

A Framework for Energy-Based Trust in Wireless Sensor Networks

Nan XIAO, Min TANG

School of Information Engineering, Jingdezhen Ceramic Institute, Jingdezhen, China

Email: ustbxiaonan@yahoo.com.cn

Abstract: Trust framework is the foundation that ensures trust management can provide security measures for Wireless Sensor Networks (WSNs), and sensors having sufficient energy is a necessary condition for completing all kinds of tasks including transmission and computation of trust value. Therefore, we built the framework for energy-based trust in WSNs to establishment a basic framework for trust management. We divided into many sensor clusters through the improved rapid clustering algorithm. We referred to the barycentric of sensors cluster for selected cluster head sensors and relay sensors. It can save energy consumption by shortening the total of transmission distance as less as possible. We also discussed the variation of the framework when sensors trust values and energy values have changed. Sensors energy consumption is different for the different tasks. To these characteristics, we divided these sensors into different grades according to their remaining energy. Trusted sensors were selected under the conditions of the energy is guaranteed. On one hand, sensors are fully effective used. On the other hand, sensors were responded a reliable level through sensors trust values to strengthen the security assurances of WSNs.

Keywords: wireless sensor networks; rust; energy; fast clustering algorithm;

基于能量的无线传感器网络信任架构

肖楠, 唐敏

景德镇陶瓷学院信息工程学院, 景德镇, 中国, 333043

Email: ustbxiaonan@yahoo.com.cn

摘要: 信任架构是保证信任管理能为无线传感器网络提供安全措施的基础, 同时节点能量充足是节点能完成各种任务(包括信任值计算和传递)的必要条件。因此我们搭建一个基于能量的无线传感器网络信任架构, 目的是为信任管理建立一个基本框架。通过改进快速聚类算法把网络节点分为若干个节点簇, 参考簇的重心选择合适的簇头节点和中继节点, 尽可能的缩短总传输距离以节省能耗。同时也考虑了在节点剩余能量值和信任值变化的情况时信任架构的变更方法: 针对节点在承担不同的任务时消耗的能量不同这一特点, 以能量为基础把节点分为不同的等级, 在能量得到保证的条件下, 通过节点的信任值选择可靠的节点, 一方面使节点得到充分有效的利用, 另一方面通过信任值反应节点可信赖的程度, 加强了无线传感器网络的安全保证。通过仿真实验表明, 新算法能比 LEACH、DCHS 等算法更有效地降低网络的能量消耗, 从而可进一步提高传感器网络的生命周期。

关键词: 无线传感器网络; 信任; 能量; 快速聚类算法

1 引言

近年来, 随着无线传感器网络(WSNs)越来越广泛地运用于许多领域, 特别是在一些非常敏感的领域如军事、科研等领域, 使得安全问题成为制约其发展的一个瓶颈。信任管理作为一种耗能较小的安全技术也得到了广泛的认可, 其中一个良好的信任架构是保证信任管理能为无线传感器网络提供安全措施的基础, 同时节点能量充足是节点能完成各种任务(包括信任值计算和传递)的必要条件。建立模型的基础框架主

要包括三部分: 无线传感器网络的区域划分、簇头节点的选取和框架变更的方法。其中典型的簇头选取算法有 LEACH^[1]、DAEA^[2]、HEED^[3]、ACMWN^[4]和 DCHS^[5]等。

LEACH 协议是一种基于聚类(clustering)的低功耗自适应路由协议, 它是建立在所有节点都是平等且无线信号在各个方向上能耗相同的假设上。LEACH 协议将整个 WSN 分为若干个簇, 每个簇选取一个簇头, 其它节点将自己所采集的信号传输给所属簇的簇头,

