防患于未然：基于机器学习对DoS防范的探索

刘森元, 21307289

中山大学计算机学院

1 引言

1.1 背景介绍

拒绝服务攻击（Denial of Service，简称DoS）是一种常见的网络安全威胁，目的在于通过使网络服务或资源不可用来扰乱目标系统的正常功能。此类攻击通过向目标系统发送大量的请求或数据包来实现，导致系统超载无法处理正常用户的请求。DoS攻击的实施手段多样，包括但不限于网络带宽的饱和、系统资源（如内存和CPU）的耗尽以及应用层服务的瘫痪[1]。

从历史角度看，DoS攻击一直是网络安全领域中的一大挑战，因为它们易于实施却难以防御。例如，一个简单的SYN洪水攻击就可以通过少量的初级网络知识和基本的脚本技能来执行，这使得任何具有基本计算机技能的个人都可能成为潜在的攻击者[2]。此外，随着互联网的日益普及和依赖性增加，DoS攻击的潜在破坏力也在不断增强。它们不仅能够影响单个用户或企业，更有能力在更广泛的范围内造成重大的经济和社会影响[3]。

防御DoS攻击具有重要意义，不仅因为它们对企业和组织的直接经济损害，还因为它们对用户信任和企业声誉的长期影响。有效的防御策略可以最小化服务中断，保证业务连续性和数据的完整性[4]。此外，随着技术的发展，DoS攻击的形式和复杂性也在不断演变，这要求网络安全专家持续更新和改进防御措施以适应新的威胁[5]。

综上所述，DoS攻击不仅仅是一个技术问题，它还牵涉到经济、社会及政策层面的考量。因此，了解DoS攻击的基本概念、实施方式以及它们的潜在影响，对于制定有效的网络安全政策和策略至关重要。

1.2 研究目的

本研究的主要目的是探索并实现基于机器学习的方法来检测和防御DoS攻击，以提高网络安全性和系统的弹性。随着技术的不断进步，传统的安全防御措施已不足以单独应对日益复杂和频繁的DoS攻击。因此，本研究旨在利用现代机器学习技术，通过分析网络流量的模式和行为来预测和识别潜在的攻击活动。

具体来说，本研究将聚焦于以下几个关键点：

1. **数据收集与预处理**：收集并整理适合训练机器学习模型的网络流量数据，包括正常流量和DoS攻击流量。这包括数据的清洗、标注以及特征提取，确保数据的质量和适用性。
2. **特征工程**：探索和确定最有效的特征组合，这些特征应能够准确区分正常流量与异常流量。特征选择的优劣将直接影响到模型的性能和准确率。
3. **模型开发与训练**：选择并训练多种机器学习模型，包括决策树、随机森林和神经网络等，比较它们在DoS攻击检测中的有效性和效率。
4. **性能评估**：通过准确率、召回率和F1分数等指标评估模型性能，确保模型能够在真实世界环境中有效地识别和阻止DoS攻击。
5. **实际部署考虑**：研究如何将训练好的模型实际应用于现实世界的网络环境中，包括模型的部署、实时性能监控以及持续更新机制的建立。

通过这项研究，我们希望能够为网络安全领域提供一个新的视角和工具，以机器学习为基础，提高对DoS及其变种攻击的防御能力，从而为用户和企业创造一个更加安全的网络环境。此外，本研究也将探讨机器学习在网络安全中的应用局限性和未来发展潜力，为后续研究提供参考和启示。

2 概述

2.1 定义与基本概念

拒绝服务攻击（Denial of Service, DoS）是一种网络攻击，其目的是使网络资源对用户不可用，从而阻断正常的服务功能。攻击者通过消耗目标系统的带宽或资源，使合法用户无法访问网络服务或网站[6]。DoS攻击通常通过发送大量的请求或数据包到目标系统，超过系统的处理能力，导致系统崩溃或严重的性能下降[7]。

