基于LEACH和PEGASIS的节能可靠路由协议研究

王国芳,李腊元
(武汉理工大学 计算机科学与技术学院,湖北 武汉 430063)

摘 要:由于无线传感器网络节点的能量是有限的,因此设计能量有效的路由协议是非常重要的。LEACH和PEGASIS是无线传感器网络中典型的层次路由协议。文中在两者的基础上提出了一种改进的节能可靠路由协议,在簇形成过程中低能量簇首节点可以通过寻找替代簇首,均衡负载,避免过早死亡;在簇首之间形成一条链路主干路由,进行数据融合以及多跳传输,并针对链路易断的缺点提出一种可靠传输机制。理论分析及仿真结果表明,新提出的路由协议比LEACH更能均衡并减少能量消耗,延长了网络的生命周期。

关键词:路由协议;簇;链;数据融合
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2009)11-0115-04

Research on Energy-Saving and Reliable Routing Protocol Based on LEACH and PEGASIS

WANG Guo-fang, LI La-yuan
(School of Computer Sicence and Technology, Wuhan University of Technology, Wuhan 430063, China)

Abstract: Since sensor nodes have limited energy, energy efficient routing is very important for wireless sensor network (WSN). Among those protocols developed for WSN, LEACH and PEGASIS are two most classical hierachical routing protocols. In this paper, a novel energy-saving and reliable routing protocol was presented based on LEACH and PEGASIS. In the process of cluster formation, one selected cluster head with low energy could find a high energy node to be its replacer. A chain-based routing for inter-cluster communication between cluster heads was formed to fuse and transform data. To compensate the shortcoming of link routing, one reliable transform scheme was also proposed. Theoretical analysis and simulation results demonstrate that our novel protocol, compared with LEACH, is more efficient to balance and reduce energy consumption and hence prolongs the lifetime of WSN.

Key words: routing protocol; cluster; chain; data fusion

0 引 言

无线传感器网络(Wireless Sensor Network, WSN)是一种特殊的无线自组网,它是由大量密集部署在监控区域的智能传感器节点构成的一种网络应用系统[1]。WSN不需要固定的网络支持,具有快速展开、抗毁性强等特点,可广泛应用于军事侦察、环境监测、医疗监护、农业养殖和其他商业领域,以及空间探索和灾难抢险等特殊领域[2]。

无线传感器节点通常以电池来供电,由于环境恶劣等原因,不太可能进行电池更换,因此网络的工作能力受到了严重限制。如何节能是传感器网络中需要解决的重要问题。设计一种好的通信协议能节省大量能量,从而延长网络寿命。

在WSN体系结构中,网络层的路由技术对WSN的性能好坏有着重要影响。随着国内外WSN的研究发展,许多路由协议被提了出来。从网络拓扑结构的角度可以大体把它们分为两类:平面路由协议和分簇路由协议[3,4]。

分簇路由机制具有节能、无需维护复杂路由信息、便于分布式计算等突出优点,故文中主要基于分簇机制进行研究。在分簇的拓扑管理机制下,网络中的节点可以划分为簇首节点和成员节点两类。在每个簇内,根据一定的机制算法选取某个节点作为簇首,用于管理或控制整个簇内成员节点,协调成员节点之间的工作,负责簇内信息的收集和数据的融合处理以及簇间转发。

LEACH和PEGASIS是两种经典的分簇路由协

收稿日期:2009-02-13;**修回日期**:2009-05-28
基金项目:国家自然科学基金(60672137);教育部博士点基金(20060497015);湖北省科技攻关项目(2007AA101C65)
作者简介:王国芳(1982-),女,河南安阳人,硕士研究生,主要研究领域为无线传感器网络;李腊元,教授,博导,主要研究领域为高性能网络技术及通信协议。

