基于分簇的无线传感网络异常流量检测、通信加密算法技术研究

武少鹏[1]
WU Shaopeng

摘 要 WSN（wireless sensor networks）无线传感网络为簇头、分布簇节点组成的簇化网络结构，由分布簇感知网络环境的数据信息、簇头将采集到数据作出汇聚融合处理，然而由于外部异常用户入侵的数据特征维度高，使得面向分类节点的异常数据特征字段提取的工作量大、准确率差。基于此，文章提出了一种基于大数据及深度学习算法的无线传感网络异常流量检测管理方案，对网络节点提取的异常数据流量，利用 PCA（principal components analysis）主成分分析法将提取数据分段进行复杂特征降维，引入 FWA（fireworks algorithm）算法优化 PSO（particle swarm optimization）粒子群算法，使用更新后的初始化粒子群参数、粒子速度和位置在滑动时间窗口提取异常数据流量信息，以连续数据帧为单元提取正常数据流量，基于 RSA 非对称算法作出正常数据加密，有效提升网络异常流量检测防范鲁棒性。

关键词 分簇；无线传感网络；异常流量检测；通信加密算法

doi：10.3969/j.issn.1672-9528.2025.11.027

0 引言

无线传感器网络具备大规模覆盖、多跳自组网及节点可扩展的优势，但受制于多径信道传播的信号衰落、节点恶意攻击等因素的影响，在海量化数据、复杂化簇节点通信传输中会出现多种安全风险问题。在这一背景下，面向外网恶意用户攻击无线传感器节点的现实问题，设计融合 PSO（particle swarm optimization）粒子群自适应算法、FWA（fireworks algorithm）算法的全局寻优变异搜索算法，基于无线 TCP/IP 协议、ZigBee 协议的多跳自组网网络通信模式，引入高斯变异火花增强 PSO（particle swarm optimization）粒子寻优的深度和多样性，作出无线传感网络树形结构中网络异常流量访问的全局搜索与训练，经过数次粒子群更新以提升算法的数据分类性能、检测准确率。

1 分簇无线传感网络中异常数据流量检测的分段处理模式

1.1 无线传感网络中异常攻击数据流量的分段

无线传感网络为涵盖多维节点的树形结构，树形分布簇末端网络节点容易受到外网用户输入数据的攻击，诸如 DoS（disk operating system）拒绝服务攻击、U2R（user to root）提权攻击、R2L（remote to local）远程非授权攻击、Probing 探测攻击等类型攻击，使部分传感网络出现通信拥塞、故障或中断的异常状态问题。

面对无线传感网络不同类型的数据流量攻击，采用对长数据字段序列直接提取异常数据特征的方式，通常涉及数据识别量级过大、特征学习步骤多，为此引入时间戳马尔可夫模型的数据分段方法，依照无线传感网络数据字段的长度、移动步长，从无线传感网络相邻状态转移的概率和分布情况出发，将其分割为多个小的数据块序列[1]。诸如在 $T=\{t_0, t_1, \ldots, t_m\}$ 时间范围内，定义无线传感网络状态为 $S=\{s_1, s_2, \ldots, s_n\}$、转移概率矩阵为 $\boldsymbol{Q}_{i,j}$，表示某一时间点网络数据块传输状态从 s_i 转换为 s_j 状态矩阵的概率，计算公式为：

$$\boldsymbol{Q}_{i,j}=\lim_{\Delta t\to 0}\frac{P\left(x_j\left(t_i+\Delta t\right)=\boldsymbol{s}_j \mid x_i\left(t_i\right)=\boldsymbol{s}_i\right)}{\Delta t} \tag{1}$$