簇头将所有接收的信号和自己采集的信号通过数据融合后,传给接收器。由于簇头消耗的能量远远高于其它节点,因此在 LEACH 协议中建立了轮次方式。每个轮次分为建立阶段和稳定阶段,由于建立阶段所耗能量对于信号采集来说为无效能耗,所以稳定阶段要远远大于建立阶段。通过轮次变化重新选择簇头节点,从而把簇头高消耗的能量平均分摊到各个节点上。LEACH 协议相比平面协议来说,较好地解决了能量有效问题,能够实现能量消耗均衡机制。但是协议的缺点也是很明显的:簇头的选择没有考虑节点的剩余能量,有可能导致某些节点的能量提早耗尽;簇头都是随机产生的,难免出现簇头的分布不均匀,导致网络能量消耗不平均,从而影响 WSN 生存时间。DAEA 算法是一个三层分簇算法,它首先依据地理位置将所有的传感器区域分成大小相等且不互相重叠的正方形区域,为每个区域选择能量最多的节点作为簇头 LA,然后在所有的 LA 中选取能量最多的节点作为簇头的上层簇头节点 MA, LA 与 MA 通信, MA 负责与基站通信。HEED 算法中,簇头的选择主要依据主、次两个参数。主参数依赖于剩余能量,用于随机选取初始簇头集合,具有较多剩余能量的节点将有较大的概率暂时成为簇头,而最终该节点是否成为簇头取决于剩余能量是否比周围节点多得多,即迭代过程是否比周围节点收敛得快。在 ACMWN 算法中,由每个节点独立运行分簇算法, ID 比周围邻居低的成为簇头。DCHS 算法针对 LEACH 中的不足,综合考虑节点当前能量和阈值对簇头选取的影响。

本文结合能量与信任搭建无线传感器网络的基础信任架构,利用簇头选取算法对网络进行区域划分,在划分后的区域选取簇头节点时考虑各节点剩余能量和信任值,确保剩余能量高且信任值大的节点较其他节点成为簇头的可能性更高,最终使得无线传感器网络信任管理系统更加完善。仿真实验表明,新算法能比 LEACH、DCHS 等算法更有效地降低网络的能量消耗,从而可进一步提高传感器网络的生命周期。

2 建立无线传感器网络信任架构

2.1 架构假设

无线传感器网络由于应用的不同,网络的规模和布置方式都有很大的差异。为了更方便的描述网络,我们作了如下假设:

(1) 不考虑网络覆盖地区地势高低的影响,假设网络中各节点分布于 X-Y 平面,每个节点都可通过

GPRS 等定位方法获取自身的位置;

(2) 所有的节点具有相同的通信半径 R ,传输任意单位比特数据的平均耗能均相同,节点传输时消耗的能量与传输距离成正比;

(3) 每个节点均具有一定的计算能力,可以在必要的时候执行数据处理操作;

(4) 我们认为节点在最初被投放的时候是平等的,若没有遭到物理上的破坏,能够正常的感应和传输数据的话,它们都是可信任的。

2.2 建立网络信任架构基本步骤

由于有些大规模网络节点多、覆盖面积大且不利于统一处理,一般将网络分成多个小区域(即节点簇)。传统的方法是把网络覆盖面积平均分为若干个小矩形区域或者圆形区域,这对节点均匀分布的网络较使用。但现实中由于投掷节点的随机性以及区域的重视程度的差异,节点分布一般是不均匀的。这里我们尽量把相邻的节点分在一个区域,便于进行以后的数据处理等工作。考虑传感器节点传输数据的能耗与距离有关,我们通过节点间的距离利用快速聚类改进算法把整个网络分为若干个小区域,为每个区域分配一个地址,用 $ID_i (i=1,2,3,\dots)$ 来表示。一个区域相当于一个节点簇 (Sensors Clusters),从中选取一个簇头 C_i ,它的作用是储存和管理该区域中其它节点的信任值,以及和其它簇头节点交换信任值和进行路由选择。在每个节点簇中,簇头负责存储节点簇中其它节点的信任值及其更新。同时为了节省簇头节点的能量,在每次任务前在簇头节点周围设置一中继节点 P ,负责这次任务后的信任值的接收和计算,再发送给簇头节点。则信任值管理工作的方式为:在每次事件中,传感器节点 S_i 在与其它节点通过交往产生一些信任证据形成信任值 T_{i1}, T_{i2}, \dots 并传送给中继节点 P ,中继节点结合其它节点传来的数值,综合计算得到在本次事件中各节点的信任值 T_1, T_2, \dots, T_n ,传给簇头节点。簇头节点结合节点以前的数值,进行综合评价和更新,其结构图如图 1。

2.2.1 区域的划分和簇头节点的选取

划分的每个区域的最大直径 D 取值决定于不同应用的网络及其节点放置的疏密度,直径过小会造成资源的浪费,过大则区域的划分没有意义,一般为取节点通信半径 R 的倍数 $aR (a=1,2,\dots)$ 。设网络共有 n 个节点,通过对节点定位可以确定每个节点的位置及其网络拓扑关系;如果可知绝对位置,则用坐标来表示节点 $S_i (x_i, y_i)$;如果是相对位置,也可建立相对