议,它们比起直接传输方式以及最小能量多跳路由协议都有很大的进步,然而它们也有其缺点,笔者结合两者的优点,改善两者的缺点,提出一种新的节能可靠路由协议。

1 LEACH,PEGASIS 简介与分析

1.1 LEACH 协议

LEACH[5](Low - Energy Adaptive Clustering Hierarchy)是 WSN 中最早提出的分簇路由协议。LEACH 的基本思想是通过等概率地随机循环选择簇首,将整个网络的能量负载平均分配到每个传感器节点,从而达到降低网络能量消耗、延长网络生命周期的目的。LEACH 的执行过程是周期性的,每轮循环的基本过程是:在簇的建立阶段,每个节点选取一个介于 0 和 1 之间的随机数,如果这个数小于某个阈值,该节点成为簇首。然后,簇首向所有节点广播自己成为簇首的消息。每个节点根据接收到广播信号的强弱来决定加入哪个簇,并回复该簇簇首。在数据传输阶段,簇内的所有节点按照 TDMA(时分复用)时隙向簇首发送数据。簇首将数据融合之后把结果发给基站。在持续工作一段时间之后,网络重新进入启动阶段,进行下一轮的簇首选取并重新建立簇。

LEACH 作为一种经典的分簇路由算法,取得了比较好的性能,但是也存在缺陷:根据随机选举方式不能保证簇首在网络内均匀分布以及簇的数量,进而导致在经过一段数据传输之后,能量就会出现不均匀的情况。如果一个节点的能量较小,然而在新的一轮中又当选为簇首节点,将会导致该节点的过早死亡。

文中提出的算法,在簇形成过程中,让准簇首增加一次能量检测,如果不符合要求,就把簇首的权利转移给本簇内的高能量节点,这样就会把能量负载均衡的分布在各个节点上,从而延长了网络的生命周期。

1.2 PEGASIS 协议

PEGASIS[6](Power - Efficient Gathering in Sensor Information Systems)形成的簇的结构是一条链。数据传输时,簇首产生一个令牌,发送到链的一端,通知末梢节点开始传送数据。链上每个节点收到上一个节点传来的数据之后,先与自己采集的数据进行融合处理,然后向链上的下一个邻居节点转发,直到数据报文到达簇首,簇首再将令牌发到链的另一端开始同样过程。簇首在融合了两端所传送来的数据报文之后,将报文转发到基站。由于 PEGASIS 的数据融合是在一条链上依次进行的,虽然节省了能量,但却增加了延迟,所以 Lindsey 等人提出了二进制和三层数据融合方案。

PEGASIS 是在 LEACH 的基础上提出的一个基于链的路由协议,理论上它比 LEACH 的性能更加优越,基于分层技术,时间延迟也比 LEACH 的要好很多,然而实际上它却有着致命的缺点:把所有节点串成一个链,如果中间任一个节点失效,这次的数据传输就会失败,而 WSN 往往应用在复杂、危险、恶劣的环境中,拥有密集的、大量的传感器节点,很有可能在某个时刻由于环境的影响导致某个节点暂时或永久失效,这样链就会断裂,进而数据传输失败。

改进协议把 PEGASIS 的链路构建在簇首形成的稀疏网络中,有效降低了网络的能量开销;同时通过增加一个确认重传机制,保证了网络数据的可靠传输。

2 改进算法描述

2.1 网络模型与基本假设

传感器网络由一个基站和大量的传感器节点(简称节点)组成,监测的区域为方形。基站具有足够的能量、内存与计算资源。该传感器网络具有以下性质:

(1)节点部署后不再移动,所有的节点具有相似的能力,地位相等,能量有限,初始能量相同,节点具有 CDMA 通信能力;

(2)基站距离方形区域较远,每个节点能够与网络中任何一个节点通信,也能与基站直接进行通信;

(3)所有的传感器节点一直以一定的频率感知环境,并总是有数据需要传输到基站;

(4)节点消耗能量如公式(1)所示:

$$E_{Tx}(k,d) = E_{elec} * k + \varepsilon_{amp} * k * d^2$$

$$E_{Rx}(k) = E_{elec} * k \quad (1)$$

其中 $E_{Tx}(k,d)$ 表示传感器节点发送 k - bit 数据通过距离 d 时的能耗,$E_{Rx}(k)$ 表示节点接收 k - bit 数据的能耗,E_{elec} 为节点电路部分的能耗速率,ε_{amp} 为信道传输能耗系数,k 为数据量,d 为传输距离 。

2.2 算法描述

针对 LEACH 和 PEGASIS 的优缺点,通过糅合以及改进,提出一种新的协议,以使 WSN 更加节能可靠。新的协议把整个数据传输分为多个轮,每个轮又分为簇的建立,簇间链路路由的建立和数据的稳定传输阶段。

