无线传感网络用户访问安全等级盲检测研究

陆 洁[1]
LU Jie

摘 要 无线传感网络中的用户行为和环境条件会随时间变化，导致特征分布发生变化，即产生特征漂移问题，导致用户访问安全等级盲检测精度下降，为此，文章提出了基于K-means聚类算法的无线传感网络用户访问安全等级盲检测方法。初步确定无线传感网络用户特征，经过去噪处理后实现无线传感网络用户特征选择，降低特征漂移对于检测结果的不利影响。在确定用户特征后，K-means算法从界定覆盖盲区的边界出发明确用户访问时的安全级别，从而实现无线传感网络用户访问安全等级盲检测。由实验结果可知，该方法的无线传感网络用户访问安全等级盲检测精度高，且能够保证无线传感网络用户访问安全性。

关键词 无线传感网络；用户访问；安全等级；盲检测；K-means聚类

doi：10.3969/j.issn.1672-9528.2025.09.025

0 引言

随着大数据时代的来临，无线传感网络中的大数据访问面临着前所未有的安全挑战。无线传感网络用户访问安全等级盲检测方法能够在不依赖于具体攻击模式或特征库的前提下，通过综合分析用户访问行为、网络流量特征等多维度信息，实现对用户访问安全等级的动态评估，这种方法不仅能够提升网络对未知攻击的防御能力，还能有效应对复杂多变的网络环境，保障网络运行的安全性和稳定性[1]。

针对用户访问安全等级检测这一问题的研究已经取得了一定的进展，例如文献[2]提出了基于上下文知识增强型Transformer网络的检测方法。利用Transformer网络强大的序列建模能力，结合上下文知识增强机制，实现对用户访问安全等级的精准评估与检测。然而，面对大规模无线传感网络存在的特征漂移问题其检测结果存在偏差；文献[3]提出了基于邻域量化容差条件熵增量式更新的检测方法。该方法基于邻域量化容差条件熵，通过增量式更新机制，动态捕捉无线传感网络用户访问行为的模式变化，实现对用户访问安全等级的盲检测。然而，该方法在面临大规模、高维数据时难以确定用户特征，导致检测结果精度下降；文献[4]提出了基于SSAE-ResNet的检测方法。该方法融合堆栈自编码（SSAE）与残差网络（ResNet）优势，深度挖掘用户特征，在确定用户特征过程中，难以实现对于特征分布的精准描述，导致检测结果存在误差。

针对这些问题，无线传感网络用户访问安全等级盲检测作为一种新型的安全检测技术，通过评估用户访问行为，能够实现对用户访问安全等级的动态评估和预警。

1 无线传感网络用户特征选择

在无线传感网络中，原始数据往往包含大量的冗余信息和噪声，直接用于安全等级盲检测不仅计算量大，而且可能导致误判。通过特征选择，可以从原始数据中提取出具有代表性的、对安全等级判断有重要意义的特征，从而简化后续处理流程，提高检测效率和准确性。无线传感网络用户特征提取表式为：

$$x_i=\gamma E\iota\sin\left(2\pi t_i\right)\left(\eta_a-\eta_b\right)+\varphi\left[\left(1+\lambda\right)\left(t_i-t_0\right)\right] \quad (1)$$

式中：γ表示特征值相对于某一基准的最大偏移量[5]；E表示无线传感网络接入节点属性值[6]；ι表示网络环境噪声；t_i、t_0分别表示当前访问时刻和初始访问时刻[7]；η_a、η_b分别表示用户特征序列和节点解析序列[8]；φ表示用户特征相位分布值；λ表示特征偏移系数。

将已计算得到的用户特征序列x_i输入此滤波器中进行卷积运算，输出经过去噪处理的特征序列，可得到去噪后的特征序列：

$$x_i'=\gamma E\iota x_i\sin\left(\eta_a-\eta_b\right)+f\left(a_i\right) \quad (2)$$

式中：$f(a_i)$表示低通滤波器函数[9]。

将无线传感网络中经提取及去噪处理的用户特征作为盲检测的特征依据，以此保证检测精度与效率。

1. 宿迁幼儿师范高等专科学校 江苏宿迁 223800

2 无线传感网络用户访问安全等级盲检测

依据此前所选择出来的无线传感网络用户特征，结合K-means算法从界定覆盖盲区的边界出发明确用户访问时的安全级别，达成无线传感网络中用户访问安全级别的盲检测。为此，提出了基于K-means的盲检测方法，步骤如下：

