文章编号:1001-506X(2010)12-2711-05

能量有效的无线传感器网络可信路由协议

李凌晶, 孙力娟, 王汝传, 黄海平, 肖 甫
(南京邮电大学计算机学院江苏省无线传感网高技术研究重点实验室, 江苏 南京 210003)

摘 要: 如何更有效地利用节点有限的资源是无线传感器网络研究的热点之一。提出的能量有效的可信路由协议(energy efficient reliable routing protocol, EERRP),采用了一种能量均衡策略,使网络中的能量均衡消耗,将网络生命周期最大化。同时,EERRP 引入了信誉评价机制,通过节点在数据传输过程中对其他节点行为的监测以及信誉传播,使数据在通信过程中能够尽可能地避开问题节点到达目的节点,达到可信数据传输的目的。通过在 NS 仿真平台对 EERRP 进行测试与验证,并将其与传统路由协议进行比较,证明 EERRP 在网络能量有效性和数据可信传输方面具有明显优势。

关键词: 无线传感器网络; 路由协议; 能量有效; 可信
中图分类号: TN 911.23 **文献标志码**: A **DOI**:10.3969/j.issn.1001-506X.2010.12.44

Energy efficient routing reliable protocols in WSNs

LI Ling-jing, SUN Li-juan, WANG Ru-chuan, HUANG Hai-ping, XIAO Fu
(*Jiangsu High Technology Research Key Lab. of Wireless Sensor Networks, Coll. of Computer, Nanjing Univ. of Posts and Telecommunications, Nanjing 210003, China*)

Abstract: The recent interest in sensor networks has led to a number of routing schemes that use the limited resources available at sensor nodes more efficiently. A novel energy efficient wireless sensor network routing protocol called EERRP is proposed. This routing protocol uses a lightweight strategy, which makes the network consumption of energy balanced. And the routing protocol adopts an evaluation mechanism of credibility, by means of which the nodes monitor other nodes' action and spread of the credibility in data transmission, as a result, the data can reach the destination nodes smoothly without the interference of malicious nodes. Through the NS simulation platform for testing and verification, EERRP, which is compared with traditional routing protocols, proves the obvious advantages on the effectiveness and reliability of data transmission and energy saving.

Keywords: wireless sensor networks; routing protocol; energy efficient; reliability

0 引 言

无线传感器网络(wireless sensor networks, WSNs)的大规模性、自组织、可靠性等特点使其在军事、环境、医疗、家庭和其他的商用领域有广阔的应用前景和很高的应用价值[1]。但是,由于无线传感器网络要求节点的平均能耗更低,传感器节点通常携带能量十分有限的电池,而传感器节点个数多、分布区域广并且部署区域环境复杂,所以为大量的传感器节点频繁地更换电池是不现实的[2]。因此,为了获得最长的工作时间,要求在网络运行的过程中,每个节点都要使自身能量消耗最小化。在无线传感器网络中如何高效地使用能量来最大化网络生命周期是一个具有挑战性的问题,它已经得到了广泛的关注[3]。

随着无线传感器网络的广泛应用,尤其是在军事与商业方面。这需要网络具有足够的安全可信性,而无线传感器网络的工作环境特点使网络本身存在许多安全漏洞,易受到多种类型的攻击[4],所以可信路由成为无线传感器网络另一个重要的研究方向。但是在网络能量受限的情况下,普通的路由安全机制并不适合无线传感器网络。

因此如何在无线传感器网络能量受限的情况下,保证网络的安全性,使数据能够从源节点可信地到达目的节点,是本文所要研究的重点内容。

收稿日期:2009-08-11; **修回日期**:2010-04-27。
基金项目:国家自然科学基金(60973139,60903181,60773041,61003039,61003236);江苏省科技支撑计划(工业)(BE2010197,BE2010198);江苏省级现代服务业发展专项资金、江苏省高校自然科学基础研究(10KJB520013);高校科研成果产业化推进工程(JH10-14);国家和江苏省博士后基金(0801019C,20090451240,20090451241);江苏省高校科技创新计划(CX09B_153Z, CX10B-197Z,CX10B-200Z);江苏省六大高峰人才项目(2008118)和江苏省计算机信息处理技术重点实验室基金(2010)资助课题
作者简介:李凌晶(1986-),男,博士研究生,主要研究方向为无线传感器网络和信息安全。E-mail:WOWshaman@163.com

