校园 5G 双域专网安全认证方法实践

陈　晔[1]
CHEN Ye

摘　要　为顺应时代及产业发展，同时结合校园应用需求和师生教学、实验及生活网络应用场景的不断变化，为满足师生校内校外一体化融合接入需求，建设 5G 双域专网，与校园网相融合，将 5G 校园专网灵活便捷的优势和校园身份账号管理融合，在实现校园师生从校内到校外对网络资源无缝体验的同时，保障校内外资源的安全实名管理，积极探索 5G 融合教育行业解决方案，利用 5G+“纺织 AIoT”构建校企双元育人模式，深化产教融合，完善课程体系，培养复合型技术技能人才，促进人才链、教育链、产业链、创新链的融合。

关键词　双域专网；ULCL、Radius 协议；统一身份认证

doi：10.3969/j.issn.1672-9528.2024.07.030

0　引言

2021 年 7 月 5 日，工业和信息化部、中央网络安全和信息化委员会办公室、国家发展和改革委员会、教育部等十部门印发《5G 应用“扬帆”行动计划（2021—2023 年）》，计划通过 5G 智慧校园信息化建设推动学校管理科学化、智能化、效能化，同时构建智慧校园身份安全底座，打造数字化管理平台，解决原有的信息孤岛、业务系统独立问题，使校园资源平台使用更便捷。习近平总书记曾多次强调网络安全意识的重要性，并对强化网络安全意识提出具体要求。校园 5G 场景下，传统校园网络身份和运营商网络身份互相割裂导致校园身份管理困难，如何实现安全、可信、可溯源的分级分权资源访问是本文研究的重点。

1　校园 5G 双域专网建设背景及技术要求

1.1　以学校 5G 应用需求为导向

5G 双域专网主要服务于学生和教职工，对日常的在线学习、沉浸式虚拟环境教学、线上备课智慧化管理等场景服务，针对教育业务需求，结合 5G 特性，通过接入多种形态的智联终端和教育装备，构建全连接教育专网，部署整合计算、存储、AI、安全能力的教育边缘云，提供具备管理、安全等能力的应用使能平台，来建设智慧校园，并打造多样化教育应用。

1. 常州纺织服装职业技术学院 江苏常州 213164

[基金项目] 江苏省未来网络科研基金项目（FNSRFP-2021-YB-36）；江苏省现代教育技术研究 2021 年度课题（2021-R-88294）

1.2　学校 5G 基础设施已基本完备

常州纺织服装职业技术学院目前已建成 5 个 5G 宏站，10 个室分，涉及设备 28 套（图 1），已经实现了教学区 5G 全覆盖，性能指标理论上延时 10 ms，1000 兆的峰值速率，每平方公里 100 万连接数，为学校智能制造一体化及智能智慧教学提供大带宽、低时延、广连接的无线传输环境。

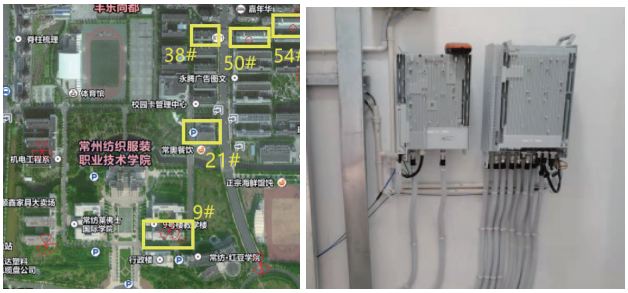

图 1　校园 5G 室分系统部署图

1.3　5G 双域专网技术已趋于成熟

数据可以完全安全隔离：校内用户进行用户分流策略签约，通过学校范围内 5G 基站互通，实现签约用户通过分流策略可以快速接入校园内网。签约校园分流业务的用户可以同时访问校园内网和 Internet，未签约的用户只能访问 Internet，不能访问校园内网 [1]。

5G 一张网：部署共享 UPF 或者下沉 UPF，将学校指定区域基站数据与 UPF 打通，提供 5G 专网服务，实现学校一张网 [2]。

取代传统 VPN：传统通过 VPN 的方式访问校内网时，VPN 存在速率低、时延大、带宽不稳定等问题，通过 5G 签约分流策略的用户访问学校内网，可以具备高速率、低时延、大带宽等特点，提升用户体验 [3]。

