一种基于信誉和能量综合评价模型的 ZigBee 网络

赵跃华， 崔琳洁
（江苏大学 计算机科学与通信工程学院，镇江 212013）

摘要：为有效解决 ZigBee 网络对于内部攻击缺少防范的问题，并兼顾网络性能受制于有限节点能量的不足，文章在 RFSN 模型的基础上，提出一种基于节点通信行为、历史评价和能量的综合评价模型，进而针对不同攻击行为给出相应的路由选择方案及监测标准。仿真实验表明，该模型比 RFSN 模型更能快速准确地识别出恶意节点。

关键词：ZigBee 网络；信誉；能量；综合评价；恶意节点
中图分类号：TP393　　**文献标识码**：A　　**文章编号**：1003-8329(2013)04-0042-06

A Comprehensive Evaluation Model Based on Reputation and Energy in ZigBee Network

ZHAO Yue-hua, CUI Lin-jie
(School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract: There is no security mechanism against internal attacks in ZigBee network, and network performance is subject to limited node energy. On the foundation of RFSN model, a comprehensive evaluation model was proposed, which was based on communication behaviors of nodes, historical evaluation and energy. Then the methods for choosing routing and detecting nodes aiming at different kinds of attacks were given. Simulation results show that the model is more quickly and accurately than RFSN model in terms of identifying the malicious nodes.

Key words: ZigBee network ; reputation; energy; comprehensive evaluation; malicious node

1 引 言

ZigBee 是一种短距离、低功耗的无线通信技术，在工业控制、家庭和楼宇自动化、医疗护理、交通和家用自动化市场等领域都发挥了重要作用，所以它的安全性极其重要。ZigBee 网络容易受到多种攻击，包括外部攻击和内部攻击，但其安全体制更多考虑了外部攻击。一旦某节点被俘获成恶意节点从而发起内部攻击，对网络造成的威胁比外部的将大得多，因此如何检测并去除恶意节点是 ZigBee 网络亟待解决的安全问题。

2 ZigBee 网络安全研究现状

安全问题一直是 ZigBee 网络研究的重要课题之一，其威胁来自于多个方面，按照攻击来源可以分为外部攻击和内部攻击。通常对外部攻击采用加密、身份认证、数字签名等技术措施。当前的 ZigBee 标准已经加入了身份认证、数据加密、数据完整性检

* 作者简介：赵跃华(1958－)，男，江苏苏州人，教授，主要研究方向为信息安全。

查和防重放攻击等安全策略，一定程度上可以抵御外部攻击。目前，ZigBee 网络安全研究也主要集中在安全技术这几个方面。如文献[1]对 ZigBee 技术在安全结构、安全模式、安全密钥等安全方面进行了全面的剖析。文献[2]提出了其安全层所用到的加密算法 AES 的优化方案。文献[3]提出了用非对称加密机制替代原有的对称加密算法的方法。文献[4]中将 SRP 协议、ZigBee 路由协议与路由跳数相结合，以此降低网络总能量和提高数据传输的安全性。另外，文献[5]针对其对称密钥体系在密钥分配和管理方面存在的局限性，提出了基于身份标识加密算法的密钥分配和管理方案。上述分析表明，ZigBee 安全体制更多考虑外部攻击，对内部攻击缺少防范，存在安全隐患。文献[6]提出了基于路由冗余算法来解决这个问题，但是并没有考虑节点能耗对网络性能的影响。

3 模型建立及分析

3.1 攻击及方法分析

本文研究的是 ZigBee 网络层攻击问题，对 ZigBee 网络层的攻击主要有以下几种：选择性转发攻击、虫洞攻击、黑洞攻击、女巫攻击、拒绝服务攻击、泛洪攻击和伪造篡改攻击等等。虽然国内外期刊会议上直接关于 ZigBee 网络内部攻击的文章很少，但是在无线传感器网络中关于内部攻击的研究已取得一些成果，因此可以分析这些研究成果并与 ZigBee 网络特性结合，得到适合 ZigBee 网络的解决方案。比如现在研究较多的基于信誉的恶意节点检测方法就有助于解决其内部攻击的问题。

现有的基于信誉的无线传感器网络恶意节点检测方法主要有：

2002 年，Pietro Michiardi 等人在文献[7]中提出的 CORE 方案，引入了直接和间接信誉值，通过一个公式综合直接和间接信誉值计算出节点的综合信誉值，但存在恶意诽谤和误检问题。

