高校无线网络安全态势感知系统的设计与实现

何 琳

（天津医科大学 天津 300070）

摘 要 高校无线网络的普及提高了教学与科研的数字化水平，但也带来了流量异常、用户行为异常和攻击等安全隐患。为应对这些问题，文中设计了一种高校无线网络安全态势感知系统，涵盖数据采集、态势分析、威胁评估和动态响应4个核心模块。经过7天的实地测试，系统在不同场景下表现优异。流量检测准确率为94.2%，用户行为异常检测率为91.2%，威胁评估精度为88.6%，响应时间为120～150 ms。在高频接入和异常流量干扰场景中，系统能快速识别并响应威胁，减少安全事件。测试表明，系统能提升网络安全防护能力，为高校网络管理提供科学解决方案。

关键词： 高校无线网络；安全态势感知；威胁评估；动态响应

中图分类号 TP393

Design and Implementation of Wireless Network Security Situation Awareness System in Universities

HE Lin

（Tianjin Medical University，Tianjin 300070，China）

Abstract The popularization of wireless networks in universities has improved the digitalization level of teaching and research, but it has also brought security risks such as abnormal traffic, abnormal user behavior, and attacks. To address these issues, thispaper proposes a university wireless network security situational awareness system, which includes four core modules: data collection, situational analysis, threat assessment, and dynamic response. After 7 days of field testing, the system performed excellently in different scenarios. The accuracy of traffic detection is 94.2%, the detection rate of abnormal user behavior is 91.2%, the accuracy of threat assessment is 88.6%, and the response time is 120-150 ms. In high-frequency access and abnormal traffic interference scenarios, the system can quickly identify and respond to threats, reducing security incidents. Tests have shown that the system can significantly enhance network security protection capabilities and provide scientific solutions for university network management.

Key words University wireless networks，Security situation awareness，Threat assessment，Dynamic response

0 引言

高校无线网络的广泛部署，便利了教学与科研，也带来了中间人攻击、流量劫持等安全威胁。传统安全管理难以覆盖流量监控盲区及复杂用户行为，导致隐私泄露和服务中断。设计有效的无线网络安全态势感知系统成为高校网络安全的关键。本文探讨了系统设计、架构、关键技术及其实际效果，为高校网络安全管理提供了借鉴。

1 高校无线网络环境概况

1.1 高校无线网络部署条件

高校无线网络用户多、设备类型复杂、接入场景广泛（如教学楼、实验室、图书馆），需满足高密度接入与高质量服务需求。当前架构主要依赖无线接入点（AP）与控制器集中管理，并配备认证机制与防火墙，但其开放性与管理复杂性使传统入侵检测等方法难以应对所有安全威胁。

1.2 高校网络安全面临的威胁

高校无线网络具有开放性和接入复杂性，面临着中间人攻击、流量劫持和非法设备干扰等威胁，严重影响了网络稳定性。用户不规范行为（如使用不安全热点、软件漏洞）增加了管理难度，而监控盲区和数据孤岛进一步延迟了威胁检测和响应，影响整体网络安全。

2 主要影响及关键设计原则

2.1 无线网络安全问题的主要影响

无线网络安全问题直接威胁着用户隐私、系统稳定性及高校教学科研的正常进行。隐私泄露可能导致个人资料和研究数据被非法获取，核心业务系统如在线教学平台也可能受到攻击，影响系统性能或中断服务。安全威胁可通过网络扩散形成多点攻击，增加其危害[1]。因此，系统性解决方案在减少安全问题对高校活动的影响上至关重要。

作者简介：何琳（1981—），本科，高级工程师，研究方向为网络安全。

2.2 无线网络安全态势感知系统的设计关键原则

高校无线网络态势感知系统应遵循以下原则。(1)实时性,确保信息的快速获取与响应。(2)可扩展性,支持多设备和场景数据集成。(3)精确性,结合多源数据提高检测精度并控制误报。(4)动态性。采用自适应策略应对复杂威胁。这些原则为高效、安全的态势感知系统提供了基础。