可延展性强：如在地市范围内有新增校区，仅需要将新建校区完成 5G 覆盖，同步将对应基站加入 5G 专网即可（图 2）。

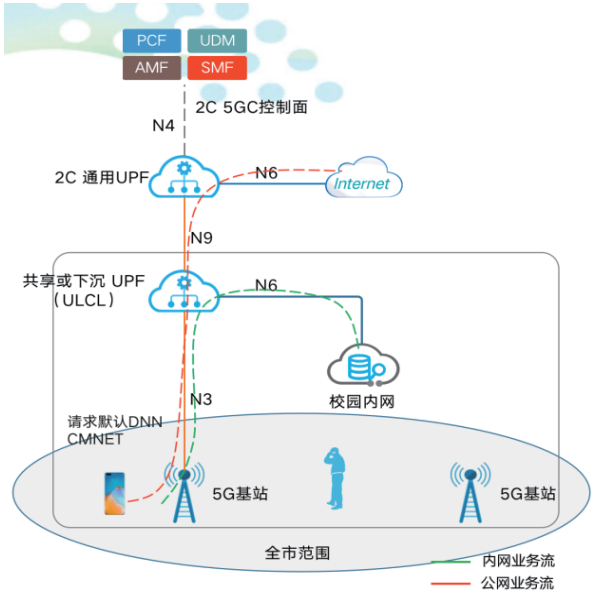

图 2 5G 双域专网业务流向图

1.4 学校已建成统一身份认证系统

经过多年持续不断的投入和完善，我校已经完成统一身份认证系统的建设，可以实现有线无线准入准出的一体融合认证（图 3），PPPOE 智能代拨，无需对接 ISP AAA，充分保障了校园网管理的自主性，为 5G 双域专网用户的实名二次鉴权提供技术支撑。

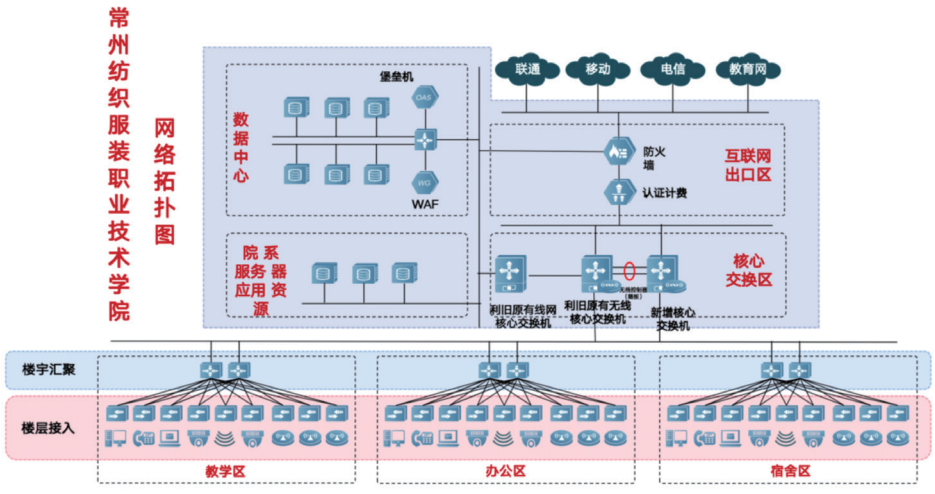

图 3 校园网拓扑图

2 推进 5G 校园专网建设的现实意义

2.1 便利的 5G 专网访问

签约的学校师生在一定范围内（如校园范围、城市范围等）通过 5G 校园专网既可以访问校园内网，又可以访问互联网；终端尽可能无配置或少配置，提供高易用性。

2.2 低建设成本和高开放性

无论对学校还是运营商来说，建设成本和投入应尽可能低。高开放性即减少运营商和学校之间的系统或耦合，利于快速建网、简化规划和运维。

2.3 可信用户准入

可信用户准入包含实名准入和可信终端两部分：实名准入是指虽然用户在运营商购买 5G 专网套餐是实名制，但 5G 双域专网属于校园网的一部分，学校需要学校侧接入实现实名准入；可信终端是指接入终端需与合法用户“人、卡、号”一致，防止离校学生使用在校学生账号登录入网的情况。

