结合贝叶斯网与SFMEA技术的软件故障诊断框架

王学成 李海峰 陆民燕 杨顺昆
(北京航空航天大学工程系统工程系 北京 100191)

摘 要 软件故障已经成为导致系统出错、失效甚至崩溃的潜在与重要根源。因此,故障诊断技术对于保证软件质量具有非常重要的意义。基于人工智能理论的故障诊断技术已经得到越来越多的关注。贝叶斯网理论具有表述方便、推理严密等优点,将其与软件失效模式及影响分析方法相结合,提出了具有四层网络结构(原因层、模式层、故障层以及观察层)的WCMF贝叶斯网诊断模型。在此基础上,提出了基于故障信息数据库及诊断数据库的智能化软件故障诊断框架。最后,针对某数传导航机载软件进行了实例应用。结果表明,提出的WCMF诊断模型及诊断框架是可行且有效的,具有故障诊断方便及时、充分利用历史信息以提高诊断效率、降低时间和资源消耗等优点。

关键词 贝叶斯网,SFMEA,软件故障诊断,WCMF
中图法分类号 TP311 **文献标识码** A

Software Fault Diagnosis Framework Combining Bayesian Networks with SFMEA

WANG Xue-cheng LI Hai-feng LU Min-yan YANG Shun-kun
(Department of Engineering and System Engineering, Beihang University, Beijing 100191, China)

Abstract Software faults are the underlying and important roots which result in the mistake, failure and even breakdown of system. Therefore, the fault diagnosis technology is very significant to software quality assurance. Recently, the fault diagnosis technology based on the artificial intelligence theory attracts more and more attention. Because Bayesian networks theory has some significant advantages, such as easy expression and precise reasoning, a software fault diagnosis model with four layers(namely, reason, mode, fault and watch, short for WCMF) was firstly proposed by combining Bayesian networks with SFMEA(Software Failure Modes and Effect Analysis). Secondly, a software fault diagnosis framework based on the fault information database and the fault diagnosis database was presented. Finally, a case study on navigation software was proposed. The results shown that the fault diagnosis model and presented framework is feasible and effective, which have the following advantages, such as timely and convenient fault diagnosis, improving diagnosis efficiency by utilizing the history information of the faults and their diagnosis.

Keywords Bayesian networks, SFMEA, Software fault diagnosis, WCMF

软件故障已经成为导致系统出错、失效甚至崩溃的潜在与重要根源。软件故障对于软件可靠性甚至软件质量都有重要的影响。因此对故障进行有效诊断,即针对故障现象完成故障的分析和定位,是提高测试中软件质量及可靠性水平的有力保证。随着人工智能技术的不断发展,基于人工神经网络[8]等机器学习技术的各种智能故障诊断方法已经成为故障诊断领域的研究热点。与传统故障诊断技术相比,智能故障诊断技术具有快速、灵活、准确以及智能等优点。其中,贝叶斯网理论由于具有严密的推理过程、语义清晰、可理解性强以及有效的局部计算机制和直观的图形化知识表述等特点,非常适合根据事件(故障)推测原因(诊断)这类不确定性问题的描述,因此已经被广泛应用于软件故障诊断领域。文献[1,3-5]从不同角度对基于贝叶斯网的故障诊断方法进行了深入研究,文献[1]提出了一种具有网络结构的诊断模型,并给出了基于诊断贝叶斯网络的故障诊断算法;文献[3]将贝叶斯网应用于计算机网络节点的故障诊断方法;文献[4]则在基于贝叶斯网的故障诊断方法中引入了专家系统;文献[5]研究了如何利用贝叶斯网不确定推理技术实现端到端服务故障诊断的方法。

上述基于贝叶斯网的软件故障诊断方法基本上都包含如下两个关键步骤[1]:1)根据已知证据来计算这些故障原因的概率信息;2)根据概率信息选择下一步执行的最佳操作(观测或排除操作)。但多数已有成果[1,3-5]都将研究重点放在了如何根据已有信息建立贝叶斯网进而计算故障原因的概率信息上,不足之处体现在:1)未充分讨论如何依据故障特征进行故障原因的定性分析;2)未充分讨论如何根据故障原因概率等信息进行后续的故障诊断操作(例如故障监视、定位等);3)只关注利用贝叶斯网建立故障诊断模型这一个体行为,没有对基于贝叶斯网的故障诊断技术在整个软件开发阶段中的应用过程进行研究。

