Answer

1. 翻译

标题

分布式拒绝服务攻击检测的分类算法评估

摘要

分布式拒绝服务（DDoS）攻击的目标是通过恶意流量使目标网络瘫痪，这对服务的可用性构成了威胁。在过去的二十年里，随着互联网的发展，人们提出了许多检测系统，特别是入侵检测系统（IDS），尽管用户和组织在应对DDoS攻击时不断面临挑战并一再遭受失败。即便如此，IDS仍是保护关键网络免受入侵活动影响的第一道防线，但是，它必须始终保持最新，以便检测到任何异常行为，从而确保服务的完整性、机密性和可用性。但是，新的检测方法、技术、算法的准确性在很大程度上依赖于存在专门为训练目的和通过创建分类器模型进行评估的精心设计的数据集。在这项研究中，我们使用主要的有监督分类算法进行实验，以准确地将DDoS攻击从合法流量中分类出来。在所有分类器中，基于树的分类器和基于距离的分类器表现最好。

关键词

机器学习，分布式拒绝服务，逻辑回归，朴素贝叶斯，支持向量机，决策树，随机森林，k近邻算法

1. 介绍

DDoS 攻击已经成为最严重的网络入侵行为之一，并对计算机网络基础设施和各种基于网络的服务构成严重威胁[1]。它们非常突出，因为它们可以轻易发起，并对组织造成灾难性的损失，而且很难追溯和找到真正的攻击者。DDoS 攻击通过耗尽网络资源来影响其可用性，导致服务被拒绝，并且在过去几年中，这种攻击在数量和规模上迅速增加。攻击持续时间缩短但数据规模增大的趋势越来越普遍[6]。大多数现有的工作使用KDD Cup '99数据集[2]或DARPA数据集[3]来检测DDoS攻击。然而，随着时间的推移，网络犯罪和攻击以一种狡猾的方式发生，以侵入目标环境。因此，使用包含所有新颖攻击特征的最新数据集来训练分类器将提高分类器的性能。我们使用

CICDDoS2019数据集进行分析[4]。 我们的工作目标是使用CICDDoS2019数据集训练模型，实施多个有监督分类器来检测DDoS攻击。我们的重点是降低误报率，提高准确性，最终有助于提高生产系统的正常运行时间，以及组织的声誉。

2. 背景及相关工作

基于网络服务器记录的特征，例如平均数据包大小、入站码率对出站码率、源 IP 对目标 IP 及其端口等[5]，可以检测网络流量是否异常。大致上，拒绝服务攻击有两种类型。第一种是网络级 DoS 攻击，该攻击耗尽网络资源，从而禁止实际用户的连接，而另一种类型的攻击是应用级 DoS 攻击，在这种攻击中，服务器资源耗尽，合法用户请求被拒绝。在 DDoS 攻击中，攻击者控制多台被称为僵尸的机器，攻击者从这些机器运行被称为机器人代码的脚本并攻击受害服务器。 主要有两个类别。第一个是反射攻击，另一个是利用攻击。在反射攻击中，攻击者的身份保持不会暴露，而在利用攻击中则不然。反射攻击和利用攻击都可以通过应用协议以及传输层协议或二者的组合来实施。基于 TCP 的反射攻击包括 MSSQL，SSDP，而基于 UDP 的反射攻击包括 CharGen，NTP，TFTP。 Kurniabudi 在[7]中分析了庞大网络流量的相关性和显着特性。Ring 等人，已确定了 15 种不同的属性以评估单个数据集的适用性[8]。Idhammad 基于网络熵估计、群集、信息增益比和树算法描述了 DDoS 检测的半监督 ML 方法[9]。在[10]中的研究人员提出了使用朴素贝叶斯方法的 INDB（入侵检测）机制来检测入侵数据包。使用朴素贝叶斯算法的原因在于其预测性特征。Alenezi 和 Reed 在[11]中提出了 IDS 的广泛分类。已经讨论过 DoS/DDoS 攻击的困难以及特性，并且使用三种不同的分类方法进行了数据分析。Alpna 和 Malhotra 利用 KNN 和随机森林开发了检测 DDoS 攻击的体系结构[12]。Singh 等人，开发了一种改进的 SVM 算法用于检测网络攻击[13]。存在很多涉及 DDoS 攻击检测的相关工作。然而，这些研究大多使用特定的分类算法评估数据集，并试图专注于优化性能[14-16]，例如使用像 KDDCup'99[2] 或 DARPA[3] 这样的旧数据集。在这篇论文中，我们使用最新的 CICDDoS2019[5] 对六种不同的分类算法进行比较分析。