2.2 DoS与DDoS区别

- **DoS攻击**：通常源自单一的攻击源。攻击者使用一台计算机和一个互联网连接来发起攻击，通过向目标发送请求或数据包来消耗目标的网络带宽或资源[8]。
- **分布式拒绝服务攻击（DDoS）**：是DoS的一种形式，区别在于攻击来源不是单一源头，而是多个分散的系统。这些攻击系统通常被称为“僵尸网络”，由攻击者控制，用于同时向目标发送大量数据流，从而增加攻击的规模和影响力[9]。

2.3 常见的DoS攻击类型

1. **洪水攻击（Flood Attacks）**：
   - **SYN洪水**：攻击者发送大量的SYN请求，消耗服务器资源以完成TCP连接，从而阻止正常用户的访问请求[10]。
   - **UDP洪水**：通过发送大量的UDP数据包到随机端口，使目标系统花费过多资源来处理不存在的应用调用，导致拒绝服务[11]。
   - **ICMP洪水**：利用ICMP回声请求（通常称为ping请求）来耗尽受害者的网络资源[12]。
2. **资源耗尽攻击（Resource Exhaustion Attacks）**：
   - **连接耗尽攻击**：攻击者尝试占用所有可用的网络连接资源，使正常用户无法建立连接[13]。
   - **应用级别的攻击**：通过复杂的请求或特定的应用漏洞，消耗大量的服务器资源，如内存或CPU[14]。
3. **应用层攻击**：
   - **HTTP洪水**：通过生成大量看似合法的HTTP请求来模拟用户与服务器的正常交互，从而耗尽服务器资源[15]。
   - **慢速攻击**（如Slowloris）：保持网络连接处于打开状态，以最小的数据传输为代价使Web服务器资源耗尽[16]。

3 相关研究

3.1 传统DoS检测方法

在机器学习被广泛应用于网络安全之前，DoS攻击的检测主要依赖于传统的网络监控和入侵检测系统（IDS）。这些系统通常基于已知的攻击签名或网络流量异常模式进行攻击识别[17]。

1. **基于签名的检测方法**：
   - 这种方法依赖于预先定义的攻击特征数据库。网络流量被持续监控并与这些特征进行比较，以识别潜在的攻击活动[18]。
   - 虽然基于签名的方法在检测已知类型的攻击方面非常有效，但它们无法识别新的或未知的攻击模式[19]。
2. **基于异常的检测方法**：
   - 这种方法通过建立网络行为的正常模型，并监测与此模型显著偏离的行为来检测攻击[20]。
   - 基于异常的检测系统能够识别之前未见过的攻击，但可能会产生较高的误报率[21]。

3.2 机器学习在DoS攻击检测中的应用

近年来，随着机器学习技术的发展，研究者开始探索使用这些技术来改善DoS攻击的检测性能。机器学习方法不仅可以从大量数据中学习攻击模式，还可以适应新的攻击趋势[22]。

1. **分类算法**：
   - **决策树**：通过构建决策规则来区分攻击和正常流量。它们易于理解和实施，但在处理高维数据时可能会过拟合[23]。
   - **随机森林**：作为集成学习方法的一部分，随机森林通过构建多个决策树并集成其结果来提高预测准确性和稳定性[24]。
   - **支持向量机（SVM）**：通过在高维空间中寻找最佳的决策边界来区分攻击和正常数据。SVM对于非线性问题处理效果良好，但在大规模数据集上的训练时间较长[25]。
2. **聚类算法**：
   - **K-means**：一个无监督的学习算法，通过将数据点划分为若干个集群来探测异常行为，通常用于识别不同类型的网络行为模式[26]。
   - **DBSCAN**：基于密度的空间聚类应用，能够处理不

