文章编号:1001-9944(2013)01-0017-05

两信道物联网协议分析仪的设计与实现

王　平[1],方　燕[1],谢昊飞[1],张　军[2],陈庆华[1]
(1.重庆邮电大学 工业物联网与网络化控制教育部重点实验室,重庆 400065;2.中国四联仪器仪表集团有限公司,重庆 400065)

摘要:在研究了物联网协议和无线射频技术的基础上,设计并实现了两信道物联网协议分析仪。该分析仪由数据采集器和上位机协议分析软件组成,采用空中捕获的无线射频技术,能实时采集2.4 GHz ISM频段上任意两个信道的无线数据报文;并提出了一种基于特征位的快速匹配算法,应用于协议解码模块,从而快速提高协议分析仪的分析速率。本协议分析仪实现了协议分析、网络监控、故障诊断等功能,可面向ISA100.11a、ZigBee、WIA-PA、6LoWPAN、IEEE802.15.4E五套物联网协议。实验结果表明,该分析仪单帧处理时间小于10 s,且10 m监控范围内丢包率小于1%,是一款简单、实时和有效的网络查错、测试以及性能维护工具。

关键词:物联网协议;无线射频技术;数据采集;协议分析;快速匹配
中图分类号:TH702　　**文献标志码**:B

Design and Implementation of Two-channel Protocol Analyzer of the IOT

WANG Ping[1],FANG Yan[1],XIE Hao-fei[1],ZHANG Jun[2],CHEN Qing-hua[1]
(1.Key Laboratory of Industrial Wireless Network and Networked Control,Ministry of Education,Chongqing University of Posts and Telecommunications,Chongqing 400065,China;2.China Silian Instrument Group Co.,Ltd.,Chongqing 400065,China)

Abstract:On the basis of studying Internet of Things(IOT)protocols and wireless RF technology,designing and implementing the two-channel protocol analyzer,which was make up with data collect device and the PC protocol analysis software,using wireless radio frequency technology to capture wireless data packets on any two channels of the 2.4GHz ISM band in real-time,In addition,proposing one fast matching algorithm and applied it to the protocol decoding module which rapidly improve the analysis of the rate of the protocol analyzer. The protocol analyzer have achieve functions like protocol analysising,network monitoring,fault diagnosis and so on,it can works under ISA100.11a,ZigBee,WIA-PA,6LoWPAN,IEEE802.15.4E five IOT protocols. The processing time was less than 10ms and the packet loss rate was less than 1% within 10 meters. The experiment results showed that the analyzer was a simple,real and effective network troubleshooting,testing and performance maintenance tools.

Key words:internet of things(IOT)protocol;wireless RF technology;data collect;protocol analyzer;fast matching

近年来,集成了嵌入式技术和传感器技术的物联网技术成为了研究热点。目前, 物联网协议有ISA100.11a、ZigBee、WIA -PA、6LoWPAN、IEEE802.15.4E等,随着物联网应用的不断扩大,专业的协议分析仪对于一个网络的稳定运行是至关重要的。首先,在组网过程中,实时掌握各结点当前状态决定了组网

收稿日期:2012-07-20;修订日期:2012-08-15
基金项目:重庆邮电大学研究生教育创新计划重点项目;重庆市研究生教育教学改革研究项目(yjg110207);科技创新工程重大项目培育基金项目(教技司计[2008]6号)(708074)
作者简介:王平(1963—),男,教授,博士生导师,研究方向为工业以太网及网络控制技术、汽车电子控制系统;方燕(1987—),女,硕士研究生,研究方向为网络控制技术、无线控制网络及其应用、无线传感器网络;谢昊飞(1978—),男,副教授,研究生导师,研究方向为网络控制技术、协议测试、网络故障诊断等。

的成功与否;其次,顺利完成组网后,实时监控各结点的工作状态,如能量剩余、是否掉线等也是一个重要的问题,决定了该网络能否正常、高效地完成任务。文献[1–2]中采用的是多点分布全信道监听方法,经网关上传至计算机网卡结合 WireShark 软件进行协议分析,系统庞大、造价高、只面向 WirelessHART 协议,且无法在 WireShark 上添加特制功能。