3. 数据集和方法论

该数据集具有七个 csv 文件，含有超过 10GB 的数据。我们应用了特征提取算法来找出最重要的特征，并对数据进行了预处理技术，如数据清洗、标准化、无穷值的移除。一旦模型准备好，就会通过测试集来检测准确性，精确度，召回率、F1 分数、真正例和真负例。如果准确度无法接受，则针对每个分类算法进行优化。此外，还分析了训练测试切分比率。

DDoS 攻击通常通过一个 botnet 或多个 bot 进行。因此，当目标服务器接收数据包时，会有多个 IP 地址或 MAC 地址，但是像数据包长度、流持续时间、前向方向的总包数等这样的属性使我们可以识别出是否是正常的请求还是恶意的请求。为了比较数据包，可以应用数据挖掘技术来测量概率或出现次数以对数据包进行分类。在这里，我们使用以下六种机器学习算法对异常流量进行分类：逻辑回归，支持向量机，朴素贝叶斯，K-最近邻，决策树和随机森林。

我们的实验使用了由纽布伦瑞克大学创建的含有 88 个特征的数据集。该数据集在加拿大网络安全研究所网站[5]上公开可用。数据收集了不同类型的攻击，如 Portmap、LDAP、MSSQL、UDP、UDPLag 等。如果请求来自合法用户，那么就标记为“Benign”，否则标记为特定的攻击名。该数据集明确用于分析目的，并按天进行组织。对于每一天，CIC 都已经记录了每台服务器机器的原始数据，包括网络流量和事件日志。实际的数据集具有超过 88 个特征，但是 CIC 本身已经进行了降维处理，他们使用了 CICFlowmeter-V3 [17]，并生成了最重要的 88 个特征用于分析并提供 csv 文件。如果有人想用自己的方式提取特征，他们也共享了 PCAP 文件。

我们对数据集进行了两种类型的实验。最初我们对数据集做了采样，从每个 csv 文件中随机选择了 30,000 行，总共达到了 200,000 行用于我们的数据分析样本，这是我们的不平衡数据集，对于第二个实验，我们从每个 csv 文件的数据集中得到了同样数量的良性与攻击数据组，形成了一个完全平衡的训练和测试数据集。

表1 显示了每个文件中总记录数与普通类（例如，标签=“BENIGN”）的比较。数据集的更多细节可以在[18]中找到。在训练模型之前，数据集中的IP地址被转换为数值整数。

我们选择了单变量选择技术。这是一种可以用来选择与输出标签关系最强的特征的统计测试。scikit-learn 库提供了 SelectKBest 类，它帮助我们实现算法并给出与我们类标签最相关的特征的结果。我们使用了前 25 个特征来训练我们的模型。为了获得数据集的每个特征的重要性，我们使用了基于树的分类器内置的特征重要性类。图1 解释了最重要的 15 个特征。

4. 实验结果与讨论

A. 评价指标

为了评估分类器的性能，我们使用了基于混淆矩阵的主要性能指标。这个矩阵包含了由机器学习模型进行的真实的和预测的分类信息。为了公平，我们还在结果表中包括了 TP（真正）、TN（真负）、FP（假正）和 FN（假负）值。如前一节所述，我们在不平衡数据集以及平衡数据集上实施了六种不同的机器学习分类算法。我们使用 Python 的 scikit-learn 库实现了这两种技术。

B. 实验

我们对每个单独的 7 个 csv 数据文件进行了随机抽样，从每个文件中选择了 30K、40K 和 50K 个元组，以测量良性流量与攻击流量的比率。我们对每个单独的 7 个 csv 数据文件进行了随机抽样，从每个文件中选择了 30K、40K 和 50K 个元组，以测量良性流量与攻击流量的比率。实际的数据集中良性流量的数量较少，而在进行抽样时，这本身就有偏见。当使用不平衡数据训练模型时，良性流量与攻击标签相比，平均只有 0.5% 到 0.7%。表 2 显示了类分布。为了避免偏差对分类模型准确度的影响，我们也创建了平衡的数据集，其中我们选择了来自每个 7-csv 文件的所有良性流量，同样数量的元组被随机抽样自攻击流量。我们最终从所有文件中收集了 105042 行，包含了相等数量的攻击和良性数据。由于这个数字非常小，我们在现有的数据框中再次添加了同样的数据，以使训练集的大小超过 200K 行，这与不平衡数据集是相当的。

C. 结果

每个分类器都使用准确率和其他评估指标（如Precision、Recall和F1-score）进行评估和评价。对于不平衡的数据集，每种分类算法的总体准确性在表3中显示，而表4显示了平衡数据集的输出结果。数据的选择基于五轮观察中最优值的基础上。

