图书馆无线网络认证系统的研究与实现

钟 明 钱 庆 方 安

（中国医学科学院医学信息研究所 北京 100020）

〔摘要〕 介绍中国医学科学院图书馆无线局域网的使用现状，指出无线网络管理存在的问题，分析图书馆无线网络认证系统的功能需求，详细阐述该网络认证系统的设计和实现，最后对新的图书馆无线网络认证系统的使用情况进行总结和展望。

〔关键词〕 无线网络；Web 认证；图书馆管理系统；轻量目录访问协议

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2015.12.009

Research and Implementation of the Library WLAN Authentication System *ZHONG Ming, QIAN Qing, FANG An, Institute of Medical Information, Chinese Academy of Medical Sciences, Beijing 100020, China*

〔**Abstract**〕 The paper introduces the current use of Wireless Local Area Networks (WLAN) in the library of Chinese Academy of Medical Sciences, points out problems existing in WLAN management, analyzes the functional demands of the library WLAN authentication system, elaborates the design and implementation of the system, summarizes the use of the new library WLAN authentication system and indicates its prospects.

〔**Keywords**〕 WLAN; Web authentication; Library management system; LDAP

1 引言

无线技术、计算机技术及通信技术在过去十几年的进步使无线网络的发展日新月异、突飞猛进，无线设备层出不穷，无线接入渐成主流，无线网络已成为国内外最为活跃的研究领域之一。无线局域网（Wireless Local Area Network，WLAN）是指以无线信道作为传输媒介并且支持用户终端移动的数据传输系统。相对于传统的有线局域网，无线局域网具有移动性、部署方便、灵活性和成本低等优点[1]，被越来越广泛地使用。中国医学科学院图书馆（简称医科院图书馆）在 2008 年搭建了图书馆无线局域网为读者提供无线网络服务，读者可以使用笔记本电脑、手机、iPad 等移动设备在图书馆内任意位置查阅图书馆的各种网络信息资源，图书馆馆员也可以随时利用无线网络进行各项业务工作。然而，由于无线局域网使用无线电波传播数据，任何 WLAN 终端只要在 AP（Access Point）信号覆盖的范围内都可以访问无线网络，所以无线局域网在为图书馆的馆员和读者带来便利的同时，也不可避免地出现了数据安全和用户管理问题。

目前，医科院图书馆使用 H3C 公司的无线网络接入控制器（Access Controller，AC）和智能管理中心软件（intelligent Management Center，iMC）来解决无线网络下无线设备管理、用户接入认证和用户管理等问题。经过一段时间使用后，发现该系统出现用户许可证数目限制、用户管理不便等问题，并且无法和图书馆管理系统的用户库相匹配，导致图

〔修回日期〕 2015－11－09

〔作者简介〕 钟明，硕士，实习研究员。

书馆用户信息不统一。为了解决上述问题，基于城市热点无线网络认证方案设计新系统，替换 H3C 无线网络系统中的用户接入认证和用户管理部分，并与图书馆管理系统的用户库进行对接，完成医科院图书馆无线网络用户认证和管理的功能。

2 无线网络接入认证技术应用现状

2.1 无线网络用户认证技术

无线网络管理中最重要的技术之一，移动终端在物理上很容易接入无线网络，所以必须采用接入认证技术来识别接入无线网络的用户身份，保证授权合法用户访问被允许的网络资源。目前，国内外使用最普遍的接入认证技术有 3 种，即 PPPoE 认证、802.1x 认证和 Web 认证，这 3 种认证技术都可以使用用户名 + 密码的认证方式应用到无线网络中。

2.2 PPPoE

Point - to - Point Protocol over Ethernet（PPPoE），即在以太网上承载点对点协议，使以太网中的大量主机通过远端接入设备连入因特网，并且远端接入设备能够对接入的每一台主机进行控制和计费。PPPoE 认证方式是传统的 PSTN 窄带拨号接入技术在以太网接入技术上的延伸，不仅有以太网快速、简便的优点，而且和原有窄带网络用户接入认证体系一致，用户认证速度快，计费方式灵活，主要用于电信运营商的 ADSL 业务中。