软件失效模式及影响分析(Software Failure Modes and Effect Analysis,SFMEA)是一种成熟的可靠性设计分析技术[2],可以识别失效的根本原因并评价其可能带来的影响。

到稿日期:2009-10-26 返修日期:2010-01-19 本文受国防技术基础项目"基于软件FTA/FMEA的故障诊断技术研究"(2132007B002)资助。
王学成(1986-),女,硕士生,主要研究方向为软件可靠性设计与分析,E-mail:xc_w@dse.buaa.edu.cn;李海峰(1981-),男,博士生,主要研究方向为软件可靠性建模;陆民燕(1963-),女,研究员,主要研究方向为软件可靠性测试与建模等;杨顺昆(1979-),男,博士生,主要研究方向为软件故障诊断。

文献[6,10]将软件可靠性分析技术与贝叶斯网理论相结合，提出了结合 SFMEA 技术与贝叶斯网的故障诊断方法。虽然该方法从定性分析故障原因的角度对基于贝叶斯网的故障诊断方法进行了完善，但依然没有完全解决前述的不足 2)和 3)。

因此，本文对结合 SFMEA 贝叶斯网理论的软件故障诊断技术展开扩展性研究，主要内容包括：1)结合贝叶斯网与 SFMEA 技术，提出包含故障节点、故障模式节点、故障原因节点以及故障观察节点的四层贝叶斯网故障诊断模型；2)提出基于故障信息数据库与故障诊断数据库的软件故障诊断框架；3)将本文研究成果(四层贝叶斯网络故障诊断模型及故障诊断框架)应用于某型号数传导航机载软件的故障诊断，以验证本文研究成果的可行性以及较已有研究成果的优越性；4)文章的结论及总结。

1 基于贝叶斯网与 SFMEA 的故障诊断模型

本文提出的故障诊断模型是根据 SFMEA 的分析结果，利用贝叶斯网进行图形化定量描述的、具有网络结构的故障诊断模型。模型包含故障节点(F)、故障模式节点(M)、故障原因节点(C)及故障观察节点(W)四层元素集合(简称 WCMF 模型)，其中故障观察节点集 $W=\{W_1,W_2,\cdots,W_s\}$ 表示针对故障原因的监视操作；故障原因节点集 $C=\{C_1,C_2,\cdots,C_l\}$ 表示导致各种故障模式的可能因素；故障模式节点集 $M=\{M_1,M_2,\cdots,M_k\}$ 表示与故障相对应的故障模式；故障节点 F 表示测试过程中发生的故障。C 层、M 层及 F 层可根据 *SFMEA* 分析结果转化得到，而 W 层则需要根据贝叶斯网的推理结果，由软件项目人员针对故障原因分析并进行相应的设置(例如程序插桩)得到。

构建完整的基于贝叶斯网的四层 WCMF 故障诊断模型主要包括如下几个步骤：

第一步　进行软件 FMEA 分析。针对故障所在系统或模块，进行软件故障模式及影响分析，生成 SFMEA 分析表格(具体过程可参见文献[7])。

第二步　从 SFMEA 分析表格中提取三层贝叶斯网故障诊断结构。首先将表格中的故障模式对应贝叶斯网中的模式层节点 $M_1,M_2,\cdots,M_k$，将故障原因对应为原因层节点 $C_1,C_2,\cdots,C_l$，总故障对应为故障层 F 节点。然后将模式节点与对应的原因节点指向模式节点的箭头连接，以表示原因层与故障模式之间的依赖关系。同理，再将模式节点与故障节点连接，得到如图 1 中的三层 CMF 故障诊断结构。

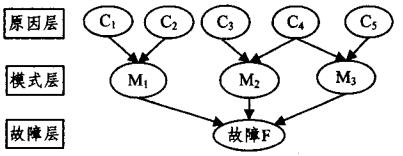

图 1　CMF 三层贝叶斯网故障诊断模型

第三步　量化三层故障诊断结构中各层节点之间的因果关系，形成条件概率表(CPT，Conditional Probability Table)，即给出图 1 中 $p(M_j|C_i)$，$j=1,2,3$，$i=1,2,\cdots,5$ 以及 $p(F|M_j)$，$j=1,2,3$ 的值。该值可由专家经验直接给出，或者依据历史数据进行统计给出。