S. Bansal 和 M. Baker 在文献[8]中使用了 OCEAN 的方案，该方案完全只采用本地信誉值，不发送间接信誉值，有效避免了恶意诽谤问题，但是信誉值计算不准确，存在不能及时检测出恶意节点的问题。

2004 年，Ganeriwa - Srivastova 在文献[12]中针对无线传感器网络特性提出了 RFSN 模型，引入贝叶斯公式整合直接信誉和间接信誉，然后将信誉低于阈值的节点判断为恶意节点，但同样无法避免恶意诽谤的问题。

文献[10]对文献[9]提出的方案进行了改进，该方案考虑了网络中多种内部攻击行为，同时引入节点评价行为的概念，并给出了节点间接信誉参数的更新计算方法。

不过现有基于信誉的恶意节点检测方法大都只单独考虑节点的行为是否可信并没有考虑到节点能耗问题。事实上，恶意节点检测会增加节点能耗开销，所以只考虑保障网络安全性却忽视节点能量有限，必将缩短网络的生命周期，进而影响 ZigBee 网络性能。

3.2 综合评价模型说明

在信誉模型中，路由的选择以节点的信誉值高低为衡量标准，通常会选择信誉较高的节点进行通信。因为节点的信誉值越高，说明该节点的可信度就越高，那么该节点被选择执行通信的概率就越大。如果频繁使用这些高信誉值的节点，网络安全性得到一定保障的同时，必然造成这些节点的能量被快速消耗，节点的生命周期就会剧减，不可避免影响网络性能。

提高网络安全性的同时如何保证网络性能良好是必须考虑的问题，本文在 RFSN 模型的基础上，提出一种基于节点通信行为信誉、历史评价和能量的综合评价模型，如图 1 所示。模型将节点能量作为评价节点可信度因素之一，将能量过低的节点赋予相应的低评价值，这样既能避免正常节点由于频繁被选中执行通信而损耗能量，造成生存周期急剧缩短，又可避免选中恶意节点进行通信带来安全威胁。

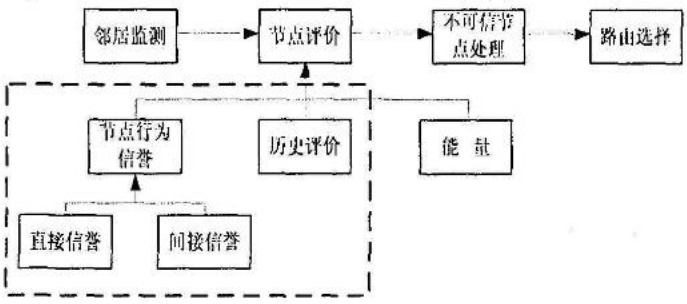

图 1 综合评价模型

图 1 模型中分为四个模块：邻居监测、节点综合评价、不可信节点处理和路由选择。邻居监测用于观测邻居节点的行为，因为 ZigBee 协议允许节点丢弃路由请求 RREQ、路由回复 RREP 和路由错误 RRER，所以邻居监控只需监测数据包。节点综合评价考虑节点行为信誉、历史评价和能量三个因素。节点行为信誉由直接信誉和间接信誉组成，其中直接信誉是监测节点通过自身观察获得对被监测节点行为的评价，间接信誉是监测节点通过第三方节点获得的对监测节点的行为评价。历史评价值是指上一个评价计算周期的节点评价结果。对节点能量的评价值表示该节点的通信能力高低，能量低的节点被赋予低评价值。而各部分将按照一定的权重计算可得最终的节点评价值，当节点的评价值低于阈值的时候，判定节点不可信，将其排除出网络。路由选择以节点评价值为依据。需要注意的是，考虑到 ZigBee 路由特点，模型只用在 ZigBee 的父节点上。

3.3 节点评价的计算

3.3.1 符号说明

相关符号说明如表 1。

表 1 相关符号说明

符号名称	含 义
i,j,k	ZigBee 网络父节点
BR_{ik}	节点 i 得到的关于节点 k 行为的直接信誉
$\alpha(\beta)$	节点 i 对节点 k 行为监测正常(异常)次数的统计结果
BR_{jik}	间接信誉值，是节点 i 得到的其它节点 j 关于节点 k 行为的直接信誉值
BR	节点行为信誉
EE	能量评价值
EV	节点评价值
EV_{old}	历史评价值
EV_{min}	表示阈值，节点评价值一旦低于此阈值，该节点将被判定为不可信
λ_n、w_n	权值