1 现有的无线传感器网络路由

目前,现有的无线传感器网络路由协议在各个方面、不同程度的存在一些缺陷[5]。大致上可以将现有的无线传感器网络路由协议分为以下几类:能量感知路由协议、基于查询的路由协议、地理位置路由协议和提供可靠保证的路由协议等[6]。

能量感知路由协议是最早提出的无线传感器网络路由协议之一,从节点的能量利用效率及网络生存期的角度考虑路由选择,但是条件太过理想化,而且需要知道整个网络的拓扑结构。因此,Shah 等人在 2002 年提出了一种改进的能量感知的多路径路由机制[7],但是它需要通过周期性地从目的节点到源节点实施洪泛查询来维持所有路径的活动性。定向扩散(directed diffusion, DD)是一种典型的基于查询的路由协议[8],基于查询的路由协议给路由带来的问题是,建立路径开销较大。地理位置路由需要知道整个网络所有节点的地理位置和拓扑结构,有较大的通信开销,还具有被攻击的隐患,因此杨光等人在 2008 年提出了一种基于 GEAR 改进的 R-GEAR 路由机制[9],他们在 GEAR 的基础上提出了加入信任机制,使得 GEAR 的安全性大大增强。提供可靠保证的路由协议主要从传输可靠性和实施性方面讨论了传感器网络的路由机制,但是通常是通过增加冗余的方式来达到保证通信可靠性的目的,造成网络能量的部分浪费,虽然保证了数据可靠性,却造成了其他的安全隐患。而在 2006 年,Lou 等人在 SPREAD 机制的基础上又提出了一种混合多路径机制[10],把一个数据分组分成多个分片在 N 条路径上传输,攻击者需要截获至少 $M(M<N)$ 条路径上的消息才能获得消息,而在接收端,只需要接收到 M 条路径以上的消息即可复原数据信息。这种机制在安全性上对多路径路由提出了改进方法,但是未讨论能量的消耗。许多目前讨论传感器网络安全性的路由协议对能量的消耗也没有过多考虑。

由于传感器网络中路由协议具有应用相关性,所以还没有出现一个普遍适用的无线传感网络路由协议。针对上面路由中存在的问题,本文在现有的一些研究基础上提出一种新的能量有效的可信路由协议(energy efficient reliable routing protocol, EERRP)。该协议在无线传感器网络中各种资源有限的情况下,合理地利用有限的能量使数据信息能够通过一条可信路径最终到达 Sink 节点,并且均衡网络中能量消耗,最大化延长网络的生命周期。

2 能量有效的可信路由协议

在无线传感器网络中,Sink 节点处理能力和存储能力很高,而且一般不存在普通节点的能量有限的问题[11]。因此,本文提出的能量有效可信路由协议 EERRP 假设 Sink 节点是绝对安全而且是值得信任的,Sink 节点的所有行为都是正确的。

EERRP 主要分为网络初始化、路由建立、可信度更新和路由更新 4 个阶段:

(1) 网络初始化阶段:在网络初始时,由 Sink 节点开始进行洪泛,使全网建立拓扑关系,每个节点建立自己的邻居节点列表。

(2) 路由建立阶段:当网络中某个节点产生数据要发送给 Sink 节点时,通过自己邻居列表中记录的邻居节点信息选择下一跳数据转发节点,并且监听下一跳节点行为。

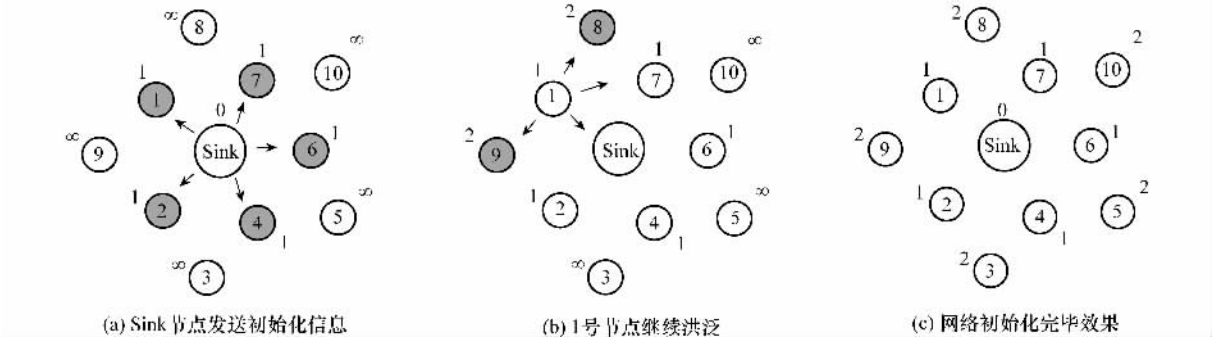
(3) 可信度更新阶段:与第(2)阶段路由建立阶段同时进行,当发现节点可疑行为的时候,对其可信度进行更新,并通知周围节点。

(4) 路由更新阶段:当网络的拓扑结构发生变化后,更新节点与 Sink 的距离信息。

2.1 初始化阶段

在网络刚刚部署完成时,由 Sink 节点开始每个节点发送次 HELLO 消息进行洪泛,使收到 HELLO 消息的节点获得发送方的 ID 号,能量以及距 Sink 节点的跳数等信息,并且计算出自己距离 Sink 节点跳数的信息,为数据转发选择路径做好准备。初始化阶段完成后,全网中的所有节点都保存其邻居节点的信息,以及邻居节点到 Sink 节点的跳数信息。

图 1(a)表示由 Sink 节点发起洪泛,图 1(b)表示 1 号节点收到 Sink 节点的 HELLO 消息后继续进行发送,8、9 号节点修改自己距离 Sink 节点跳数,7 号节点只将 1 号节点加入自己邻居列表而不修改自己距离 Sink 节点的跳数,最终效果如图 1(c)。



(a) Sink 节点发送初始化信息 (b) 1 号节点继续洪泛 (c) 网络初始化完毕效果

图 1 初始化阶段过程示意图

每个节点收到 HELLO 消息后,在邻居表中记录的信息格式如下:

NODE ID	ENERGY	HOP	CREDIBLE	FAIL NUM

2.2　路由建立阶段

当节点 i 产生数据要发送给 Sink 节点时,开始建立路由。节点 i 根据自己的邻居节点的剩余能量、到 Sink 节点的跳数及节点 i 对其邻居节点的信任度进行综合考虑,通过计算节点 i 的每个邻居节点的 EHC(能量、跳数、可信的综合加权参数)来选择下一跳节点。

$$EHC_j = \alpha E_j + \beta H_j + \chi C_j \tag{1}$$

式中,$\alpha+\beta+\chi=1$,可以根据需要选择三个因素的权重因子大小,决定在下一跳节点的选择上是更偏向安全还是能量。E_j、H_j、C_j 分别代表节点 j 的能量参数、距离 Sink 的跳数及可信度参数。

节点 i 在选择某一邻居节点 j 并发送了数据之后,会等待其返回的 ACK 确认信息,对节点 j 进行信誉评价,更新节点 j 的可信度,为下一次选择数据传输节点做准备(具体见 3.3 节可信度更新阶段)。假如节点 j 并未在规定的时间内返回一个 ACK确认信息,节点 i 在 EHC 列表中选择 EHC 值第二小的节点 k,作为新的下一跳数据传输节点继续进行发送。