2.2.1 簇的建立

首先根据 LEACH 中的方法选择簇首,簇首节点选出之后,广播自己当选簇首的信号 (advertisement message, ADV),周围节点收到消息后,根据信号强度,选择所属簇首,然后发送一个请求加入信息,此信息除了包含簇首节点 ID 以及自己的 ID 号以外,还需要包含自己的剩余能量状态。簇首在一定的时间内接收到所有簇内成员的加入请求信息后,需要进行一次简单

计算,根据接收到的各成员剩余能量信息,计算簇内平均能量,然后与自己的能量比较:

(1)如果自己的剩余能量大于等于平均能量的百分之三十(该百分比参数可以进一步优化),则与 LEACH 一样,以自己为簇首根据簇内成员数量设置 TDMA 时隙分配表,广播给簇内成员,簇建立完成。

(2)如果自己的剩余能量小于平均能量的百分之三十,则选择簇内剩余能量最大的节点作为替代簇首节点,接着基于该替代簇首计算 TDMA 时隙分配表,然后把替代簇首节点的 ID 号以及已经分配好的 TDMA 表广播给每个簇内成员,自己也作为簇内成员获得自己的时隙分配,同时又要标记自己在本轮中已经充当过簇首角色,以避免再次选为簇首。每个簇内成员接收 TDMA 时隙分配表,同时确认或修正簇首节点 ID。其中簇首代替者接收到该信息后发现其簇首 ID 与自己的相等,则改变自己的状态为簇首,不再发送数据而是接收数据,其它簇内成员的机制与 LEACH 一样。高能量节点代替低能量节点充当簇首的示意图如图 1 所示。簇建立阶段完成。

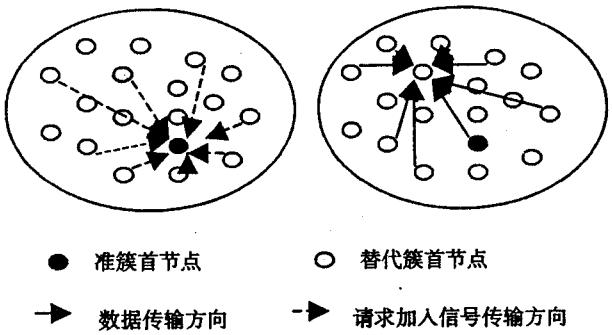

图 1　低能量簇首寻找替代簇首机制示意图

2.2.2　簇间多跳路由的形成

簇建立之后,每个簇首广播一个非持续性强度信号,信号中还要包含自身的 ID,每个簇首接收到其它簇首广播的强度信号,确定出模拟距离信息,记录下来,然后所有簇首节点把这些模拟距离信息发送给基站,同时还要发送自己的剩余能量状况。基站接收到这些信息后采用拓扑扩展技术和贪婪算法,规划出一条链路,确保相邻节点之间的距离最短,同时还要记录下剩余能量匮乏的簇首节点。接下来把这条链路数据结构广播给所有簇首节点,并应用 PEGASIS 中的方法选择一个节点直接与基站进行通信(称这个簇首节点为链首)。链首通过传送一个简单的令牌通知每个簇首的传输方向。这样,簇首间的主干网络就已形成。簇间的链路多跳路由如图 2 所示。

2.2.3　数据传输阶段

数据的簇内传输与 LEACH 中的方法是一样的,每个簇内节点根据 TDMA 表,在自己的时隙内向簇首传输数据。簇首接收完簇内成员的数据并进行融合后,开始向链首方向传输,每个簇首节点接收到上一级节点的数据后进行数据融合,然后再发送给下一跳节点。需要注意的是,发送节点每发送出数据后并不立即清除该数据,而是存储一定的时间,接收数据的簇首一旦接收到上级节点的数据立即返回一个已接收信号,发送节点收到后再把已发数据清除,如果在一段时间内没有接收到反馈信号,则表明该数据发送丢失,则重发一次,如果还是发送不成功,则把该数据发送给链路表中的下一跳簇首节点。在这个过程中,每个接收节点同样设置一个定时器,如果长时间接收不到上一级簇首节点的数据,则不再等待,而是直接把自己的数据向下一跳节点传输。