第四步　贝叶斯网定量推理过程。该过程包括先验概率计算及后验概率计算两部分。

1)计算先验概率。首先依据历史故障信息或者专家经验，分析原因层各节点的先验概率 $p(C_i)$，然后结合 CPT 表中的依赖关系，计算模式层各节点的先验概率 $p(M_j)$，最后计算故障发生的先验概率 $p(F)$，计算公式如下：

$$p(F)=\sum_{j=1}^{3}[p(F|M_j)\cdot p(M_j)] \tag{1}$$

$$p(M_j)=\sum_{i=1}^{5}[p(M_j|C_i)\cdot p(C_i)],j=1,2,3 \tag{2}$$

2)依据证据计算后验概率。在给定根节点证据 $F=1$ 的前提下，计算原因节点的后验概率：

$$p(C_i|F)=\frac{p(F|C_i)\cdot p(C_i)}{p(F)}=\frac{p(F|C_i)\cdot p(C_i)}{\sum_{i=1}^{5}p(F|C_i)\cdot p(C_i)} \tag{3}$$

将各原因节点按其对应的后验概率大小进行排序，依次进行诊断，每诊断一个原因节点后试运行软件，若软件恢复正常，则停止诊断；否则继续进行诊断，直至找出故障原因。

第五步　若发现的故障足够重要(发生频率高或失效后果严重)，则可以考虑在其对应的故障诊断模型中后验概率最大的原因节点处设立故障观察节点。即使该节点并不一定是导致故障发生的原因，但基于最大可能性的考虑，在资源或时间允许的情况下，建议为其设立故障观察节点，以便进行监控操作，使得在测试过程中可以直接查看故障观察节点所处的状态(正常运行或者故障)，为后续诊断过程提供更多的证据及信息，从而有效缩短诊断时间，减少因故障软件运行停滞产生的损失。

可通过程序插桩、数据记录等方式来实现故障观察节点的设置。本文还建议在故障观察节点设置上实现多节点备份，即针对原因节点设立两个或多个故障观察节点，通过表决等手段来保证故障观察节点所提供的监视信息的正确性。

第六步　将故障观察节点层加入到三层故障诊断结构中(假如对节点 C_2 设立故障观察节点)，即可得到完整的 WCMF 四层故障诊断模型，如图 2 所示。

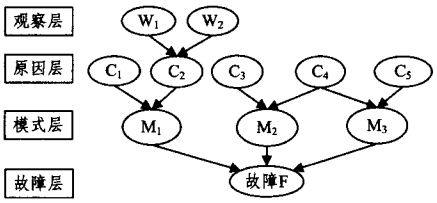

图 2　WCMF 四层贝叶斯网故障诊断模型

2 基于故障信息数据库与故障诊断数据库的诊断框架

将软件测试过程中收集的故障分析信息(故障征兆、故障模式以及故障原因等)整合在一起，可以建成故障信息数据库。而基本上，每个重要(发生频率高或失效后果严重)故障都应有其所对应的 WCMF 故障诊断模型。将这些故障诊断模型整合在一起，即可建成故障诊断数据库。这两个数据库可以为整个软件开发过程的故障诊断提供重要的信息与帮助。因此，本文提出一种基于故障信息数据库与故障诊断数据库的故障诊断框架，如图 3 所示。

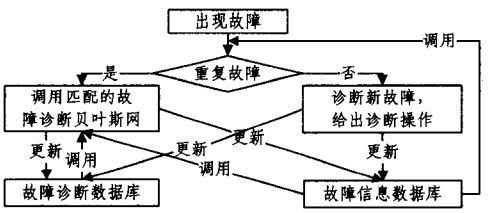

图 3　基于故障信息数据库与诊断数据库的故障诊断框架

构建故障信息数据库和故障诊断数据库是一个收集信息、整理信息的反复过程。限于篇幅，本文不赘述这两个数据库的具体构造过程，而是根据图 3 来阐述由这两种数据库组成的故障诊断框架所包含的主要步骤。

第一步　发现故障

进行软件测试，发现故障，并记录故障时间、位置、现象等征兆信息。

第二步　故障匹配

依据所收集到的故障征兆信息，与故障信息数据库中存储的历史故障信息进行匹配(具体匹配方法可参考文献[8])，判断其是否为历史故障，若是，转第三步；否则，转第四步。

第三步　历史故障诊断

调用故障诊断数据库中与之对应的 WCMF 四层贝叶斯网诊断模型。若该诊断模型中设立观察节点的原因节点未呈现故障状态，则在原 WCMF 模型中去除该原因节点及其故障观察节点。针对新的诊断模型，计算各原因节点的后验概率，按后验概率大小依次诊断。每排除一个故障原因，如果软件正常运行，诊断结束；否则，继续定位故障，直至正常运行，转第五步。若已设立故障观察节点的原因节点呈现故障状态，则将原因节点故障作为发现的子故障，转第二步。