为了应对这些挑战,本实验室在深入研究了物联网无线通信技术[3]的基础上,研发了这款两信道物联网协议分析仪,它具有体积小、易携带、低成本、可面向多种协议等特点,可提供协议测试、网络监控、故障诊断等服务,具有良好的应用前景。

1 基于特征位的快速匹配算法

基于特征位的快速匹配算法用于协议分析软件的协议解码模块,所谓协议解码,就是根据协议所规定的报文格式,逐层地解析数据,得到相应的数据信息。虽然采用逐层次逐字节甚至逐个比特位比较的协议解码方式,能够准确地进行解码。但是,由于需要逐个字节甚至比特位的比较判断,会影响解码的效率。借鉴图像处理中基于特征位的快速匹配算法[4],利用不同协议的相关特征位的取值不同,提取特征位的值进行快速匹配处理,以节省协议解码处理的时间。所谓特征位的快速匹配算法,就是指根据已有的协议数据格式到数据包特定的位置去取值,然后把此取出的值同协议类型中定义的值进行对比可以得出此数据包的具体协议类型,以便于做进一步分析处理。

2 两信道物联网协议分析仪的硬件设计

两信道物联网协议分析仪在硬件结构上比较紧凑,使用单 CPU 处理器结构。系统硬件结构与接口如图 1 所示,主控模块(LPC1114FB)通过两个 SPI 总线通信接口拖带两个无线射频通信模块(UZ2400D),可以实现对两个无线通信模块的寄存器的读写,从而完成对模块通信参数的配置,进一步控制模块对无线数据的收发;主控模块获取两个无线模块传送过来的数据,通过串口转 USB 接口上传至上位机。

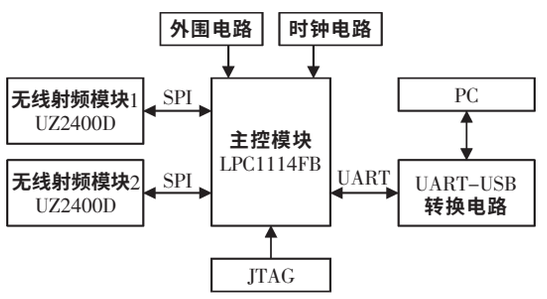

图 1 系统硬件结构

Fig.1 System hardware architecture

本系统数据采集器外形设计为市面上常见的 U 盘模样,体积小,非常便于携带,而且设计为 USB 接口,支持热插拔,可以即插即用;另外系统设计简练,结构紧凑,所以成本也非常低廉。

