DDoS Intrusion Detection Method of Wireless Sensor Networks Based on PSO Optimized SVM*

HU Xiaodong*
(Department of Digital Engineering, Shanxi Institute of Economic Management, Taiyuan Shanxi 030024 China)

Abstract: DDoS intrusion is a common type of attack in wireless sensor networks. In order to ensure network security, a DDoS intrusion detection method for wireless sensor networks based on PSO optimized SVM is proposed. DDoS intrusion detection standards based on DDoS intrusion principles and processes are describedf. Based on the comprehensive consideration of the composition structure and working principle of the wireless sensor network, the real-time operation data of the wireless sensor network are collected by using network crawler technology, the particle swarm optimization algorithm is used to optimize the support vector machine algorithm, the network operation characteristics are extracted, and the detection results of network DDoS intrusion state and intrusion intensity are obtained according to the feature matching results. Through performance simulation analysis, it is concluded that compared with traditional methods, the accuracy of intrusion state detection of optimized design method is significantly improved, and the average intrusion intensity detection error is 0.005.

Key words: particle swarm optimization; support vector machine algorithm; wireless sensor network; network intrusion; DDoS intrusion; intrusion detection
EEACC: 6140; 6150P **doi**: 10.3969/j.issn.1004-1699.2026.09.029

基于粒子群算法优化 SVM 的无线传感网络 DDoS 入侵检测方法*

胡晓东*
(山西经济管理干部学院数字工程系 山西 太原 030024)

摘 要: DDoS 入侵是常见的无线传感网络攻击类型,为保证网络运行安全,提出基于粒子群算法优化 SVM 的无线传感网络 DDoS 入侵检测方法。根据 DDoS 入侵原理和流程,设置 DDoS 入侵检测标准。综合考虑无线传感网络的组成结构和工作原理,利用网络爬虫技术收集无线传感网络实时运行数据,利用粒子群算法优化支持向量机算法,提取网络运行特征,根据特征匹配结果,得出网络 DDoS 入侵状态和入侵强度的检测结果。通过性能仿真分析得出结论:与传统方法相比,优化设计方法的入侵状态检测准确率明显提升,平均入侵强度检测误差为 0.005。

关键词: 粒子群优化; 支持向量机算法; 无线传感网络; 网络入侵; DDoS 入侵; 入侵检测;
中图分类号: TP393 **文献标识码**: A **文章编号**: 1004-1699(2026)09-2164-07

随着物联网技术的飞速发展,无线传感网络(Wireless Sensor Networks, WSNs)作为物联网的重要组成部分,在环境监测、智能农业、工业控制等领域展现出巨大的应用潜力[1]。然而,无线传感网络也面临着日益严峻的安全威胁,其中分布式拒绝服务(Distributed Denial of Service, DDoS)攻击尤为突出。DDoS 攻击通过控制大量被感染的节点或僵尸网络,向目标网络发送大量无用的数据包,导致网络资源耗尽,服务中断,对国家安全、社会稳定及个人隐私构成严重威胁。

为了降低 DDoS 入侵对无线传感网络产生的负面影响,及时制定相应的入侵防御与维护方案,提出入侵检测方法。入侵检测方法是网络安全领域中的一项重要技术,用于监控网络和系统以发现潜在的威胁和异常行为,其主要目的是及时发现并应对各种入侵行为,从而保护网络的安全和稳定。现阶段发展较为成熟的网络入侵检测方法众多,其中景雯等[2]提出了基于区块链技术的无线传感网络入侵

项目来源: 山西省教育厅职业教育教学改革与实践研究重点课题项目(202402012); 全国高校计算机教育研究会教学改革研究项目(山西地区)(SXCF202412)
收稿日期: 2024-07-11 **修改日期**: 2024-09-18

