高校无线数字化校园网络安全防护方案

■ 潘艳艳 王可心

随着移动互联网、物联网和云计算的快速发展，高校正在全面推进校园数字化转型，构建智能化的校园网络环境。据教育部统计，截至 2023 年 6 月 15 日，全国高等学校共计 3072 所。随之，高校无线网络用户数量呈现爆发式增长。面对庞大的用户规模和智能终端接入，高校无线网络不仅需要满足日益增长的接入需求，还需要确保网络及数据安全，进而防范各种新型网络攻击手段，保障正常的教育教学秩序。因此，加强无线数字化校园网络安全防护研究，制订切实可行的安全防护方案，对于高校网络安全建设至关重要。

一、高校无线网络的特点

（一）用户群体庞大且多变

高校校园网是一个庞大而开放的网络环境，容纳了来自五湖四海的师生，构成了一个多元化、高度流动的用户群体。不同年龄阶段、不同学科专业的师生，在网络使用习惯和需求上都存在明显差异 [1]。例如，年轻学生对网络娱乐和社交网络有着更高的要求，文科师生对网络获取知识资源的便捷性更为关注。新生与老生的持续交替、助教和访问学者的不定期进出、学校举办大型会议和社会培训的情况时有发生，这些都使得高校校园网用户群体处于一种动态变化的状态。这种用户结构和使用特征的多样性，对于无线网络的规划建设、运行维护、安全防护，提出了更高的挑战。

（二）承载业务种类多样

高校无线数字化校园网络需要承载多种多样的业务，这是其与普通无线网络有所区别的重要特征之一。高校无线数字化校园网络不仅要满足师生上网冲浪、收发电子邮件等基本需求，还需要支撑各类教学和科研活动。例如，高校无线数字化校园网络常常需要传输大量的视频资料，以满足多媒体辅助教学的需要；校园会议、讲座等场合也经常需要提供无线网络现场直播服务。高校无线数字化校园网络还需要支持移动办公、远程教育、电子化校园一卡通系统等众多服务，以适应校园信息化建设发展的新要求。总体来说，高校无线数字化校园网络所承载的业务种类繁杂，对网络的带宽、时延、可靠性等各方面都提出了更高的要求，因此高校无线数字化校园必须有完善的解决方案予以应对。

（三）网络覆盖范围广泛

高校无线网络的覆盖范围广泛，这一点与传统的有线网络形成了鲜明对比。有线网络主要局限于办公区和教学区等核心区域，而无线网络则需要覆盖整个校园的各个角落，包括教学楼、图书馆、食堂、宿舍区、操场等多个功能区。由于校园占地面积广阔、地形多样，再加上建筑物的屏蔽效应，因此校园要实现无线网络的全覆盖并非易事。高校需要在整个校园内部署大量的无线接入点，并合理规划接入点的位置和覆盖范围，才能确保无线网络信号到达各处，为师生提供无缝的网络接入体验。由于接入点数量众多，因此无线网络的部署、运维和优化工作也给网络管理带来了极大的挑战 [2]。

二、高校无线网络面临的安全威胁

（一）无线接入安全威胁

无线接入层是高校无线网络体系中最为脆弱的环节，它直接暴露在空中无线电信号覆盖范围内，面临着诸多安全隐患。首先，无线接入点作为无线网络的基础设施，其硬件本身如果配置不当或存在漏洞，就可能被攻击者利用对其进行控制或破坏。其次，由于无线接入点覆盖范围较广，难免会有无线电波信号泄漏到室外，从而被不经意接入的非法用户监听或窃取数据。再次，在无线网络中，无线数据在空中传输时极为容易被攻击者截获，因此加密措施的实施对于保障数据的机密性和完整性至关重要。然而，现有的无线加密协议，如 WEP、WPA 等均存在一定的缺陷和漏洞，如果无线加密协议配置不当或使用了较为陈旧的加密模式，那么无线数据就极有可能被破解和窃听。尤其在人口密集的校园环境中，无线信号的干扰和重叠更增加了解密的难度。从次，随着无线网络接入的普及，接入无线网络的客户端的设备种类和数量都在快速增长，这无疑加大了无线接入的攻击面。移动终端存在操作系统漏洞、恶意代码感染等问题，因此其一旦接入无线网络就可能导致整个无线网络受到威胁和破坏。最后，现代无线技术如 802.11n/ac 提高了传