利用时间戳 T 计算无线传感网络状态 s_i 的停留时间、服从 $f(\Delta t \mid \lambda)=\left\{\lambda \mathrm{e}^{-\lambda \Delta t} \mid \Delta t \geq 0\right\}$ 的指数分布，且 $\lambda=\frac{m}{\sum_{k=1}^{m}\left(t_{k+1}-t_k\right)}$ 为指数分布参数，对于无线传感网络分段设置状态 s_i 停留的时间阈值为 θ_i，则 $\Delta t=t_{k+1}-t_k>\theta_i$ 时，认为无线传感网络的状态发生转移，也即网络异常攻击数据流量 $X=\{x_1, x_2, \ldots, x_n\}$ 应发生分段，则无线传感网络数据序列的状态转移率估计用公式可表示为：

$$\hat{\boldsymbol{Q}}_{i,j}=\frac{N_{i,j}}{\sum_{i=1}^{n}\Delta t\left(x_i\left(t_i\right)=\boldsymbol{s}_i\right)\mathrm{dt}} \tag{2}$$

1. 武警内蒙古总队乌兰察布支队 内蒙古乌兰察布 012000

1.2 基于 PCA 主成分分析法的数据分段特征降维

在无线传感网络内海量化用户数据流量传输的监测过程中，要以时间窗口的数据流序列为基础，对实时更新、规模庞大的数据流量作出主成分分析的特征降维。依照 $\{\Delta t_0, \Delta t_1, \cdots, \Delta t_n\}$ 的滑动时间窗口设置，截取不同长度的数据序列，若 n 个网络数据字段样本有着 q 种特征、则可用 $n\times q$ 表示网络数据字段的特征矩阵，为消除不同特征的量纲影响对每个特征进行标准化处理，得到的标准化特征值计算公式为 [2]：

$$\mathrm{Stancv}_{i,g}=\frac{\boldsymbol{x}_{i,g}-\mu_g}{\sigma_g} \tag{3}$$

式中：$\boldsymbol{x}_{i,g}$ 表示第 i 个样本的第 g 个特征值；μ_g 和 σ_g 分别表示第 g 个特征的均值、标准差，其中 $\mu_g=\frac{1}{n}\sum_{i=1}^{n}\boldsymbol{x}_{i,g}$、$\sigma_g=\sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(\boldsymbol{x}_{i,g}-\mu_g\right)^2}$。经过标准化后的网络数据流量特征矩阵为 $q\times q$ 的标准化协方差矩阵，用 $\boldsymbol{\Sigma}_{\mathrm{Cov}}$ 表示在时间窗口相邻的网络数据流量的特征值协方差矩阵，也即计算 g 维特征值与其对应维数均值的差值得到协方差矩阵，计算公式为：

$$\boldsymbol{\Sigma}_{\mathrm{Cov}}=\frac{1}{n}\sum_{i=1}^{n}\sum_{g=1}^{q}\left(\mathrm{Stancv}_{i,g}-\bar{\mathrm{Stancv}}_{g}\right)\left(\mathrm{Stancv}_{i,k}-\bar{\mathrm{Stancv}}_{k}\right) \tag{4}$$

式中：$\bar{\mathrm{Stancv}}_{g}$和$\bar{\mathrm{Stancv}}_{k}$分别表示第 g 个、第 k 个特征值的均值，数据标准化后两个均值为 0。而后将特征值协方差矩阵 $\boldsymbol{\Sigma}_{\mathrm{Cov}}$ 按照特征值大小对 $\{x_{i,1}, x_{i,2}, \cdots, x_{i,q}\}$ 的 q 种特征作出重新排序，更新为 $\{y_{i,1}\geqq y_{i,2}\geqq\cdots\geqq y_{i,k}\geqq 0\}$，设置更新后 q 个特征值的特征向量为 $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_q\}$，选择 $y_{i,k}$ 和 e_q 的集合作为主成分，选择前 o 个主成分对其进行解释方差占总方差比例的计算，得到累计方差贡献率的计算公式为：

$$\mathrm{CR}_o=\frac{\sum_{o=1}^{q}\boldsymbol{x}_{i,o}\cdot\boldsymbol{e}_o}{\sum_{i=1}^{n}\boldsymbol{x}_{i,q}\cdot\boldsymbol{e}_q} \tag{5}$$