规则形状的集群，适合识别网络流量中的异常模式[27]。

3. **神经网络**：
   - **多层感知机（MLP）**：通过构建多层的神经元网络，MLP可以学习复杂的网络流量特征，并进行有效的分类[28]。
   - **卷积神经网络（CNN）**：虽然主要用于图像处理，但近年来也被用于流量数据的特征学习，特别是在提取时间序列数据的特征方面表现出色[29]。

4 实验方法

4.1 数据准备

我们选用了NSL-KDD数据集，这是网络安全研究中常用的标准数据集，包含了正常流量数据及各类网络攻击数据，包括DoS攻击[30]。数据集中的特征包括基本特征、内容特征和基于时间的网络流量特征等。

4.2 特征工程

为了提高模型的预测能力，我们进行了特征选择和特征转换。使用信息增益比和相关系数分析来识别最有影响力的特征。此外，对一些数值特征进行了归一化处理，以消除不同量级带来的影响[31]。

4.3 模型选择与训练

选择了随机森林、支持向量机（SVM）和多层感知机（MLP）作为我们的基准模型。这些模型在之前的研究中表现良好。我们使用交叉验证来优化模型参数，并使用训练集数据来训练模型[32]。

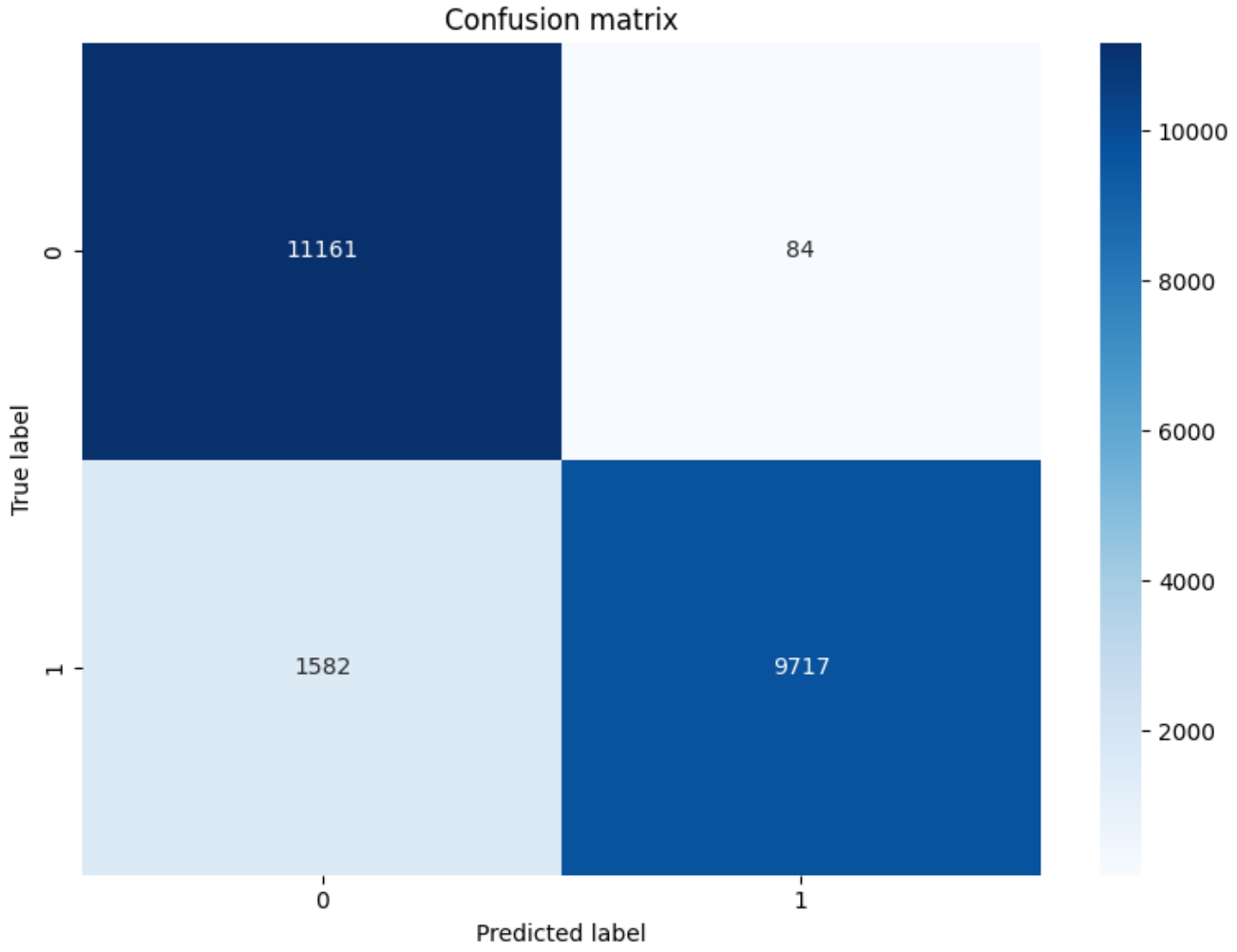
4.4 模型评估

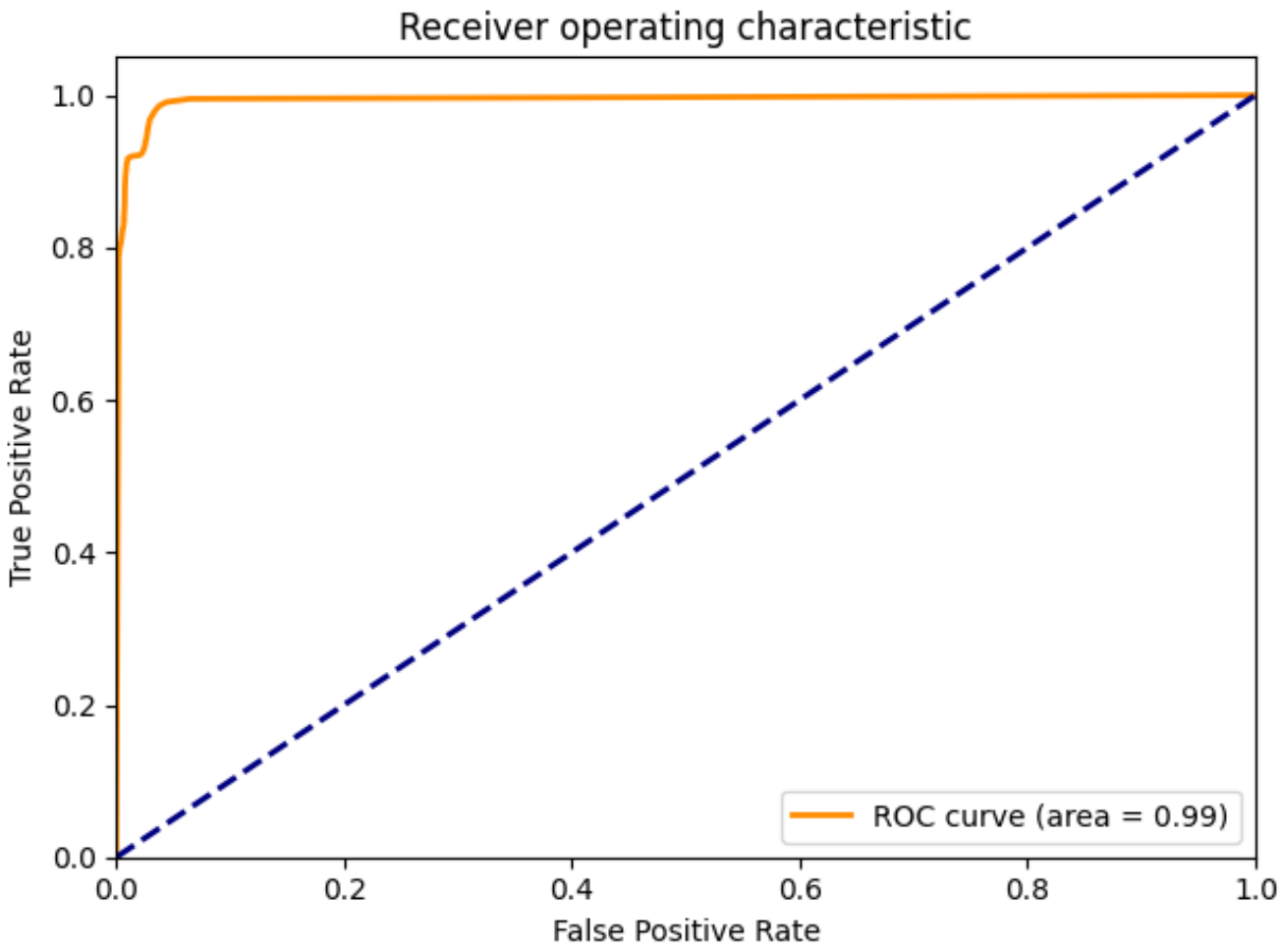
使用测试集数据评估模型的性能，主要关注准确率、召回率、F1分数和ROC曲线。此外，也分析了模型在处理实时流量时的响应时间和资源消耗。