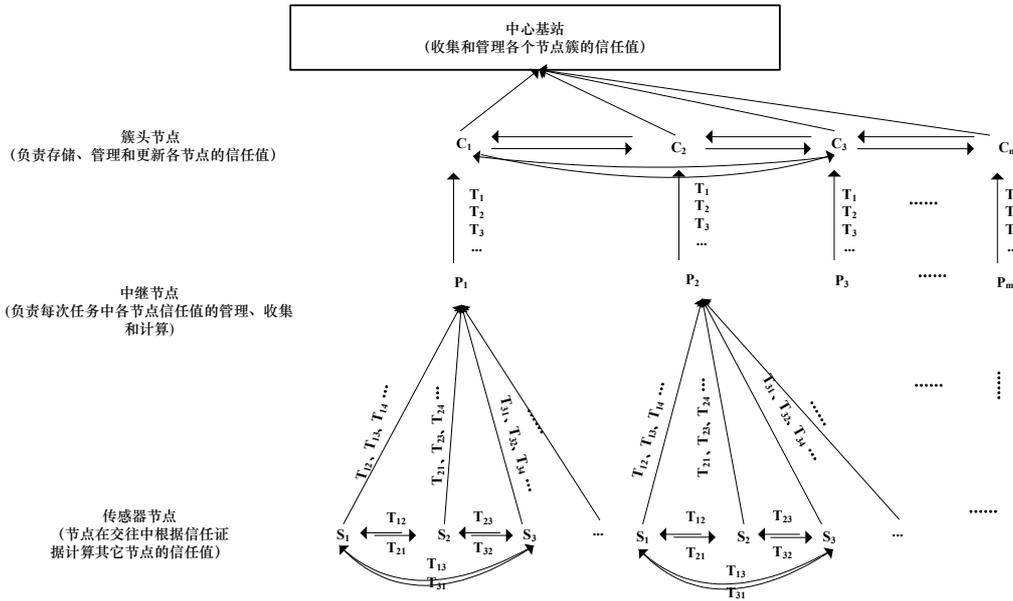


Figure 1. Trust management in wireless sensor network structure

图 1. 无线传感器网络信任管理结构图

直角坐标系，以某个节点为坐标原点，其它节点可用相对坐标表示，对于区域划分没有影响。其中节点 $S_i(x_i, y_i)$ 与节点 $S_j(x_j, y_j)$ 间的距离以欧氏距离计算， $d_{ij} = d(S_i, S_j) = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2}$ 。

(1) 先择所有节点中相距最远的两个节点作为聚点 S_{i1}, S_{i2} ，即 $d(S_{i1}, S_{i2}) = \max\{d_{ij}\}$ ；

(2) 然后再选择第三个聚点 S_{i3} ，它是剩下的节点中最不靠近 S_{i1} 和 S_{i2} 的节点，即 $\min\{d(S_{i3}, S_{i1}), d(S_{i3}, S_{i2})\} = \max\{\min[d(S_j, S_{i1}), d(S_j, S_{i2})]\}$ 。同理，按照下式 $\min\{d(S_{ik}, S_{i1}), d(S_{ik}, S_{i2}), \dots, d(S_{ik}, S_{i,r})\} = \max\{\min[d(S_j, S_{i1}), d(S_j, S_{i2}), \dots, d(S_j, S_{i,r})]\}$ ， $j \neq i_1, i_2, \dots, i_r$ ， $r = k-1$ 。依次选取 $S_{i4}, S_{i5}, \dots, S_{ik}$ ，要求：

$$\max\{d(S_{im}, S_{in}), m \neq n, m, n = 1, 2, \dots, k\} \leq D;$$

$$\max\{d(S_{im}, S_{in}), m \neq n, m, n = 1, 2, \dots, k-1\} \geq D;$$

(3) k 个初始聚点分别记为 $S_1^{(0)}, S_2^{(0)}, S_3^{(0)}, \dots, S_k^{(0)}$ ，它们的集合记为 $L^{(0)}$ 。进行初始分类，把节点划在距离它的最近的聚点那一类： $G_i^{(0)} = \{S: d(S, S_i^{(0)}) \leq d(S, S_j^{(0)}), (1, 2, \dots, k \text{ 且 } j \neq i, i = 1, 2, \dots, k)\}$ ，这样每个节点都以最靠近的初始聚点归类，得到一个初始分类 $G^{(0)} = \{G_1^{(0)}, G_2^{(0)}, \dots, G_k^{(0)}\}$ ；