检测方法,该方法通过区块链的监控机制,收集无线传感网络中的异常节点数据,运用主成分分析法对这些异常节点的特征进行提取,构建一个以信任值的计算、更新和分发为核心的信任模型,将提取的特征输入到该模型中,经过处理,模型会输出每个节点的信任值,完成无线传感网络入侵的检测工作。该方法利用 PCA 特征提取提高了入侵检测的准确性,但区块链技术的引入增加了系统复杂性和计算成本,影响实时性。白文荣等[3]提出了基于菌群优化深度学习的网络入侵检测方法,该方法构建一个基于深度置信网络的入侵检测模型,首先要对深度置信网络中的受限玻尔兹曼机层进行核心参数的初始化。这些参数包括权重和偏置,它们共同构成了模型的菌群。通过比较深度置信网络检测到的攻击数量与实际攻击数量的差值,确定一个适应度函数。在此基础上,运用驱化、繁衍和迁徙等操作来不断优化适应度值,以找到最优的个体,利用这个最优个体所对应的权重和偏置进行深度置信网络的入侵检测。该方法的全局搜索能力有助于找到最优解,但菌群算法中的参数设置对结果影响较大,需精细调整。Baldini 等[4]提出了基于自适应滑动窗口和形态分形维数的网络入侵检测方法,该方法使用滑动窗口和熵对网络流量进行统计度量,根据网络流量的变化特征,得出网络入侵检测结果。该方法将自适应滑动窗口和形态分形维数结合,能有效捕捉网络流量的动态变化,提高入侵检测的灵敏度,但对参数设置的依赖性较大,设置不当易导致误报或漏报。另外,Akgun 等[5]提出了基于深度学习的网络入侵检测方法,该方法利用深度学习算法中的深度神经网络、卷积神经网络和长短期记忆算法,对网络的运行特征进行提取,根据网络特征确定网络入侵的检测结果。该方法能全面捕捉网络运行特征,提高入侵检测的准确性和效率,但深度学习模型训练复杂度高,需要大量标注数据。

为解决上述方法中存在的问题,研究基于粒子群算法优化 SVM 的无线传感网络 DDoS 入侵检测方法。粒子群优化算法(Particle Swarm Optimization,PSO)作为一种基于群体智能的优化技术,以其简单易实现、收敛速度快等优点,在解决复杂优化问题中展现出独特优势[6]。支持向量机(Support Vector Machine,SVM)作为一种强大的分类工具,能够在高维空间中寻找最优分类超平面,实现高精度的分类效果[7]。将 PSO 与 SVM 相结合,利用 PSO 的全局搜索能力优化 SVM 的参数,可以有效提升模型的分类性能和泛化能力,为无线传感网络 DDoS 入侵检测提供新的解决方案。

1　无线传感网络 DDoS 入侵检测方法设计

无线传感网络 DDoS 入侵检测方法,综合考虑 DDoS 入侵原理和特征,判断当前网络中是否存在 DDoS 入侵行为。优化设计的入侵检测方法以无线传感网络作为研究对象,在粒子群算法优化 SVM 算法的支持下,提取无线传感网络的运行数据特征,采用特征匹配的方式,确定当前网络的入侵状态以及入侵类型检测结果。

1.1　设置 DDoS 入侵检测标准

在深入探讨无线传感网络 DDoS 入侵检测的具体实现之前,需要首先设定明确的检测标准。这些标准将作为判断网络是否遭受 DDoS 攻击的依据,为后续的数据分析和算法应用奠定基础。

现有的 DDoS 检测标准多针对有线网络环境,而 WSN 由于其资源受限、通信方式特殊等特点,需要更为精细和高效的标准[8]。因此,本文提出的标准考虑了 WSN 的数据传输特性,从而实现对 DDoS 攻击行为的精确识别和分类。

根据 DDoS 入侵在无线传感网络中的运行原理和流程,确定 DDoS 入侵作用下无线传感网络的运行特征,以此作为 DDoS 入侵的检测标准。图 1 表示的是 DDoS 入侵工作原理。

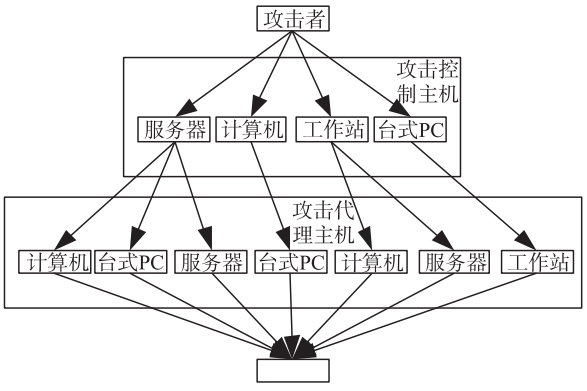


图 1　DDoS 入侵原理图

从图 1 中可以看出,DDoS 攻击行为涉及攻击者、攻击控制主机、攻击代理主机、受害者四个主体,在入侵攻击中,攻击者采取了一种多对一的策略,即利用多台傀儡主机对单一受害机发起攻击。攻击者首先在网络中筛选出存在安全漏洞、链路状态良好且性能优异的主机。随后,攻击者会入侵这些主机,获取管理权限,并安装控制程序,从而实施攻击。根据上述 DDoS 入侵攻击原理,可以得出 DDoS 入侵下无线传感网络的工作特征 τ_b 为:

$$\tau_b = \kappa_{\mathrm{DDoS}} \times q \times \tau_{\mathrm{net}} \tag{1}$$

式中：κ_{DDoS}和 q 分别表示的是 DDoS 入侵攻击系数和攻击强度，τ_{net}为无入侵攻击作用下无线传感网络的基本运行特征[9]。将式(1)表示的求解结果，作为 DDoS 入侵检测标准的设置结果。为了有效实施这些检测标准，还需要收集并分析无线传感网络的实时运行数据。

1.2 收集无线传感网络实时运行数据

数据的收集是网络安全分析的基础，在本研究中，为了给 DDoS 入侵检测工作提供数据支持，在无线传感网络中采集实时运行数据，为后续的 DDoS 入侵检测提供可靠的数据支持。

针对 WSN 中节点分散、数据传输受限的问题，设计一种基于无线传感网络的实时数据采集机制。该方法能够显著降低数据传输量，同时保证数据的完整性和实时性，为后续的 DDoS 入侵检测提供可靠的数据基础。图 2 表示的是无线传感网络的内部拓扑结构。

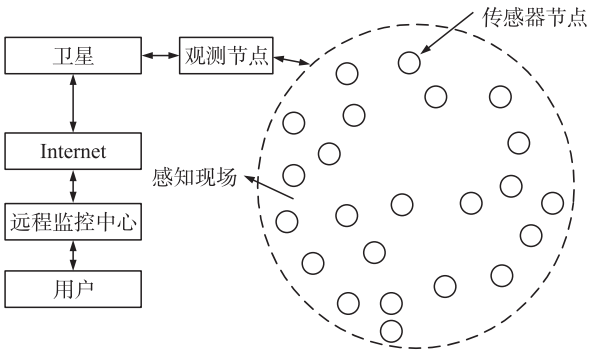


图 2 无线传感网络拓扑结构图

图 2 表示的无线传感网络中，传感器节点在完成相互通信后，具备自动构建无线网络的功能。在数据传输过程中，无线传感器通过与相邻节点进行中继，实现多跳传输，最终将检测到的数据发送至数据汇聚节点。汇聚节点进一步利用移动通信网、卫星等传输媒介，将数据上传至上层节点进行统一管理[10]。这一流程使得用户能够实现对整个传感器网络的远程控制。在上述无线传感网络环境中，利用网络爬虫技术实现网络实时运行数据的采集，在实际采集过程中按照一定的规则和算法，遍历网络上的网页，从中提取所需的信息，最终采集的无线传感网络运行数据的采集结果 x 为：

$$x=\kappa_{\mathrm{reptile}}x_{\mathrm{net}} \tag{2}$$

式中：x_{net}为无线传感网络中的实际运行数据，$\kappa_{\mathrm{reptile}}$为网络爬虫的工作系数，其中 x_{net}的具体取值如下：

$$x_{\mathrm{net}}=x_{\mathrm{send}}\times P_{\mathrm{send}}\times(\kappa_{\mathrm{sense}}+\kappa_{\mathrm{tran}}-\kappa_{\mathrm{loss}}) \tag{3}$$

式中：x_{send}为无线传感网络中任意网络节点的实际发送数据，P_{send}为网络数据的发送功率，κ_{sense}、κ_{tran}和 κ_{loss}对应的是网络节点的传感系数、传输系数和路径损耗系数[11]。为保证无线传感网络的采集质量、降低网络环境中干扰元素对数据采集结果产生的负面影响，需要对初始采集的数据进行清洗处理，处理过程可以量化表示为：

$$\begin{cases}x_{\mathrm{filtering}}=h_{\mathrm{filtering}}(x)\\ x_g=\dfrac{x_{\max}-x_{\min}}{x_{\max}-x}\end{cases} \tag{4}$$

式中：$h_{\mathrm{filtering}}(\,)$为滤波函数，$x_{\max}$和 $x_{\min}$为采集数据的最大值和最小值，$x_{\mathrm{filtering}}$和 x_g 分别为网络数据的滤波和归一化处理结果。重复上述操作，完成网络数据的采集与处理操作。在获取了数据之后，还需要从这些海量数据中提取出有用的特征信息，以便进行进一步的分析和判断。

