基于基准和新数据集的入侵检测机器学习分类器性能比较

刘京龙

石河子大学 新疆维吾尔自治区 石河子 832003

【摘 要】：随着互联网发展与网络攻击增加，组织广泛采用入侵检测系统(IDS)，但仍面临高误报(FP)、高漏报(FN)及精度不足的挑战。引入机器学习分类器能有效解决上述问题。本研究基于 NSL-KDD、UNSW-NB15 和 Phishing 三个数据集，评估了 J48、RF、K-NN、NB、SVM 及 ANN 六种模型。结果表明，K-NN 和 J48 在检测精度与测试时间上综合表现最佳。

【关键词】：入侵检测；NSL-KDD；UNSW-NB15；K-近邻；支持向量机；机器学习；Weka；朴素贝叶斯；决策树；随机森林

DOI:10.12417/3041-0630.26.02.039

1 引言

网络安全是数字时代的核心挑战。随着物联网和云服务的普及，数据流量激增，安全威胁不断扩大[1]。传统的基于签名的 IDS 难以应对未知威胁，而基于异常检测的技术虽能识别零日攻击，却受困于高误报率[2]。机器学习(ML)和深度学习(DL)为解决上述问题提供了新思路。ML 分类器能够智能区分正常与入侵活动[3]，DL 则能自动提取复杂特征。然而，当前研究常受限于数据质量，过度依赖 KDD Cup'99 等过时数据集，难以反映现代攻击特征，导致评估偏差[4]。本文旨在通过在 NSL-KDD（基准）、UNSW-NB15（现代）和 Phishing（特定领域）三个数据集上评估六种经典 ML 分类器，分析其在精度、效率及误报率方面的表现，以探索更具适应性的入侵检测方案。

2 相关工作

现有研究[1][5][6]表明，K-NN、Rotation Forest 及 Random Tree 在准确率和时间成本上优于 SMO 和 MLP，且随机森林在噪声环境中表现更佳[7][8]。尽管深度学习特征提取能力强，但其计算昂贵且解释性弱。相比之下，J48、K-NN 和 RF 等经典分类器兼顾高准确率与低耗时。因此，本文重点评估这些高效分类器在现代数据集上的适用性。

3 数据集

本实验选用 NSL-KDD（去冗余的经典基准，含四类攻击）、UNSW-NB15（反映现代复杂威胁，含九类攻击）以及 Phishing（针对在线交易场景的钓鱼检测）三个数据集，涵盖了从经典基准到现代威胁及特定应用领域的不同维度[9][10]。

4 机器学习分类器概述

本研究选取 Weka 中的六种模型进行评估：J48 决策树（规则推理）、ANN（三层权重网络）、朴素贝叶斯（独立概率计算）、K-NN（基于距离的邻域分类）、SVM（高维空间模式识别）以及随机森林（多树集成学习）。这些模型涵盖了从概率统计到几何空间映射的多种主流分类技术。

5 实验分析

在这项工作中，我们将使用 Weka（用于数据挖掘任务的机器学习算法集合）直接将算法应用于数据集。Weka 拥有支持数据预处理、分类、回归、聚类、关联规则和可视化的资源。实验使用 Weka 进行数据预处理与分类，采用交叉验证法。评估指标包括检测精度(Accuracy)、测试时间、真阳性率(TPR)、假阳性率(FPR)、精确率(Precision)、召回率(Recall)和 F-度量(F-measure)。

6 结果

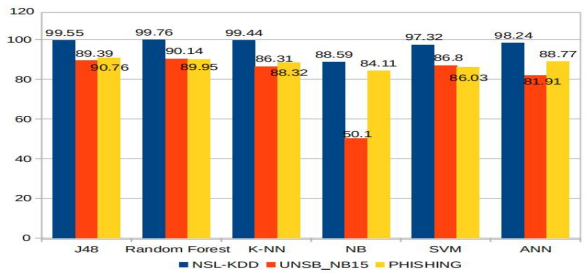

图 1 展示了三个数据集的检测精度对比。

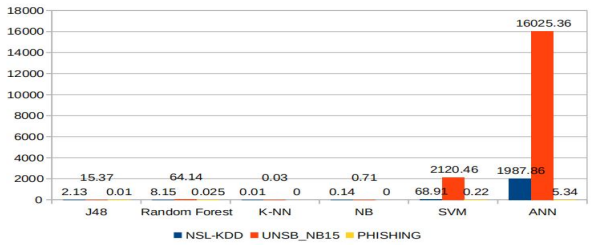

图 2 展示了三个数据集的测试时间对比。

NSL-KDD:所有分类器的检测精度都很高。NB 精度最低(88.59%)但时间快；SVM 和 ANN 精度很好(97.32%和 98.24%)但时间最差。J48 精度为 99.55%，时间为 2.13 秒。K-NN 精度为 99.44%，时间最佳(0.01 秒)。随机森林(RF)产生了最高的精度 99.76%。UNSW-NB15:NB 精度最低(50.1%)；SVM 和 ANN

精度较好(86.80%和 81.91%)但执行时间极高。RF 产生了最佳精度 90.14%。Phishing:J48 具有最高的精度 90.76%。K-NN 和 NB 执行时间几乎为 0。