由于不平衡的数据集偏向于攻击类别，所有分类算法的准确性都极高。但是，这并不能帮助我们选择用于DDoS攻击检测的最佳性能算法。在此，除了朴素贝叶斯外，所有算法对于不平衡的数据都有着极好的表现。相反，我们注意到平衡数据集的准确性变化不大。如表4所示，基于树的算法如决策树、随机森林以及基于距离的分类算法K-NN的表现最好，而朴素贝叶斯的准确性也相当不错，但是其余的分类技术——SVM和Logistic回归表现较差。图2显示了各种分类算法在不平衡数据集和平衡数据集中的准确率比较。更重要的是，图3、4和5分别显示了不平衡数据集和平衡数据集的Precision、Recall和F-1 score之间的比较。

在分析输出结果之后，我们发现基于树的分类算法如决策树和随机森林，以及基于距离的分类算法在两种类型的数据集上都表现得最好，准确率几乎达到100%。即使在考虑其他指标时，这三种分类器也表现得最好。然而，当改变每种分类器的参数时，可以注意到性能稍有变化。在这里，我们试图寻求每种算法的最佳性能。

5. 未来工作建议

虽然我们的初步实验结果令人鼓舞，但这项工作可以从多个方向扩展：a) 在我们的实验中，由于硬件限制，我们仅使用了稍多于200,000行数据。在未来，我们可以计划选择超过1百万行的数据集。这将为我们提供更准确的预测训练模型。b) 我们可以根据每种不同类型的DDoS攻击进行数据挖掘，因为可能Portmap可以通过K-NN检测到具有良好的效率，但对于UDPlag，朴素贝叶斯可能更好。如果这一点得到证实，那么我们可以将所有独立的模型合并到一个模型中，以获得对所有类型的DDoS攻击的准确率接近100%。c) 我们可以尝试不同的特征选择技术。

6. 结论

在这篇论文中，我们使用的是CICDDoS2019数据集，这是一个相对较新的数据集，包含了DDoS最新的攻击签名。我们使用主要的监督分类算法进行了实验，以从合法流量中准确地分类出攻击。当将结果与所有分类器中的其他算法比较时，决策树、随机森林和K-NN的表现最好。尽管初步结果令人鼓舞，但我们计划将工作扩展到更大的数据集，并针对不同类型的DDoS攻击。我们将把未来的工作重点放在这些方向上。

2. 特征字段选用

利用`scikit-learn`库中的`SelectKBest`类，从原数据集的所有特征字段中选取了25个得分最高的特征字段用于训练。下对这25个字段进行解释说明。

Index	Feature_Name	Explanation
81	Inbound	表示流量的方向，是否进入系统（例如，在入侵检测系统中，进入系统的流量可能更有可能是恶意的）
11	Fwd Packet Length Mean	正向数据包长度的平均值

56	Avg Fwd Segment Size	前向段的平均大小
41	Min Packet Length	数据包的最小长度
10	Fwd Packet Length Min	向前数据包的最小长度
43	Packet Length Mean	数据包长度的平均值
0	Source Port	源端口号
54	Down/Up Ratio	下行/上行比例
55	Average Packet Size	平均数据包大小
2	Protocol	网络协议类型
51	URG Flag Count	紧急标记（URG）的数量，它是TCP标头中的一个字段
1	Destination Port	目的端口号
9	Fwd Packet Length Max	向前数据包的最大长度
17	Flow Bytes/s	每秒流量字节数
14	Bwd Packet Length Min	回向数据包的最小长度
39	Fwd Packets/s	每秒正向数据包数
18	Flow Packets/s	每秒流量数据包数
52	CWE Flag Count	CWE标志计数，CWE是TCP头部的一个字段
69	Init_Win_bytes_forward	前向初始窗口字节数

15	Bwd Packet Length Mean	后向数据包长度的平均值
57	Avg Bwd Segment Size	后向段的平均大小
71	act_data_pkt_fwd	实际数据包转发
33	Fwd PSH Flags	前向数据包PSH标志计数，PSH是TCP头部的一个字段，当设置了PSH标志时，表示应立即将这个包发送到上层
48	RST Flag Count	RST标志计数，RST是TCP头部的一个字段，用于复位连接
5	Total Fwd Packets	总共的前向数据包数量

3. 算法评估结果

根据要求，评估了如下模型在数据集上的分类性能：

- Support Vector Machine(SVM)
- Logistic Regression(LR)
- K Nearest Neighbor(k == 3)(kNN)
- Random Forest(RF)
- Decision Tree(DT)
- Naive Bayes(NB)

评估结果及性能指标如下：

Method	Accuracy	Precision	Recall	F1_Score	Average
SVM	0.99479533	0.99088897	0.99877419	0.99481596	0.99481861
LR	0.99485562	0.99038174	0.99941724	0.99487898	0.99488339
kNN	0.99816128	0.99789114	0.99843257	0.99816178	0.9981617
RF	0.99991962	0.99993971	0.99989952	0.99991962	0.99991962
DT	0.9680385	0.99850178	0.93748367	0.96703114	0.96776377
NB	0.83910737	0.99483901	0.6817515	0.80906218	0.83119002