3.3.2 邻居监测

监测模块中，节点被设置成混杂模式，监听任何到达它的数据包，同时观察邻居节点如何处理收到的数据包。模型只应用在 ZigBee 父节点上，父节点之间关系对等，任何节点只能监测自身通信范围内的节点的行为是否正常，如图 2 所示。

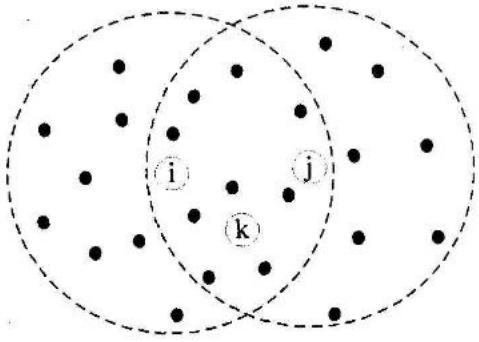

图 2 节点 i、j 的监测范围

图 2 中虚线分别表示为 i、j 的通信范围，节点可以监测自身通信范围内的所有节点，那么一个节点也会被多个节点监控，以节点 k 为例，它在节点 i、j 的监测范围内，同时被 i、j 监控着。

针对不同的攻击行为给出相应的监测标准：

(1) 选择性转发攻击的监测识别方法：对于其它节点给被监测节点 k 发送的每一个数据包，监控节点 i 都需要比较数据包中目的节点是否为 k，若是则不作处理；若不是，则缓存起来。在时间 t_1 内，根据节点 k 发送的数据包数量，计算节点 k 丢包率 r。若 $r > R$(设定的最大丢包率)，将判定节点 k 行为异常，那么 β 的次数增加一次；否则，α 次数增加一次。

(2) 黑洞攻击和自私性攻击的监测识别方法：对于其它节点向被监测节点 k 发送的每一个数据包，监控节点 i 需比较数据包中目的节点是否为节点 k，若是则不作处理；若不是，则缓存起来。观察 t_2 时间内，节点 k 是否发送了和缓存的数据包相同的数据包，若否将判定节点 k 行为异常，那么 β 的次数增加一次；否则，α 次数增加一次。

(3) 虫洞攻击的监测识别方法：监控节点 i 维护一个目的节点列表，对于节点 k 发送的每一个数据包，将数据包中的目的节点地址加入目的节点列表，并将节点地址对应的计数器 C 值加 1。i 保持监听时间 t_3，在时间 t_3 内若列表内某个目的节点地址对应的计数器值远大于其它的，而该目的节点又不是 ZigBee 协调器，则判定节点 k 行为异常，那么 β 的次数增加一次；否则，α 次数增加一次。

(4) 拒绝服务攻击的监测识别方法：如果节点 k 在单位时间内接收到的同一个节点发送的数据包数量 n 超过预定最大值 N，则认为节点 k 的行为异常，那么 β 的次数增加一次；否则，α 次数增加一次。

3.3.3 节点行为信誉计算

(1) 直接信誉

本文参考 RFSN 模型，采用 Beta 概率函数进行节点行为直接信誉的计算。直接信誉 BR_{ik} 即是节点在一个监测周期内直接观察得到的结果，初始时被监测节点相关的 $\alpha(\beta)$ 值均为 0。根据 RFSN 模型给出的直接信誉的计算方法可以得到直接信誉值为 $BR_{ik} = \frac{\alpha + 1}{\alpha + \beta + 2}$。

(2) 间接信誉

间接信誉 BR_{jik} 是节点 i 通过信誉信息交换，从第三方节点 $j(j \geqslant 1)$ 处获得的信誉。实际上，第三方节点发送的信誉值不一定是真实的，存在节点的通信行为正常，却专门恶意提高或诋毁其它节点信誉的可能。是否采纳第三方节点提供的信誉，就需要进行信誉筛选。如果网络中没有恶意节点，也不存在误判，那么 i 和 j 对 k 的直接信誉值的偏差不会太大。所以为了抵御出现恶意提高或诋毁信誉值的问题，将获得的间接信誉进行筛选，将与直接信誉值的偏差在可接受范围 θ 内的间接信誉值进行求均值计算，则 i 将采纳的间接信誉值 $BR_{jik} = \frac{\sum_{j=1}^{n} BR_{jk}}{n}$，$| BR_{ik} - BR_{jk} | \leqslant \theta$。