输速率，但也扩大了无线电的覆盖范围，这就增加了被非授权接入的风险。

（二）内部网络安全威胁

高校无线网络内部面临的安全威胁不容忽视。病毒、木马、蠕虫等恶意代码对网络和终端进行破坏。这些恶意程序能够利用系统和应用程序的漏洞，在网络中迅速蔓延，窃取敏感数据、破坏程序正常运行，甚至可能被非法人员利用对师生进行勒索或其他违法行为，从而对学校的教学科研工作造成严重阻碍。内部人员的操作失误和违规行为也可能成为网络安全的巨大隐患。由于内部人员对网络安全意识的淡薄或疏忽大意，因此其有可能无意间将系统暴露在危险之中，如误导入木马病毒、误发敏感信息等。更有甚者，一些内部人员或许存在违规操作的恶习，如私自拷贝敏感数据、未经授权扩展系统权限、使用非法软件等，这无疑会为网络安全制造极大的风险隐患。

三、高校无线数字化校园网络安全防护方案设计

（一）无线接入层安全防护

1. 加固无线接入点硬件

首先，加固无线接入点硬件需要选择性能稳定、支持加密认证的无线接入点设备，并使用最新的无线标准和协议。其次，加无线接入点硬件还需要对设备进行防拆解措施，如使用防拆螺丝、加装防拆外壳等，进而避免设备被非法拆卸或植入硬件木马。最后，无线接入点应当安装在安全可靠的位置，防止被人为破坏或非法接触，以确保无线网络基础设施的物理安全。

通过上述硬件加固措施，可以从根本上保障无线接入层的安全性，为无线网络的健康运行提供基础保障 [3]。

2. 合理规划覆盖范围和信号强度

首先，需要根据高校各区域的使用密度与流量需求，对无线接入点的部署位置进行科学配置，防止覆盖重叠或漏洞出现。其次，结合建筑物的结构特征和使用场景，调节每个无线接入点的发射功率与天线方向，使其实现最佳覆盖效果，消除盲区，并避免不必要的无线电污染。最后，还需要持续监测区域内各个节点的实际使用情况，及时发现并修正规划中的不足，实现动态优化。

3. 设置强密码和定期修改

用户设置简单或者常用的密码将极大地提高其被暴力破解的风险，因此必须使用足够复杂、难以猜测的密码以保证其安全。密码应当是包含大小写字母、数字和特殊字符的组合，且长度不低于一定的安全门槛。为了防止密码被窃取或暴露后遭受持续性攻击，高校有必要制定严格的密码修改制度，如每隔一段时间例行修改密码，或者在发生安全事件之后及时进行密码更新。

（二）内部网络层安全防护

内部网络层是高校无线数字化校园网络中至关重要的部分，其安全问题一旦被忽视，后果将不堪设想。因此，为应对内部网络安全威胁，高校需要从以下几个方面着手。首先，需要部署统一的安全管理和监控系统，对内部网络的运行状态进行全方位的监视，及时发现异常情况并采取相应的防护措施。该系统应当具备立体化的架构，包括边界防护、行为审计、风险评估、漏洞扫描等多种功能模块，形成环环相扣、层层把控的安全防护体系 [4]。其次，还需要配备专业的安全管理团队，对系统进行运维，并根据网络运行情况及时调整防护策略。再次，在内部网络中实施端口级别的访问控制和数据加密。具体而言，需要对内部各节点间的数据传输通道设置严格的访问控制权限，只有经过授权的主机和用户才能获取相应的访问权限；对重要数据进行加密传输，以防止被非法窃取。最后，为了确保访问控制和加密的有效性，内部网络需要划分不同的安全域，对具有不同安全级别的业务系统和数据资源进行逻辑隔离，从而最大限度地降低风险。

（三）外部网络层安全防护

1. 部署入侵检测和防御系统

为及时发现和阻止各种网络攻击行为，高校需在网络边界部署入侵检测和防御系统。这类系统通常基于模式匹配、Anomaly 检测、协议分析等技术，能够识别和防御各种已知和未知的攻击行为，如分布式拒绝服务攻击、溢出攻击、端口扫描等。IDS/IPS 系统的安装位置、检测策略、响应方式等都需合理规划和配置。