2.3 802.1x

由 IEEE 制定的基于端口的网络访问控制协议，应用有线局域网交换机和无线局域网接入点对接入用户进行认证。该认证技术采用客户端/服务器模式，客户端必须运行遵循 802.1x 标准协议的认证软件，通过与认证服务器进行加密信息交互，完成安全高效的认证与授权。802.1x 认证实现简单，单点故障出现概率小，对设备的整体性能要求不高，既方便开展组播业务，又节省了建网成本[2]；并且基于端口的方式将认证和业务分开，传输效率高。该方式主要用于用户比较少的网络中。

2.4 Web 认证

一种业务类型的认证方式，利用 Web 页面进行接入认证。该认证技术首先为用户分配一个 IP 地址，用于访问允许的站点；如果用户访问受限网络资源，认证节点强制用户登录到认证服务器站点进行认证，认证通过后为用户分配一个可以访问外网的 IP 地址。

2.5 3 种认证技术的比较[3]（表 1）

与 PPPoE 和 802.1x 相比，Web 认证主要有如下优点：（1）不需要安装客户端软件，用户使用浏览器或其他软件弹出的 Web 页面即可以进行接入认证，操作简单，同时降低了网络维护的工作量，比较适合图书馆等公共场所使用。（2）采用全 3 层处理，能够跨越多个网络，具有很好的灵活性，特别适合于有多个独立无线网络区域的图书馆。（3）允许大规模用户接入，可以提供高密度用户接入的解决方案，集中管理，保证服务质量。（4）兼容性好，应用业务扩展性强，其认证服务器可以进行业务推送。因此医科院图书馆选择采用 Web 认证技术对无线网络用户进行接入认证。

表 1 3 种认证技术的比较

认证技术	PPPoE	802.1x	Web
标准化程度	RFC 2516	IEEE Std 802.1x	厂家私有
封装开销	较大	小	小
接入控制方式	用户	设备端口	用户
IP 地址分配时机	认证后	认证后	认证前
组播支持	差	好	好
客户端软件	需要	需要	不需要
服务器端接入设备	BAS	Switch	BAS
跨 3 层网络认证	不能实现	不能实现	能实现

3 医科院图书馆无线网络认证系统需求分析

3.1 无线网络管理存在的问题

目前，医科院图书馆已经利用 H3C 公司的无

线网络接入控制器 WX5002 和智能管理中心软件 iMC3.0 实现了图书馆无线网络的设备管理、用户接入认证和用户管理，其中无线认证采用 Web 认证。但随着无线网络用户数量的增加，目前的 Web 认证系统已经不能满足图书馆的无线网络管理需要，主要存在以下问题：（1）注册用户数量限制。由于购买的 iMC 许可证数有限，于是设置了允许多人同时在线的 test 账号供无线用户使用，由此导致了非法用户蹭网的现象。（2）无线用户的注册和审核工作量大。如果为每个用户注册无线认证账号，则需要管理员人工确认每个注册用户的身份信息。（3）不能和图书馆管理系统的用户库相关联，造成图书馆用户信息不统一。（4）管理员无法监控用户上网行为。认证系统中没有用户上网行为管理功能，只能靠 IP 地址和 MAC 地址区分用户，如果出现恶意下载、网络泄密等违法现象，管理员不能有效地追根溯源。（5）用户体验较差。使用手机登录认证页面时登录窗过小，不方便输入用户名和密码；认证页面颜色对比度较低，看不清登录按钮；使用手机认证接入无线网络时偶尔掉线。