2.4 学校自主用户授权接入管理

高校具有用户数量和流动性大的特点，如果依赖人工与运营商端进行 5G 专网用户全生命周期同步，就会存在效率低、易出错和易产生安全漏洞等问题，因此学校需要自主独立管理本校 5G 专网用户。

2.5 与校园身份认证系统融合

为统一安全访问策略，与校园用户管理进一步融合提高管理效率，5G 专网准入认证需要与校园现有 AAA 系统、统一身份系统融合，进行统一管理 [4]。

2.6 实名访问审计，满足合规要求（网络安全法、等保等要求）

为避免学校产生安全审计漏洞，并满足网络安全法及等保相关要求，5G 专网访问校园网，甚至 5G 专网通过校园网访问互联网，均需要进行实名访问审计，以便实名溯源。

3 校园 5G 双域专网安全认证问题

将校园网现网（有线网络 + 无线网络）与运营商 5G 网络打通，建设 5G+ 无线网络 + 有线网络的全网全域全时的校园网络全覆盖，提升实时化、高带宽、多连接、高并发教学场景的网络支持能力，以安全身份认证为基础，即构建基于 5G 网络为入口的统一身份认证平台，实现校园三网统一身份管理，需要解决以下几个主要问题。

（1）5G 双域专网的签约接入主体是运营商，用户的管理主体是学校，运营商关注的是 ARPU 值 [5]，学校关注的是安全管理和使用率，但两者的管理系统是相互独立的，运营商处签约的 5G 双域专网用户在校园网中可能已经失信被拒绝访问，因此运营商签约的 5G 专网用户与校园网用户的生命周期很难同步。

（2）5G 运营商的核心网都是部署在省平台，运营商只提供校园边界数据通路，其业务系统、网络系统都是标准化的，而校园网的管理更加细化，不同的用户组使用校园网的权限是不同的，因此在安全管理策略方面，5G 双域专网与校园网也难以同步。

（3）学校如果将 5G 双域专网完全交给运营商做准入认证和审计管理，就无法自主鉴权，也无法获得运营数据（如在线数、活跃用户数等），这会导致安全管理边界模糊（不符合网络安全法及等保要求），5G 双域专网签约用户既是运营商活跃用户，同时也是校园网的授权用户。

（4）学校经常有校外的教科研任务，当课题小组或团队需要通过 5G CPE 接入校园 5G 双域专网时，难以对 5G CPE 的 Wi-Fi 终端实现实名准入管控。

（5）根据国家工信部规定，运营商不能直接向学校提供 AAA 对接和用户身份及 ID 的对应信息，如何实现用户的可信接入（如离校学生借用在校学生身份接入），就成为一大难题。

4 安全认证方法的研究

本文主要解决传统校园网络身份和运营商网络身份互相割裂导致校园身份管理困难、用户终端通过运营商 5G 网络难以直接访问校内资源及身份难以识别的问题，结合 5G 分域能力和 ULCL 分流特性与账号识别规则等技术进行可行性理论分析，配合校园已有身份体系架构和运营商 5G 网络基础设施能力，进行实践创新，以理论指导实践，实践验证理论，设计一种可信接入认证系统（认证网关），和学校现有统一身份认证进行 Radius 对接，将 5G 网络身份与校园网络身份相融合，为智慧校园数字资源和服务提供可管可控的身份认证及管控。

5 5G 可信接入认证系统的设计

5G 可信接入认证系统部署在 5G 专网与校园网边缘位置，采用串接方式（图 4），实现对 5G 专网用户的实名二次鉴权、可信接入控制，将 5G 专网用户的全生命周期管理融合到校园原有管理体系，提升管理效率和统一安全访问策略。

设计可信接入认证系统：认证网关（图 5），即实现“人、卡、号”在线实名一致的接入身份鉴权，确保学校合法用户使用本机接入，杜绝非法用户使用合法手机访问。由于运营商和学校无法实现用户资料的实时同步，所以这里的合法用户是指学校侧的合法用户，而非仅限于运营商的合法签约用户，如学生已离校，但手机专网套餐在运营商侧仍在有效期内，则访问受限。该系统基于号码认证技术，通过本机号码校验与学校侧准入认证（统一身份认证）联动，提供便利的可信接入管理。