在获取到无线传感网络的实时运行数据后首先进行数据清洗，旨在识别并剔除异常值、重复数据以及因设备故障或环境干扰而产生的噪声数据，确保数据的准确性和可靠性。随后进行数据的归一化处理，将所有特征变量的值缩放到同一量纲和范围内，以消除不同量纲对模型训练的影响，提高模型的收敛速度和稳定性。

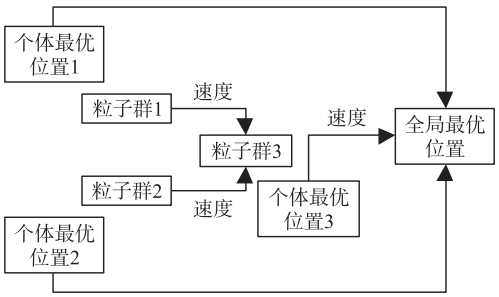
考虑到无线传感网络数据的高维性和冗余性，进一步采用降维技术来减少特征数量，提取最具代表性的特征子集，以此降低模型的计算复杂度，提高训练效率，减少过拟合风险，增强模型的泛化能力。在本研究中，根据数据的特性和分析需求，选择主成分分析 PCA 降维方法，在保留主要信息的同时去除冗余信息，优化特征空间，为后续的 DDoS 入侵检测模型提供更有价值的输入。

1.3 利用粒子群算法优化 SVM 提取运行特征

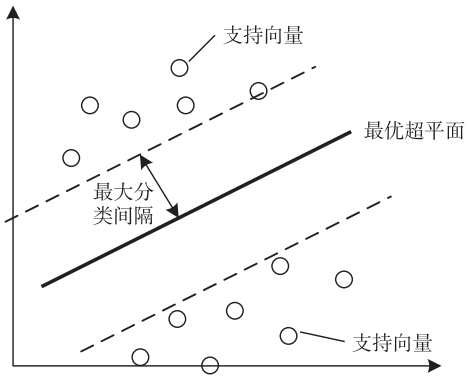
为了从无线传感网络的运行数据中提取出关键特征，以初始采集并处理完成的无线传感网络运行数据为支持，利用粒子群算法优化 SVM，进而提取网络的运行特征。这种算法结合了粒子群优化和支持向量机的优势，能够在复杂的数据集中快速准确地识别出与 DDoS 攻击相关的特征，为后续的检测和防御提供有力支持。在实际运行中，需要利用粒子群算法对支持向量机算法进行优化，粒子群算法和支持向量机算法的基本运行原理如图 3 所示。

粒子群算法中任意粒子均具有位置和速度两个属性，食物的位置对应所求问题的最优解，各个粒子通过信息交流，相互协作，找到食物的所在位置[12]。粒子以个体和全局最优值为参考，决定下一步的飞行活动，逐渐向食物靠近。

在粒子群算法运行过程中，首先对种群系数进



(a) PSO算法



(b) SVM算法

图 3　粒子群和支持向量机算法原理图

行初始化,将个体最优位置和全局最优位置的初始值设置为 W_{ind} 和 W_{ove},在迭代训练过程中,粒子的位置和速度的调整更新结果为:

$$\begin{cases} v_i(k+1)=\omega v_i(k)+a_1\beta_1[W_{ind}-W_i(k)]+ \\ \quad a_2\beta_2[W_{ove}-W_i(k)] \\ W_i(k+1)=W_i(k)+v_i(k+1) \end{cases} \tag{5}$$

式中:$v_i(k)$、$v_i(k+1)$、$W_i(k)$ 和 $W_i(k+1)$ 分别为粒子群中第 i 个粒子在第 k 和第 $k+1$ 次迭代中的速度和位置,ω 为惯性权重,a_1 和 a_2 为学习因子,β_1 和 β_2 为随机数[13]。根据目标函数计算粒子的适应值,得出粒子个体和全局最优位置的更新结果如下:

$$\begin{cases} W_{ind}(k+1)=\begin{cases} W_i(k+1) & \sigma_i(k+1)\leqslant\sigma_{ind}(k+1) \\ W_{ind}(k) & \sigma_i(k+1)\geqslant\sigma_{ind}(k+1) \end{cases} \\ W_{ove}(k+1)=\min[W_i(k+1)] \end{cases} \tag{6}$$