3.2 无线网络认证系统功能需求

为了解决目前无线网络的管理问题，需要选择合理的图书馆无线网络认证方案，使其能够取代原有的 Web 认证系统。图书馆无线网络认证系统的功能需求有如下几点：（1）低成本解决无线网络用户管理和认证问题，尽量减少购买硬件、软件和许可证数，保证图书馆网络管理的完整性和可靠性。（2）使用 Web 认证，并且不改变用户认证过程和上网流程。（3）利用图书馆管理系统的用户库自动完成用户的注册审核，降低管理员的工作量。（4）具有上网行为管理功能，对无线网络用户访问流量进行记录和控制，保证用户对图书馆无线网络的合理使用。（5）优化无线网络认证页面和 Web 认证功能，保证各种移动设备、各种浏览器的兼容性，使得用户体验良好。（6）提供基于 Web 页面的认证服务器管理功能，方便管理员进行无线网络服务策略配置、用户在线信息查看、用户使用量统计等操作。

4 医科院图书馆无线网络认证系统设计与实现

4.1 无线网络认证系统功能模块划分

图书馆无线网络认证系统是多个功能模块集成的分布式系统，其功能模块的划分和模块间的关系，见图 1。

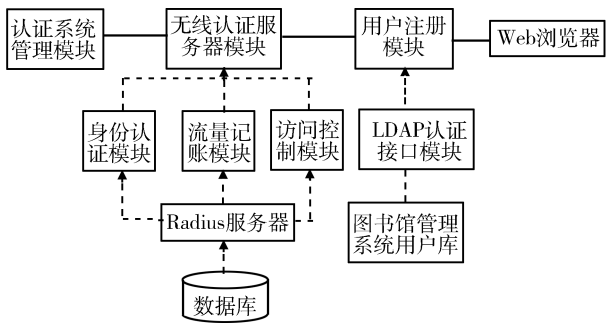

图 1 图书馆无线网络认证系统功能模块划分

图书馆无线网络认证系统主要分为 3 大部分：无线认证服务器模块、用户注册模块和认证系统管理模块。其中无线认证服务器模块是图书馆无线网络认证系统的核心，负责处理无线用户的接入认证请求，包括身份认证模块、流量记账模块和访问控制模块[4]；用户注册模块实现无线网络认证系统与图书馆管理系统的轻量目录访问协议（Lightweight Direetony Access Protocol，LDAP）数据库对接，完成自动审核无线用户注册信息的工作；认证系统管理模块负责对图书馆无线网络认证系统进行 Web 管理，包括配置无线网络认证服务器、管理无线用户账号和控制上网流量等。

4.2 无线认证服务器模块设计

无线认证服务器模块用来实现对所有经由无线接入控制器 WX5002 进入的无线网络用户进行身份验证、流量记账和访问控制，主要完成 Web 认证的过程。Web 认证主要由认证客户端、无线接入点、无线接入控制器、Portal 服务器和认证/计费服务器等几部分构成，其中 Portal 服务器提供免费站点服务和认证页面，认证/计费服务器通常由 RADIUS 服务器承担。WLAN Web 认证流程，见图 2。WLAN 用户终端连接到无线服务并访问网站后，经过 AC

重定向到 Portal 服务器；Portal 服务器向用户推送统一的认证页面；用户在认证页面输入用户名、密码，向 Portal 服务器发送连接请求；Portal 服务器向 RADIUS 服务器发送用户信息查询请求，由 RADIUS 服务器进行用户合法性校验并向 Portal 服务器返回查询到的用户信息及系统设置的用户上网时长等信息；如果查询成功，Portal 服务器与 AC 进行 Challenge 报文交互；交互完成后，Portal 服务器向 AC 请求认证，AC 携带用户名和密码向 RADIUS 服务器发起认证；若认证成功，AC 将认证结果发至 Portal 服务器，Portal 服务器推送出定制的门户页面[5]。