式中：CR_o 表示前 o 个主成分的累积方差贡献率，若 $\mathrm{CR}_o\geq 90\%$ 则表明网络数据字段的重要特征信息得到保留，降维后的分段数据集特征在训练模型中呈散点分布状态，据此可观察到不同类异常数据流量的入侵特征与分布情况。

2 基于 FWA-PSO 粒子群联合算法的无线传感网络异常流量检测方案

2.1 基于 PSO 粒子群算法的网络异常簇数据流量搜索检测模式

PSO 粒子群算法为模仿鸟类捕食的空间点搜索迭代方法，假设 D 维空间内存在粒子群，每个粒子个体在空间搜索中都通过数据特征的迭代跟踪得到个体极值（Indbest）、全局极值（Globest），若设置第 i 个粒子在第 t 次迭代时的更新速度为 v_i、更新空间位置表示为 z_i，则可用 $\{z_{i1}, z_{i2}, \cdots, z_{iD}\}$ 表示第 i 个粒子多次迭代后的更新位置，面对网络异常流量入侵时的异常数据特征值加权计算公式为 [3]：

$$\mathrm{Weight}=\sum_{i=1}^{n}z_{iD}\cdot y_{i,k} \tag{6}$$

式中：z_{iD} 的更新粒子位置作为网络异常数据特征值的权重而存在；Weight 表示某一时刻网络异常数据流量特征值的加权之和。在这一粒子空间搜索的异常数据特征寻优过程中，引入 c_1 和 c_2 作为学习因子，一般 c_1=c_2 且为正值；引入均匀分布随机数 γ_1 和 γ_2，一般 γ 处于 [0,1] 的区间范围内。两种参数分别用于调节粒子的全局寻优位置、寻优搜索的随机性。基于现有粒子位置等参数更新后的粒子速度公式为：

$$v_i^{t+1}=\mathrm{z}_{iD}v_i^t+c_1\gamma_1\left(\mathrm{Ind}_{\mathrm{best}}-y_{i,k}^t\right)+c_2\gamma_2\left(\mathrm{Glo}_{\mathrm{best}}-y_{i,k}^t\right) \tag{7}$$

式中：v_i^t和v_i^{t+1}分别表示第 i 个粒子原有的空间搜索飞行速度、更新后的搜索飞行速度；$y_{i,k}^t$表示 t 时刻网络异常数据的特征值。

而后基于适应度函数来量化网络异常数据流量特征的检测成果，用异常数据特征加权值、正常数据特征加权值计算粒子群搜索的信息熵紧凑性，计算公式为：

$$\mathrm{Fitness}=-\sum_{i=1}^{n}\left(\mathrm{Weight}(y_{i,k})-\mu_{i,k}\right)^2 \tag{8}$$

式中：Fitness 表示粒子群搜索的信息熵紧凑性；Weight($y_{i,k}$) 和 $\mu_{i,k}$ 分别表示异常、正常数据特征加权值。

但由于 PSO 粒子群算法存在泛化能力弱、收敛速度快而易陷入局部最优解的问题，因而引入FWA算法对粒子群参数、适应度函数等要素作出更新优化，通过高斯变异增加多样性，避免算法在全局搜索时陷入早熟收敛。

2.2 基于改进 FWA-PSO 联合算法的网络异常流量检测模式

FWA 算法是以烟花爆炸现象为主开发的群体智能寻优算法，选用烟花粒子对 PSO 算法迭代更新后的最优粒子作出爆炸、高斯变异操作。假设 D 维空间内存在的粒子群为 $R=\{r_1,r_2,...,r_n\}$，在经式（6）（7）的粒子位置、速度等参数更新后，对当前更新后的第 i 个粒子作出烟花爆炸，根据式（8）的适应度函数值 Fitness 进行爆炸强度计算，用公式表示为 [4]：

$$A_i=\frac{\alpha\cdot\left(\mathrm{Fitness}_{\max}-\mathrm{Fitness}(y_{i,k})\right)}{\mathrm{Fitness}_{\max}-\mathrm{Fitness}_{\min}+\varepsilon} \tag{9}$$