式中:σ_i 为粒子 i 的适应度,按照上述流程完成一次迭代工作,判断是否达到最大迭代次数,如果达到,算法结束。否则重复位置、速度更新工作,继续执行迭代操作。针对 WSN 的特点,对算法进行适应性改进,使其能够更好地适应 WSN 的复杂环境,有效提取出 DDoS 攻击行为的特征。

支持向量机算法是一种强大的机器学习技术,它通过非线性映射,将原始样本空间转换至一个高维甚至可能是无穷维的特征空间,并解决可分离的问题,同时确保了所得解为全局最优[14]。在 d 维空间中设置分类超平面:

$$\psi x+b=0 \tag{7}$$

式中:ψ 和 b 分别为斜率和截距。最优分类面的求解问题可以转换为约束优化问题,最终输出的最优分类函数结果 $h_{SVM}(x)$ 为:

$$h_{SVM}(x)=\mathrm{sgn}\left(\sum\lambda_i L_i x+b\right) \tag{8}$$

式中:λ_i 和 L_i 分别为支持向量和样本 i 的类别,sgn( )为阶跃函数。在无线传感网络特征提取工作中,利用粒子群算法对支持向量机算法进行优化,优化流程如图 4 所示。

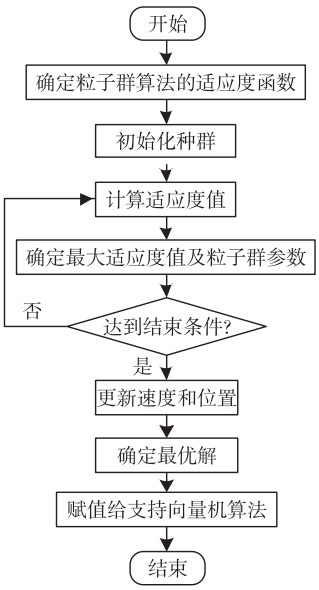


图 4　PSO 对 SVM 的优化流程图

利用粒子群算法优化 SVM 后,得出无线传感网络运行特征的提取结果 τ_{net}:

$$\tau_{net}=\mathrm{sgn}\left[\sum\lambda_i L_i x+W_{ove}(k+1)\right] \tag{9}$$

利用粒子群算法和支持向量机算法确定网络特征的提取参数,将无线传感网络实时运行数据的采集与处理结果代入到式(9)中,即可得出网络运行特征的提取结果。基于提取出的特征,将设计并实现一种有效的 DDoS 入侵检测方法。

1.4　实现无线传感网络 DDoS 入侵检测

本文构建完整的无线传感网络 DDoS 入侵检测方法,以便实时监测网络的运行状态,并根据粒子群算法优化 SVM 提取出的特征进行自动分析和判断,一旦检测到 DDoS 攻击行为,将立即采取相应的防御措施,保障网络的安全稳定运行。

采用特征匹配的方式,判断当前无线传感网络是否存在 DDoS 入侵现象,特征匹配过程如下:

$$s=\frac{\tau_b\times\tau_{net}}{\|\tau_b\|\times\|\tau_{net}\|} \tag{10}$$

将 DDoS 入侵标准特征的设置值与粒子群算法

优化 SVM 的输出结果代入到式(10)中,将式(10)的计算结果与阈值 s_0 进行比对,若 s 高于阈值,则说明当前无线传感网络存在 DDoS 入侵现象,否则认为当前网络无 DDoS 入侵行为[15]。针对存在 DDoS 入侵行为的无线传感网络,需要对 DDoS 入侵强度进行进一步检测,检测结果为:

$$Q=\frac{f_{\text{intrusion}}\times t_{\text{intrusion}}}{N_{\text{net}}} \tag{11}$$

式中:$f_{\text{intrusion}}$ 和 $t_{\text{intrusion}}$ 分别为入侵频率和入侵持续时间,N_{net} 为无线传输网络的传输总流量值。最终将 DDoS 入侵状态和入侵强度的检测结果以可视化的形式输出,完成无线传感网络的 DDoS 入侵检测工作。

至此,本文详细阐述了基于粒子群算法优化 SVM 的无线传感网络 DDoS 入侵检测方法的设计思路。首先,针对 WSN 的特性制定专门的 DDoS 入侵检测标准;其次,通过高效的实时数据收集方法,确保数据的完整性和实时性;接着,利用粒子群算法优化 SVM 对 WSN 的运行特征进行精确提取;最后,基于这些特征设计并实现 DDoS 入侵的实时检测。这一方法不仅对 WSN DDoS 攻击行为进行了深入理解与研究,也是机器学习算法在网络安全领域的广泛应用,体现了其显著优势。