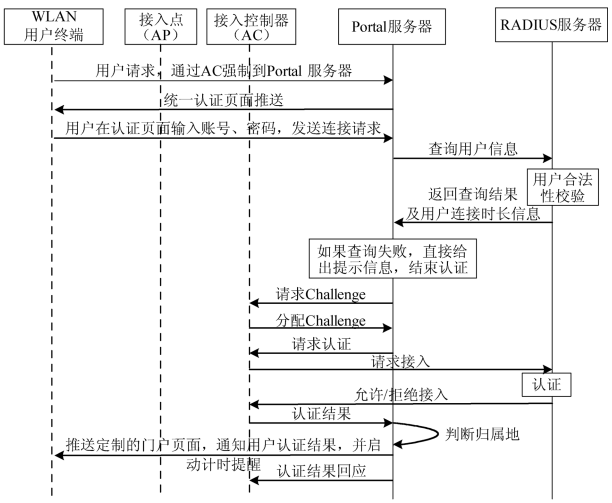

图 2 WLAN Web 认证流程

Web 认证具有很好的兼容性和业务扩展性，其认证服务器支持页面定制和业务推送。为了展示医科院图书馆无线认证方案的特色，本着功能简单易用、用户体验良好的原则设计了无线网络的认证页面，见图 3。该页面整体以淡蓝色为主色调，中间的登录框以动感时尚的图案做背景，突显出具有文字描述的主窗口。主窗口部分，考虑到手机屏幕输入用户名和密码的方便性，设计了较大尺寸的输入框和按钮；登录窗和注销窗的文字描述和按钮采用中英文结合的方式，方便外籍读者使用。对认证成功后的推送页面进行分类设计：如果用户在浏览器中输入认证服务器的 IP 地址，认证成功后，Portal 服务器将推送医学信息研究所/图书馆网站首页；如果用户输入其余网址，认证成功后跳转到之前输入的网址。用户认证成功后就可以使用图书馆无线网络提供的各类服务。无线认证服务器将用户访问记录以写文件的方式存储到数据库服务器硬盘里，在访问记录中可以随时查询到用户名、登录访问时间、在线人数、总使用时间、目标网址、目标 IP、目标端口、源 IP、源 MAC 地址等信息。

图 3 图书馆无线网络统一认证页面

4.3 用户注册模块设计

用户注册模块采用统一身份认证方式，利用图书馆管理系统的用户库进行无线网络用户的身份认证。医科院图书馆使用的图书馆管理系统为汇文系统，该系统内部包含 LDAP 用户信息库，其中存放了用户 uid、password 等个人信息。用户注册模块通过对图书馆管理系统进行二次开发得到 LDAP 验证模块，完成与无线认证服务器模块的交互。LDAP 认证的通信过程，见图 4。

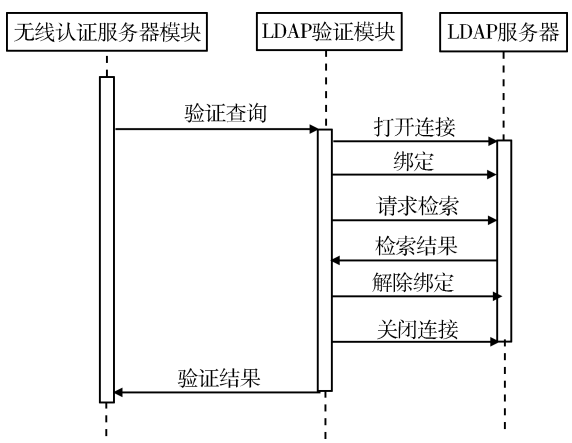

图 4 LDAP 认证的通信过程

当无线用户在无线网络认证页面输入图书馆管理系统的读者证号和密码后，无线认证服务器模块通过 LDAP 验证模块向 LDAP 服务器发出验证查询请求；经过连接、绑定、检索等操作后，LDAP 服务器将检索结果送回 LDAP 验证模块；无线认证服务器模块根据 LDAP 验证模块返回的验证结果，允许或禁止用户身份认证的通过。

