

浅谈医院物联网工程的实施

陈磊,周敏,傅许彦

(浙江大学医学院附属第一医院信息中心,浙江 杭州 310003)

摘要: 物联网技术在医疗领域的应用一直备受国内外的广泛关注。而这一应用的前提是物联网网络在医院安全、完整的敷设。着重介绍了物联网网络工程在医院的规划设计及具体实施情况。

关键词: 物联网;AP;信道规划;IP规划;无线安全

中图分类号: TP391.76

文献标识码: A

文章编号: 1674-7720(2013)14-0056-03

Implementation of Internet of Things in hospital

Chen Lei, Zhou Min, Fu Xuyan

(Information Center of the First Affiliated Hospital, College of Medicine, Zhejiang University, Hangzhou 310003, China)

Abstract: Things technology in the medical field has always been widespread concern at home and abroad. The premise of this application, complete the laying of Things network security at the hospital. This article focuses on the Internet of Things network engineering planning and design in our hospital, and the actual implementation.

Key words: Internet of Things; AP; channel planning; IP planning; wireless security

1 项目背景

浙江大学医学院附属第一医院(浙江省第一医院)系三级甲等综合性医院,是浙江省医疗、教学、科研指导中心之一。医院现有职工 3 780 余人,其中高级职称医护专家 430 余人,有中国工程院院士 2 名、长江特聘教授 2 名、长江讲座教授 2 名、“千人计划”1 名、国家杰出基金获得者 2 名,求是特聘教授 2 名,占地面积 150 余亩,分为庆春、城站、大学路和良渚四个院区,核定床位 2 500 张。

医院设有传染病诊治国家重点实验室、卫生部器官联合移植研究重点实验室、国家中医药科研三级实验室(分子生物学、肾病、血液)等国家级实验室,以及浙江省的 40 余个重点实验室。近年来,医院积极探索公立医院改革之路借助主持的“十一五”重大科技攻关项目——“国家数字卫生关键技术和区域示范应用研究”,构建“省、县(区)、乡三级医疗服务网络”,成功使优质医疗资源垂直延伸到基层。目前,医院已拥有 1 家托管医院、3 家合作医院、89 家协作医院及网络服务单位和 1 家对口基层医院,提供了上万次的远程会诊服务。

医院敷设物联网网络,主要应用于药品管理、远程监护和护理、输液管理、移动护理、医生电子病历移动医疗、消毒供应中心质量追溯系统、医疗设备的跟踪与管理、医疗垃圾的处理、医疗手术中的跟踪监控、血液制品

的管理与监控、病人的定位跟踪及管理、医院感染控制等各方面涉及医疗安全的物联网应用。

本项目工程主要覆盖医院本部 1、2、3、5、6、7、9、10 号楼及入院服务中心等楼的物联网网络。

2 基本概念

2.1 物联网的概念

所谓“物联网”,即是指利用条码、射频识别(RFID)、红外感应器、全球定位系统、激光扫描器等信息传感设备,按约定的协议,完成任何物品间在任何时间、任何地点的连接,进行信息交换和通信,以实现智能化识别、定位、跟踪、监控和管理的一种网络^[1-2]。

2.2 物联网在医疗领域的应用

在医疗领域,物联网在条码化病人身份管理、移动医嘱、诊疗体征录入、药物管理、检验标本管理、病案管理数据保存及调用、护理流程、临床路径、传染病感染等管理中,均能发挥重要作用^[3]。例如:通过物联网技术,可以将消毒器械包和手术器械包的名称、品种、批次及清洗、灭菌、存储、运输等环节的有关时间、操作员、各种仪器的运作状态等信息,都存于电子标签中,当出现问题时可以追溯整个消毒清洗过程。

3 物联网网络工程的实施

本物联网网络工程项目需要实现我院 1、2、3、5、6、

欢迎网上投稿 www.pcachina.com 57

网络与通信 Network and Communication

7、9、10 号楼、入院服务中心等楼的全方位物联网网络的覆盖。无线网络解决方案基于 802.11a/b/g 传输标准,采取无线控制器加瘦 AP 的架构,所有 AP 都通过无线控制器进行统一管理,通过不同的服务集标识来定义各种结构。采用的物联网无线设备为:物联网无线控制器 WNAC9505-2 台,做双机热备。物联网 AP:WNDAP350-ER-258 台,WNDAP356-316 台。POE 物联网供电交换机:GA724TP-55 台。对于物联网 AP 布线要求,由于物联网 AP 集成了无线网(WIFI)与传感网(RFID)功能,所以每个 AP 需要两根网络线,分别用于传输无线网与传感网。