2. Web 应用防护和邮件防护

高校网络中运行着大量的 Web 应用系统和电子邮件服务，这些服务极易受到各种 Web 攻击和垃圾邮件的影响。为此，高校需要部署专业的 Web 应用防火墙和邮件安全网关，对所有的 Web 流量和邮件流量进行深度内容检测和防护。Web 应用防火墙能够防御 SQL 注入、跨站脚本、文件包含等 Web 攻击行为；而邮件安全网关则能有效过滤垃圾邮件、病毒邮件等有害邮件，保证邮件服务的安全运行 [5]。

3. VPN 远程访问安全加固

为了满足教职员工的远程办公需求，高校网络一般都会开放 VPN 远程访问服务。然而，VPN 服务若配置不当，则极易沦为网络入侵的突破口。因此，高校必须对 VPN 服务器和 VPN 客户端进行全方位加固，包

括使用强密码、启用两因素认证、配置访问控制策略等，以确保 VPN 远程访问的安全性。

4. 数据中心及关键系统加固

高校网络中有许多重要的数据中心和关键业务系统，这些设施的安全至关重要。高校需要对数据中心的物理环境、网络环境、服务器主机等进行全方位加固，确保其网络隔离、访问控制、身份认证、日志审计等安全防护措施到位。高校网络对关键业务系统进行入侵防御测试，并持续修复发现的各类漏洞，从而最大限度地提高其安全可靠性。表 1 是外部网络防护中可能涉及的一些配置参数，可供高校网络进行设置参考。

表 1　外部网络防护典型配置参数

防护设备	防护功能	典型配置参数
IDS/IPS	入侵检测 / 防御	检测规则、告警级别、自动阻断条件等
Web 应用防火墙	Web 攻击防护	检测模式、CC 防护、虚装路径防护等
反垃圾邮件网关	垃圾邮件过滤	RBL 列表、邮件附件控制策略等
VPN 服务器	远程访问控制	加密算法、身份认证方式、访问控制列表等
统一威胁管理设备	综合防护	IPS/IDS、防病毒、UTM 策略等

（四）安全管理及应急响应

1. 制定完善的安全策略和制度

高校应结合实际情况，制定全面的网络安全管理制度，对网络建设、运行维护、安全防护等各个环节作出明确规定。制度应当涵盖访问控制策略、数据备份策略、密码管理策略、日志审计策略、漏洞管理策略等多个方面的内容，并根据新的安全形势和技术发展状况，适时进行修订和完善。高校也需要加强相关制度的宣传和培训，增强全校师生的网络安全意识和操作水平。

2. 组建专业的安全管理团队

高校应配备专业的网络安全管理团队，以负责日常的网络运维和安全防护工作。团队成员不仅需要具备扎实的网络技术和安全防护知识，还需要掌握一定的管理经验和应急响应能力。网络安全管理团队还应定期组织团队培训，使其能够及时了解最新的网络攻击手段和防护技术，并根据实际需求适当扩充团队人员配备。

四、结语

综上所述，高校无线数字化校园网络在提升教学科研水平和校园智能化管理方面发挥着重要作用，但也面临着无线接入、内部网络和外部网络等多方位的安全威胁。建立完善的无线网络安全防护方案对于确保高校网络环境的安全可控至关重要。高校应该从无线接入层、内部网络层和外部网络层全方位对高校无线数字化校园网络加强防护，并建立健全的安全管理制度和应急响应机制，从而为师生提供一个安全可靠的网络学习和工作环境，保障教育信息化的顺利推进。

引用

[1] 朱斌勇.大数据环境下高校校园网络信息安全隐患与防护措施[J].网络安全技术与应用,2024(3):76-78.

[2] 张瑞霞,冯冰洁.高校校园网安全防护建议[J].网络安全技术与应用,2021(10):88-90.

[3] 闫思瑾.高校计算机网络信息管理安全防护问题与策略[J].数字技术与应用,2021,39(6):174-176.

[4] 王宇,王卫东,温占考.网络攻防视角下的高校网络安全防护[J].中国教育网络,2020(12):64-65.

[5] 罗伟.高校校园网络信息安全问题及防护策略探析[J].河南财政税务高等专科学校学报,2019,33(5):88-91.

作者简介：潘艳艳，辽宁大学外国语学院（武圣校区），本科，实验师，研究方向为计算机管理；王可心，辽宁大学外国语学院（武圣校区），研究生，助理实验师，研究方向为图像检测。