3 高校无线网络安全态势感知系统设计

3.1 态势感知模型的设计

系统包含数据采集、态势分析、威胁评估和响应决策4个模块。数据采集层实时获取无线接入点日志、流量镜像和用户认证信息;态势分析层对流量特征和用户行为进行多层次分析;威胁评估层基于异常检测和风险量化,动态识别潜在威胁;响应决策层通过动态规则生成和策略配置实现快速自动响应,完整覆盖数据采集、分析和威胁处置,提升高校网络安全防护能力。

3.2 数据采集与仿真分析参数

在流量特征提取中,系统可以提取数据包的协议类型、包长和流量方向等关键维度,特征提取式如式(1)所示:

$$F_i=\frac{\sum_{j=1}^{n}P_j^{type}}{T_{window}} \tag{1}$$

其中,F_i表示在时间窗口T_{window}内的协议$type$的流量总量,P_j^{type}为第j个数据包的大小。该式可以帮助捕获协议特性和流量分布模式,用于进一步检测异常。

基于用户行为分析,定义用户在时间窗口T内的访问序列特征为$B_u=\{S_1,S_2,\cdots,S_n\}$。其中,$S_i$为第$i$次访问的资源路径和访问频率,用户行为异常通过$K$均值聚类算法与历史访问模式的欧几里得距离判断,如式(2)所示:

$$D=\sqrt{\sum_{k=1}^{m}\left(x_k-\mu_k\right)^2} \tag{2}$$

其中,当D超过设定阈值时,判定该用户行为异常。

网络威胁评估基于流量异常检测得分和关联性分析,通过计算威胁等级R_w,如式(3)所示:

$$R_w=\alpha\cdot S_{flow}+\beta\cdot S_{user}+\gamma\cdot S_{correlation} \tag{3}$$

其中,S_{flow}为流量异常评分,S_{user}为用户行为异常评分,$S_{correlation}$表示攻击相关性得分,权重参数α,β,γ根据场景调整,确保综合评估的准确性。

动态响应机制可以生成防护规则,如式(4)所示:

$$R_d=\arg\max_{r\in R}\{E_{impact}(r)-C_{cost}(r)\} \tag{4}$$

其中,$E_{impact}(r)$为规则r的威胁减轻效果评估,$C_{cost}(r)$表示规则实现的资源消耗和响应时间,系统动态选择最大化效果的规则以优化防护策略。

3.3 系统功能阶段划分

高校无线网络安全态势感知系统主要由3个环节组成,即数据采集与预处理、态势感知与威胁评估、响应与优化。数据获取阶段通过无线接入点日志、流量镜像和用户认证信息进行流量过滤与特征提取,构建多维数据集[2]。在态势感知阶段,采用深度学习和图分析进行异常检测和威胁量化。响应阶段结合动态策略与自动化配置,优化防护规则,确保闭环处理,全面保障网络安全。

3.4 数值模拟分析与验证

为了验证系统性能,基于4个关键指标(流量检测准确率、用户行为异常检测率、威胁评估精确性、响应时间)进行数值模拟分析。数据模拟结果如表1所列。由表1可知,系统在常规环境下表现出较高的流量检测准确性和用户行为异常检测率,威胁评估准确率达到90.8%。在异常流量干扰和多设备高频接入场景中,尽管检测指标略降,但仍保持较高水平[3]。系统的平均响应时间为120~150 ms,满足实时响应需求,证明其在复杂网络环境中具有出色性能和威胁检测鲁棒性。

表1 高校无线网络安全态势感知系统仿真测试数据

测试场景	流量检测准确率/%	用户行为异常检测率/%	威胁评估精确性/%	响应时间/ms
正常流量环境	95.4	93.2	90.8	120
异常流量干扰环境	92.7	88.9	85.3	140
用户多设备高频接入场景	90.1	87.5	82.7	150
攻击场景模拟(DNS劫持)	93.8	91.4	88.6	130

4 系统实现的关键技术

4.1 数据采集技术

高校无线网络的数据采集要求全面且实时。系统通过多源数据采集技术集成接入点日志、流量镜像和用户认证信息,涵盖流量方向、协议类型和设备标识等关键特征。采用分布式架构分散采集压力,使用高性能流处理引擎进行数据去噪和特征提取,确保数据质量。智能缓存策略动态调整采样频率,避免流量冲击造成数据丢失。在高频接入环境中,数据完整性和传输效率保持在90%以上。

