基于改进 Adaboost 算法的无线通信网络 DOS 攻击检测方法

毛一鸣[1] 于怡然[1]
MAO Yiming YU Yiran

摘 要 无线通信网络中的 DOS（拒绝服务）攻击手段多样且隐匿性强，攻击者常常能在已知攻击样本的基础上，通过微小扰动生成具有特征相似性的攻击变种样本。这类攻击难以被常规的基于 Adaboost 算法的检测方法有效识别，因此漏检率较高，检测时间也较长。针对这一问题，提出了一种基于改进 Adaboost 算法的无线通信网络 DOS 攻击检测方法。该方法通过构建无线通信网络 DOS 攻击数据的输出阵列模型，用于拾取网络中的 DOS 攻击信号。采用随机森林算法对拾取的信号进行特征处理，提取出能够表征已知 DOS 攻击的关键特征。利用改进后的 Adaboost 算法对提取的特征样本进行二分类。通过增加对特征空间中边界区域样本的学习权重，改进后的 Adaboost 算法能够更精确地划分攻击变种样本的特征，从而实现 DOS 攻击的有效检测。经实验证明，该方法在检测时间上不超过 100 μs，漏检率不低于 1%，能够实现对无线通信网络 DOS 攻击快速且精准检测。

关键词 改进 Adaboost 算法；DOS 攻击；随机森林算法；无线通信网络；二分类

doi：10.3969/j.issn.1672-9528.2025.05.031

0 引言

无线通信网络以其方便、快捷、高效的特点，契合现代社会增长的移动办公和数据处理需求。特别在 IEEE 802.11n 标准出台后，无线局域网（WLAN）在商业、医疗、教育等各个领域得到广泛应用，并展现出强劲的发展势头和应用前景 [1]。然而，随着无线通信网络的普及，其安全问题也日益突出，其中拒绝服务（DOS）攻击成为无线通信网络面临的最大威胁之一。DOS 攻击是指通过占用或耗尽网络资源，使得合法用户无法获得服务的一种攻击方式。在无线通信网络中，DOS 攻击的危害尤为严重，不仅影响网络的可用性，还可能造成数据丢失、系统崩溃等严重后果。因此，对无线通信网络 DOS 攻击检测方法的研究，具有重要的现实意义和学术价值。

目前，已有研究致力于解决这一问题。文献 [2] 提出基于 Attention-GRU 检测方法，利用改进的 Borderline-SMOTE 进行数据平衡处理，引入自注意力机制构建双层 GRU 分类网络，对预处理后的数据进行学习训练，实现对攻击流量的检测。但在训练过程过度依赖相似特征样本，对新的 DOS 攻击变种，即使具有相似但细微变化的特征，模型也将其误判为正常流量或已知攻击类型，从而无法有效检测新的攻击变种。文献 [3] 提出了基于人工蜂群算法的检测方法，通过获取 DDOS 攻击的同态样本分布时间序列输出，构建自适应的入侵检测信息分析模型，采用人工蜂群算法对计算机网络攻击检测的个体最优值和全局最优值进行寻优，实现对 DDOS 攻击的检测。但该方法同态样本分布时间序列输出主要反映攻击样本在时间维度上的分布特征，当面对特征相似的 DOS 攻击时，这些攻击在时间序列上的分布特征也可能相似，导致自适应模型难以从时间序列特征中准确区分不同变种的 DOS 攻击，从而造成检测漏洞。为此，本研究提出基于改进 Adaboost 算法的无线通信网络 DOS 攻击检测方法。

1 无线通信网络 DOS 攻击信号拾取

无线通信网络环境复杂，DOS（拒绝服务）攻击手段多样且隐匿性强，隐藏在大量的网络流量数据中，难以直接获取。为构建无线通信网络 DOS 攻击数据的输出阵列模型。利用模型的特性，通过对各种相关性特征量的分析以及复杂的运算组合，从复杂的网络数据中提取出与 DOS 攻击相关的信号，解决在复杂环境下攻击信号难以捕捉的问题，为后续准确提取无线通信网络 DOS 攻击特征提供基础。

本研究构建的无线通信网络 DOS 攻击的时间序列模型利用特征样本之间的相关性，设计自适应的无线通信网络 DOS 攻击入侵信息拾取机制。该机制旨在从潜在与真实空间分布的样本集合中精准捕捉 DOS 攻击的时频特征。特别关注 DOS 攻击的幅频响应，借助核心判别技术和过程衰减分析，推导出了相邻两点间 DOS 攻击时间样本序列的关联关系，其

