Hans Journal of Wireless Communications 无线通信, 2011, 1, 43-46
http://dx.doi.org/10.12677/hjwc.2011.12009 Published Online November 2011 (http://www.hanspub.org/journal/hjwc/)

Research of Sniffer Technology of Wireless Sensor Network*

Lei Zhang, Minghui Yuan
College of Optics and Electronics, University of Shanghai for Science and Technology, Shanghai
Email: cumt_zhanglei@126.com; yuan.minghui@163.com
Received: Sep. 1st, 2011; revised: Oct. 7th, 2011; accepted: Oct. 26th, 2011.

Abstract: In order to effectively analysis and evaluate the performance of Wireless Sensor Network (WSN: Wireless Sensor Network), a design of sniffer network based on TinyOS was proposed to monitor the whole network through monitoring the IEEE802.15.4 frame.

Keywords: WSN; Protocol Analysis; Sniffer; TinyOS

无线传感器网络测试技术研究*

张　磊，袁明辉
上海理工大学光电学院，上海
Email: cumt_zhanglei@126.com; yuan.minghui@163.com
收稿日期：2011 年 9 月 1 日；修回日期：2011 年 10 月 7 日；录用日期：2011 年 10 月 26 日

摘　要：为了有效地分析和评估无线传感器网络(WSN：Wireless Sensor Network)性能，提出一种基于 TinyOS 的 Sniffer 网络设计，通过监测 IEEE802.15.4 协议帧来监测整个网络。

关键词：无线传感器网络；协议分析；Sniffer；TinyOS

1. 引言

无线传感器网络(WSN)在国防军事、环境监测、现代农业等诸多领域的应用越来越广泛，已成为新兴物联网的核心组成部分。无线传感器网络工作环境通常较特殊，节点通常采用电池供电，能耗受到严格限制，网络拓扑不稳定，且易受到同频段其他信号如 WIFI，蓝牙等的干扰。因此如何有效监测网络状态，对无线传感器网络的研究和应用都有重要意义。

目前分析和研究无线传感器网络主要有三种方法：理论分析，计算机仿真模拟和实时监测。理论分析模型较易建立，但难以全面反映无线传感器网络，且算法复杂，简化后结果难以让人满意。计算机仿真模拟只能反映网络中部分情况，而且难以实时反映网络的动态变化。通过建立无线传感器监测网络，能够真实地实时反映网络的各种状况，对无线传感器网络的研究和应用具有重要意义。

2. 相关研究

国外的一些大学和研究机构对无线传感器网络监测平台的研究起步较早，但还处于初始阶段。比较著名的有美国俄亥俄州立大学开发的 Kansei 平台[1]、哈佛大学开发的 MoteLab 平台[2]，Crossbow 公司开发的 MoteWorks 平台。Kansei 平台通过便携网络在真实环境中采集数据，采用实际节点与理论模型相结合的混合模拟方法，增大了网络的规模，增强了测试效果，但混合模拟的可信度有待进一步验证。文献[3]中也提出了一种混合式仿真方法。MoteLab 平台节点形式单一，网络规模小，在测试方法和测试评估上有欠缺。网络中的传感器节点采集的数据除了通过射频模块进

*资助信息：上海市教育委员会重点学科建设项目资助项目编号(J50505)；上海理工大学 2011 年度光电学院教师创新基金建设项目(GDCX-T-1102)。

行无线传输外，还将数据送至以太网，占用了自身的CPU 资源。MoteWorks 平台主要缺点在于，节点采集的数据和测试数据都通过无线方式传输，占用了信道的带宽，一定程度上影响了无线传感器网络的通信质量。文献[4]中对以上 3 中方案作了较详细的比较，并讨论了监测平台的通用设计原则和方法。

本文所述的技术方案与以上三种平台不同，采用被动方式监测。在无线传感器网络外部搭建监测节点和监测网络，监测网络与被测的无线传感器网络相互独立。参考文献[5]中介绍了一种被动监测方案，但方案中只有一个监测节点，没有将监测节点网络化。文献[6]中提出了一种采用以太网和路由器实现网络化的方案，测试网络干扰了被测网络的运行。本技术方案通过以太网将监测节点网络化，监测数据通过有线方式传送至监测客户端，对无线传感器网络没有影响。