3 两信道物联网协议分析仪的软件设计

整个系统软件由下层数据采集器软件和上层协议分析软件组成。

3.1 下层两信道数据采集器软件设计

下层数据采集器软件流程图如图 2 所示。

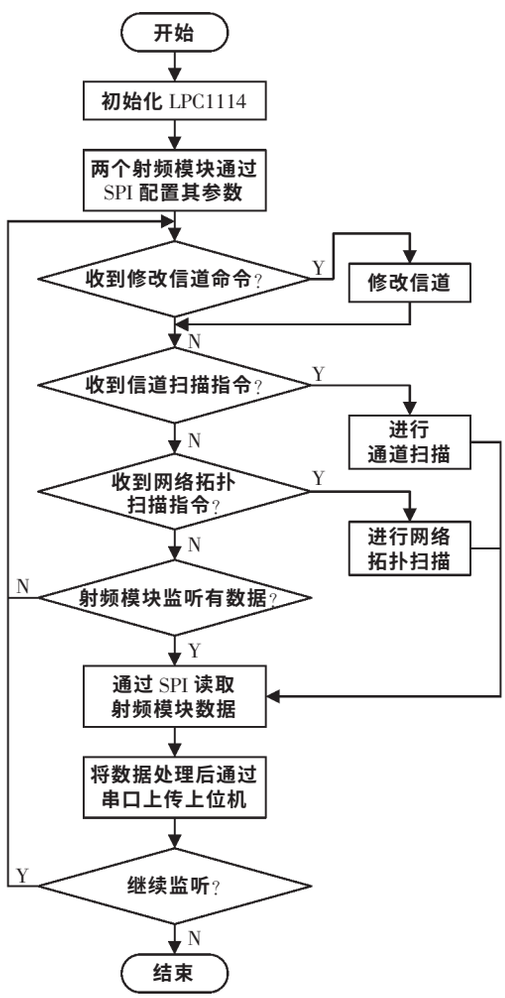

图 2 数据采集器软件流程图

Fig.2 Software flow chart of data collector

首先进行各模块初始化，根据所收到的上位机下发的命令来执行相应的操作：若收到修改信道的指令，则修改监听信道号；若收到信道能量扫描指令，则根据上位机下发的参数进行能量扫描或有效扫描，并将扫描结果暂存于射频模块。若上位机没有下发命令，则处于数据监听状态，主控模块轮询两个射频模块，一旦发现射频模块缓存中有数据包，就将其取出进行处理，添加报文头、信道号、长度、LQI 等信息，并上传给上位机进行协议分析。

3.2 上层协议分析软件设计

3.2.1 数据解码模块

本协议分析仪可以分析 ISA100.11a、ZigBee、WIA-PA、6LoWPAN、IEEE802.15.4E 网络下的报文，通过人机交互界面来设定协议分析仪工作在哪个协议下，虽然协议不同，但解码的思路一致，本文以 6LoWPAN 网络报文为例做一个详细的论述，结合快速匹配算法，剖析协议报文的解码思路。分析 6LoWPAN 协议的报文格式，可以得到几类特征位：物理层的帧长度、MAC 层的帧控制中的帧类型子字段、适配层的 Dispatch 类型字段、网络层的下一个头字段(Next Header)。因此，利用这些特征位对接收到的数据提取对应特征位，进行快速匹配以选择相应的解码方式。解码模块软件流程图如图 3 所示。具体步骤如下：

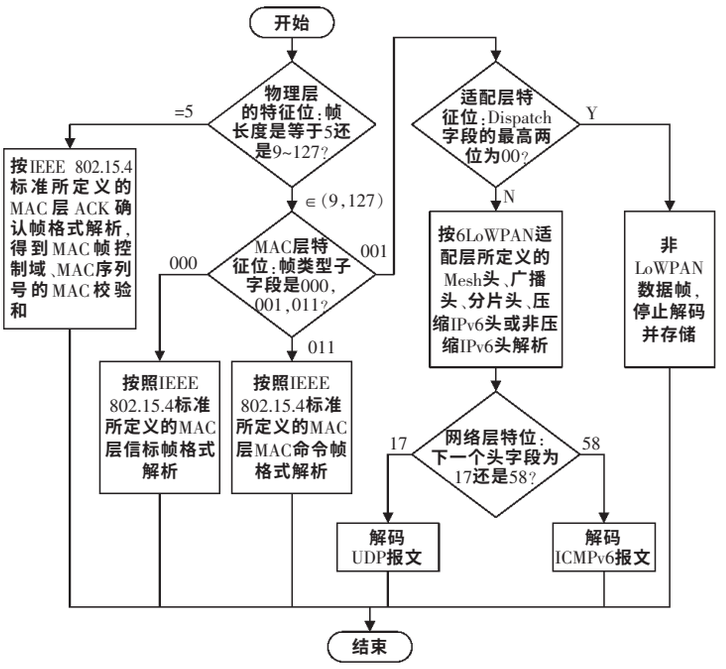

图 3 快速匹配算法解码流程图

Fig.3 Software flow chart of protocol analyzer mode

1)提取物理层的特征位即帧长度，判断取值是等于 5 还是在 9~127 之间。若取值为 5，则表明是 MAC 的 ACK 确认帧，只需要直接解析出 MAC 层的帧控制字段、序列号字段和 MAC 层帧即校验和。若是在 9~127 之间，则需要提取 MAC 层的特征位。