3.1 无线网络规划设计

该无线网络的主要目的是通过真实的使用环境和实际效果,来满足和保证未来医疗网络系统和资源有良好的使用感受。未来无线移动网络在医院病区的实际效果主要是应用于病区移动查房、移动护理、质量追溯、输液管理、病区订餐、心电数据回传、物联网等功能。作为有线网络应用的补充方式,在每个区域使用的移动终端个数将在 10~15 个左右。如图 1 所示。

3.1.1 WLAN AP 部署设计

该项目总共有 582 个物联网 AP。按照一栋大楼的 WLAN AP 部署方法,即要根据建筑楼层房间的分布基本一致性,充分利用无线信号对单体墙壁和天花板的信号穿透性,将 WLAN AP 交叉摆放,这样可以充分利用上、下层 AP 穿越楼板的信号,以起到上下、左右间无线信号的互补和利用;既节省了 WLAN 建设成本,也最大化地有利于信号的充分覆盖和利用。

以 6 号楼 B 区的一层为例,根据建筑自身特点,为了保证每个房间的信号有效覆盖,共部署了 6 个 AP,以 802.11a/n 和 g/n 覆盖区域信号最强化为目标,只有信号足够强,无线高速率才有保证。

在每个楼层的井道内,放置一台 NETGEAR GS724TP

千兆 802.3af POE 交换机,提供 6 台 AP 以太网线远程供电和数据的传输;GS724TP 的一个千兆端口通过以太网上连至有线网络内。

3.1.2 无线信道及漫游规划

虽然 2.4 GHz~2.483 GHz 之间的 802.11 标准的无线频点有 13 个,但由于设计为相互重叠,所以只有 3 个不重叠频点(一般设计工作在 1、6、11 这 3 个完全不重叠的频点),这样使得频点配置工程十分必要。合理地进行信道规划,降低同频干扰,同时楼层之间的泄漏信号干扰也要考虑在内。信道采用手动静态设置。如图 2 所示。



图 2 无线信道及漫游规划

漫游需求的规划一是要确定漫游的范围,二是要确保覆盖范围内无线信号的无缝覆盖。

3.1.3 无线发射功率自动选择及覆盖故障自动修复

AP 在默认情况下,会按照相邻 AP 的发射功率自动调节自身的发射功率,使之能实现相邻 AP 间的全覆盖。当其中一个 AP 发生故障不能正常工作时,与之相邻的 AP 就会自动增强发射功能,从而弥补因为 AP 故障而导致的覆盖缺失。