3. 系统设计

本监测系统主要由传感器节点，串口转以太网模块，监测客户端和以太网络四部分组成，如图 1 所示。

单个监测节点只能监测周围一跳范围内的数据包，无法反映整个无线传感器网络的状况，建立无线传感器监测网络有助于更全面的了解网络状况。监测网络采用有线方式，通过局域网连接。在无线传感器网络中布置若干个监测节点，监测节点与串口转以太网模块连接，串口转以太网模块通过网线接入局域网，监测客户端同样连接于局域网中。每个串口转以太网模块和监测客户端分配独立的 IP 地址，监测节点将监测到的数据通过局域网送至监测客户端，监测客户端根据无线传感器网络的网络协议调用相应的 XML 协议文件，对收到的数据包进行解析。监测节点被动地接收数据包，对被测网络没有造成影响，因此可以真实的反映整个网络的工作状况。

4. 系统实现

4.1. 监测节点设计

监测节点采用 TI 提供的 CC2430 芯片，该芯片支持 IEEE 802.15.4 协议，软件平台采用 TinyOS 系统。TinyOS 系统是专门为无线传感器网络开发的操作系统，采用 nesC 语言编程。TinyOS 系统以组件为基础，通过接口进行连接，用户可以选择或者开发需要的模块，提高了使用的灵活性。

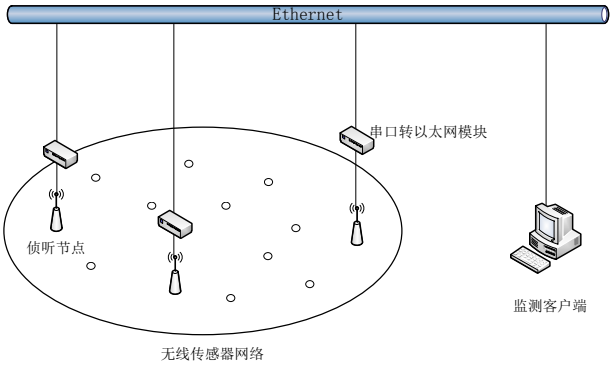

Figure 1. Monitoring system diagram of WSN
图 1. 无线传感器网络监测系统原理图

监测节点只需接收数据包，无需协议栈，因此只需要射频收发组件，串口组件，定时器组件，如图 2 所示。监测节点设计参考了文献[7]中的模块化设计。设置射频组件接收模式为混杂模式，不进行数据包地址确认，接收所有媒介中传播的数据包。串口组件负责向监测客户端传送数据包和接收监测客户端的指令。时钟组件负责提供帧的接收时间，将 32 Mhz 的外部晶振 32 分频后作为时钟，时钟精度达到 1 us。

监测节点接收到环境中的数据包后构造新的帧格式，然后从串口送至以太网。帧格式如图 3 示。

4.2. 串口转以太网模块

串口转以太网模块提供多种工作模式：TCP Server 模式，TCP Client 模式，Real COM 模式，UDP 模式。考虑到网络通信量不是太大，并且为了获得尽可能大的通信速度，这里采用基于无连接的 UDP 模式，以保证数据包的实时性，减少不必要的延时。我们在硬件基础上进行二次开发，根据提供的接口编

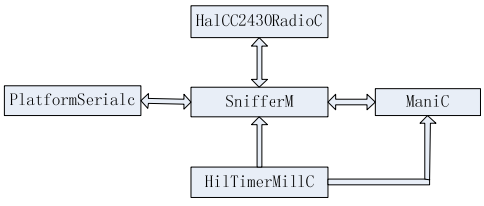

Figure 2. Monitoring node structure
图 2. 监测节点结构图

Figure 3. Serial port frame format
图 3. 串口帧格式

写自己的协议分析软件。

为每个串口转以太网模块分配一个独立的 IP 地址，这些 IP 与监测客户端 IP 在一个网段内。监测客户端协议分析软件启动后，使用 AT 指令配置每个串口转以太网模块的工作模式、IP 地址、端口号等参数。参数配置完成后，即可通过串口转以太网模块实现监测客户端与监测节点间的通信。监测节点将收到的数据包送至监测客户端，并从监测客户端接收指令。

4.3. 监测客户端软件设计

监测客户端协议分析软件负责完成监测网络的同步，汇总融合收到的数据包，解析整合后的数据包，并以图表、曲线等方式显示数据。分析软件主要包括初始化模块，网络同步模块，协议分析模块和显示模块。

4.3.1. 初始化模块

程序启动后首先进入初始化流程，主要完成 3 个方面的工作。IEEE 组织只定义了 802.15.4 协议帧的物理层和 MAC 层，网络层及上层根据使用网络协议不同而不同，对协议的解析放在 XML 文件中。在初始化程序中，根据选择不同的 XML 文件解析不同的协议。