2 检测性能仿真分析

为了测试基于粒子群算法优化 SVM 的无线传感网络 DDoS 入侵检测方法的检测性能,设计检测性能仿真分析。此次仿真过程分别从入侵状态检测准确率和入侵强度检测误差两个方面反映方法的检测性能,并通过与文献[2]的基于区块链技术的无线传感网络入侵检测方法、文献[3]的基于菌群优化深度学习的网络入侵检测方法的对比,体现出优化设计方法在检测性能方面的优势。

2.1 配置无线传感网络环境

此次性能仿真分析选择了覆盖到发电厂中的某无线传感网络作为仿真环境,网络环境拓扑结构的配置情况如图 5 所示。

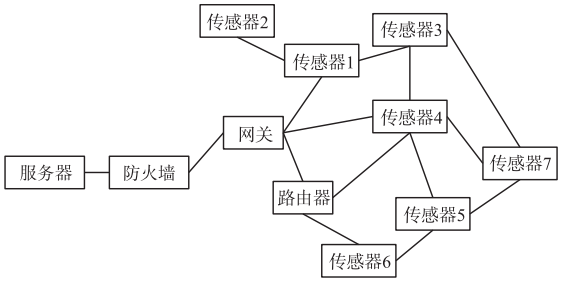


图 5 无线传感网络环境拓扑结构图

仿真分析选择的无线传感网络中包含 50 个传感器设备,网络中的各个节点都在一台高性能服务器上执行,服务器的 CPU 为 Intel XeonCPU E5-2603v3,其主频为 1.60 GHz。基于 KVM 技术,服务器上创建了 5 个虚拟机。每个虚拟机配置了 10 GB 内存、三核 CPU 以及 250 GB 硬盘。这 5 台虚拟机均安装了 CentOS7 操作系统,并搭建了一个基于 Hadoop2.8.5 的集群,该集群包含了 HDFS 和 YARN 组件。为了进行数据处理和检测,采用了 Scala2.12.6 编写算法。完成程序打包后,通过终端提交到 YARN 集群,利用 YARN 进行资源调度。

2.2 编写入侵攻击程序

在配置的无线传感网络环境中安装一个虚拟机,用来执行 DDoS 入侵攻击操作。根据 DDoS 入侵原理与流程,开始编写代码。编码时应遵循之前制定的规范,确保代码的可读性、可维护性和可扩展性,为保证入侵攻击程序的可控性,在程序编写过程中需要添加两个强制终止指令。DDoS 检测端连接一台收集服务器与一台探测服务器,并通过万兆网卡直接连接两个设备,实现数据同步。除 DDoS 入侵攻击程序外,还需要设置并编写 R2L 入侵、U2R 入侵以及 Probe 攻击程序。

2.3 设定粒子群算法优化 SVM 运行参数

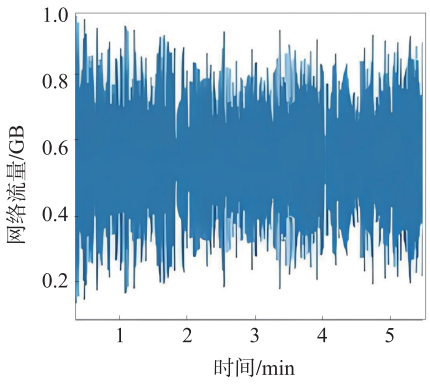
为保证粒子群算法优化 SVM 在无线传感网络 DDoS 入侵检测方法中的正常运行,需要对粒子群算法和支持向量机算法的运行参数进行设定,粒子群算法中初始粒子种群数量为 60,迭代次数为 80,权值为 0.67,学习因子 a_1 和 a_2 分别设置为 1.0 和 2.0。支持向量机算法选择线性核函数,分类超平面的初始斜率和截距分别为 0.3 和 0.5。

