为单位给出。从表格中可以看出，随着滑动窗口大小的增加，模型的性能显著提高。当滑动窗口大小为 50 时，模型的误差率最低，仅为 0.01%，准确率最高，达到 99.99%。然而，随着窗口大小的增加，训练时间也增加，从 5 分钟 37 秒（窗口大小为 5）到 1 小时 2 分钟 12 秒（窗口大小为 50）。表格中的数据表明，使用较大的滑动窗口大小可以提高 Bi-D4C 模型的性能，但代价是更长的训练时间。

V. 结论

本文提出了一种基于深度学习的 DDoS 攻击检测技术，并基于该技术设计了一个基本的 DDoS 攻击分类器 **D4C**，可以高精度地识别 DDoS 攻击流量和正常用户访问流量。然而，由于计算资源的缺乏，我们无法在更大的数据集上测试更大的模型，尽管在小规模的数据子集上我们的模型有着接近百分百的准确率，但是在

复杂的网络环境中我们的模型能否正确地被训练正确地进行分类仍然是一个未知数。目前我们只能使用小模型在小规模数据集上进行实验，但是我们相信基于历史模式学习的 DDoS 检测是一种具有潜力的发展路径。

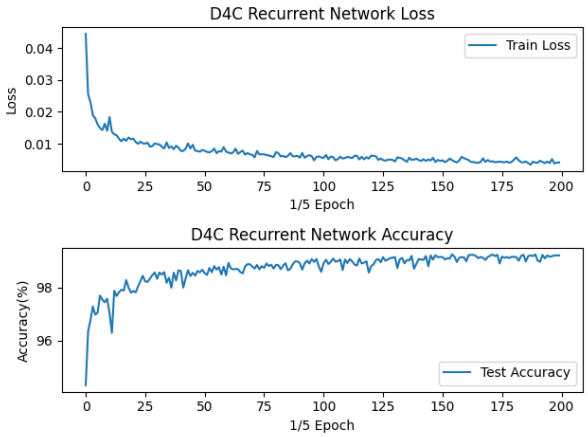

图 4. 测试过程中的损失和准确率曲线

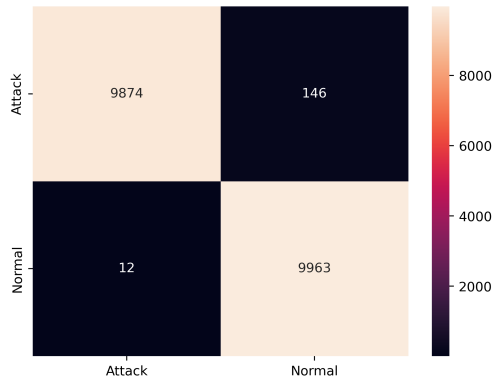

图 5. 测试过程中的混淆矩阵