高校校园网与运营商5G融合环境下的分层安全管理体系设计

颜杰森

泉州工艺美术职业学院，福建 泉州 362500

DOI: 10.61369/TACS.2025050027

摘　　要： 随着5G技术的飞速发展与广泛应用，高校校园网与运营商5G融合已成为提升高校网络服务质量、满足师生多元化需求的重要趋势。然而，融合环境下网络结构愈发复杂，安全风险点增多，传统的安全管理模式已难以应对。本文针对高校校园网与运营商5G融合环境的特点，深入分析了融合过程中面临的安全挑战，提出了一套分层安全管理体系设计方案。该体系从物理层、网络层、数据层和管理层四个层面进行安全架构设计，通过各层协同联动，形成全方位、多层次的安全防护机制，旨在为高校校园网与运营商5G融合环境提供可靠的安全保障，确保高校教学、科研和管理活动的顺利开展。

关 键 词： 高校校园网；运营商5G；融合环境；分层安全管理；安全体系设计

Design of Hierarchical Security Management System in Integrated Environment of College Campus Network and Operator 5G

Yan Jiesen

Quanzhou Arts and Crafts Vocational College, Quanzhou, Fujian 362500

Abstract: With the rapid development and wide application of 5G technology, the integration of college campus networks and operator 5G has become an important trend to improve the quality of college network services and meet the diversified needs of teachers and students. However, in the integrated environment, the network structure becomes increasingly complex, security risk points increase, and the traditional security management model is difficult to cope with. Aiming at the characteristics of the integrated environment of college campus network and operator 5G, this paper deeply analyzes the security challenges faced in the integration process and puts forward a set of hierarchical security management system design schemes. The system designs the security architecture from four levels: physical layer, network layer, data layer and management layer. Through the collaborative linkage of each layer, it forms an all-round and multi-level security protection mechanism, aiming to provide reliable security guarantees for the integrated environment of college campus network and operator 5G, and ensure the smooth development of college teaching, scientific research and management activities.

Keywords: college campus network; operator 5G; integrated environment; hierarchical security management; security system design

一、高校校园网与运营商5G融合模式概述

虽然传统的校园网主要是建立在有线网和Wi-Fi上，能满足教学及工作基本需要，但在带宽、时延和移动性等方面存在一定的局限。随着高校信息化工作的深入推进，智慧校园项目建设不断深化，在线直播类课堂教学、VR/AR教学实验、大量物联网设备的连接等使得网络性能需求进一步提高[1]。而5G网络的发展为高校解决了诸多问题提供了解决方案，其高速特性可以保证高清视频流的传输和大型文件的快速下载；低延时特性满足了实时交互类应用的需求；而超大连接能力可以满足大量物联网设备的连接。电信运营商已经建立了较为成熟的5G网络架构并具有较为丰富的运营经验，因此，高校与电信运营商合作推进校园网与5G的融合，可以扬长避短，极大地提升校园网服务能力。

学校内部网络与移动运营商提供的5G服务有着不同类型的整合方式，常用的几种方式如下：第一种是混搭式接入方案，意为校内的既有校园网络又有移动运营商的5G网络，通过核心网门户

基金项目：福建省中青年教师教育科研项目（科技类）课题《高校校园网与5G安全融合应用技术研究》，课题编号：JAT232034，主管部门：福建省教育厅。

作者简介：颜杰森（1977.12—），男，汉族，泉州工艺美术职业学院，网络与信息管理中心高级实验师，主要从事网络信息安全与教育信息化的研究。

使得两者可以互联起来并且供学生随意选择使用什么样的途径接入网络；第二种为承载网络融合方案，利用移动运营商提供的高效5G承载技术优势提升学校网络的带宽效率；第三种为共建共享方案，此种方案需要学校以及移动运营商共同投资构建校园5G基础设施，如无线电塔或是机房等，彼此共同享用基础设施的使用权并且共同管理维修，每种整合方案都有自身特点和适用范围，学校在选择何种整合方案时需要综合考虑学校网络需求、财务规划、技术能力等各种因素，找到与实际情况最匹配的整合解决方案[2]。

二、高校校园网与运营商5G融合环境下的分层安全管理体系设计

（一）物理层安全设计

物理层是网络的安全底线，其稳定程度将影响网络的安全与否。构建物理层安全，在高校校园网与5G运营商的融合网络中，其安全物理层设计主要包括以下内容。

1. 网络设备安全防护

针对内网设备，如智慧一体机、交换机、服务器、安全防护设备等，要采取严密的物理防护措施，如将内网设备放置在具有良好防盗、防火、防水、防雷等物理防御数据中心，该机房应采取全天候门禁监控措施，非授权人员不允许进入；定期对设备进行巡检和维护，具体包括检查设备运行情况、端口连接情况等，及时发现并解决设备问题和隐患；对设备进行设置高强度的登陆密码，而且定期更新，防止非授权人员擅自进入设备。