第四步　新故障诊断

根据第 2 节中介绍的故障诊断方法建立新故障的 WCMF 四层贝叶斯网诊断模型，定位排除故障，转第五步。

第五步　更新数据库

若为新故障，将故障征兆及故障原因等信息添加至故障信息数据库，将其故障诊断模型添加至故障诊断数据库，诊断结束。若为历史故障，将其故障征兆及故障原因等信息添加至故障信息数据库，诊断结束。

3　实例应用与分析

本实例为某数传导航机载软件随机故障问题的故障诊断。限于篇幅，本文仅对“输出随机故障、无输出、输出混乱”这一故障(包含若干子故障)进行诊断，具体过程如下。

第一步　故障匹配

将“输出随机故障、无输出、输出混乱”的故障征兆与故障信息数据库中的故障数据进行匹配，确认其是历史故障。

第二步　调出历史故障诊断模型

由于是历史故障，调用故障诊断数据库中对应的 WCMF 四层贝叶斯网诊断模型。如图 4 所示，其中“控制指针信号突变”这一原因节点处设有观察节点，通过故障观察节点发现“指针信号”确实发生了跳变，即该节点状态处于 Fault，因此确认“控制指针信号跳变”为导致“输出随机故障、无输出、输出混乱”故障的发生原因，对其进行进一步的故障诊断分析。

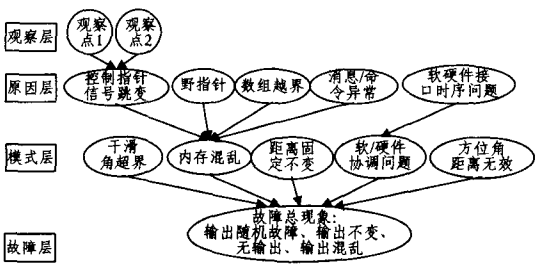

图 4　“输出随机故障、无输出、输出混乱”故障模型

第三步　诊断“控制指针信号跳变”子故障

1)将“控制指针信号跳变”视为子故障做进一步的 FMEA 分析，分析结果如表 1 所列；2)结合 FMEA 分析结果对“控制指针信号跳变”建立一个三层贝叶斯网诊断模型，如图 5 所示；3)与开发人员讨论后得知，故障模式与对应故障原因之间是或门关系，总故障与故障模式之间也是或门关系，即任一故障模式发生均导致输出故障；4)与开发人员讨论，并结合专家意见，得到图 5 中原因层各节点先验概率依次是 40%，40%，10%，20%，10%，20%(自左向右)，则模式层各节点的先验概率为信号干扰 64%、中断处理不当 28%、内存读写同步问题 44%，进而得到指针跳变的先验概率为 88.6%。通过故障观察节点，发现指针发生跳变，因此将“控制指针信号跳变”概率设置为 100%，进而计算其他各节点的后验概率。模式层中，信号干扰、中断处理不当、内存读写同步问题的后验概率分别为 77.2%，31.6%，49.7%；原因层中，干扰源一信号干扰与干扰源二信号干扰的后验概率均为 45.1%，未进行开/关判断的后验概率为 11.3%，现场保护错误的后验概率为22.6%，软件读写同步问题对应概率为 11.3%，软硬件读写同步问题后验概率为 22.6%；5)根据 4)中的计算结果得到故障原因层各节点的后验概率排序为干扰源一→干扰源二→ 现场保护错误→软硬件读写同步问题→未进行开/关判断→软件读写同步问题。此时测试人员按照这样的测试顺序进行定位排错，诊断故障原因为干扰源二，修复后将故障原因添加到故障信息库；6)为干扰源一及干扰源二设立故障观察节点，形成针对“控制指针信号跳变”的 WCMF 四层诊断模型，并将其添加到故障诊断操作数据库。继续运行软件，软件正常工作，则诊断结束。

表 1　指针跳变 FMEA 分析表

故障	故障模式	故障原因
控制指针信号跳变	信号干扰	(1)干扰源一信号干扰
		(2)干扰源二信号干扰
	中断处理不当	(1)未进行开/关中断
		(2)现场保护错误
	内存读写同步问题	(1)软件读写同步问题
		(2)软硬件读写同步问题