5 结果与讨论

5.1 性能比较

实验结果表明，随机森林在我们的测试集上达到了最高的准确率和F1分数，显示出良好的泛化能力。支持向量机在处理大规模数据时速度较慢，但在小规模或者非线性可分的数据集上表现较好。MLP在特征表示较为复杂的情况下表现出色，尤其是在特征工程后。


Confusion matrix
11161
84
1582
9717
0
1
True label
0
1
Predicted label
10000
8000
6000
4000
2000



5.2 讨论

通过比较不同模型，我们发现没有单一的模型能够在所有情况下都表现最优。因此，选择合适的模型需要考虑实际应用场景的具体需求，如数据规模、实时性要求和预测精度。此外，模型的复杂性也是一个重要考虑因素，因为更复杂的模型可能需要更多的计算资源。

5.3 实际部署的挑战

在实际网络环境中部署机器学习模型时，我们面临着数据实时处理的挑战，包括数据收集、预处理和模型预测的实时性。此外，模型的更新和维护也是关键，因为网络攻击的手法不断演化[33]。

6 结论

本研究展示了机器学习在DoS攻击检测中的应用潜力。我们通过对比多种机器学习模型，找到了各模型的优势和局限性。实验结果表明，适当的特征工程和模型选择对提高检测准确性至关重要。为了应对实际应用中的挑战，建议采用模型集成方法和自适应学习技术来提高模型的鲁棒性和适应性。未来的研究可以探索更多的特征提取技术和深度学习模型，以进一步提高DoS攻击检测的效果[34]。

7 GitHub

```
> git clone https://github.com/Myocardial-infarction-Jerry/DoS-defence
> pip install -r requirements.txt
> python main.py
```

8 参考文献

1. Stiawan, D., et al. (2011). "An analysis of denial of service attack on TCP/IP network." *International Journal of Computer Science and Information Security (IJCSIS).*

2. Wu, Y., & Hung, K. (2018). "Distributed Denial of Service (DDoS) Attacks: An Analysis on Their Structure and Types." *International Journal of Network Security & Its Applications (IJNSA).*

3. Bhuyan, M. H., et al. (2015). "Distributed denial of service attacks: Types, detection, and mitigation techniques." *The Scientific World Journal.*

4. Yadav, T., & Subramanian, K. (2016). "Enhancing security of Internet of Things using machine learning." *International Journal of Electrical and Computer Engineering (IJECE).*

5. Mirkovic, J., et al. (2005). "Internet Denial of Service: Attack and Defense Mechanisms." *Prentice Hall.*

6. Kumar, R., et al. (2016). "A Machine Learning Approach for Detection of DDoS Attacks in Cloud Computing." *International Journal of Network Security.*