2)提取 MAC 层的特征位，即帧控制中的帧类型子字段。该子字段为 3 个比特位，若取值为 000(二进制)时，则表明是信标帧，需要按照 IEEE 802.15.4 标准规则的信标帧格式进行解析；若取值为 010 则为 ACK 帧；若取值为 011，则表明为 MAC 命令帧，需要按照 IEEE 802.15.4 标准规则的信标帧格式进行解析；若取值为 001，则表明是数据帧，需要提取适配层的特征位。

3)提取适配层的特征位 Dispatch 字段，得到调度头的类型是非 LoWPAN 帧(0x00)，非压缩的 IPv6 数据(0x41)，LOWPAN_HC1 压缩的 IPv6 数据(0x42)，LOWPAN_BCO 广播(0x50)，Mesh(最高两比特位为 10)或分片(最高两比特位为 10)。然后按照调度头的类型解析各类头部，提取网络层的特征位。

4)提取网络层的特征位下一个头字段(Next Header)。若其取值为 58，则表明是 ICMPv6 协议数据，则按 ICMPv6 协议规定的帧格式解码即可；若其取值为 17 则表明是 UDP 协议数据，调用 UDP 协议规定的帧格式解码即可。

3.2.2 信道能量扫描模块

为更好地了解信道和网络的通信状态，设计并实现了信道能量扫描功能，上位机软件给数据采集器发送命令，数据采集器接收到命令后响应并触发相应的扫描函数，获取每个信道的 LQI 值，并将扫描结果上传给上位机进行显示。通过能量扫描可掌控 2.4G 上各信道的信道质量信息。

4 两信道物联网协议分析仪的测试与应用

4.1 功能测试平台的搭建

为了测试两信道物联网协议分析仪进行有效的测试，搭建了一个由两信道物联网协议分析仪、发包设备和 PC 机组成功能测试平台。

4.2 测试内容和方法

测试内容有：数据采集准确性测试、协议

解码正确性测试、能量扫描测试和丢包率测试四个方面。

数据采集准确性测试：用协议分析软件（通过上位机设置分析仪工作在 ZigBee 协议模式下）和无线龙的 Packet Sniffer 同时采集数据包，所得结果分别如图 4 和图 5 所示，对比两者的原始数据包视图（即两图中的 B 区域），发现数据是完全一样的，说明数据采集器采集到的数据是正确的。