3.2 实施方案

3.2.1 物联网整体网络拓扑结构图

为了方便网络管理、减轻有线网络承载负担,也为了避免当无线物联网网络出现问题时累及有线网络,有线

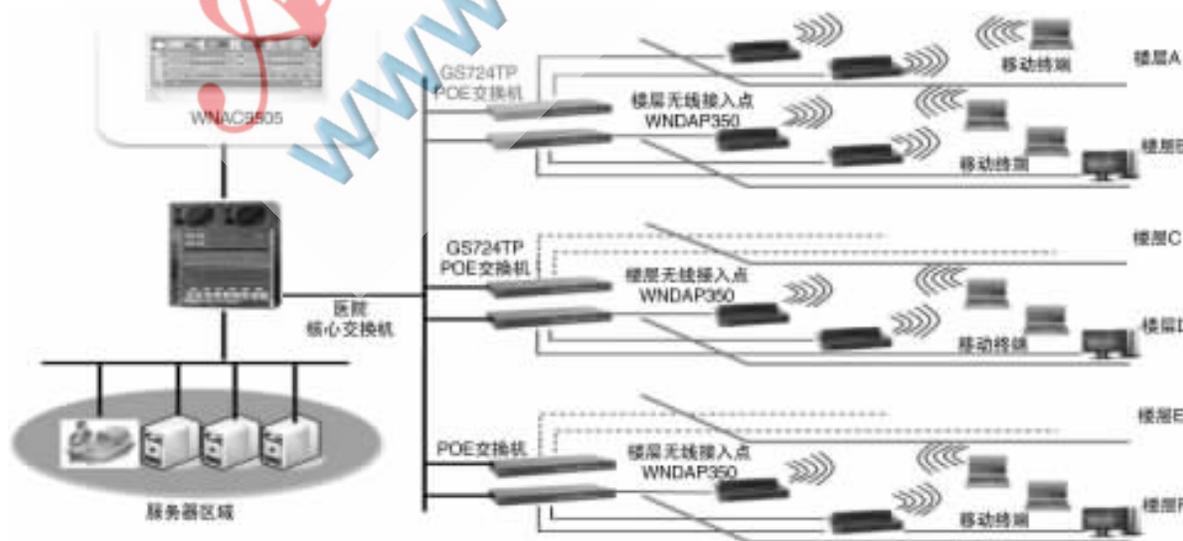


图 1 无线网络设计拓扑图

网络与通信 Network and Communication

网络的汇聚交换与物联网的汇聚交换机实现物理隔离。即有线网与物联网各自单独使用汇聚交换机,通过各自的汇聚交换机再与医院的有线核心交换机相连。

整体网络拓扑如图3所示。

3.2.2 IP 地址的规划

AP的管理IP地址及RFID传感网的管理IP地址在网络中添加新的网段,按照网络的IP规划来给AP及RFID分配IP。保证AP及RFID获取到的IP地址与AC、RFID获取到的IP地址与AC、RFID服务器之间能够三层可达。为了方便管理及安全考虑,采用固定IP地址的方式实现AC与AP、RFID与RFID服务器之间的三层部署。一幢楼启用一个全新的VLAN。

客户端接入端IP规划:每幢楼为一个接入单元,采用同一个SSID实现三层漫游,并采用动态IP分配方式。

3.3 无线与RFID安全接入规划

为了保证无线的安全接入,采用目前较为流行的MAC认证与WPA2认证结合的方式来确保无线网和传感网的网络安全。

3.3.1 MAC 认证方式

MAC地址认证是一种基于端口和MAC地址对用户访问网络的权限进行控制的认证方法,它不需要用户安装任何客户端软件,AC控制器在首次监测到用户的MAC地址以后,即启动对该用户的认证操作。在控制器上设置白名单,把允许进入网络的合法用户列入名单中,而一旦发现可疑的非法用户,则将其列入黑名单。

3.3.2 WPA2 认证方式

无线数据的加密采用WPA2安全架构的AES-CCMP

(高级加密标准-计数器模式密码区块链接消息身份验证代码协议)。CCMP采用AES加密模块,AES既可以实现数据的机密性(加密),又可以实现数据的完整性。这是在IEEE802.11i标准中指定的用于无线传输隐私保护的一个新办法。AES-CCMP是面向大众的最高级无线安全协议。总体来说,CCMP提供了加密、认证、完整性检查和重放保护四重功能。CCMP使用128位AES加密算法实现机密性,使用其他CCMP协议组件实现其余3种服务。CCMP基于CCM方式,该方式使用了AES加密算法,所以AES-CCMP加密协议也称AES-CCM加密协议。从名称可以看出,CCM配备了两种运算模式,即计数器模式和密码区块链信息认证模式,其中计数器模式用于数据流的加密/解密,而密码区块链信息认证码模式用于身份认证及数据完整性校验。CCM保护MPDU数据和IEEE802.11 MPDU帧头部分域的完整性。AES定义在FIPS PUB197,所有在CCMP中用到的AES处理都使用一个128位的密钥和一个128位大小的数据块;CCM方式定义在RFC3610。CCM是一种通用模式,可以用于任意面向块的加密算法。

加密和认证可以相互结合,整体保证无线接入的安全性。

3.3.3 RFID 安全性规划

因为RFID采用UDP发包方式,而且RFID芯片本身也具有加密功能,所以安全性得以保障。

认证的流程可以分为以下几个步骤:

(1)应用程序通过RFID读写器向RFID电子标签发送认证请求;