4.2 态势分析技术

通过深度学习的流量分类模型有效区分正常与异常流量,结合时间序列分析捕捉流量与用户行为变化的动态趋势[4]。图模型建立用户-流量关联网络,挖掘异常模式和多步攻击路径。模拟测试表明,在异常流量干扰下,系统流量检测准确率为92.7%,用户行为异常检测率为88.9%,适用于复杂网络环境。

4.3 威胁评估技术

系统结合聚类算法分析流量特征和用户行为离群点,采用关联规则分析事件间的相关性,通过综合评分公式快速评估风险等级。模拟测试显示,在高频接入和DNS劫持场景下,威胁评估准确率分别为82.7%和88.6%,为响应策

略优化提供支持。

4.4 动态响应技术

动态响应技术通过自动化防护策略迅速制止攻击并优化配置。系统使用自适应策略生成算法，根据威胁等级和网络状态动态调整防护规则，如限制异常设备访问或切换通信通道。实时事件流分析和缓存技术缩短了响应时间，确保系统响应时间在120~150 ms，满足实时防护需求并优化网络性能，保证高密度用户环境的稳定性。

5 控制措施实施效果

5.1 实地测试与现场监测数据

在某高校无线网络环境中，系统的流量检测准确率、用户行为异常检测率、威胁评估精确性和响应时间等关键性能指标进行了为期7天的实地测试。数据采集设备安装在校园核心交换机和主要无线接入点（AP），涵盖宿舍、教学楼、图书馆等高密度流量场景。不同时间点的核心性能指标如表2所列。现场监测数据表明，系统在正常流量环境下保持较高性能，在高峰时段如下午测试中，性能指标略有波动，但整体稳定，响应时间始终控制在150 ms以内，满足实时性需求。

表2 实地测试监测数据

时间点	流量检测准确率/%	用户行为异常检测率/%	威胁评估精确性/%	响应时间/ms
第一天-上午	94.3	92.1	89.5	125
第一天-下午	95	91.8	88.9	130
第三天-上午	93.5	90.4	87.6	140
第三天-下午	92.8	89.7	86.2	150
第五天-上午	95.2	93	90.2	120
第五天-下午	94.7	92.6	89.9	125
第七天-上午	93.9	91.5	88.3	135

5.2 实施效果评价

监测数据分析表明，该系统在多个维度上表现优异。流量检测准确率平均超过94%，用户行为异常检测率始终保持在90%以上，确保在高密度环境中性能稳定。威胁评估准确率达到88.6%，证明系统在多源数据分析和威胁量化方面可靠。响应时间控制在120~150 ms，验证了动态响应技术的高效性。与传统方法相比，本系统提高了态势感知和威胁响应效率，减少了误报漏报，且对网络正常运行影响最小，实现了高效、实时的安全防护。

6 结语

本文设计并实现了高校无线网络安全态势感知系统，从数据采集、态势分析、威胁评估到动态响应进行全流程安全防护。现场测试显示，系统流量检测准确率超过94%，用户行为异常检测率和威胁评估精度分别超过90%和88.6%，响应时间为120~150 ms。结果表明，该系统具备实时感知和快速响应功能，有效提升了网络安全性，减少安全事件。未来，研究将优化威胁评估和响应策略，以适应更复杂的网络场景。

参考文献

[1] 潘艳艳，王可心.高校无线数字化校园网络安全防护方案[J].数字技术与应用，2024，42(10)：77-79.

[2] 干俊.无线网络安全防范措施在高校网络中的应用[J].电子技术与软件工程，2022(17)：4.

[3] 任如广.高校无线网络的优化与安全管理研究[J].网络安全技术与应用，2022(1)：82-83.

[4] Zhang M，Guo J，Chen S. Safety management for laboratory renovation and expansion in colleges and universities based on the joint review mechanism[J]. Experimental Technology and Management，2024，41(4)：215-221.