下一节点 k 接收到 i 的数据后按照以上过程继续转发,直到数据传输至 Sink 节点。

在数据传输过程中某个节点被选中作为下一跳数据传输节点后,由于能量消耗,下一次优先被选中的概率降低,使得整个网络中节点能量可以呈平均消耗的趋势。

2.3　可信度更新阶段

通过节点对自己的下一跳节点行为的监测,来对其信誉进行评价,如果下一跳节点工作正常一次,则对其信誉进行奖励;否则进行处罚。方法如式(2)和式(3)

$$C_{\text{now}} = C_{\text{now}} + Value_1 \tag{2}$$

$$C_{\text{now}} = C_{\text{now}} - Value_2^n \tag{3}$$

式(2)与式(3)中的 $Value_1$ 与 $Value_2$ 分别可以根据情况设定,式(3)中的 n 代表失败次数。通过这个机制,当节点发生若干次不正常的通信行为后,其信任值将呈指数型降低,周围节点可以迅速发现问题节点的存在;而如果只是网络拥塞造成的节点 i 某次未能收到节点 j 的确认消息,节点 j 仍然能够通过之后的正常通信,使自身的信任值线性增加。

节点监测到可疑行为后,还要向周围节点通报。如图 2 所示,当 1 号节点检测发现 2 号节点的行为可疑并更新其信任值之后,要向 1 号节点的其他邻居节点通报 2 号节点的信任值变化,要求其他节点同步修正 2 号节点的信任值。而 4 号节点的邻居节点中没有 2 号节点,所以将忽略这个消息,而 3 号节点将根据消息修改自己对 2 号节点信任值。

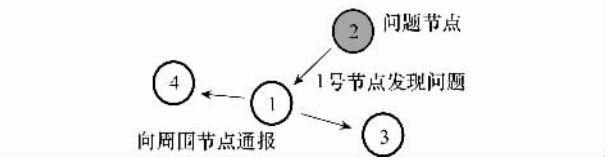


图 2　更新信任过程示意图

消息中报告 1 号节点对 2 号节点的信任值已经被更改为 C_{12},3 号节点对 2 号节点的可信度修改需要联合自己原本对 2 号节点的信任值 C_{32} 以及 3 号节点对 1 号节点的信任值 C_{31} 三个方面来计算对 2 号节点新的信任值。3 号节点对 2 号节点的信任值更新方法为

$$C_{32} = \mu C_{32} + \eta C_{31} C_{12} \tag{4}$$

若将 1、2、3 号节点分别对应节点 i、j、k,式(4)形式化为

$$C_{kj} = \mu C_{kj} + \eta C_{ki} C_{ij} \tag{5}$$

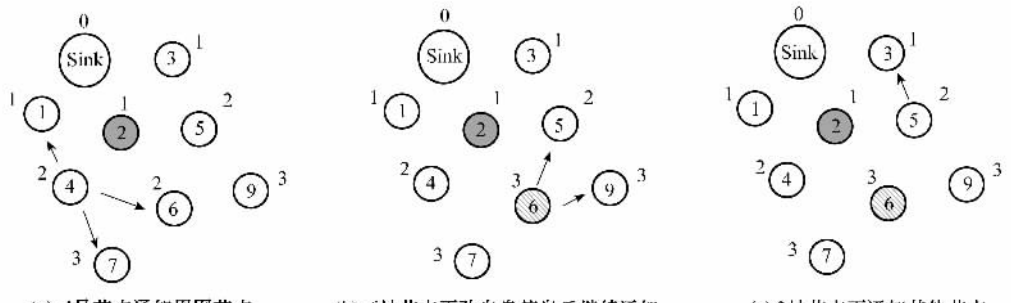
式中,$\mu+\eta=1$,由于节点要信任自己本身的监测情况,所以一般来说取 $\mu > \eta$。