1. 郑州工业应用技术学院信息工程学院 河南郑州 451100

表达式为：

$$s_i(n)=\sum_{i=1}^{2q}\mu_i(n)s_i(n-1)\psi(n)m(n) \tag{1}$$

式中：$s_i(n)$ 表示相邻两点间的 DOS 攻击时间样本序列耦合系数；q 表示无线通信网络流量集；i 表示无线通信网络节点数量；$\mu_i(n)$ 表示真实空间中原始数据的维度；$\psi(n)$ 表示蕴含判别信息的潜在攻击行为参数；$m(n)$ 表示无线通信网络 DOS 攻击的幅频 [4]。

根据相邻两点间的 DOS 攻击时间样本序列关系，进一步推导出 DOS 攻击的同态样本分布时间序列输出，其表达式为：

$$\rho=\xi_{er}s_i(n)-\sin\alpha \tag{2}$$

式中：ρ 表示 DOS 攻击同态样本分布的时间序列；ξ_{er} 表示真实空间中原始数据的特征维度；α 表示 DOS 攻击的入侵参数。

为在大范围搜索环境中更高效地检测 DOS 攻击，进一步构建了无线通信网络 DOS 攻击数据的输出阵列模型。该模型表达式为：

$$\begin{bmatrix}\rho_1(t)\\ \rho_2(t)\\ \vdots\\ \rho_m(t)\end{bmatrix}=\sum_{i=1}^{q}T_i\xi_{er}s_i(n)-\sin\alpha+k(t) \tag{3}$$

式中：$\rho_m(t)$ 表示长度为 m 的 DOS 攻击数据的输出阵列模型；T_i 表示 DOS 攻击信号的时域分量；$k(t)$ 表示 DOS 攻击联合自相关特征分量 [5]。

通过上述模型的构建与运用，本研究成功实现了在复杂无线通信网络环境中自动拾取 DOS 攻击时间序列信号的目标，为后续准确检测 DOS 攻击奠定了坚实基础。

2 DOS 攻击特征提取

无线通信网络中的 DOS 攻击手段多样且隐匿性强，攻击变种样本具有特征相似性。在提取出与 DOS 攻击相关的信号后，原始信号数据非常复杂，包含大量冗余、不相关或对攻击识别贡献不大的特征，直接对信号进行处理不仅复杂度高，而且耗时较长。因此，需要通过特征提取技术来筛选出最能代表 DOS 攻击特征的子集，从而降低数据的维度，显著提升处理效率。为实现这一目标，本研究采用随机森林算法（RF）进行特征处理。

随机森林算法由多棵决策树构成，每棵树都能够独立地对数据进行分类和预测 [6]。在利用 RF 进行特征提取时，采用基尼值这一关键评价指标。基尼值代表了全部决策树内节点分裂的平均变化程度，是衡量决策树中节点分裂均衡性的重要指标。对于无线通信网络数据集中的 M 个特征向量，通过公式计算每个特征向量的基尼值：

$$\boldsymbol{G_M}=1-\sum_{j=1}^{M}a_{\rho_m(t)}^{\ 2} \tag{4}$$

式中：$\boldsymbol{G_M}$ 表示 DOS 攻击信号基尼值；j 表示 DOS 攻击信号数据集的分类指标数量；$a_{\rho_m(t)}$ 表示分类指标 a 在 DOS 攻击信号数据集 $\rho_m(t)$ 中的占比 [7]。

通过计算相邻节点基尼指数的变化量，可以评估特征向量对节点的重要度，其计算公式为：

$$\boldsymbol{K}=\boldsymbol{G_M}-\boldsymbol{G_{M-1}}-\boldsymbol{G_{M+1}} \tag{5}$$

式中：$\boldsymbol{K}$ 表示相邻节点基尼指数，用于描述特征向量对无线通信网络节点的重要度。

为确定特征向量在每棵决策树中的重要度，考虑包含在决策树内、与特征向量相关的节点集合。对于每个特征向量，通过累加其在所有相关节点上的重要度，得到其在决策树中的重要度评分，其计算公式为：

$$\boldsymbol{B}=\boldsymbol{K}_v,\ \ v\in F \tag{6}$$

式中：$\boldsymbol{B}$ 表示特征向量在第 v 棵决策树中的重要度评分；F 表示 DOS 攻击特征集合。

为更直观地比较不同特征向量的重要度，对这些评分进行归一化处理。随后，将 DOS 攻击信号数据集随机均匀地划分为若干个子集，并对每个子集中的特征向量进行重要度排序 [8]。这些特征向量包括共有特征、私有特征和相关性较弱的特征。以共有特征作为结果输出，将其作为后续 DOS 攻击识别检测的依据。