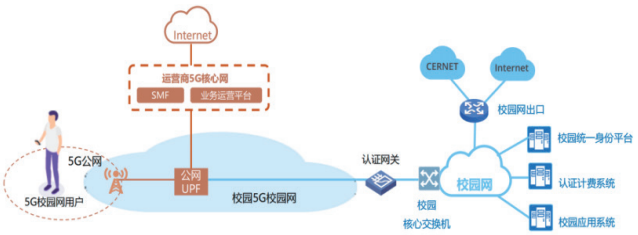

图 5 可信接入认证（认证网关）系统图

5.1 5G 双域专网可信接入认证系统拟实现目标

（1）运营商 5G 号卡身份和校园身份的融合绑定；（2）运营商 5G 号卡分域分流策略的实现，包括校内接入、本地漫游的实现；（3）运营商 5G 签约 UE 进入校园网的身份识别管理流程及其对校内资源访问权限的分发管理控制；（4）运营商 5G 签约 UE 访问校内外采资源（如知网资源、超星课堂等），以校园身份访问的实现；（5）运营商 5G 签约 UE 对校内资源及服务应用的数据分析和日志审计；（6）学校信息中心对运营商 5G 接入数据的实时化监控管理。

5.2 5G 可信接入认证系统（认证网关）主要功能

（1）以 5G 接入为切入点，从运营商侧对校内外资源通过 ULCL 分流，实现校内资源（服务器资源、校内服务或教学实验资源）的分域访问路由规划，默认路由为主；（2）对运营商账号和校园账号的融合绑定，实现校园四网互通（有线网、无线网、物联网和移动 5G 网）的身份统一管理和权限分级分权管理；（3）以校

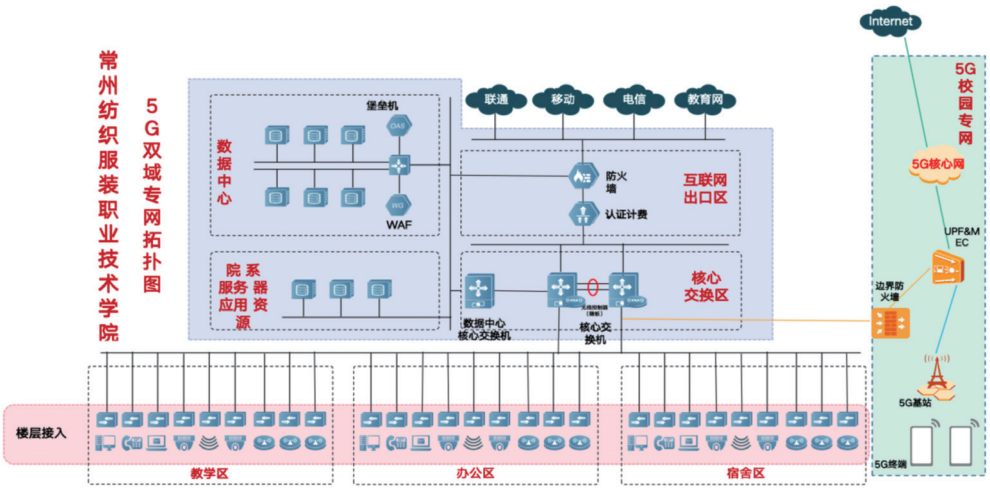

图 4 5G 校园网拓扑图

园统一身份中心为账号基础，在满足校园已有网络接入身份安全环境之上，提供来自运营商 5G 网络的直接访问，在 5G 终端首次进行校园网时，需验证终端身份和账号绑定关系合规后，终端可访问对应授权的校园资源或服务；（4）当 5G 终端在授权许可期限内再次对校园资源或服务发起访问时，5G 终端可在无感知状态下实现对校内资源的快捷访问（此时终端没有授权和验证交互界面，该过程由后台自动完成验证）；（5）5G 终端对校内资源和服务的访问轨迹将被合规采集并提供审计入口，5G 终端以校园身份对校内资源或服务进行的任意行为将以日志形式在 5G 网络与校园网络边界进行采集，最终将以图形化界面对用户行为或服务类型等数据标签进行可视化数据分析呈现；（6）结合运营商实际 IP 地址分配情况，如终端获取 5G 地址与校园网地址重复，5G 可信接入认证系统（认证网关）实现 DNAT 和 SNAT 的转换。

5.3 5G 可信接入认证系统（认证网关）实现步骤

本研究采用实验法，以 5G 接入网链路与校园现有网络实现链路互通，在以校园统一身份为基础的环境下，使用可信接入认证系统将 5G 网络手机号码与校园身份相融合，配合安全实名身份技术的多种实现，以达到对智慧校园资源系统和服务的统一身份权限管理和身份轨迹审计。以下为具体实现步骤。