2.4 入侵检测性能仿真分析过程设计

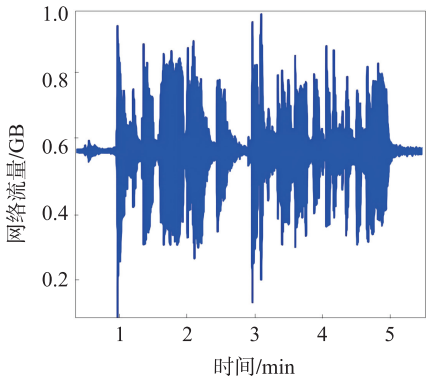
在仿真分析开始之前,不启动入侵攻击程序,执行无线传感网络的传感与数据传输工作,得出网络运行数据的初始生成样本,在此基础上,启动 DDoS 入侵攻击程序,得出攻击场景下的网络运行数据样本。任意时段无线传感网络数据样本的生成结果,如图 6 所示。

按照上述过程,可以得出无线传感网络在仿真过程中的数据样本生成结果。利用开发工具,完成优化设计入侵检测方法的开发,生成的数据样本输入到检测方法对应的运行程序中,输出任意时刻无线传感网络 DDoS 入侵攻击的检测结果,如图 7 所示。

按照上述方法,可以得出其他时刻的网络入侵攻击检测结果。仿真中设置的对比方法分别为:文



(a) 正常场景



(b) DDoS入侵攻击场景

图 6　无线传感网络运行数据样本波形图

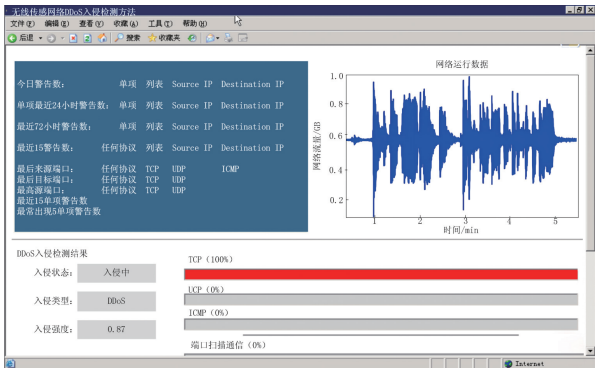


图 7　无线传感网络 DDoS 入侵攻击检测结果

献[2]中的基于区块链技术的无线传感网络入侵检测方法和文献[3]中的基于菌群优化深度学习的网络入侵检测方法,在相同的实验环境下完成对比方法的开发,并得出对应的入侵攻击检测结果。

2.5　入侵检测性能仿真分析结果与分析

仿真设置网络入侵状态检测准确率和入侵强度检测误差作为检测性能的量化验证指标,其中网络入侵状态检测准确率 η 的数值结果为:

$$\eta=\frac{n_{\mathrm{suc}}}{n_t}\times 100\% \tag{12}$$

式中:n_{suc} 和 n_t 分别表示的是入侵状态检测准确的仿真次数和入侵检测总次数。另外,入侵强度检测误差 ε 的公式为:

$$\varepsilon=|Q-Q_{\mathrm{set}}| \tag{13}$$

式中:Q_{set} 为网络入侵强度的设置值。最终计算得出网络入侵状态检测准确率取值越大、入侵强度检测误差越低,证明对应方法的检测性能越优。

通过相关数据的统计以及式(12)的计算,得出入侵检测状态检测准确率的仿真对比结果,如图 8 所示。

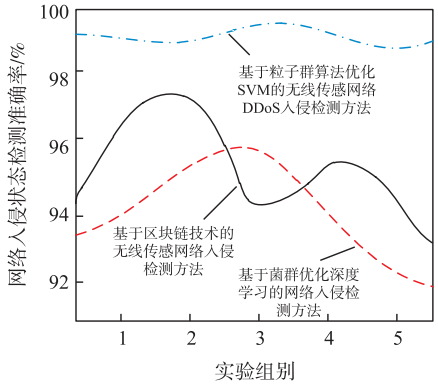


图 8　入侵状态检测准确率对比曲线

从图 8 中可以直观看出,与两种传统方法相比,优化设计方法的入侵状态检测准确率明显降低。这是因为本文方法结合了粒子群优化和支持向量机各自的优势,其中,PSO 算法在全局搜索最优解方面具有出色的能力,能够在复杂的无线传感网络数据中找到最佳分类边界;SVM 算法具备强大的泛化能力和对高维数据的处理能力,在 DDoS 入侵检测中能够得到更加精确的结果。