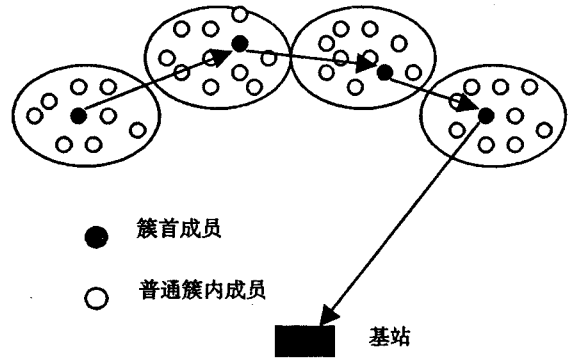

图 2　网络主干链路示意图

数据传输一段时间后,基站选择一个新的簇首节点作为链首与自己直接通信,同时根据记录下来的能量匮乏节点信息,避开这些节点充当链首,以均衡负载。网络主干路由依据这个新的链首再进行一段数据传输。当所有簇首(除了能量匮乏节点)充当过链首之后,整个数据传输将进入新的一轮,进行簇的建立、簇首间路由的建立和数据传输阶段,循环往复。

3　改进算法分析

在分析网络路由协议的时候,需要根据传感器节点的类型,网络类型,以及基站的能力等因素进行适应性研究分析,在此除了考虑能量有效,负载均衡外,还要考虑传输时延以及数据传输可靠性等。

在 LEACH 协议中,每个节点选择所属簇首的时候只是考虑了与簇首的距离,而没有考虑簇首的剩余能量情况。这可能导致当选簇首的低能量节点快速死亡,进而缩短整个网络的生命周期。改进算法在簇建立阶段,通过能量比较和寻找替代簇首,均衡了能量消耗。同时新增的能量比较算法很简单,TDMA 的计算分配与 LEACH 相比基本不增加能量开销,故整体上

增加的延迟与能耗开销很小。

PEGASIS理论上的性能是非常好的。改进算法把链路加在了簇首形成的网络之间能有效利用 PEGASIS 比较适合稀疏网络的特性,而且链路长度比较短。这里要注意几点:

(1)考虑到让每个节点拥有整个网络所有节点的位置信息将会是一个很大的存储开销,改进算法只是让每个簇首节点通过接收其他簇首节点广播的非持续强度信号,根据信号强度估算两者之间的模拟距离,并把该距离信息发送给基站进行链路规划。基站具有充足的能量和较强的计算能力,适合于用来计算并广播主干路由。

(2)有些文献提出了树状主干路由[7],树状路由有其固有缺陷:首先是与基站直接通信的节点不容易更换,每轮换一次就需要重新计算一次路由,而且距离基站较近的节点承担了较大的负载,容易过早死亡。相反,PEGASIS 结构单纯,基站可以方便地选择链首而把能量负载均衡分布在整个链上。树状路由更多考虑的是多跳,而 PEGASIS 更多考虑的是数据融合,同时也实现了多跳。另外,树状路由结构比较复杂,每个节点的子节点个数不等,造成路由控制、时间同步比较复杂。链路性能的其它优越性在文献[6]中已经阐述并证明,此处不再赘述。考虑到数据延迟,在改进协议的基础上还可以运用二进制以及三层数据融合算法。

(3)针对链路易断的缺点提出的可靠传输机制,由于确认信号很小,在链路质量好的时候能耗也就很小;在链路质量差的时候虽增加了一些延迟以及能耗,但却能有效提高数据传输可靠性,因此是值得的。

(4)由于簇间链路能有效减少簇首的能量消耗,同时数据传输阶段存在链首轮换机制,所以在实际网络规划中需要把数据稳定传输阶段时间设置得更长些。

4 仿真实验

这里主要是与 LEACH 进行比较,虽然 PEGASIS 理论上性能比 LEACH 好很多,但前文中笔者已经阐明其实用性有待验证提高,在其上的改进主要是可靠性。同时注意到文中提出的协议更适合于实际的大型 WSN。为了便于仿真分析,采用 NS2 对 LEACH 协议和改进后的算法进行了仿真和比较,假设节点初始能量为 1J, $E_{elec}=50nJ/bit$, $\varepsilon_{amp}=100pJ/bit/m^2$,其中基站位置为(50m,200m),100 个节点随机分布在(0m,0m)到(100m,100m)的方形检测区域中,仿真时间为 700s。图 3 描述了存活节点数与时间的关系,可以看出,改进算法的大部分节点与 LEACH 相比能够延续更长的生命时间,而到了一定时间存活节点数又会骤然下降。这是因为簇间的主干路由能有效降低网络的能耗,同时链首的轮换机制以及成簇阶段避免使用低能量节点的机制都更加均衡了能量负载。图 4 描述了基站接收数据量与网络总能量消耗之间的关系。这里应该清楚:由于改进的协议在主干链路上增加了一些延迟,所以在单位能耗接收数据量的性能上提高不会太多。然而从图中仍可以清楚地看出改进算法比 LEACH 的单位比特能耗要低,这是因为改进路由协议使得每个簇首(除了链首)只是与距离自己最近的簇首节点通信,更重要的是,中间节点通过数据融合,大大减少了需要传输的数据量,减少了能量消耗[8]。