程序在完成上述工作后，开始配置与监测节点连接的串口转以太网模块，在一个网段内查询所有的设备，设置各个设备为 UDP 工作模式，并分配各自的 IP 地址和端口号。

4.3.2. 网络同步模块

协议分析软件为每个监测节点提供一个数据表用来存放数据包，数据包中含有接收时刻。系统启动后通过比较各个数据表中相同帧的接收时刻完成监测网络的同步。同步后监测网络拥有统一的时钟，根据时钟分别读取各个数据表中的数据，存入一个新表中并去除重复帧。文献[8]中采用 PTP 主从时钟模式实现监测网络的同步，较为复杂，对网络规模不大时本设计更为简便。

4.3.3. 协议分析模块

数据包融合线程将各个表中的数据融合到新表中，数据包协议分析线程取表中的数据进行分析，流程如图 4 示。根据数据包中的源地址和目标地址可查询数据包的传输路径。采用逆邻接表保存网络的拓扑结构，将数据包的源地址和目的地址存入邻接表，

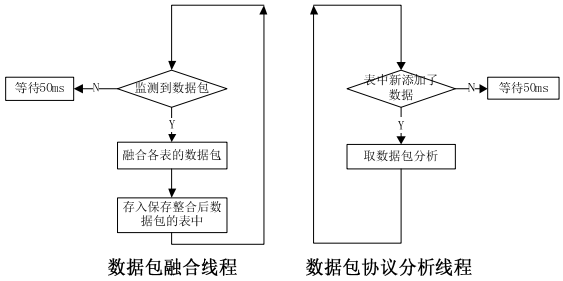

Figure 4. Protocol analysis flow chart
图 4. 协议分析流程图

实时更新邻接表的结构，并可以获取拓扑结构的稳定性。根据数据包的序列号计算丢包率等。文献[9]中提到了无线链路测试，能量消耗测试等方面的测试，在后续的研究中将展开更多方面的测试。

4.3.4. 显示模块

显示模块主要为了方便直观分析和调试，其主要任务包括实时显示监测到的帧信息以及动态显示被监测网络的拓扑结构等。本设计参考了文献[10]提到的多界面显示方式。

5. 实验验证

基于以上方案设计，利用本系统对一组由 30 个节点组成的无线传感器网络进行了测试，无线传感器节点间距 5 米。网络协议采用 CTP 协议，节点间组成树形网络。终端节点定期向根节点传送光度值。在此网络中布置 3 个监测节点并通过串口转以太网模块接入局域网。网络中实时数据包信息如图 5 示。其中，表格中左边信息为数据包各部分内容，右边为该数据包的进一步解析，路由帧将进一步显示它的拓扑父节点，邻居节点以及链接质量等信息，数据包将显示它的传输路径等信息。图 6 中表述了网络拓扑结构的变化，其中横轴为时间轴，单位为秒，纵轴为拓扑的变动次数。

6. 结论

本文设计的监测网络克服了单个监测节点的片面性，并且监测网络和被测网络相互隔离。在 30 个终端节点组成的网络中能够有效的监测整个网络状态，动态显示网络的拓扑结构，监测信息全面。本设计只是初步搭建了监测系统，但具有扩展性，在以后的工作中将逐步深入研究网络的稳定性，网络延迟，节点能量消耗等内容。