(3) 节点行为信誉的计算

设 BR 表示节点行为信誉，则 $BR = w_1 BR_{ik} + w_2 BR_{jik}$，其中 $w_1 + w_2 = 1$，$w_1 > w_2$。

3.3.4 能量评价值

本文将监测节点 i 根据对节点 k 的剩余能量的估计值 E_0 和节点 k 自身宣告的能量剩余值 E 进行对比，如果自身宣告的能量剩余值介于能量最低信任值 E_{min} 和估计值 E_0 之间，那么认为节点 k 的剩余能量值是真实可信的，否则认为不可信。那么，能量评价值为 $EE = \begin{cases} E/E_{max} & E_{min} \leqslant E \leqslant E_0 \\ 0 \end{cases}$。

3.3.5 节点评价值的计算

计算时考虑到时限性，只使用最近两个计算周期内得到的评价值参与评价计算。当一个评价计算周期结束，将进行评价值计算，得到的节点评价值在新的计算周期开始后，就成为了历史值。

节点评价值的计算公式：

$$EV = \lambda_1 BR + \lambda_2 EV_{old} + \lambda_3 EE$$
$$\lambda_1 + \lambda_2 + \lambda_3 = 1$$

3.3.6 不可信节点的处理

节点评价值一旦低于阈值，意味着该节点不可信，考虑到二次机会机制可能造成重复攻击问题，所以被评价为不可信的节点将被永久排除出网络。

3.4 路由对策

本文模型的路由对策都是基于节点评价值高低，只与评价值高于阈值的节点进行合作。路由选择过程如下：

(1) RREQ 的转发规则：节点接收到 RREQ 报文后，首先要判断报文是否转发过及自身是否是源节点，如果报文已被转发或自身为源节点，则丢弃该报文，否则，遍历其路由表，根据 RREQ 报文的上一跳节点的评价值高低决定报文发送的次序，优先转发评价高的节点的路由请求，拒绝被评价为不可信节点发起的路由请求，且将数据发送给路由中评价最高的可信节点。如果没有可信的路径，就要发起路由修复，直至找到新的可信路由。

(2) RREQ 的回复规则：

①节点判断该 RREQ 的目的节点是否为自身，检查路由表，查询是否已经回复过 RREP，如果已经回复，则丢弃该 RREQ；

②如果没有回复，则在节点的信誉表中查询该 RREQ 的上一跳节点的评价情况，如果是不可信节点，直接丢弃该 RREQ；否则就回复该 RREQ，并在路由表中记录已回复该 RREQ。

(3) RREP 的回复规则：如果 RREP 报文的上一跳节点不可信，则丢弃该 RREP。如果上一跳节点可信，自身是该条路由的源节点，那么就完成相应的路由表项，否则就完成相应的路由表项并转发该 RREP。

4 实验分析

实验旨在验证本文的模型比 RFSN 模型更能快速准确地检测出不可信节点，选择 Ubuntu 环境下的 NS2 软件进行仿真，将从评价值变化、检测准确率、端到端延迟三个方面对两种模型进行分析比较。

4.1 实验参数

实验参数具体设置如表 2。

表 2　实验参数

名　　称	参数取值
节点数目	50 个
节点分布范围	200m * 200m
移动模式	静止
通信距离	15m
通信模型	CBR
恶意攻击节点比例	0% ~25%
节点的初始能量	2J
仿真时间	300s
评价因素权重($\lambda_1/\lambda_2/\lambda_3$)	0.5/0.3/0.2
节点行为信誉权重 (w_1/w_2)	0.6/0.4
最大丢包率 R	3%
攻击监测时间 $t_1/t_2/t_3$	5s/10ms/5s
能量最低信任值 E_{min}	0.01 J
阈值 EV_{min}	0.3
评价采集周期	10s