3 基于改进 Adaboost 算法的 DOS 攻击识别检测

无线通信网络中的 DOS 攻击具有手段多样、隐匿性强以及攻击变种样本特征相似等特点，常规基于 Adaboost 算法的检测方法存在漏检率较高、检测时间较长的问题。提取出最能表征 DOS 攻击的信号特征后，需要一种更有效的方法对这些特征样本进行分类，以准确识别 DOS 攻击。为此，本研究对 Adaboost 算法进行了改进。改进后的 Adaboost 算法能够根据 DOS 攻击特征的初始权重训练弱分类器，特征权重根据分类准确与否动态调整，确保算法聚焦于更具区分度的特征。这种改进方法能够在保证分类精度的同时，提高检测效率，降低误报率和漏报率。

改进后的 Adaboost 算法在训练弱分类器时，充分考虑 DOS 攻击特征的初始权重，这些权重精准地反映了特征在训练过程中的重要性。在训练中，特征的权重会根据其分类的准确性进行动态调整，确保算法能够聚焦于那些更具区分度的特征，从而提高分类的精度和效率。

接下来，算法会计算每个弱分类器的加权错误率，这一指标是衡量分类器性能的关键。加权错误率越低，意味着该分类器的性能越出色，因此在最终决策中将占据更大的比

重 [9]。为实现这一目标，引入加权函数，以确保对分类错误的样本施以更严厉的惩罚，从而进一步提升算法的分类性能。

随后，算法会根据每个弱分类器的分类结果，对特征的权重分布进行更新。被错误分类的特征的权重会增加，而被正确分类的特征的权重则会相应减少。这样的机制确保了算法能够不断自我优化，逐步提升分类的准确性，同时降低误报率和漏报率。

假设有一个二分类的训练无线通信网络 DOS 攻击特征集 A，其中包含由多个子集 x 和 y 构成的信号样本。x 描述样本的特征空间，y 描述样本所属的类别空间，基于改进后的 AdaBoost 算法的 DOS 攻击识别检测过程如下：

步骤 1：输入训练特征数据集，该特征数据集由 N 个数据组成。同时，选择一个弱学习算法作为弱分类器，并设定迭代次数为 O。

步骤 2：初始化训练特征数据的权值分布，使得每个样本的权重相等。然后，在每一次迭代中，根据当前的权值分布训练一个弱分类器。

$$g\left(x,y\right)_{O+1}:X\to\left[1-,+1\right] \tag{7}$$

式中：g 表示弱分类器；$g\left(x,y\right)_{O+1}$ 表示对应的加权错误率；X 表示输入的 DOS 攻击特征样本。

根据加权错误率计算弱分类器的话语权，即其在最终决策中的比重，其用公式表示为：

$$\theta_{O+1}=\frac{1}{2}\ln\left(\frac{1-g\left(x,y\right)_{O+1}IX}{g\left(x,y\right)_{O+1}}\right) \tag{8}$$

式中：θ_{O+1} 表示弱分类器 g 在最终决策中所占的比重；I 表示加权函数。

步骤 3：更新训练数据的权值分布。通过引入规范化系数来实现，确保更新后的权值分布满足概率分布，其公式为：

$$\varpi_{o+1}=\frac{\varpi_0}{b}\exp\left(-\theta_{O+1}g\left(x,y\right)_{O+1}\right) \tag{9}$$

式中：ϖ_{o+1} 表示更新后弱分类器输入的网络 DOS 攻击特征样本权重；b 表示规范化系数。

步骤 4：构建强分类器。与原始 Adaboost 算法采用的普通集成方法不同，本研究改进的 Adaboost 算法根据每个弱分类器的性能为其分配不同的权重系数。这样构建出的强分类器不仅性能更加出色，而且能够更准确地识别具有特征相似性的 DOS 攻击变种样本。构建强分类器用公式表示为：

$$f\left(X\right)=\mathrm{sign}\left(\sum_{c=1}^{N}\omega_c g\left(X\right)\varpi_o+1\right) \tag{10}$$