LDAP 验证模块采用 LdapAuth 组件实现，包含了以下主要功能[6]：LdapAuth. SetLdapIP（“192. 168. 0. 1”）——初始化 LDAP 服务器的 IP 地址；LdapAuth. LdapInitPort（389）——初始化 LDAP 服务器的端口；LdapAuth. LdapSearch（“o = isp”，“uid = T0004”）——查找读者证号为 T0004 的读者；Dn = LdapAuth. GetEntryDN——得到读者证号为 T0004 的读者的 DN；LdapAuth. AuthUser（User Password，Dn）——检查该用户的合法性；LdapAuth. LdapFree——释放相关资源。

无线认证服务器模块通过调用 LdapAuth 组件，验证用户名与密码的合法性。如果验证通过，则用户可以接入无线网络，同时用 MD5 算法对用户的密码进行散列，并在本地系统中保存备份，以便用户下次接入无线网络时直接在认证系统数据库中进行身份验证；如果汇文系统中读者的密码有变化，那么读者下次登录时在本地认证系统数据库中身份验证失败，需要继续通过 LDAP 验证模块向汇文用户信息库发起检索请求，如果验证通过，则用户可以接入无线网络，并更新本地认证系统数据库中的用户信息。这样的机制使得认证系统数据库中的用户信息与汇文系统用户库中的读者信息保持同步，节省了无线认证的时间，而且在汇文系统出现网络故障时，用户也可以顺利进行无线认证。

4.4 认证系统管理模块设计

为了对图书馆无线网络认证系统进行 Web 管理，本文搭建了认证服务器的 Web 管理系统，其设计参考已有的成熟的认证计费管理系统，包括用户管理、策略管理、设备管理、查询统计、系统配置等模块。用户管理模块包括用户查询和业务受理功能，认证成功的无线网络用户在该系统中有账号记录，管理员可以查看这些账号的在线状态并为其修改个人信息和销户；对于特殊用户，比如临时入馆维修设备的工程师，可以在该系统中人工为其开通无线账号。策略管理模块完成带宽组、时段控制策略、目标地址带宽策略的配置，实现对用户或用户组的流量控制和时段控制。查询统计模块包括上网详单和认证日志的查询，用户详细资料和可用状态的查询，使用时长、使用流量、登录时段分别对应的户数分布的查询。

4.5 无线网络认证系统功能流程（图 5）

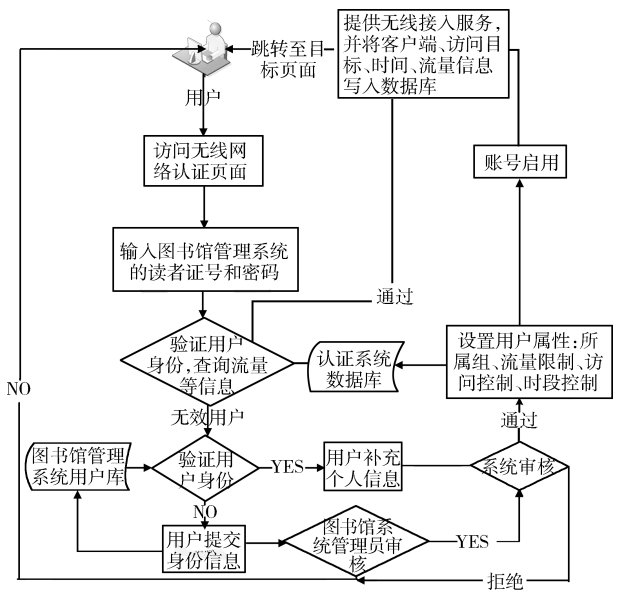

图 5 图书馆无线网络认证系统工作流程

4.6 无线网络认证系统实现

医科院图书馆无线网络认证系统是基于城市热点无线认证方案实现的，该系统由 Dr. COM 2166 B – RAS 认证计费服务器、Dr. COM Billingware 管理平台服务器、日志服务器组成，并与 H3C 无线控制器 WX5002、图书馆管理系统 LDAP 服务器共同组成医科院图书馆新的无线网络 Web 认证运行环境，以实现网络监控、用户管理、策略配置、统计输出报表、互联网访问记录存储等业务功能。该系统的拓扑图，见图 6。Dr. COM 2166 B – RAS 设备安装在无线控制器和信息所核心交换机之间，将信息所 AP 的 IP 地址段、2166 B – RAS 设备 IP 所在网段、信息所无线用