当某个节点的可信度降低到某个门限值以下,则将其列为恶意节点加入黑名单,之后其不会再被挑选作为数据转发节点。

2.4　路由更新阶段

当网络中的节点由于各种原因而失效,比如被列入黑名单,能量耗尽等,将有可能会影响原本的拓扑结构,因此需要进行检查并更新节点与 Sink 节点的距离。

如图 3 所示,当 4 号节点发现网络中的 2 号节点成为失效节点后,则需要计算自身周围邻居节点与 Sink 节点距离以修改自身距离,并通知周围节点。当 4 号节点的邻居节点接到该类型的消息后,根据情况选择是否修改自身距离 Sink 节点的距离。从图 3 中可以看出,更新完毕后,只有 6 号节点更改了自己距离 Sink 节点的距离,而其他节点都不需要变化。可以得出在大规模部署的无线传感器网络中,即使出现了少数的失效节点,网络也只需要进行局部的改动。



(a) 4号节点通知周围节点　(b) 6号节点更改自身信息后继续通知　(c) 2号节点再通知其他节点

图 3　路由更新阶段示意图

3 路由仿真

3.1 仿真指标选择

为了验证本文提出的能量有效可信路由协议在能量与可信方面的表现，使用了以下几种评价方案[12]。

定义 1 衡量运行协议的网络在时刻 t 的能量均衡性可采用网络能量均值

$$AVG_E(t) = \frac{\sum_{i=1}^{M} E_i(t)}{M} \tag{6}$$

和网络能量方差

$$D_E(t) = \frac{\sum_{i=1}^{M} \{E_i(t) - AVG_E(t)\}^2}{M} \tag{7}$$

对该协议的能量使用率进行评价。在式(6)和式(7)中，M 表示网络中节点数；$E_i(t)$ 表示在 i 时刻节点 i 的能量。在时刻 t，具有较高的网络能量均值和较低的网络能量方差的协议则具有更好的能量均衡性能。

定义 2 整个网络的生命期定义为

$$T_L = \min\{T_{Li}; i \in N\} \tag{8}$$

其中 N 表示网络中的节点集合，所以整个网络周期代表出现第一个能量耗尽节点的时间，网络生命周期的长短也是整个网络检查能量消耗的一个显著指标。

定义 3 数据信息经过可疑节点的概率

$$P_i = \frac{A_i}{N_i},\ i \in t \tag{9}$$

式中，P_i 表示在时刻 i 时数据包经过可疑节点的概率；A_i 表示在时刻 i 经过恶意节点的数据包；N_i 表示在时刻 i 发出的总包数。

为验证 EERRP 的性能，本文选取传统的最短路径路由协议(shortest path protocol, SPP)及 Ad Hoc 网络中的安全路由协议(secure efficient Ad hoc distance vector routing, Sead)与本文提出的 EERRP 进行比较。

3.2 仿真环境

为了验证无线传感器网络中本协议的运行情况，在 NS2 中建立了一个模拟场景，其拓扑边界为 1 000 m×1 000 m 的区域，区域中有 49 个节点以正方形分布，分成 7 行，每行之间距离 150 m，每行 7 个节点，节点距离为 150 m，MAC 层遵从 802.11 协议。

3.3 仿真结果

从图 4 中可以看出，EERRP 在能量均值上要略低于最短路径路由协议 SPP，但要优于 Sead，这是由 EERRP 的策略决定的，随着时间的推移，某些数据是经过“绕路”到达 Sink 节点的，因此，与 SPP 相比，EERRP 发送相同数量的数据消耗能量略多，然而 Sead 协议中每个节点需要周期性的广播自己的路由信息，能量消耗较大。但是结合网络能量方差比较，可以看出最短路径路由协议 SPP 和 Sead 的网络能量方差增幅明显。由于 SPP 的能量消耗主要集中在某些节点上，而绝大多数的节点能量消耗较少，这也是 SPP 在网络能量均值性能上略高于 EERRP 的原因。结合网络能量均值和网络能量方差上的比较分析，EERRP 在网络能量均衡性上要明显优于其他两个协议。