2. 传输介质安全保障

结合环境下，数据通讯的路径主要存在于有线与无线两种媒介中，对于有线通讯媒介，包括光缆、电缆等，高校要做好布线维护、保护管理等工作，以防止线路被破坏、被监听，在定期检查的同时确保线路的有效与安全。而对于无线通讯媒介，虽然5G网络已经采用了最先进的安全加密技术，但同样要完善对应的无线信号覆盖区域等管理工作，避免信号外溢，避免未获允许的设备私自接入5G网络[3]。

3. 环境安全控制

从机房设备角度，如正常运行还主要取决于其所在的机房环境中的温度、湿度、电压等。所以，需要建设一个监测设备的环境监控系统，跟踪环境监测指标，并在监测到的异常情况时，触发警报与相应的调整措施。同时为了满足机房防火的义务，设置一定的消防设备，并对其实施定期检查、维护等保持性能完好有效。

（二）网络层安全设计

数据传输是融合环境中的一个核心环节，网络层的安全性关系到数据传输的安全性，即传输时的数据保密性、传输后的完整性及有效性。网络层安全设计主要包括网络拓扑设计安全、协议安全及访问控制等几个方面。

1. 合理规划网络拓扑结构

网络设备内部配置网卡，多种网络拓扑结构直接影响着内部网络，因此企业在进行信息化构建时，要合理搭建网络拓扑结构，在配备网卡时要尽可能匹配不同类型的网卡，并对设备进行引导、记录和保存[4]。

构建层次型网络结构，在整个整合环境中要将网络分为三个区：核心、集中和接入。核心区主要用于快捷地进行通信，采取双机冗余备份的模式来提升网络的可靠性；集中区则主要用于集中信息的传递和交换，并实现了对接入区的控制及管理；接入区是放置各类终端的区域，因此接入区采取了端口隔离、VLAN的隔离等措施，避免不同终端发生未被授权的访问行为。优化后的网络结构能够降低网络风险、增加网络的稳固与可靠性。

2. 加强协议安全防护

在一体化的环境下，高校往往要使用一些网络协议，比如TCP/IP、5G协议等，但是由于一些网络协议自身可能存在的安全隐患，也可能容易遭到黑客的攻击。所以为了防止出现这样的情况，高校应该定期对这些协议进行安全审核，从而快速地检测并修补漏洞。而且，可以借助加密技术保护网络协议，比如使用IPsec协议对IP数据包进行加密、校验从而保证传递数据的机密性和完整性。对5G而言，则应该加强对其信令协议和用户面协议的防护，预防发生信令攻击和篡改数据事件的发生。

3. 实施严格的访问控制策略

通过部署安装防火墙、入侵检测系统（入侵防御系统—IDSidps）等防御装置严格监控网络接口。其中防火墙按照预先设定的安全政策筛选入网或出网的信息流来拦截访问非许可访问；IDS不断监测网络中的异常事件并能随时向管理员发出警告；IPS是在IDS的基础上，能主动拦截异常信息流。同时采用如802.1X验证、MAC地址绑定等手段对所有的网络设备登入过程进行严格的身份验证和授权许可，仅获得审批的设备方可接入[5]。

（三）数据层安全设计

数据是高校的主要资产，在整合环境中数据的产生、传播、存储、应用均更加频繁、更加复杂，数据安全性面临严峻考验。数据层的安全设计主要是数据加密、数据备份与恢复以及数据访问控制。

1. 数据加密

针对融会贯通于系统中的重要资讯，例如教育资源资料、教职工和学生的个人信息资料等，需要密码学技术进行确保[6]。在发送这些资料的过程时，可使用SSL/TLS等加密技术对资料实施加密操作，避免资料在传输的环节发生监听或篡改；对资料存储的过程中，可采用存储加密的方式来对资料实施加密，例如利用硬盘加密、库的加密等操作，从而确保了资料在存储的环节中的保密性。除此之外，要注重密钥管理工作的落实，建立相关的密钥生成、分发、存储与销毁流程，避免密钥泄露的可能性。

2. 数据备份与恢复

高校应该建立完备的备份系统，并经常实施重点数据的备份工作。可采用各类磁盘、磁带或者是云存储为备份载体，并应该保管和维护这些备份器具以避免其发生丢失或者损坏。高校应该定期检测备份文件的恢复功能以确保备份资料保持完备性和可用性。高校在遭受数据丢失或者破坏之时可运用这些备份资料及时