式中：$\mathrm{Fitness}_{\max}$ 和 $\mathrm{Fitness}_{\min}$ 分别表示粒子种群的最大、最小适应度值；Fitness($y_{i,k}$) 表示第 i 个粒子的适应度；α 表示调节系数，用于控制爆炸强度范围与适应度之间的差距；ε 表示极小的常数量，用于防止公式的分母为 0。那么选取粒子群的第 i 个粒子进行粒子的爆炸生成，结合爆炸强度得到的火花总数、爆炸半径可用公式表示为：

$$B_i=B_{\max}\frac{\mathrm{Fitness}_{\max}-\mathrm{Fitness}(y_{i,k})+\varepsilon}{\sum_{i=1}^{n}\left(\mathrm{Fitness}_{\max}-\mathrm{Fitness}(y_{i+1,k})\right)+\varepsilon} \tag{10}$$

$$\mathrm{Rad}_i = \frac{\alpha \cdot A_i}{\sum_{i=1}^{n} A_i} \tag{11}$$

式中：B_i 和 $B_{\max}$ 分别表示第 i 个烟花粒子产生的火花数量、预设最大火花数；Fitness($y_{i,k}$) 和 Fitness($y_{i+1,k}$) 分别表示相邻烟花的适应度函数值，那么第 i 个烟花粒子爆炸后生成火花的位置可用$Z_i = \mathrm{z}_{iD} + \mathrm{Rad}_i \cdot \mathrm{rand}_n$的公式进行计算，式中 rand_n 表示服从标准正态分布的随机数。而后对第 i 个烟花粒子作出高斯变异操作以增加种群的多样性，随机选择部分维度进行扰动、选取最高适应度的烟花粒子加入变异迭代，通过轮盘赌方法确定不同批次加入变异迭代的个体，假设烟花粒子 r_i 为加入变异的个体，Z_i 为烟花位置，则高斯变异后生成的火花位置用公式 [5] 表示为：

$$Z_i^{'} = Z_i + \beta \cdot \mathrm{N}\left(0, \sigma_g^2\right) \tag{12}$$

式中：β 为高斯变异系数；N(0, σ^2) 为网络数据流量均值为 0、方差为 σ^2 的高斯分布。在烟花粒子变异后的火花位置超出搜索空间范围时，可对火花位置按照$Z_i^{'} = \begin{cases} L_d + \left(L_d - Z_i\right) \\ U_d - \left(Z_i - U_d\right) \end{cases}$的公式重新进行映射操作，使之回到可行域内完成多次迭代寻优，式中 L_d 和 U_d 分别表示 D 维搜索空间的上下位置边界。

3 基于 RSA 非对称算法的网络数据通信安全加密

面向无线传感网络通信的数据字段，引入 RSA 非对称加密算法生成密钥对，通过公钥（PR, η）加密、私钥（PR, d）解密实现网络簇节点数据安全传输。假设 p、h 为两个足够大的素数，其中 PR=p×h，PR 为密钥加密的模数，模数的二进制长度决定密钥长度；PU=(p-1)×(h-1) 表示与模数 PR 互质的正整数个数，则 RSA 加密算法的公钥指数 η、私钥指数 d 的计算公式为 [6]：

$$\begin{cases} \gcd(\eta, \mathrm{PU}) = 1 \\ 1 < \eta < \mathrm{PU} \qquad d \equiv \eta^{-1} \mathrm{mod PU} \end{cases} \tag{13}$$

式中：gcd() 表示两个数的最大公约数；mod 表示公钥指数 η 与 PU 之间的模运算，也即求取 d×η 除以 PU 的余数为 1。在此基础上，面对 SSL/TLS、SSH 无线网络协议的通信环境，由密钥中心生成随机的非对称密钥，后台服务器借助 RSA 公钥 / 私钥完成通信数据加密、解密传输，用 Plain 和 Cipher 分别表示网络节点传输数据的明文和密文，对网络数据通信的明文加密、解密公式可表示为：

$$\begin{aligned} \mathrm{Cipher} &= \mathrm{Plain}^{\eta} \bmod \mathrm{PR} \\ \mathrm{Plain} &= \mathrm{Cipher}^{d} \bmod \mathrm{PR} \end{aligned} \tag{14}$$