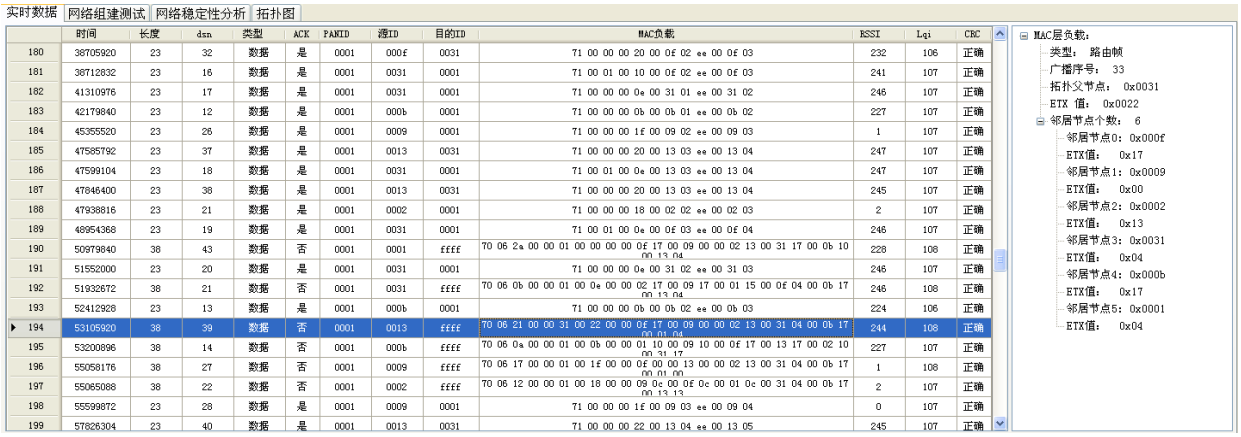

Figure 5. Monitoring test results
图 5. 监控测试结果

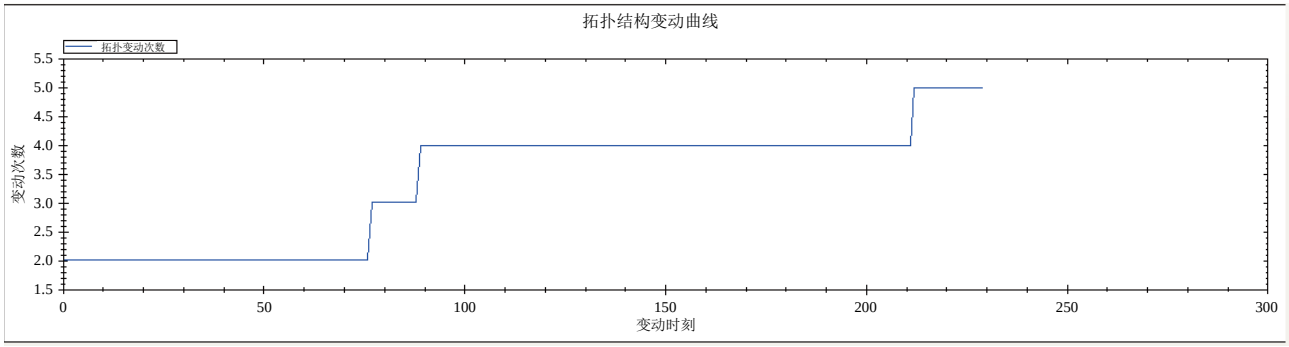

Figure 6. Topology changes curve
图 6. 拓扑变动曲线

7. 致谢

在此特别感谢上海市教育委员会重点学科建设项目(J50505)和上海理工大学 2011 年度光电学院教师创新基金建设项目(GDCX-T-1102)的资金支持。

参考文献 (References)

[1] E. Ertin, A. Arora, R. Ramnath, et al. Kansei: Sensor testbed for at-scale experiments. Information Processing in Sensor Networks, Nashville. New York: ACM Press, 2006: 399-406.

[2] G. Werner-Allen, P. Swieskowski and M. Welsh. Mote Lab: A wireless sensor network testbed. Information Processing in Sensor Networks. Cambridge: ISPN Press, 2005: 483-488.

[3] 王沁, 潘光荣, 王磊等. 一种混合方式的无线传感器网络测试调试系统[J]. 北京科技大学学报, 2009, 31(9): 1200-1206.

[4] 江涌, 谷建华, 杜鹏雷, 马峻岩. 无线传感器网络测试平台研究[J]. 计算机技术与发展, 2009, 20(9): 188-192.

[5] 卢良进, 徐向华, 童超. 无线传感器网络协议分析技术研究与实现[J]. 传感技术学报, 2009, 22(12): 1828-1833.

[6] 焦楠, 龙吟, 王霄, 冯仁剑. 一种无线传感器网络实际环境测试系统[J]. 测控技术, 2010, 29(5): 14-18.

[7] 王建新, 赵鹏伟, 王伟平. Com-WSN: 一种组件化的无线传感器网络测试平台[J]. 计算机工程与应用, 2010, 46(31): 111-114.

[8] X. Kuang, J. H. Shen. SNDS: A distributed monitoring and protocol analysis system for wireless sensor network. Proceedings of 2rd IEEE Conference on Networks Security: Wireless Communications and Trusted Computing, Wuhan, 2010: 422-425.

[9] 柯欣, 舒坚, 任雍, 孙利民. 无线传感器网络测试技术与测试平台研究[J]. 计算机科学, 2007, 34(1): 120-127.

[10] Y. Yang, P. Xia, L. Huang, Q. Zhou, Y. J. Xu and X. W. Li. SNAMP: A multi-sniffer and multi-view visualization platform for wireless sensor networks. Proceedings of 1st IEEE Conference on Industrial Electronics and Applications, Singapore, 2006: 1-4.