7 讨论

NSL-KDD 的检测精度和时间比 UNSW-NB15 好得多。这是因为 UNSW-NB15 数据集拥有更多的特征和攻击类别。分类器在 UNSW-NB15 上的性能下降，且执行时间更长。Phishing 数据集的总体测试时间最短，因为它的攻击类别、实例和属性都比前两者少。

实验结果表明，SVM 和 ANN 更适合大型数据集，因为它们分析并同等对待数据集中的所有实例以确保精度，但缺点是需要大量时间进行分类，这对于（实时）入侵检测来说并不理想。K-NN 非常适合实时系统，因为它无论数据集大小如何，都能在极短时间内产生良好的检测精度。

8 结论

本研究证实了没有一种完美的分类器适用于所有场景，但 K-NN 和 J48 在检测精度、测试时间和 F-measure 方面表现最为均衡，最适合作为 IDS 的核心算法。未来的研究应致力于优化这些分类器，并探索混合分类器或集成学习方法，以进一步降低误报率并提升对零日攻击的检测能力。

表 I 显示了分类器在三个数据集上的性能结果。

Datasets	Performance Metric	J48	RF	K-NN	NB	SVM	ANN
NSL-KDD	Accuracy	99.55	99.76	99.44	88.59	97.32	98.24
	Time (sec)	2.13	8.15	0.01	0.14	68.91	1987.86
	TPR	0.995	0.996	0.993	0.877	0.959	0.973
	FPR	0.005	0.001	0.004	0.088	0.014	0.009
	Precision	0.995	0.999	0.995	0.897	0.983	0.989
	Recall	0.995	0.996	0.993	0.877	0.959	0.973
	F-Measure	0.995	0.997	0.994	0.887	0.971	0.981
UNSW_NB15	Accuracy	89.39	90.14	86.31	50.1	86.8	81.91
	Time (sec)	15.37	64.15	0.03	0.71	2120.46	16025.36
	TPR	0.982	0.978	0.972	0.627	0.963	0.965
	FPR	0.003	0.001	0.006	0.015	0.001	0.019
	Precision	0.991	0.998	0.981	0.927	0.996	0.938
	Recall	0.982	0.978	0.972	0.627	0.963	0.965
	F-Measure	0.986	0.987	0.976	0.748	0.979	0.952
PHISHING	Accuracy	90.76	89.95	88.32	84.11	86.03	88.77
	Time (sec)	0.01	0.025	0	0	0.22	5.34
	TPR	0.916	0.912	0.889	0.9	0.922	0.906
	FPR	0.083	0.089	0.084	0.126	0.117	0.1
	Precision	0.923	0.917	0.919	0.855	0.895	0.907
	Recall	0.916	0.912	0.889	0.9	0.922	0.906
	F-Measure	0.919	0.914	0.904	0.893	0.908	0.907

参考文献：

[1] T.Garg and S.S.Khurana,"Comparison of classification techniques for intrusion detection dataset using weka",in Recent Advances and Innovations in Engineering(ICRAIE),IEEE,2014,pp.1-5.

[2] J.O.Nehinbe,"A critical evaluation of datasets for investigating idss and ipss researches,"In Cybernetic Intelligent Systems(CIS),2011 IEEE 10th International Conference on,IEEE,2011.pp.92-97.

[3] A.Shiravi,H.Shiravi,M.Tavallaee,and A.A.Ghorbani,"Toward developing a systematic approach to generate benchmark datasets for intrusion detection,"computers security,31(3):357-374,2012.

[4] A.Gharib,I.Sharafaldin,A.H.Lashkari,and A.A.Ghorbani,"An evaluation framework for intrusion detection dataset,"In Information Science and Security(ICISS),2016 International Conference on,IEEE,2016.pp.1-6.

[5] C.So-In,N.Mongkonchai,P.Aimtongkham,K.Wijitsopon,and K.Rujirakul,"An evaluation of data mining classification models for network intrusion detection,"In Digital Information and Communication Technology and its Applications(DICTAP),2014 Fourth International Conference on,IEEE,2014.pp.90-94.

[6] P.Aggarwal and S.K.Sharma,"An empirical comparison of classifiers to analyze intrusion detection,"In Advanced Computing Communication Technologies(ACCT),2015 Fifth International Conference on,IEEE,2015.pp.446-450.

[7] N.Rani and R.Kr.Purwar,"Performance analysis of various classifiers using benchmark datasets in weka tools,"International Journal of Engineering Trends and Technology(IJETT),47(5),pp.290-294.

[8] P.Vijay,"Performance evaluation of classification techniques for intrusion detection in noisy datasets,"International Journal on Recent and Innovation Trends in Computing and Communication,5(6):1011-1016,2017.

[9] S.Duque and M.N.B.Omar,"Using data mining algorithms for developing a model for intrusion detection system(ids),"Procedia Computer Science,61:46-51,2015.

[10] L.Dhanabal and S.P.Shantharajah,"A study on nsl-kdd dataset for intrusion detection system based on classification algorithms, "International Journal of Advanced Research in Computer and Communication Engineering.4(6):446-452,2015.