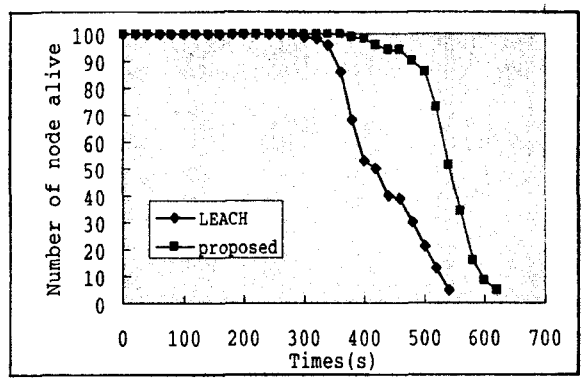

图 3 存活节点数与时间的关系

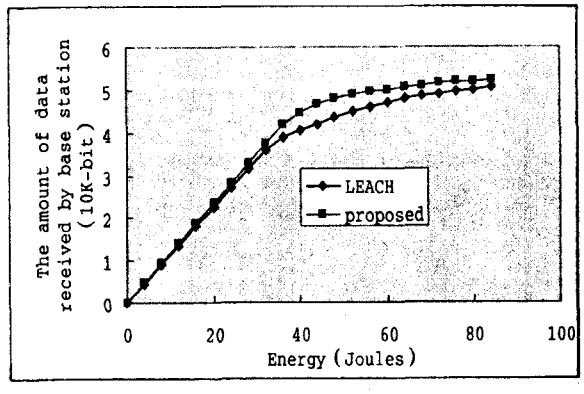

图 4 基站接收数据量与总能量消耗的关系

5 结束语

在分析 LEACH 和 PEGASIS 优缺点的基础上,把两者结合起来,提出了一种改进路由协议。新的协议在成簇阶段加入一个机制用来实现高能量节点替代低能量节点担任簇首,避免低能量节点过早死亡;在簇间形成一个主干链路,用来实现数据融合和转发,同时针对 PEGASIS 的缺点,加入一种可靠传输的机制。理论分析和仿真结果一致表明改进的算法能有效减少节点能量消耗,降低节点死亡速度,有效延长网络生命周期。在一些具体参数的设置优化上,例如链首的更换

(下转第 127 页)

计算量较文献[2]也有改进。其中算法[6,7]所提出的算法基于属性的签名,设每个用户所拥有的属性数量为 U,则其签名密钥和验证密钥的长度均与属性数量成正比,其计算量同样比较复杂,一般要计算一组属性大小的双线性对;设文献[2]中,每个用户用来标识身份的属性个数依然为 m,则在验证签名算法中,需要计算的双线性对为 $3m$,而在 FIBSA 中仅仅需要计算 $m+1$ 次。它们之间的详细差别请见表 1。

表 1　FIBSA 算法与文献[2,6,7]算法的比较

算法	密钥/密文长度			计算复杂度		动态
	λsk	λtk	λc	签名	验证/双线性对	门限
文献[6]	$k\cdot\lvert U\rvert$	$k\cdot\lvert U\rvert$	$k\cdot\lvert U\rvert$	$O(\max(l,t))$	L	否
文献[7]	$k\cdot\lvert U\rvert$	$k\cdot\lvert U\rvert$	$k\cdot\lvert U\rvert$	3	$O(\lvert u\rvert)$	否
文献[2]	$k\cdot\lvert m\rvert$	无	$k\cdot\lvert m\rvert$	$O(m)$	$3m$	否
FIBSA	constant	constant	constant	$O(m)$	$m+1$	是

5　结束语

FIBSA 签名算法由于其签名密文是固定大小的,且计算量也比较小,因此对资源的要求不高,可以用于资源受限的网络,如 Ad-hoc,WSNs 中。下一步的工作将进一步降低在验证签名时算法的复杂性。

参考文献:

[1] Delerabl'ee C', Pointcheval D. Dynamic Threshold Public-Key Encryption[C]//Wagner D. Advances in Cryptology-Proceedings of CRYPTO2008. Santa Barbara, California, USA: Springer-Verlag, 2008: 317-334.