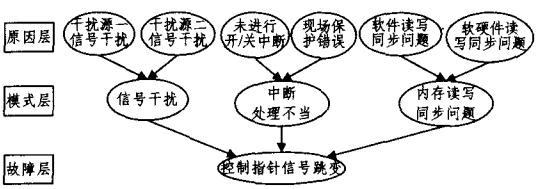

图 5　“控制指针信号跳变”贝叶斯网诊断模型

通过上述实例应用的过程与结果可以看到，本文提出的结合贝叶斯网与 SFMEA 技术的软件故障诊断技术是可行且有效的，与已有的类似软件故障诊断方法[1,2-6]相比，具有如下主要优点：1)快速建立新故障的贝叶斯网故障诊断模型(SFMEA 技术)；2)快速确认并诊断历史软件缺陷(软件故障诊断框架)；3)在后续测试过程中快速定位引发重要故障的原因(四层贝叶斯故障诊断网络中的故障观察节点)。因此，该技术可以有效地帮助测试人员快速排除故障，降低由于软件运行停滞带来的经济损失。结合实例，进一步对比说明如下。

1)与基于贝叶斯网的故障诊断方法[1,3-5]相比：在实例 WCMF 中，对“控制指针信号跳变”这一故障进行 SFMEA 分析(见表 1)，根据 SFMEA 分析结果，可以迅速有效地构建三层贝叶斯网络诊断模型(见图 5)；2)与结合 FMEA 和贝叶斯网的故障诊断方法[6,10]相比：在实例中，利用本文提出的故障诊断方法可以在“控制指针信号跳变”处设立故障观察节点，

这样一旦发生控制指针信号跳变，测试人员可以迅速对子故障进行定位排除，大大缩短了诊断时间；3）此外，在实例中，“输出随机故障、无输出、输出混乱”经与本文提出的故障诊断框架中所包含的故障信息数据库相匹配，判断其是否是重复发生的历史故障，再利用故障诊断框架中的故障诊断数据库，可以直接调用诊断数据库中的历史模型来诊断该故障，从而迅速定位并排除该故障。而传统的故障诊断方法[1,3-6,10]则需要针对该历史故障重新建立贝叶斯网诊断模型，有可能造成测试时间与资源的浪费。

结束语 本文提出含有故障观察节点的四层 WCMF 贝叶斯网诊断模型，在此基础上提出基于故障信息数据库与故障诊断数据库的软件故障诊断框架。本文的研究成果具有如下的优点：首先，本文充分利用 SFMEA 的定性分析结果，可以快速建立有效的贝叶斯网结构；其次，给出了明确的诊断操作，即依据各原因节点的后验概率大小依次诊断，并依据诊断结果实时更新诊断模型；再次，模型中的故障观察节点可以为后续测试过程中及时进行故障定位提供信息；最后，能够充分利用历史故障诊断信息，避免重复的故障诊断，在提高故障诊断效率的同时，降低故障诊断可能带来的时间和资源消耗。综上所述，本文提出的基于贝叶斯网与 FMEA 的诊断模型及框架，能够为复杂系统软件以及安全关键软件快速有效地进行故障诊断提供帮助。需要说明的是，本文所提出的故障诊断模型以及诊断框架尚未工具化，并且实例中各节点或（与）门关系也比较简单，这些将是未来的研究方向。

参 考 文 献

[1] 陈琳，黄杰，龚正虎. 一种网络环境中的故障诊断模型[J]. 北京航空航天大学学报，2004，30(11)：1092-1096

[2] Lutz R R，Woodhouse R M. Experience Report：Contributions of SFMEA to Requirements Analysis[A]// Second International Conference on Requirements Engineering[C]. 1996：44-51

[3] Lee G J，Poole L. Diagnosis of TCP overlay connection failures using Bayesian networks[A]// Workshops of SIGCOMM[C]. 2006：305-310

[4] Ting Han，Bo Li，Limei Xu. A Universal Fault Diagnostic Expert System Based on Bayesian Network[A]// International Conference on Computer Science and Software Engineering[C]. 2008：260-263