式中：$f(X)$ 表示强分类器输出结果，即输入的 DOS 攻击特征样本属于 DOS 攻击概率；ω_c 表示第 c 个弱分类器的权重系数。强分类器的输出结果表示输入的 DOS 攻击特征样本属于 DOS 攻击的概率，根据该概率将输入样本分类到概率最高的类别中，从而实现 DOS 攻击与正常网络流量的二分类。

4 实验论证

4.1 实验场景布设

为验证改进 Adaboost 算法的 DOS 攻击检测有效性，设计对比实验。实验针对含 1 000 用户的 2.5 Gbit/s 无线通信网，用 IFA-A8F8 高精度采样器实时收集网络数据。采样器连接终端主机，获取 DOS 攻击流量。实验场景如图 1 所示。

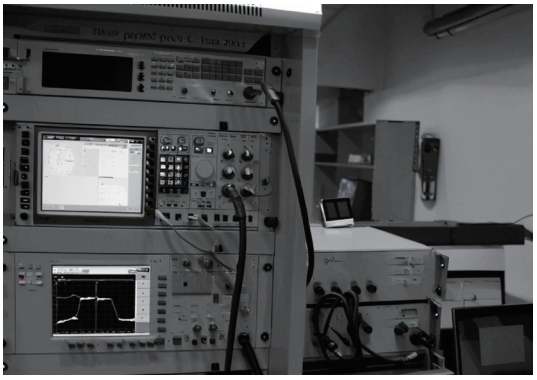

图 1 实验场景图

从图 1 看到 FA-A8F8 采样器与网络终端主机的连接关系，以及采样器如何采集网络中的 DOS 攻击流量数据，并将其发送到安装有无线通信网络 DOS 攻击检测程序的主机上。该主机配置 WindowsCP 操作系统，Inter CORE i8 处理器，采用 1.2 版本 Python 编辑检测程序，执行 DOS 攻击检测流程。在实验过程中，将采集到的网络数据输入到 DOS 攻击检测程序中，通过对比改进前后的 Adaboost 算法在检测 DOS 攻击方面的性能差异，来验证所提出方法的有效性。同时，还设置了对照组实验，使用传统的 DOS 攻击检测方法进行比较分析，以进一步凸显改进算法的优势。

4.2 实验参数及指标

在以上实验环境中开展对比实验，将文献 [2] 提出的基于 Attention-GRU 的检测方法、文献 [3] 提出的基于人工蜂群算法的检测方法与本文方法进行对比。实验利用 HJUG 软件模拟了 DOS 攻击，具体实验参数如表 1 所示。

表 1 实验参数表

序号	参数	设定值
1	DOS 攻击类型数量	6
2	DOS 攻击频率 /Hz	5.62
3	DOS 攻击周期 /s	10
4	通信频率 /Hz	1.34
5	数据包大小 /Byte	200