4.2　结果及其分析

（1）评价值

实验默认初始时的节点都是可信的，根据模型计算公式，评价值介于 0 和 1 之间，且初始值为 1。为了有效评估两种模型下节点评价值的变化情况，本文在仿真中设定某个节点为发动选择性转发攻击的恶意节点，该恶意节点的评价值变化如图 3 所示。可以看出，本文模型下的恶意节点评价值下降趋势更快，评价值在 100s 后低于阈值 EV_{min}；而 RFSN 模型中直至 150s 评价值才低于 EV_{min}。可见考虑了能量因素的本文模型能够更加快速地反映节点的变化，非常有利于识别出不可信节点。

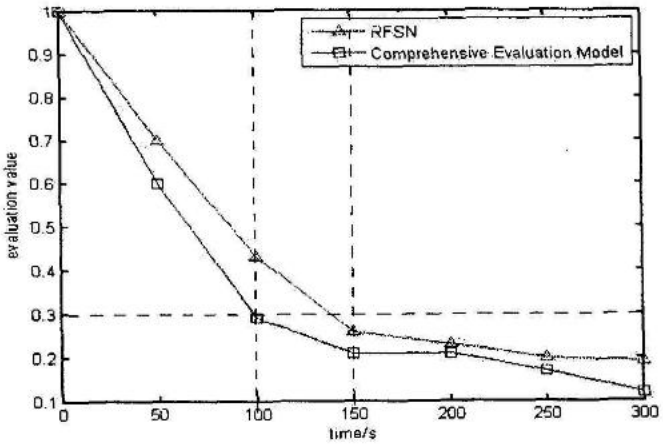

图 3　评价值变化

（2）检测准确率

图 4 描述的是不同恶意节点数目下检测准确率。仿真中恶意节点的数目和类型分别由随机分配数目和平均分配类型得到。仿真中没有将正常节点误检为恶意节点，只有将恶意节点误检为正常节点。图 4 说明本文模型整体的检测率高于 80%，且恶意节点数目低于 6 个时，准确率接近 100%，随着恶意节点数目的增多，检测准确率逐渐降低；相比较而言，RFSN 模型的检测准确率较低。

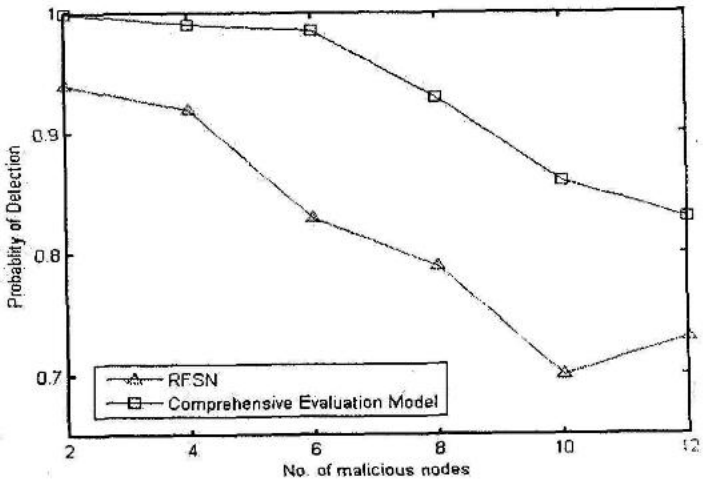

图 4　检测准确率

（3）端到端延迟

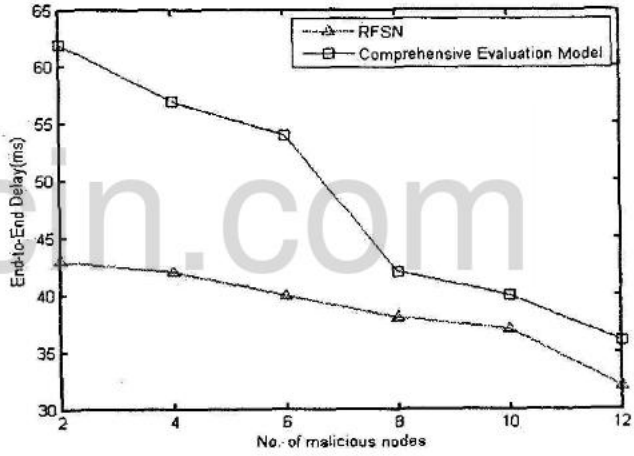

图 5　端到端延迟

从图 5 可以看出本文模型下延迟时间明显高于 RFSN。一方面，本文的模型多考虑了历史评价和能量因素，所以计算量比 RFSN 模型略高；另一方面，模型根据节点评价高低进行路由选择，取代了 AODV 类路由只选择最短路径进行通信的规则。恶意节点的比例较小时，路径的选择较多，需要花较多的时间衡量路由中各节点的评价值高低，选择评价最高的路径来保证安全性，这样的路径不一定是最短路径，会造成延迟现象；而当恶意节点所占比重逐