[5] 谭琳，胡谷雨，等. 基于贝叶斯网络的计算机网络端到端服务故障诊断[J]. 海军工程大学学报，2005，17(5)：5-9

[6] 何鑫，杨顺昆，刘斌. 基于 FMEA/FTA 的嵌入式软件故障诊断模型与应用[J]. 计算机测量与控制，2009，17(1)：42-45

[7] 申光耀，张刚. SFMEA 技术综述与应用航天型号的探索[A]// 中国宇航学会计算机应用专业委员会学术交流会论文集[C]. 2004

[8] Lee Inhwan，Iyer R K，Diagnosis Rediscovered Software Problems Using Symptoms[J]. IEEE Transactions on Software Engineering，2000，26(2)：113-127

[9] 胡志刚，马好，廖麟. 基于模糊神经 Petri 网的故障诊断模型[J]. 小型微型计算机系统，2005，26(11)：1978-1982

[10] 陈小岗，孙宇，张晓阳. 基于 FMEA 的贝叶斯诊断网络构建方法研究[A]//第十二届全国设备检测与诊断学术会议[C]. 2005

（上接第 71 页）

[2] Ganeriwal S，Kumer R，Srivastava M B. Timing-Sync Protocol for Sensor Networks[M]. New York：ACM Press，2003：138-149

[3] Ganeriwal S，Kumar R，Adlakha S，et al. Network - wide time synchronization in sensor networks[OL]. http://www.ee.ucla.edu/ram，2002

[4] Elson J，Romer K. Wireless sensor networks：A new regime for time synchronization[C]// The First Workshop on Hot Topics in Networks(HotNets-I). New Jersey，USA，2002

[5] Wan Y，Li L，He J，et al. Anshan：Wireless Sensor Networks for Equipment Fault Diagnosis in the Process Industry[A]// Sensor，Mesh and Ad Hoc Communications and Networks，2008. SECON '08. 5th[C]. San Francisco，CA，June 2008：314-322

[6] Edgar H C. Wireless Sensor Networks：Architecture and Protocol[M]. New York：Auerbach Publications，2004：21-110

[7] Industrial communication networks-Fieldbus specifications-WIA-PA communication network and communication pro[EB/OL]. http://www.iec.ch，65C/518/RVD

[8] http://www.isa.org/

[9] 彭瑜. 无线 HART 协议——一种真正意义上的工业无线短程网协议的概述和比较[J]. 仪器仪表标准化与计量，2007(05). http://www.hartcomm2.org/hart_protocol/wireless_hart/wireless_hart_main.html

[10] Romer K，Blum P，Meier L. Time synchronization and calibration in wireless sensor networks[C]// Proceedings of the Ivan Stojmenovic，Handbook of Sensor Networks：Algorithms and Architectures. 2005：199-237

[11] Su Ping. Delay measurement time synchronization for wireless sensor networks[J]. IEEE Micro，2002，122(6)：12-24

[12] Ganerwal S，Kumar R，Srivastava M. Timing-sync protocol for sensor networks[C]// Proceedings of the 1st ACM Conference on Embedded Networked Sensor Systems. Los Angeles，2003：138-149

[13] Maroti M，Kusy B，Simon G，et al. Flooding time synchronization in wireless sensor networks[C]// ACM SenSys'04. Baltinore，Maryland，November 2004

[14] Elson J，Griod L，Esrein D. Fine-grained network time synchronization using reference broadcasts[C]// Proc. 5th Symp Operation Systems Design and Implementation(OSDI 2002). Boston，MA，December 2002

[15] Dai H，Han R. TSync：a lightweight bidirectional time synchronization services for wireless sensor networks[J]. ACM Mobile Computing and Communication Review，2004，8(1)：125-139

[16] Xu Chaonong，Zhao Lei，Xu Yongjun，et al. Broadcast time synchronization algorithm for wireless sensor networks[C]// The 1st Conf on Sensing，Computing and Automation(ICSCA'06). Chongqing，2006

[17] 徐朝农，赵磊，徐勇军，等. 无线传感器网络时间同步协议的改进策略[J]. 计算机学报，2007，30(4)：514-523

[18] Charles S P. Mathematical aspects of heart physiology[OL]. http://www.math.nyu.edu/faclty/peskin/heartnotes/index.html，1975

[19] Hu A，Servetto S D. On the scalability of cooperative time synchronization in pulse-connected networks[J]. IEEE Trans on Information Theory，2006，52(6)：2725-2748

[20] 徐朝农，徐勇军，李晓维. 无线传感器网络时间同步新技术[J]. 计算机研究与发展，2008，45(1)：138-145

[21] Hu A，Servetto S D. A scalable protocol for cooperative time synchronization using spatial averaging[C]// the IEEE/ACM Transactions on Networking. October 2006