步骤1：设定统计论域，论域包含 n 个节点，每节点有 m 个行为特征。

步骤2：无线传感节点间的感知共性会随实际距离增大而增强，通过计算各样本至聚类中心的距离，归类至最近聚类，记录距离与数组，并标记数组最大值。

步骤3：通过构建无线传感网络感知模型，可确定感应半径是节点至感应边界的距离。在无线传感网络中，界定的边界节点弧代表覆盖盲区的边界，相应方向角则为盲区角。

步骤4：更新所有样本平均值。

步骤5：循环执行步骤5，直至聚类中心稳定或达到预设迭代次数。

步骤6：将无线传感网络中导致用户访问不安全的原因分为3种：数据重要性、脆弱性及威胁性。

（1）数据重要性：在无线传感网络中，数据重要性和所面临的潜在风险各不相同。因此，有必要根据数据重要性进行分级处理，分级越高，意味着这些数据越为关键和重要。设 H 代表数据重要性，分级为：H_1 代表一般重要性；H_2 代表重要性；H_3 代表较为重要性；H_4 代表非常重要性；H_5 代表极其重要性。

（2）脆弱性：在无线传感网络中，网络存在漏洞，设 C 代表数据脆弱性，分级为：C_1 代表一般重要性；C_2 代表重要性；C_3 代表较为重要性；C_4 代表非常重要性；C_5 代表极其重要性。

（3）威胁性：所有攻击均通过行为体现，将用户异常、违规及蓄意破坏行为视为威胁表现。设 K 代表数据威胁性，分级为：K_1 代表轻微影响；K_2 代表影响较小；K_3 代表中等严重；K_4 代表高度严重；K_5 代表极其严重。

步骤7：标记用户安全状态，不安全则拒绝访问。结合访问请求与用户信任级别制定控制策略，用户可信则允许访问。综合上述风险因素，确定盲检测的用户访问安全等级：

$$G_m = W\left(\frac{H_m \cdot C_m \cdot K_m}{x'}\right), m = 1,...,5 \tag{3}$$

式中：$W(\cdot)$ 表示盲检测函数。

结合公式对用户访问安全等级进行划分，具体为：G_1 表示低级；G_2 表示中低级；G_3 表示中级；G_4 表示高级；G_5 表示最高级。

通过上述步骤可获取盲检测结果，能够实现对用户访问的安全限制，避免个别用户出现随意访问行为，以此保证无线传感网络安全。

3 实验

3.1 实验过程

在一个覆盖面积为1 km^{2}的无线传感网络区域中，部署了数百个传感器节点，用于监测电力通信数据。在2023年10月15日下午3时，某用户尝试访问无线传感网络，以获取最新的通信数据。采用MATLAB 2020B软件，在150 km×150 km的无线传感网络区域内，随机分布传感器节点。由于网络中的部分传感器节点因长时间暴露在恶劣环境中而失效，导致某些关键区域的数据无法被采集和传输，这些失效的节点形成了一个数据空洞，即覆盖盲区，使得该用户无法获取这些区域的实时监测数据。无线传感网络节点分布如图1所示。

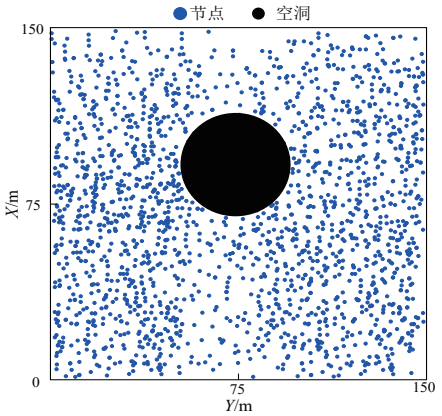


图1 无线传感网络节点分布

实验环境相关参数如表1所示。

表1 实验环境相关参数

参数	数值
节点感知半径	20 m
节点初始能量	3 500 J
网络传输速率	0.5 Mbit/s
工作频率	2.5 GHz
通讯协议	Zigbee

无线传感网络体系中包含总计7 200条数据记录，其中涵盖了1 500条内部攻击事件数据以及2 500条非授权访问行为数据，这些数据条目各自独立，相互之间不存在逻辑依赖关系，确保了各个数据子集在虚拟网络环境中的隔离性，即单一虚拟网络发生故障时，其余虚拟网络仍可保持正常运行。为了分析这些数据，采用了Monte Carlo模拟环境，通过50轮次的随机抽样从这些数据中提取出具有代表性的统计结果。原始无线传感网络用户特征及其特征选择结果分别如表2~3所示。