渐增加时，因为要避开这些不可信的节点，所以可选择的路径反而变少，造成的网络延迟就会降低了。图3、图4表明同等情况下本文的模型比RFSN模型更能快速反映节点评价变化也更能准确识别出恶意节点。也就意味着本文的模型在通信过程中，路径选择造成的延迟时间比RFSN模型的延迟时间更长；但却能更均匀化地使用节点，延长节点生存周期，更好地保证网络性能。

5 总结语

本文提出了一种综合评价模型以解决ZigBee网络的内部攻击问题。仿真实验表明，本文模型的安全性明显优于只考虑节点通信行为的RFSN模型。但由于该模型增加了计算量，在路由操作方面花费更多时间，造成端到端延迟高于基于RFSN模型的网络延迟。该模型可推广运用到使用其他无线通信协议的传感器网络。下一步工作是在保证准确率的前提下降低延时，提高网络性能。

参考文献

[1] 黄太波，赵华伟，潘金秋等. ZigBee安全协议栈的安全体系综述[J]. 山东科学，2012，25(2)：59－66.

[2] 虞志飞，邬家炜. 物联网中基于ZigBee协议的安全算法研究[D]. 华南理工大学，2012.

[3] 冯道水. 基于ZigBee的环境检测系统的安全与干扰分析[D]. 北京邮电大学，2011.

[4] 蒋建平，陈辉. 降低ZigBee网络能耗的路由安全算法[J]. 电子技术应用，2012，38(7)：140－143.

[5] 房国志，李超. 一种基于IBE算法的ZigBee网络加密方法[J]. 通信技术，2010，2(43)：134－135.

[6] 覃志松，黄廷磊. ZigBee无线传感器网络安全研究及改进[J]. 微计算机信息，2010，3－2：116－117.

[7] J. SANG A. A logic for uncertain probabilities[J]. International Journal of Uncertainty Fuzziness and Knowledge－Based Systems，2001(03)：279－311.

[8] J. SANG A. The beta reputation system[C]. Proceedings of the 15th Bled Conference on Electronic commerce. Bled，Slovenia，2002：324－337.

[9] GANERIWAL S，SRIVASTAVA MB. Reputation－based frame work for high integrity sensor networks[J]. SASN'04，New York. Y，USA：ACM，2004，1(1)：66－77.

[10] 杨光，印杜生，杨武等. 无线传感器网络基于节点行为的信誉评测模型[J]. 通信学报，2009，30(12)：18－26.

(收稿日期：2013-04-08)

(上接第41页)

本文提出了硬件课程共享实验平台的思想，采用由PC机实验软件、嵌入式实验控制器和实验模块组成的三层次结构方案，设计了基于PC机和ALTERA DE2－70教育开发板的通用实验平台。通过下层实验模块提供通用端口与上层实验软件自适应性相结合的方法实现了实验内容的自定义，使平台可以完成不同硬件课程的实验；以嵌入NIOS软核的SOPC系统作为实验控制逻辑为实验平台的功能扩充和升级提供了方便。用数字逻辑和计算机组成原理实验为例对平台进行了测试，测试表明，该平台能完成多门硬件课程的实验，除了提供对实验整体方便、直观的测试手段之外，还提供了对任意局部进行验证的功能，为实验者提供了一种快速排错的机制，这些都是传统实验平台很难做到的，因此具有一定的实用价值。

参考文献

[1] 姚爱红. 计算机专业硬件课程实践教学研究[J]. 计算机教育，2007，12：29－30.

[2] 纪金松. 基于可编程器件的实验平台设计与实现[J]. 计算机工程与应用，2006. 34：86－88.

[3] 张丽艳. 基于FPGA平台的计算机硬件实践教学探索[J]. 计算机教育，2010. 7：113－115.

[4] 陈文智. 面向系统设计能力的递进式可扩展课程群的改革探索[R]. 浙江大学. 2012. 4. 21.

[5] 江晋剑. 基于SOPC实验平台的创新型实验方法研究[J]. 微型电脑应用，2009. 3：36－38.

(收稿日期：2013-03-18)