地进行数据恢复，以此将数据的丢失概率降到最小[7]。

3. 数据访问控制

高校需要建立严格的获取信息管控机制，根据不同用户权限、身份限制信息获取渠道，通过基于角色访问控制模式（RBAC）对用户进行角色划分并赋予各自权限，只有符合其权限的用户才能访问相应内容。另外，对于获取信息的过程做好详细记录，包括用户登录时间、访问的资料内容以及进行的操作动作等等，这样一旦有数据保护问题出现时可以追溯到相应原因。

（四）管理层安全设计

管理层是融合环境安全管理的核心，通过对安全规则流程体系的建立完成对整个融合环境的安全监测与协调。管理层的设计安全主要包括安全管理制度、安全管理人员及安全管理紧急响应等[8]。

1. 建立健全安全管理制度

实施安全管理制度建设，真正把安全第一的方针落实到位，建立健全安全管理体系，有效实现安全生产，强化安全生产管理，加强宣传教育与培训，使员工能够熟悉应急避险的方式。在特定的工作中，要实时加强员工安全意识培训，确定各个岗位在施工时必须穿着统一工作服与统一鞋子，进而开展危险环境下的安全操作培训。高校要依据融合的空间特征和安全需求来制定系列安全管理政策和规范，如网络安全管理规范、信息安全规范、设备管理规范、应急预案等，明确各个部门及个体的安全职责，规范网络使用和管理流程，确保安全管理工作有章可循。同时要强化安全管理的政策宣传和教育，增强师生的安全意识和落实能力。

2. 加强安全人员管理

高校需要成立专门的安全管理团队，该团队所有人都要有较高的互联网安全理论知识与实践经验。应当定期接受培训并通过考核以锻炼自己的专业技术能力和安全意识[9]。与此同时要明确这些人的具体工作内容与权限，推行工作岗位责任制以确保安全管理机制的有效实施。此外对于外部人员也要有良好的管理，如电信人员、设备维护人员等也要严格进行准入审核与监管。

3. 建立完善的安全应急响应机制

高校应该制定完整、齐全的安全危机应急预案，并且对应急响应机构的组成、各自职责、操作流程等内容予以明确。同时，高校需要定期进行安全危机演练提高校园网络管理团队的协同作战能力和处理问题的能力，当出现网络安全问题后可以立刻启动危机预案，进而采取有效措施来遏制问题的损害程度，使得安全事故造成的损害能够降到最低。除此之外，高校还需要构建完整的有关事故的信息报告与通报机制，以此来帮助上级组织与相关部门提供准确的事故信息来加强信息的沟通与协同解决问题的能力[10]。

三、结语

综上所述，高校校园网与运营商5G融合是高校网络发展的必然趋势，它为高校的教学、科研和管理带来了诸多便利，但同时也带来了严峻的安全挑战。构建科学合理的分层安全管理体系是保障融合环境安全稳定运行的关键。本文设计的分层安全管理体系从物理层、网络层、数据层和管理层四个层面进行安全架构设计，各层之间相互协同、相互支撑，形成了全方位、多层次的安全防护机制。未来，高校应持续关注网络安全技术的发展趋势，加强与运营商的合作与交流，不断提升安全管理水平。同时，要加强对师生的网络安全教育和培训，提高师生的安全意识和自我保护能力，共同营造安全、可靠的网络环境，为高校的高质量发展提供有力的网络安全保障。

参考文献

[1] 朱春霖 . 高校校园网络文化建设与信息安全管理研究 [J]. 中国管理信息化 ,2024,27(17):151-154.

[2] 夏龄 , 周德荣 . 基于等级保护2.0的高校校园网安全平台设计 [J]. 四川职业技术学院学报 ,2024,34(02):145-148+162.

[3] 李琳 . 高校校园网络安全管理与维护系统研究 [J]. 信息与电脑 (理论版),2024,36(06):218-220.

[4] 闫实 , 金松根 . 数据安全防护体系在高校校园网中的应用 [J]. 办公自动化 ,2024,29(06):16-18.

[5] 张杰 . 高校校园网 IPv6的部署与管理策略——以攀枝花学院 IPv6建设为例 [J]. 数字技术与应用 ,2023,41(09):128-130.

[6] 杜健持 . 高校校园网数据安全管理模型及应用研究 [D]. 山东师范大学 ,2023.

[7] 许美娟 , 朱国海 , 王颐 .5G 视域下高校校园媒体融合发展路径研究 [J]. 信息与电脑 (理论版),2020,32(15):230-232.

[8] 覃德泽 , 李立信 . 高校智慧校园网中物联网、5G、云计算及 IPv6的融合问题探讨 [J]. 网络安全技术与应用 ,2019,(12):104-106.

[9] 林健 , 武兵 , 林楠 . 面向校园网用户的电子邮件系统全生命周期管理策略 [J]. 电子技术与软件工程 ,2018,(21):187-188.

[10] 赵伟 . 基于分层机制的高职院校学生公寓网络管理 [J]. 无线互联科技 ,2014,(06):9+101.