[2] Yang Piyi, Gao Zhenfu, Dong Xiaolei. Fuzzy identity based signature. Cryptology ePrint Archive: Report 2008/002[EB/OL]. 2008. http://eprint.iacr.org/2008/002.pdf.

[3] ZHU ZhenChao, ZHANG Yuqing, WANG Fengjiao. An Efficient Identity-based Ring Signcryption Scheme. Cryptology ePrint Archive: Report 2008/254[EB/OL]. 2008. http://eprint.iacr.org/2008/254.pdf.

[4] Selvi S S D, Vivek S S, Karuturi N N. Cryptanalysis of Bohio et al.'s ID-Based Broadcast Signcryption (IBBSC) cheme for Wireless Ad-hoc Networks. Cryptology ePrint Archive: Report 2008/247[EB/OL]. 2008. http://eprint.iacr.org/2008/247.pdf.

[5] Sun Xun, Li Jian-hua, Chen Gong-liang, et al. Identity-Based Directed Signature Scheme from bilinear maps. Cryptology ePrint Archive: Report 2008/305[EB/OL]. 2008. http://eprint.iacr.org/2008/305.pdf.

[6] Li Jin, Kim Kwangjo. Attribute-Based Ring Signatures. Cryptology ePrint Archive: Report 2008/394[EB/OL]. 2008. http://eprint.iacr.org/2008/305.pdf.

[7] Maji H, Prabhakaran M, Rosulek M. Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance. Cryptology ePrint Archive: Report 2008/328[EB/OL]. 2008. http://eprint.iacr.org/2008/328.pdf.

[8] Khader D. Attribute Based Group Signatures. Cryptology ePrint Archive: Report 2007/159[EB/OL]. 2007. http://eprint.iacr.org/2007/159.pdf.

[9] Boneh D, Boyen X, Goh E J. Hierarchical identity based encryption with constant size ciphertext[C]//In Cramer R. EUROCRYPT 2005. Berlin, Germany: Springer-Verlag, 2005: 440-456.

[10] Delerabl'ee C', Paillier P, Pointcheval D. Fully collusion Secure Dynamic Broadcast Encryption with Constan-size Ciphertexts or Decryption Keys[C]//Takagi T, Okamoto T, Okamoto E, et al. Proceedings of the first International Conference on Pairing-based Cryptography (2007). [s. l.]: Springer-Verlag, 2007: 39-59.

(上接第 118 页)

频率、数据传输阶段时间长度等,需要进一步定量分析,今后需要在这方面继续研究。

参考文献:

[1] 任丰原,黄海宁,林　闯. 无线传感器网络[J]. 软件学报, 2003,14(7):1282-1291.

[2] 崔　莉,苗　勇,赵　泽,等. 无线传感器网络研究进展[J]. 计算机研究与发展,2005,42(1):163-174.

[3] 杨菊英,吕光宏. 无线传感器网络分层路由协议研究[J]. 计算机技术与发展,2008,18(6):115-118.

[4] Akkaya K, Younis M. A Survey of Routing Protocols in Wireless Sensor Networks[J]. Ad Hoc Networks, 2005, 3(3): 325-349.

[5] Heinzelman W B, Chandraskan A P, Blakrisshnan H. An Application Specific Protocol Architecture for Wireless Microsensor Networks[J]. IEEE Trans. on Wireless Communications, 2002, 1(4): 660-670.

[6] Lindsey S, Raghavendra C S, Sivalingam K M. Data Gathering Algorithms in Sensor Networks Using Energy Metrics[J]. IEEE Transactions on Parallel and Distributed Systems, 2002, 13(9): 924-935.

[7] Chen Jing, Yu Fengqi. An Uniformly Distributed Adaptive Clustering Hierarchy Routing Protocol[C]//In Proceedings of the 2007 IEEE International Conference on Integration Technology. Shenzhen: [s. n.], 2007: 628-632.

[8] 王　娟,王汝传,孙力娟. 数据融合在传感器网络协议中的节能性分析[J]. 计算机技术与发展,2006,16(11):4-6.