4 仿真实验与结果

4.1 实验环境设置

选择 NSL-KDD 数据集作为实验训练集，训练集中包含 10 000 条左右的特征数据记录，涵盖 DoS、DDoS、U2R、R2L、Probing 等类型的异常数据流量，经由 Zigbee 协议将其输入至无线传感网络的簇节点。基于 matlab2022a 仿真软件系统嵌入时间戳马尔可夫模型，将嗅探捕获的网络数据包流量依据状态转移概率，分割数据字段为多个小的数据块序列，并利用 PCA 主成分分析法对多维网络数据降维、排列为标准化特征值。

基于 FWA-PSO 联合算法的无线传感网络异常流量监测中，设定粒子群烟花数为种群大小的 5%~10%、爆炸火花总数为种群大小的 2 倍，爆炸半径为网络数据特征权重范围 20%。在此基础上，按照时间窗口提取无线传感网络的异常流量序列，由 FWA-PSO 联合算法在搜索空间范围内对数据分段作出粒子群搜索、粒子位置和速度迭代，依据最大适应度函数值保留火花粒子，分别完成异常数据流量不同特征类的全局寻优分析，实验结果如表 1 所示。

表 1 仿真实验结果

	训练集 / 条	AP/%	FNR/%	*F*-measure
FWA-PSO 粒子群联合算法	正常数据 7879 DoS 攻击：410 U2R 攻击：238 R2L 攻击：546 Proing 攻击：927	95.28	0	0.96
CNN 卷积神经网络算法	正常数据 7833 DoS 攻击：403 U2R 攻击：247 R2L 攻击：532 Proing 攻击：985	83.64	4.35	0.79

4.2 实验结果分析

选用适应度函数衡量算法的检测准确率，预先设定粒子群优化最大迭代次数为 100 次，在 t+Δt 时间内通过 FWA 烟花算法对火花粒子进行爆炸和变异操作，得到网络异常数据特征检测的目标函数变化值如图 1 所示。

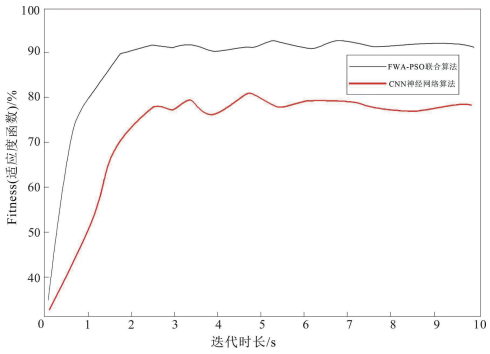

图 1 基于 FWA-PSO 算法的无线传感网络异常流量监测的适应度值

根据表 1、图 1 的仿真实验结果可得，无线传感网络中正常流量、异常入侵流量数据检测的时序概率匹配，由用户基于 HTML 网页对无线传感网络异常数据流量作出预处理、

（下转第 122 页）

图 8 批量 QoS 检查结果

可以看到，第 1 条 QoS 检查通过；第 2 条因 QoS 策略表中没有源地址为 1.0.1.2 的条目，故检查不通过；第 3 条因需求 QoS 策略中限速为 64，而交换机配置的策略表中没有该限速设置，故检查不通过。

5 总结

为了实现交换机 QoS 策略的快速核对，进行了交换机 QoS 策略配置一致性检查方法研究。实现了两种远程连接交换机方式，获取交换机 QoS 策略的配置信息。通过设计不同的正则表达式，匹配提取 QoS 策略中的源地址、目的地址、目的端口号、DSCP 优先级、限速等元素数据，构建并填充 QoS 策略表。将用户需要核对的 QoS 策略逐条或批量地输入系统，通过与 QoS 策略表内容进行比对，即可得到检查结果。结果以可视化的方式呈现给网管人员，能够直观、清晰地掌握 QoS 配置情况。