学校网络侧改造：（1）完成互联 IP、互联端口配置；（2）配置可访问资源池 IP；（3）设计 5G 双域专网可信接入认证系统，并明确该系统放置的位置，联动学校统一身份认证系统；（4）确定组网模式，正确获取互联 IP 地址等相关信息表；（5）现场测试所需的手机号卡或手机。

运营商侧 5G 双域专网部署：（1）UPF 到学校的 STN 线路；（2）UPF 与可信接入认证系统互联 IP 地址；（3）加入 5G 用于测试的 SIM 卡或自己手机加入 5G 测试项；（4）UPF 互联接口配置；（5）UPF 业务切流策略设置，包括资源域名、特定地址等；（6）根据 UPF 业务切流策略设置情况，设定路由策略，前提是可信接入认证系统与 UPF 互通，5G 终端可正常接通可信接入认证系统。

可信接入认证系统的调试：（1）协调 UPF 与核心网互联 IP 地址、管理口 IP 地址等参数，将设备上架；（2）设备加电，配置 IP 地址等参数，完成上下联设备接线（需要 UPF 和学校核心网配合）；（3）与统一身份认证后台服务联动，配置全网直通，开启守护进程；（4）检查后台基本配置：包括账号信息、网络配置、策略组配置等；（5）DNAT 和 SNAT 的转换；（6）检查硬件设备中配置信息，包括网络配置、路由配置、直通配置、专线配置、账号信息等；（7）针对学校具体情况关联老师 / 学生账号和已开 5G 服务的手机号码；（8）针对部分特定 IP 地址段取消直通，开启认证，使用测试账号 / 手机号进行认证测试。

其中，认证系统对接运营商 UPF 涉及两种方法：（1）Radios 协议直接对接运营商 5G 核心网 SMF 设备；（2）采用头增强的方式，5G 流量送达认证设备的报文中携带用户的身份标签，如果中途被监听就会存在安全性的问题，目前只支持 http1.0，不支持 http2.0 和 https 等加密。

6 结论

运营商 5G 身份和校园账号的生命周期同步针对的是不同身份源的异构管理，5G 可信接入认证系统通过 Radius 协议与校园实名账号（统一身份认证）进行同步，同时通过运营商号码签约管理流程，将 5GC 核心网元所分配的 IP 与终端签约号码形成绑定关系，在 5G 核心网与校园网边界处再对 5G UE 终端本机号码进行号码验证，通过 Portal 页面提取本机号码发送到运营商号码认证 API 接口，保证用户身份的真实性，规避从潜在的欺诈风险。在完成三位一体的终端、号卡和账号认证后，最终实现 5G UE 通过可信接入认证系统对账号权限分级分权管理，实现对校园内网资源的访问控制。

本文研究在运营商 5G 网络中已有号卡身份根据预设访问目标进行分域分流访问的基础上，结合校园实名身份的融合绑定，在运营商 5G 号专网用户对校园内部资源访问时，实现安全、可信、可溯源的分级分权资源访问，通过二次鉴权的实名访问审计进一步提升学校网络安全整体防护能力，实现校园 5G 流量的可控、可追溯、可审计。

参考文献：

[1] 刘治纲 . 校园网与 5G 融合模式研究 [J]. 中国教育网络，2022(6): 79-80.

[2] 陈庆勇，薛雨伟 . 基于“5G+ 智慧教育”理念在远程教学中的应用及发展趋势 [J]. 电子测试 ,2021(16):137-138.

[3] 李伶，王华 .5G 智慧校园业务场景中 MEC 分流方案研究 [J]. 电信科学 , 2022,38(1):170-178.

[4] 曹磊，李丽，胡圣烨，等 .5G 能力魔方赋能 5G 定制网规模化发展 [J]. 电信科学 ,2022,38(5):38-44.

[5] 冯忠义，杨福理，苗玉斌 .5G 专网在校园 2C 业务中的应用部署研究 [J]. 江苏通信 ,2022,38(4):37-41.

【作者简介】

陈晔（1981—），男，江苏常州人，硕士，高级工程师，研究方向：计算机网络技术、网络安全。

（收稿日期：2024-05-10）