图 5 显示了两种路由协议在网络生命周期上的比较，由于 EERRP 采用了能量均衡的策略，整个网络能量均衡性良好，从测试开始到结束时都未出现能量耗尽或濒临耗尽的节点。然而，由于过度集中的使用网络中某些节点，最短路径路由协议 SPP 在网络运行过程一半时出现了第一个能量耗尽节点。而 Sead 周期性的全网广播使得在同等情况下能量消耗较大，能量耗尽节点出现较多。因此，采取了能量均衡策略的 EERRP 在整个网络生命期性能上具有优势。

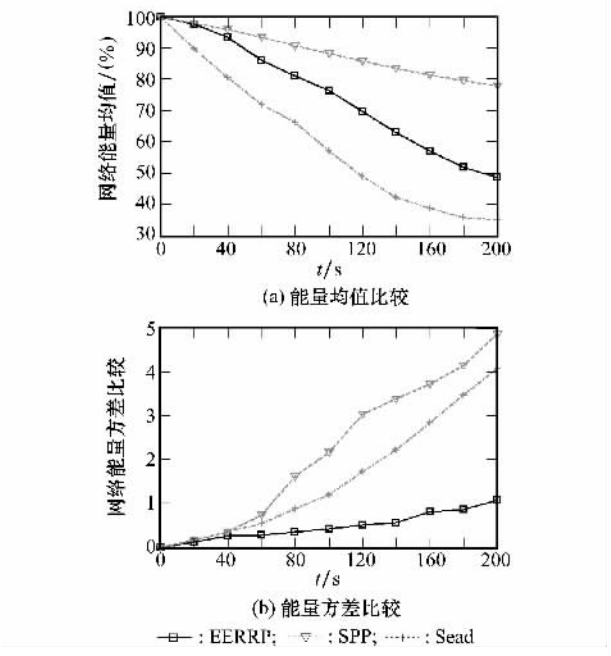


图 4 网络能量指标比较

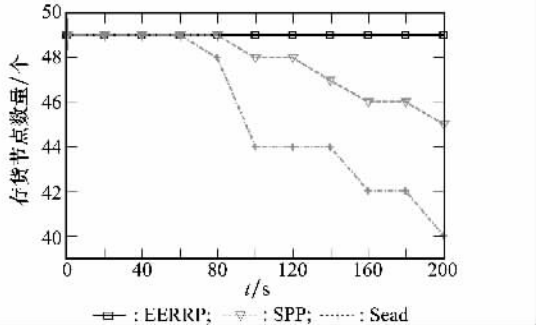


图 5 网络生命周期比较

在可信性性能的测试方面，在某个区域布置部分恶意节点，然后从布置的恶意节点上游的节点发送数据，通过对数据包经过恶意节点的概率来评价路由协议的可信性。从图 6(a)中可以看出，周围区域中存在 1 个恶意节点，EERRP协议一旦发现了节点的不可信行为，就会降低对其的信任，减少其担任下一跳数据转发节点的概率。随着对

该节点的行为的监测,将其列入黑名单,数据之后都将绕过该节点进行转发。而 Sead 通过周期性的广播确认信息,能够发现可疑节点,断开与其的通信。由于能量等其他原因,不使用信任评价的最短路径路由协议 SPP 也会减少数据包经过该恶意节点的概率,虽然如此,但是在可信性上的效果远没有 EERRP 明显。而且根据图 6 中(b)和(c)可以看出,随着恶意节点数量的增加,与 SPP 相比 EERRP 在可信性方面的优势更加显著,安全性能逼近 Sead 协议。