实验共采集 1 000 个样本数据，并利用公式（1）~（10）对样本进行 DOS 攻击识别与检测。为评估检测效果，选择检

测时间和漏检率作为评价指标。通过对比三种方法在检测时间和漏检率上的表现，评价本文方法在检测速率和精度上的优劣。

4.3 实验结果与讨论

图 2 为 3 种方法在无线通信网络 DOS 攻击检测场景中的检测时间对比，而图 3 为 3 种方法的漏检率对比结果。

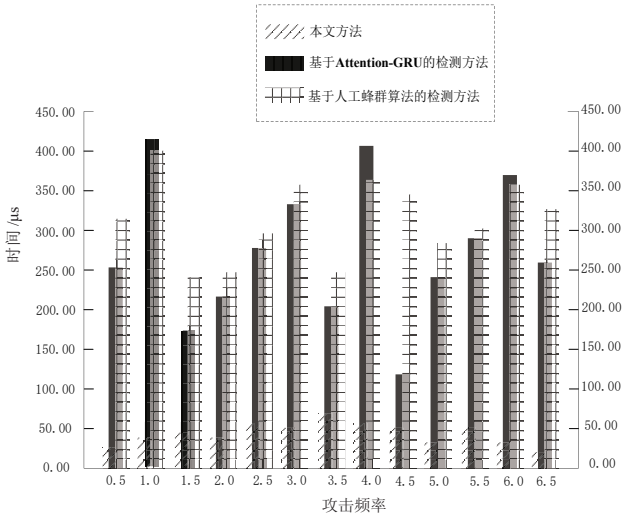

图 2 三种方法的检测时间对比

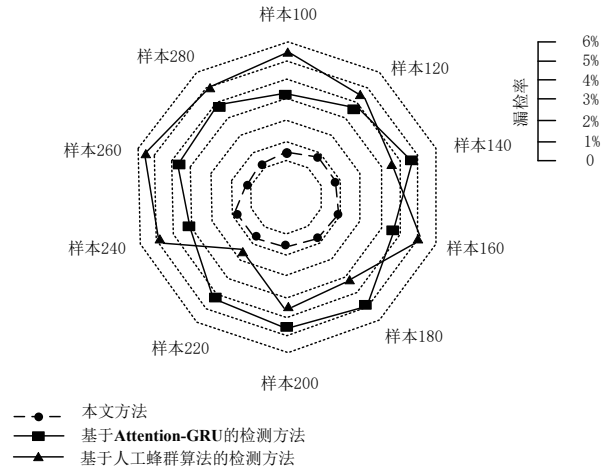

图 3 三种方法的漏检率对比

从图 2 看出，在无线通信网络 DOS 攻击检测场景中，设计方法检测时间最短，不超过 100 μs，意味着该方法能够在极短的时间内完成攻击检测，从而迅速响应并采取相应的防御措施。同时，图 3 也验证本文方法在漏检率方面的显著优势。相较于其他两种方法，本文方法的漏检率远低于 1%，表明其能够更准确地识别并检测出无线通信网络中的 DOS 攻击，有效降低攻击漏报的风险。改进的 Adaboost 算法在特征分类方面表现出色，能够准确地将 DOS 攻击与正常通信流量区分开来，从而实现对 DOS 攻击的快速精准检测，从而在最终的检测时间和漏检率上取得显著的优势。

5 结语

本研究提出的基于改进 Adaboost 算法的无线通信网络 DOS 攻击检测方法，通过增强算法对特征空间中边界区域样本的学习能力，并优化特征提取过程，提升了 DOS 攻击的检测精度与效率。实验数据验证，该方法在检测性能、误报控制及处理速度上均优于对比方法，为无线通信网络的安全防护引入了新的高效工具。然而，随着无线通信技术的持续发展以及 DOS 攻击手段的不断演变，相关研究仍需进一步深入推进。未来，需进一步探索更为高效的特征提取与选择方法，对算法参数和结构进行优化，以此提升检测系统的自适应性与鲁棒性。

参考文献：

[1] 王洋 . 基于 MFOPA 算法的 LDOS 攻击检测 [J]. 信息技术 , 2024(4):166-175.

[2] 江魁 , 卢帆 , 苏耀阳 , 等 . 基于 Attention-GRU 的 SHDOS 攻击检测研究 [J]. 信息网络安全 , 2024,24(3):427-437.

[3] 田小芳 . 基于人工蜂群算法的计算机网络 DDOS 攻击检测方法 [J]. 计算机测量与控制 , 2023, 31(12):28-33.

[4] 蒋英肇 , 陈雷 , 闫巧 . 基于双通道特征融合的分布式拒绝服务攻击检测算法 [J]. 信息网络安全 , 2023,23(7):86-97.

[5] 崔英祥 , 张幽彤 , 魏洪乾 . 基于样本熵的车载 CAN 网络入侵检测 [J]. 汽车工程 , 2023, 45(7):1184-1191.

[6] 刘金硕 , 詹岱依 , 邓娟 , 等 . 基于深度神经网络和联邦学习的网络入侵检测 [J]. 计算机工程 , 2023, 49(1):15-21.

[7] 孙扬威 , 戚湧 . 基于聚类混合采样与 PSO-Stacking 的车载 CAN 入侵检测方法 [J]. 计算机工程 , 2023, 49(1):138-145.

[8] 李瑞 , 刘珊 , 闫磊 . 基于 FP-Growth 算法的新能源配电网 CPS 网络攻击检测方法 [J]. 电信科学 , 2024, 40(11):103-113.

[9] 吕首琦 , 海涛 , 郑茂兴 . 基于 CNN 和 LSTM 结合的电网网络攻击检测 [J]. 电子器件 , 2023, 46(3):824-830.

【作者简介】

毛一鸣（1995—），女，河南新郑人，硕士，助教，研究方向：网络与通信、网络安全。

于怡然（1997—），女，河南开封人，硕士，助教，研究方向：数据挖掘、机器学习。

（收稿日期：2025-01-21 修回：2025-05-19）