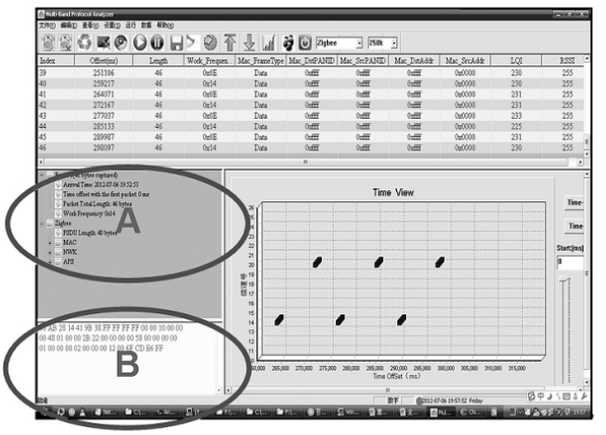

图 4　ZigBee 协议分析仪主界面

Fig.4　Main interface of protocol analyzer for ZigBee

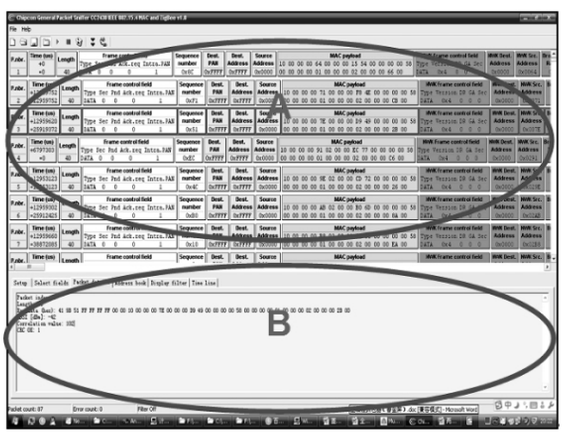

图 5　无线龙 Packet Sniffer for ZigBee 监控界面

Fig.5　Interface of Packet Sniffer for ZigBee from Wu-Xian-Long

协议解码准确性测试：将图 4 中的 A 区域树形控件信息展开得到图 6 所示的详细解析结果，与图 5 中的 A 区域进行对比，发现解析所得的各层帧控制字段、负载信息与无线龙 Packet Sniffer for ZigBee 解析所得结果完全吻合，说明协议分析软件解码模块通过测试，达到预期结果。

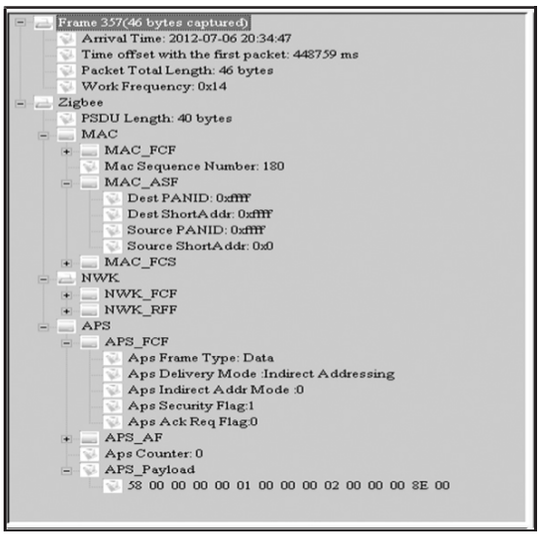

图 6　协议分析视图

Fig.6　View of protocol analyze

能量扫描测试：打开能量扫描对话框，设置扫描参数，启动扫描模块，得到图 7 所示能量扫描结果。

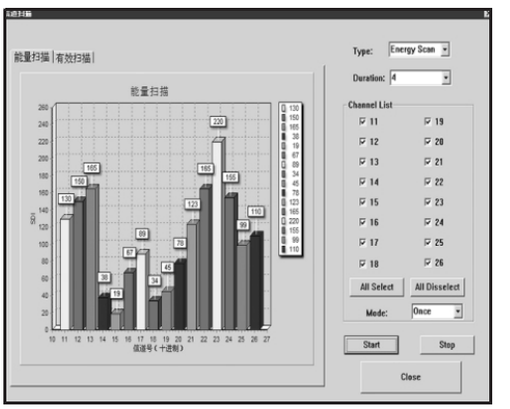

图 7　能量扫描视图

Fig.7　View of energy scanning

在能量扫描过程中，协议分析软件从捕获的数据包中实时获取各信道的 LQI 值，达到实时、动态监控各信道的质量指数，实现了预期功能。

丢包率测试：将发包设备放到 10 m 处进行测试，得到如表 1 所示结果。

表 1　丢包率测试结果

Tab.1　Packet loss rate test results

发包数/min	收包数/min	丢包率/%
600	598	0.33
1200	1194	0.5
2400	2392	0.33
3600	3588	0.33
6000	5966	0.57

测试结果表明，10 m 内丢包率小于 1%，能真实再现网络监控情况，且发包数为 6000/min 时，单帧处理时间为 10 ms，分析仪运行正常，说明分析仪处理时间小于 10 ms，满足实时性要求。