户 IP 地址段设置成直通，实现只对图书馆的所有无线终端进行 Web 认证。用户的访问记录由 Dr. COM 2166 B－RAS 设备写入日志服务器。

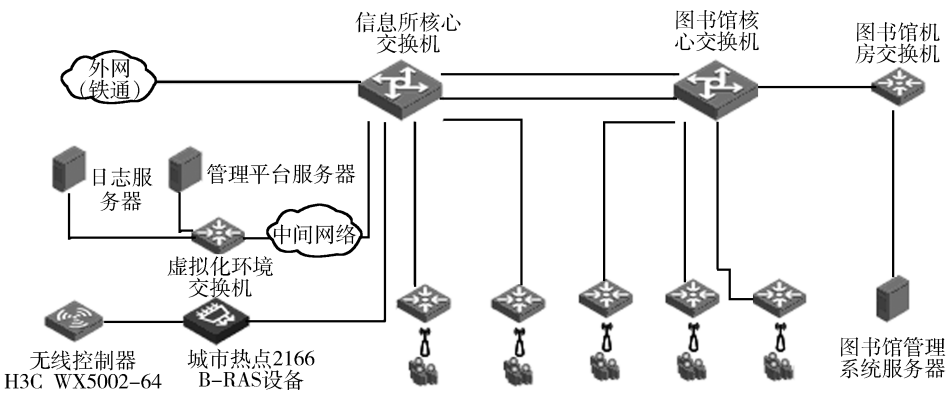

图 6 医科院图书馆无线认证系统拓扑图

5 结语

医科院图书馆无线网络认证系统是基于城市热点无线认证解决方案完成的，取代了原有 H3C 无线网络认证系统的功能。该方案采用成熟先进的软硬件系统，具有与主流厂家接入设备良好的兼容性，直观易用的 Web 管理界面和完善的用户访问日志，有效解决了用户授权访问和上网行为管理的问题。

图书馆无线网络认证系统的用户注册模块通过 LDAP 机制将图书馆管理系统和无线网络认证系统统一起来，图书馆管理系统的合法用户在认证时可以自动通过审核成为图书馆无线网络用户，既简化了管理员的维护工作，又保证了无线网络认证系统用户的独立性。同时，该系统可以对用户进行分级管理，通过在图形化的 Web 管理系统中配置无线网络服务策略，设定不同用户的访问时间和访问流量，保证图书馆无线网络的合理利用。该系统已经稳定运行 5 个多月，系统功能完全达到预期要求，有注册用户数 6 000 多人，每天访问量 200 多人次，同时在线近百人次。目前日志服务器中的访问日志是以记账形式存在的，下一步还需要开发日志分析工具，根据访问时间、目标地址快速查找对应的账号信息及所在的交换机端口，以便更好的进行用户上网行为管理。

参考文献

1 Mattbew S. Gast 著，O’Reilly Taiwan 公司编译. 802.11 无线网络权威指南［M］. 第 2 版. 南京：东南大学出版社，2007：13－23.

2 高亚军. 基于接入交换机的 Web 认证研究与实现［D］. 广州：华南理工大学，2013.

3 肖义. 3 种接入认证技术的浅析与比较［J］. 光通信研究，2006，(3)：25－28.

4 耶健，李丹，闫晓弟，等. 图书馆无线网络统一认证系统的研究与实现［J］. 现代图书情报技术，2012，(7)：121－126.

5 龙滔. 集中式 WLAN 架构下 AP 和 Station 管理的设计与实现［D］. 广州：华南理工大学，2011.

6 常潘，沈富可. 基于 LDAP 的校园网统一身份认证的实现［J］. 计算机工程，2007，33（5）：281－283.