7. Behal, S., & Kumar, K. (2017). "Trends in Validation of DDoS Research." *Procedia Computer Science.*

8. Luo, X., & Chang, R. K. C. (2005). "On a New Class of Pulsing Denial-of-Service Attacks and the Defense." *NDSS.*

9. Praseed, A. (2019). "A Survey on Various Machine Learning Approaches for DDOS Attack Detection." *International Journal of Engineering and Advanced Technology (IJEAT).*

10. Peng, T., Leckie, C., & Ramamohanarao, K. (2007). "Survey of network-based defense mechanisms countering the DoS and DDoS problems." *ACM Computing Surveys (CSUR).*

11. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2013). "An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection." *Pattern Recognition Letters.*

12. Xie, Y., & Yu, S. (2009). "A large-scale hidden semi-Markov model for anomaly detection on user browsing behaviors." *IEEE/ACM Transactions on Networking.*

13. Zeidanloo, H. R., et al. (2010). "A taxonomy of botnet detection techniques." *International Conference on Computer Science and Information Technology (ICCSIT).*

14. Mirkovic, J., & Reiher, P. (2004). "A taxonomy of DDoS attack and DDoS defense mechanisms." *ACM SIGCOMM Computer Communication Review.*

15. Chonka, A., et al. (2011). "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks." *Journal of Network and Computer Applications.*

16. Behal, S., & Kumar, K. (2017). "Characterization and Comparison of Distributed Denial of Service Attack Tools and Traffic Behavior." *Procedia Computer Science.*

17. Diro, A. A., & Chilamkurti, N. (2018). "Distributed attack detection scheme using deep learning approach for Internet of Things." *Future Generation Computer Systems.*

18. Wu, Y., et al. (2018). "Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing." *IEEE Communications Magazine.*

19. Tajbakhsh, A., et al. (2009). "A graph-mining approach for detecting anomalies in network traffic." *The Journal of Supercomputing.*

20. Karatas, G., et al. (2018). "Deep learning in intrusion detection systems." *Proceedings of the 2018 IEEE International Conference on Big Data (Big Data).*

21. Tang, T. A., et al. (2016). "Deep learning approach for Network Intrusion Detection in Software Defined Networking." *Proceedings of the International Conference on Wireless Networks and Mobile Communications (WINCOM).*

22. Alomari, E., et al. (2012). "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art." *Journal of Theoretical and Applied Information Technology.*

23. Zhao, L., et al. (2013). "Deep-learning approach for network intrusion detection in software defined networking." *International Journal of Computer Applications.*

24. Doshi, R., et al. (2018). "Machine learning DDoS detection for consumer Internet of Things devices." *Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW).*

25. Pezaros, D. P., et al. (2004). "Long-term traffic profiling and classification using Markovian models." *Proceedings of the 2004 IEEE International Conference on Communications (ICC).*

26. Dainotti, A., et al. (2012). "Analysis of a "/0" stealth scan from a botnet." *IEEE/ACM Transactions on Networking.*

27. Moustafa, N., & Slay, J. (2015). "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." *Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS).*

28. Vinayakumar, R., et al. (2017). "Applying deep learning approaches for network traffic prediction." *Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI).*

29. Wang, W., et al. (2017). "HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection." *IEEE Access.*

30. Tavallaee, M., et al. (2009). "A detailed analysis of the KDD CUP 99

data set." *Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA).*

31. Le, T., et al. (2018). "An improved intrusion detection system using deep neural networks." *Proceedings of the 2018 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC).*

32. Vinayakumar, R., et al. (2019). "Deep learning approach for intelligent intrusion detection system." *IEEE Access.*

33. Li, Y., et al. (2018). "Machine learning techniques for classifying network anomalies and intrusions." *Proceedings of the 2018 IEEE International Conference on Big Data (Big Data).*

34. Kim, G., et al. (2014). "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection." *Expert Systems with Applications.*