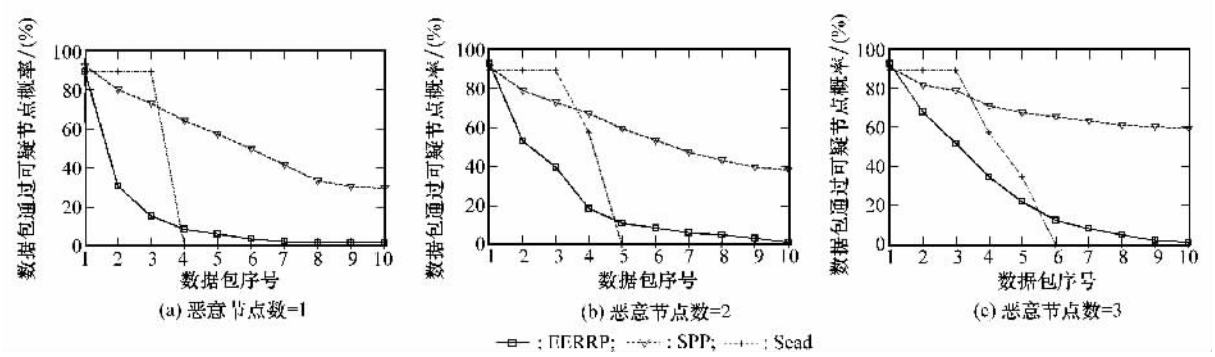


图 6　局部区域内数据包通过可疑节点的概率

4　结束语

本文针对无线传感器网络资源受限的特点,提出了一种 EERRP 协议,特别提出了一种使得整个无线传感器网络能量均衡消耗的能量有效策略,并且在此基础上又加入了信任评价机制,可以在一定程度上发现恶意节点或者能量失效节点,在此之后,协议将避开恶意节点和失效节点选择下一跳节点进行数据转发。EERRP 协议的有效性通过 NS 仿真进行了验证,并且通过与其他两种路由协议在网络能量均值、网络能量方差、网络生命期和网络可信性能方面进行了比较。仿真结果显示了 EERRP 在网络能量和可信方面具有明显的优越性。当然在一些方面上,EERRP 仍然存在着一些不足,比如在某些特定的攻击方式下,EERRP 无法察觉等,需要做进一步的改进和完善。

参考文献:

[1] Fok C L. Rapid development and flexible deployment of adaptive wireless sensor network application[C]// *Proc. of the 24th International Conference on Distributed Computing Systems*, 2005:653 - 662.

[2] Akyildiz I F, Su W, Sankarasubramaniam Y, et al. Wireless sensor networks: a survey [J]. *Computer Networks*, 2002, 38(4):393 - 422.

[3] Estrin D, Girod L, Pottie G, et al. Instrumenting the world with wireless sensor networks [C]// *Proc. of the International Conference on Acoustics, Speech and Signal Processing*, 2001: 2033 - 2036.

[4] Wood A D, Stankovic J A. Denial of service in sensor networks [J]. *IEEE Computer*, 2002,35(10):54 - 62.

[5] Akyildiz I F, Su W, Sankarasubramaniam Y, et al. A survey on sensor networks [J]. *IEEE Communications Magazine*, 2002, 40(8):102 - 114.

[6] 孙利民. 无线传感器网络[M]. 北京: 清华大学出版社, 2005: 56 - 183.

[7] Shah R C, Rabaey J M. Energy aware routing for low energy ad hoc sensor networks [C]// *Proc. of IEEE Wireless Communications and Networking Conference*, 2002:350 - 355.

[8] Intanagonwiwat C, Govindan R, Estrin D. Directed diffusion: a scalable and robust communication paradigm for sensor networks [C]// *Proc. of the 6th Annual International Conference on Mobile Computing and Networks*, 2000:56 - 67.

[9] 杨光, 印桂生, 杨武. 无线传感器网络安全路由算法的研究与设计[J]. 计算机科学, 2008, 35(5):55 - 59.

[10] Lou W, Kwon Y. H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks [J]. *IEEE Trans. on Vehicular Technology*, 2006,55(4):1320 - 1330.

[11] Rentala P, Musunuri R, Gandham S, et al. Survey on sensor networks [R]. Technical Report, UTDCS - 33 - 02, Dallas. University of Texas, 2002.

[12] 郑杰, 屈玉贵, 郭淑杰, 等. 无线传感器网络低时延能量均衡安全路由[J]. 西安交通大学学报, 2008, 42(2):161 - 165.