4.3 实例应用

两信道物联网协议分析仪已成功应用于本实验室自主开发的基于 ISA100.11a 标准的 ISA100 无线网络运行系统，该系统网络结构如图 8 所示。

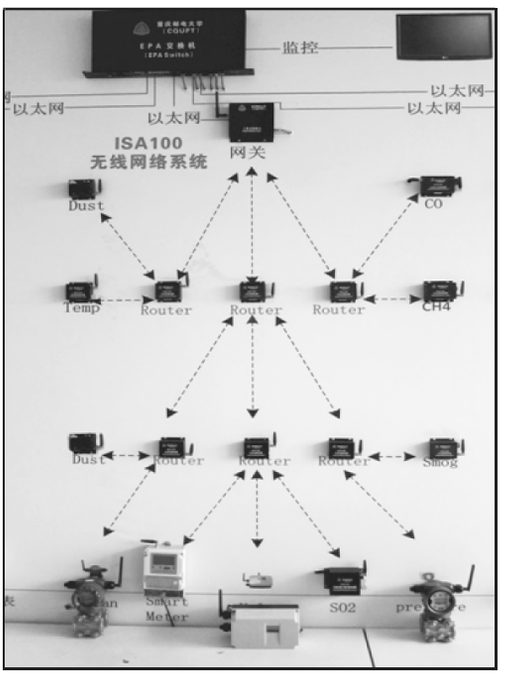

图 8 基于 ISA100.11a 标准的 ISA100 无线网络系统

Fig.8 ISA100 wireless network system based on the ISA100.11a standard

用两信道物联网协议分析仪对上述 ISA100 无线网络系统进行数据检测，得到图 9 所示界面。

因实验室开发的 ISA100 协议栈工作于 0x0D 信道，于是将一个信道设为 0x0D，另一个信道可随便设置，这里设置为 0x19。经过一段时间的观测，本协议分析仪可获取到每个设备所发出的数据包，解析到的数据信息也与预期的相吻合，实现了对整个 ISA100 网络系统的监控，达到了协议分析仪预期设计的目的。

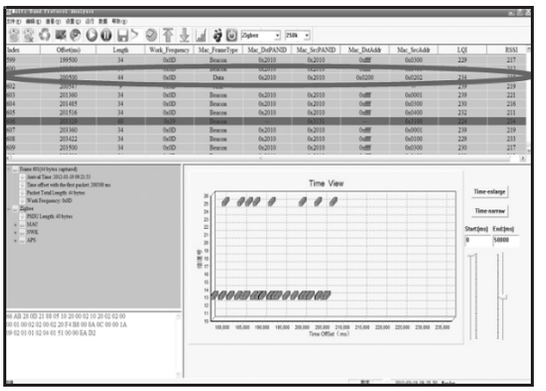

图 9 ISA100.11a 协议分析仪主界面

Fig.9 Main interface of protocol analyzer for ISA100.11a

5 结语

本文介绍了两信道物联网协议分析仪的设计与实现，该分析仪可面向 ISA100.11a、ZigBee、WIA-PA、6LoWPAN、IEEE802.15.4E 五套物联网协议，通过对网内大量报文的分析，可以总结出当前网络的运行状态，以及各个设备的连接方式和通讯状态，实现了协议测试、网络监控、故障诊断等功能。该分析仪在 10 m 内丢包率小于 1%，单帧处理时间小于 10 ms，是一款简单、实时和有效的网络查错、测试以及性能维护工具，目前，已被中国四联集团、韩国汉阳大学等单位应用，并由台湾达盛电子公司(UBEC)进行销售。

参考文献：

[1] Paolo Ferrari，Alessandre Flammini，Daniele Marioli，et al.On the implementation and performance accessment of a WirelessHART distributed packet analyzer[J].IEEE Transaction on Instrumentation and Measurement，2010，59(5)：1342-1352.

[2] A Depari，P Ferrari，A Flammini，et al.Design and priformance evaluation of a distributed WirelessHART sniffer baded on IEEE1588[C]//ISPCS 2009 International IEEE Symposium on Preci sion Clock Synchronization for Measurement，Control and Communication Brescia，Italy，October 12-19，2009.

[3] 王平，王泉，王恒，等.测量与控制用无线通信技术[M].北京：电子工业出版社，2008.

[4] 甘进，王晓丹，权文.基于特征点的快速匹配算法[J].电光与控制，2009，16(2)：64-66.