另外,网络入侵强度检测误差指标的仿真结果如图 9 所示。

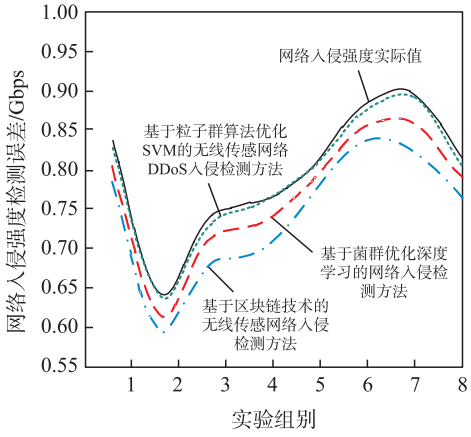


图 9　网络入侵强度检测误差测试数据

将图 9 中的数据代入到式(13)中,计算得出两种传统方法入侵强度检测误差的平均值分别为 0.060 和 0.031,而优化设计方法得出的平均入侵强度检测误差为 0.005。上述数据结果说明,本文方法

输出的网络入侵强度检测值与网络入侵强度的实际值基本一致,监测误差较小。能够实现这一结果,主要是因为 PSO 算法通过迭代优化能够找到 SVM 分类器的最佳参数,使得模型能够更好地拟合实际数据,从而提高检测精度。

3 结束语

DDoS 攻击起源于原始的 DoS 攻击,具有隐蔽性强、攻击强度大、不确定性等特征,给无线传感网络的运行工作带来较大的负面影响。在此次研究中,通过粒子群算法优化 SVM 算法的应用,实现对网络入侵检测方法的优化,为网络攻击防御提供数据支持,对于网络运行安全具有重要意义。

参考文献:

[1] 陈晨,刘曙,王艺菲,等. 基于 PSOGWO-SVM 的网络入侵检测方法[J]. 空军工程大学学报(自然科学版),2022,23(2):97-105.

[2] 景雯,张杰. 基于区块链技术的无线传感网络入侵检测算法[J]. 传感技术学报,2023,36(6):978-983.

[3] 白文荣,马琳娟,巩政. 基于菌群优化深度学习的网络入侵检测模型[J]. 南京理工大学学报,2023,47(5):636-642.

[4] Baldini G,Amerini I. Online Distributed Denial of Service (DDoS) Intrusion Detection Based on Adaptive Sliding Window and Morphological Fractal Dimension[J]. Computer Networks,2022,210(1):108923.

[5] Akgun D,Hizal S,Cavusoglu U. A New DDoS Attacks Intrusion Detection Model Based on Deep Learning for Cybersecurity[J]. Computers & Security,2022,118(1):102748.

[6] 蔡玲如,朱理,黄瑞崧,等. 基于强化学习的无线传感器网络入侵检测攻防博弈研究[J]. 计算机应用研究,2022,39(12):3786-3790.

[7] Gowdhaman V,Dhanapal R. Hybrid Deep Learning-Based Intrusion Detection System for Wireless Sensor Network [J]. International Journal of Vehicle Information and Communication Systems,2024,9(3):239-255.

[8] 肖衡,龙草芳. 基于机器学习的无线传感网络通信异常入侵检测技术[J]. 传感技术学报,2022,35(5):692-697.

[9] Srivastava J,Prakash J. Multi-Modal for Energy Optimization and Intrusion Detection in Wireless Sensor Networks [J]. Wireless Personal Communications,2023,133(1):289-321.

[10] 汪祖民,王冬昊,梁霞,等. 基于 DBSCAN_GAN_XGBoost 的网络入侵检测方法[J]. 郑州大学学报(工学版),2022,43(3):44-51.

[11] Arkan A,Ahmadi M. An Unsupervised and Hierarchical Intrusion Detection System for Software-Defined Wireless Sensor Networks [J]. The Journal of Supercomputing,2023,79(11):11844-11870.

[12] Jin J. Intrusion Detection Algorithm and Simulation of Wireless Sensor Network under Internet Environment[J]. Journal of Sensors,2021,2021(1):9089370.

[13] 李创,孙子文. IWSN 中基于属性变化率的全局信任入侵检测[J]. 传感技术学报,2023,36(2):294-300.

[14] 王振东,刘尧迪,杨书新,等. 基于天牛群优化与改进正则化极限学习机的网络入侵检测[J]. 自动化学报,2022,48(12):3024-3041.

[15] 马泽煊,李进,路艳丽,等. 融合 WaveNet 和 BiGRU 的网络入侵检测方法[J]. 系统工程与电子技术,2022,44(8):2652-2660.

胡晓东(1980—),男,汉族,山西五台人,硕士,副教授,研究方向:计算机应用、系统运维、数据库研发、数字化转型等,dxfk949@163.com。