表 2 原始无线传感网络用户特征

特征组成	特征描述
用户需求	数据采集需求
	应用场景
	服务质量需求
	用户界面偏好
设备特性	传感器类型
	设备功耗
	设备数量
	设备外观
网络环境	网络覆盖范围
	环境干扰
	移动性
	部署时间
用户属性	技术使用特征
	基本信息特征
	行为特征
	经济特征
	社会特征

表 3 无线传感网络用户特征选择结果

特征组成	特征描述
用户需求	数据采集需求
	应用场景
	服务质量需求
设备特性	传感器类型
	设备功耗
	设备数量
网络环境	网络覆盖范围
	环境干扰
	移动性
用户属性	技术使用特征
	基本信息特征
	行为特征
	经济特征
	社会特征

分析表 2~3 中数据可知，经过特征选择后，去除了主要影响用户的主观体验或设备选择，但对网络核心功能影响较小的特征，从而为后续的无线传感网络用户访问安全等级盲检测奠定坚实的基础。

无线传感网络用户访问安全等级实际结果和盲检测结果如表 4 所示，无线传感网络用户访问安全等级盲检测结果与实际结果具备一致性，说明该方法具备较高的检测精度。

表 4 无线传感网络用户访问安全等级盲检测结果

用户编号	实际结果	检测结果
101	中级	中级
102	中低级	中低级
103	最高级	最高级
104	中级	中级
105	高级	高级
106	中级	中级
107	高级	高级
108	中级	中级
109	中低级	中低级
110	中低级	中低级

3.2 对比实验结果分析

在连续 90 s 内通过模拟拒绝服务攻击和嗅探攻击两种模式，分析用户访问安全情况，如图 2 所示。

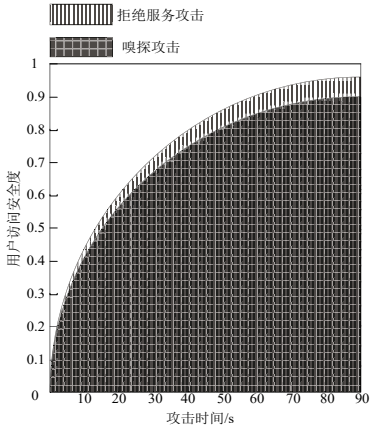
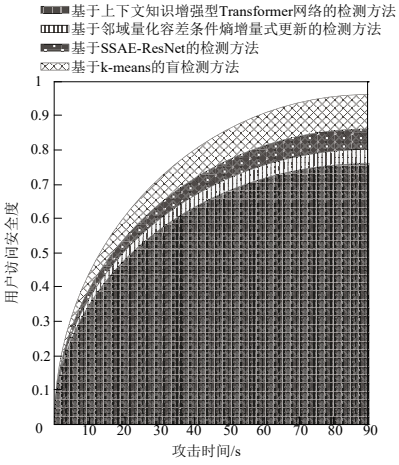


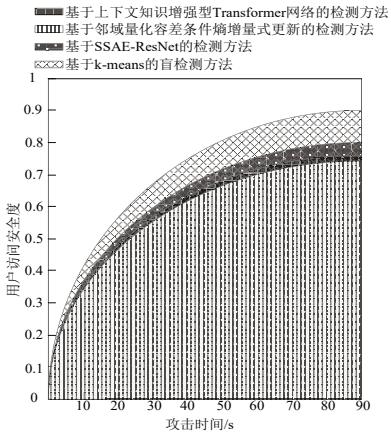
图 2 两种攻击模式下用户访问理想安全性指标

由图 2 可知，在拒绝服务攻击模式和嗅探攻击下，随着时间增加，用户访问安全度增大，最大值分别为 0.96、0.9，通过这种方式能够最大程度上保证无线传感网络用户访问安全性。

使用基于上下文知识增强型 Transformer 网络的检测方法、基于邻域量化容差条件熵增量式更新的检测方法、基于 SSAE-ResNet 的检测方法、基于 K-means 的盲检测方法，对比分析用户访问安全度，对比结果如图 3 所示。