参考文献：

[1] 陈立家，周为，吴小红，等．面向云航海模拟器网络的 QoS 保障算法研究 [J]. 中国舰船研究 ,2024,19(S2):204-215.
[2] 叶舟宇，姜家文．基于 eNSP 的拥塞与 QoS 仿真实验设计与分析 [J]. 现代计算机 ,2024,30(21):175-178.
[3] 魏德宾，李婧，潘成胜．基于 SDN 的卫星网络端到端 QoS 类映射研究 [J]. 计算机仿真 ,2024,41(7):55-60.
[4] 李岩．面向软件定义移动自组织网络 QoS 的研究与仿真平台实现 [D]. 北京：北京邮电大学 ,2024.
[5] 王张煜．面向 QoS 需求的网络流量调度与整形方法研究 [D]. 南京：南京信息工程大学 ,2024.
[6] 王竞舟．云泛在场景下 QoS 保障与成本优化的流量调度研究 [D]. 合肥：中国科学技术大学 ,2024.
[7] 夏裕涛．确定性网络的多 QoS 路由算法研究 [D]. 杭州：浙江大学 ,2023.
[8] 褚开锋，邓大鹏，程吉．基于 Diffserv 的 QoS 策略在 IP 承载网的应用探析 [J]. 长江信息通信 ,2023,36(1):93-96.

【作者简介】

苟建国（1990—），男，甘肃白银人，硕士研究生，研究方向：计算机和通信网络。

（收稿日期：2025-04-08 修回日期：2025-10-27）

（上接第 118 页）

寻优迭代训练，在 $t+\Delta t = 2\sim3$ s 时间内即可完成特定类的数据分段异常流量检测，将其与测试用例的正常数据字符做出检测匹配，对于不同特征类型异常入侵数据流量的检测精度值达到 95.28%、检测漏报率为 0，均优于 CNN 卷积神经网络算法的迭代训练结果，具有良好的数据帧跟踪效率和检测准确率，可被用于不同场域下的异常流量访问检测控制操作。

5 结语

随着大数据及云计算技术的飞速发展，无线传感网络在国内被广泛用于智能交通系统、智能家居系统和农业生产监测等领域之中。为解决无线传感网络通信的异常流量入侵访问问题，提出基于 FWA-PSO 联合优化算法、PCA 主成分分析法的多模态融合技术，将其应用至海量异构节点通信的数据分段、特征降维之中，在滑动时间窗口作出异常数据流全局寻优检测、粒子群学习更新，为构建更加安全可靠、高效互联的网络环境奠定坚实基础。

参考文献：

[1] 苗长云，郭芮，李杰．基于节点剩余能量和位置的无线传感网络分簇方法 [J]. 天津工业大学学报 ,2023,42(2):61-66.
[2] 杨华，耿烜，孔宁．一种采用 Dueling-DDQN 算法的无线网络 MAC 协议 [J]. 北京邮电大学学报 ,2023,46(3):25-30.
[3] 邵瑞雪，田秀霞．智能电网中基于 MQTT 协议的 ABAC 访问控制方案 [J]. 计算机应用研究 ,2022,39(11):3436-3443.
[4] 应晨铎，伍益明，徐明，等．欺骗攻击下具备隐私保护的多智能体系统均值趋同控制 [J]. 自动化学报 ,2023,49(2):425-436.
[5] 王悦，贾新春，游秀，等 .DoS 攻击下基于多率采样的多智能体系统安全一致性 [J]. 控制理论与应用 , 2022, 39(10): 1890-1897.
[6] 张翊，王瑞杰，王远航，等．基于卷积神经网络的指挥控制专网 DDoS 检测方法 [J]. 舰船电子工程 ,2023,43(5):115-118.

【作者简介】

武少鹏（1986—），男，内蒙古呼和浩特人，本科，工程师，研究方向：密码通信。

（收稿日期：2025-04-21 修回日期：2025-11-11）