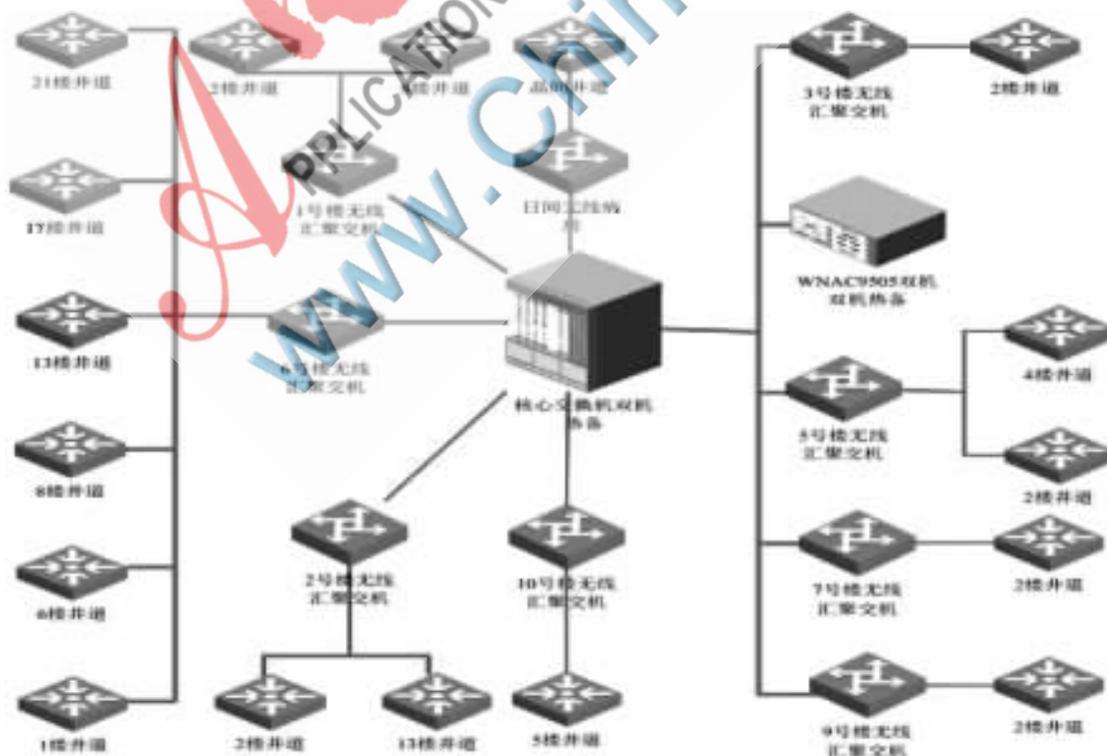


图3 物联网整体网络拓扑结构图

(2)RFID 电子标签收到请求后向读写器发送一个随机数 B;

(3)读写器收到随机数 B 后,向 RFID 电子标签发送使用要验证的密钥加密 B 的数据包,其中包含了读写器生成的另一个随机数 A;

(4)RFID 电子标签收到数据包后,使用芯片内部存储的密钥进行解密,解出随机数 B 并校验与之发出的随机数 B 是否一致;

(5)如果一致,则 RFID 使用芯片内部存储的密钥对 A 进行加密并发送给读写器;

(6)读写器收到此数据包后,进行解密,解出 A 并与前述的 A 比较是否一致。

物联网技术在医疗领域的应用一直备受国内外的

广泛关注。本文详细讨论了物联网在医疗领域应用的基础架构——物联网网络工程的构建,及在本院的一个实施情况,借此能给兄弟医院提供一个有益的参考。

参考文献

- [1] 冯杰,郝家贞.对物联网组网架构的探究[J].信息与电脑,2010(8):87.
- [2] 李航,陈后金.物联网的关键技术及应用前景[J].中国科技论坛,2011(1):81-85.
- [3] 俞磊,陆阳,朱晓玲,等.物联网技术在医疗领域的研究进展[J].计算机应用研究,2012,29(1):1-7.

(收稿日期:2013-04-23)

作者简介:

陈磊,女,1976年生,工程硕士,主要研究方向:医疗领域信息化、物联网在医疗领域的应用。