（a）拒绝服务攻击



（b）嗅探攻击

图 3 不同方法用户访问安全程度对比分析

由图 3（a）可知，检测结果中使用基于上下文知识增强型 Transformer 网络检测方法检测的用户访问安全程度最低，其最大值为 0.76，其次是基于邻域量化容差条件熵增量式更新的检测方法、基于 SSAE-ResNet 的检测方法，对应的安全程度最大值分别为 0.8、0.86，均与实验指标不一致。而使用基于 K-means 的盲检测方法，检测的用户访问安全程度最高，其最大值为 0.96，与实验指标一致。由图 3（b）可知，只有使用基于 K-means 的盲检测方法，检测的用户访问安全程度与实验指标一致，对应的最大值为 0.9%。使用基于邻域量化容差条件熵增量式更新的检测方法与实验指标相差最大，其次是基于上下文知识增强型 Transformer 网络检测方法、基于 SSAE-ResNet 的检测方法，对应的最大值分别为 0.76、0.74。

为了进一步验证所研究方法的高效性，使用不同方法对比分析检测准确率，对比结果如图 4 所示。

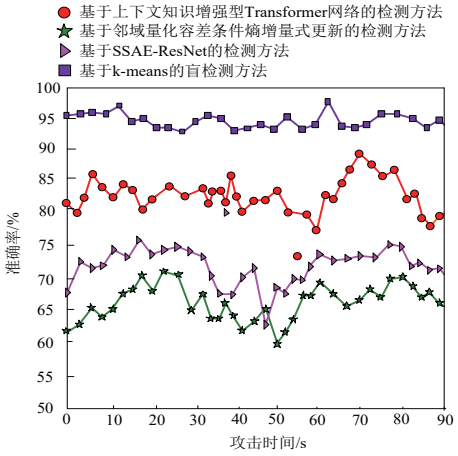


图 4 不同方法的检测准确率对比分析

由图 4 可知，使用基于 K-means 的盲检测方法的检测准确率始终在 93 以上，且准确率曲线变化较为稳定，始终位于实验对比方法上方，说明该方法的检测精度高，可以在实际中得到进一步应用。

4 结语

无线传感网络构成了一种高度功能化的无线覆盖网络，具备节点组织有序、通信稳定可靠及自我联通的特性，为了确保无线传感网络不受覆盖盲区限制，同时保障用户访问的安全性，引入了一种基于 K-means 聚类算法的用户访问安全等级盲检测技术。该技术首先对无线传感网络用户特征进行筛选，随后运用 K-means 算法，从数据重要性、脆弱性及威胁性等维度对用户访问进行安全等级划分，进而实现盲检测功能。实验验证显示，该方法不仅显著提升了用户访问的安全性水平，还确保了检测精准度，这一成果有力地证明了所提方法能有效增强无线传感网络中节点通信效能，并大幅度减轻盲区对用户访问带来的不利影响。

参考文献：

[1] 陈振峰，陈纪鑫．基于 Voronoi 图的无线传感网络覆盖盲区检测方法 [J]. 传感技术学报 ,2024,37(1):136-141.

[2] 张亚洲，和玉，戎璐，等．基于上下文知识增强型 Transformer 网络的抑郁检测 [J]. 计算机工程，2024, 50(8):75-85.

[3] 骆公志，侯若娴．基于邻域量化容差条件熵增量式更新的网络入侵检测方法 [J]. 数据采集与处理，2024, 39(1):181-192.

[4] 王海珍，崔志青，闫金鋆．基于 SSAE-ResNet 的入侵检测模型的研究 [J]. 计算机仿真 ,2024,41(9):314-318.

[5] 陈力夺，温蜜，张研博．一种基于两级 K- 异步联邦学习的隐私保护入侵检测方案 [J]. 计算机应用研究，2024, 41(11): 3471-3476.

[6] 苗新亮，常瑞，潘少平，等．可信执行环境访问控制建模与安全性分析 [J]. 软件学报，2023, 34(8):3637-3658.

[7] 刘凯，王恒．智慧网络大规模未知访问源的安全性预警研究 [J]. 计算机仿真 ,2024,41(8):404-407.

[8] 滕志军，王幸幸，刘佳林 .WSN 中融合优选机制和变螺旋策略的自适应黑洞覆盖策略 [J]. 传感技术学报，2024, 37(7): 1258-1264.

[9] 吴润发，鄂振伟，付东，等．基于声表面波技术的变压器无线温度传感器信号处理方法 [J]. 压电与声光，2023, 45(1): 82-88.

【作者简介】

陆洁（1980—），女，江苏宿迁人，本科，高级讲师，研究方向：计算机网络安全。

（收稿日期：2025-03-11 修回日期：2025-08-29）