(4) 从 $G^{(0)}$ 出发计算新的聚点集合 $L^{(1)}$ ，可计算 $G_i^{(1)}$

的重心 $X_i^{(1)} = \frac{1}{n} \sum_{S_j \in G_i^{(0)}} S_j$ ， $i = 1, 2, \dots, k$ ，但在中心位置不一定有节点存在，这里以最接近中心的节点作为新的聚点 $S_i^{(1)}$ ，这样得到新的聚点集合： $L_{(1)} = \{S_1^{(1)}, S_2^{(1)}, \dots, S_k^{(1)}\}$ 。进行重新分类 $G_i^{(1)} = \{S: d(S, S_i^{(1)}) \leq d(S, S_j^{(1)}), j = 1, 2, \dots, r \text{ 且 } j \neq i, i = 1, 2, \dots, k\}$ ，得到 $G^{(1)} = \{G_1^{(1)}, G_2^{(1)}, \dots, G_k^{(1)}\}$ 。重复计算得到第 m 部分类

$G^{(m)} = \{G_1^{(m)}, G_2^{(m)}, \dots, G_k^{(m)}\}$ ，其中 m 满足：区域重心与聚点的距离不大于聚点与其它节点的最小距离即可。按照这种聚类方式，把网络分成若干个区域，其中所找到的聚点即为簇头节点 C_i 。

2.2.2 中继节点的选取及其工作方式

中继节点的任务是帮助簇头节点分配某次任务需要的信任值以及事件后的信任值的收集和计算。所以它到其它节点距离和应该较小，而且和簇头的距离很近。由于最初时节点的信任值相同，在簇头节点的邻居节点中选择即可。记 $d_{min} = \min[d(S_i, C), S_i \in G]$ ，在集合 $P_o = \{S_i | d(S_i, C_i) \leq \min(R, 2d_{min})\}$ 任意选择一个节点或者由节点自荐作为中继节点，然后向其它节点广播告知，如图 2（黑色表示簇头节点，灰色表示中继节点）。

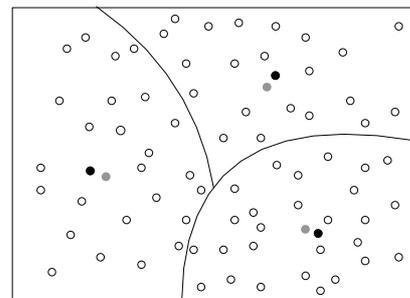


Figure 2. Relay node selection and its working methods

图 2. 中继节点的选取及其工作方式

3 框架变更

完成若干次任务后，每个节点都有新的能量 E 和信任值 T 。假设节点担任簇头节点完成一次任务所需的能量为 E_x ，担任中继节点完成一次任务所需的能量为 E_y ，担任普通节点完成一次任务所需的能量为 E_z ($E_x > E_y > E_z$)。同时给普通节点的信任值设定一个阈值 T_2 ，当节点的信任值 T 小于 T_2 ，则这个节点不被信任，即把它作为不合理节点，向周围节点广播，将它排出网络；为中继节点设定阈值 T_y ，为簇头节点设定阈值 T_x ，当簇头节点的信任值小于 T_x ，则改节点失去簇头节点的身份，其中 ($T_x > T_y > T_2$)。

(1) 检测节点的剩余能量和信任值，如果节点 i 的剩余能量 E_i' 小于 E_z 或者信任值 T_i' 小于 T_2 ，则把它作为不合理节点排出。当剩下的节点数不到原总节点的 55%，则判断网络不能工作了；

(2) 检测每个簇的簇头节点，如果 C_i 的能量大于 E_x 且信任值大于 T_x ，则节点继续担任簇头。否则重新选择簇头节点：对所有剩余能量值大于 E_x 的节点 j 计算

$$M_j = \alpha \frac{E_j' - E_x}{2 - E_x} + \beta \frac{T_j' - T_x}{1 - T_x}$$

其中 $\alpha + \beta = 1$ ， α 、 β 分别表示能量与信任值标准化后各自的权重。当节点信任值较高的时候，它有更大的机会被选做其它节点交流和传输数据的对象，能量也会消耗比其它节点更快。结果可能出现信任值高的节点往往能量较小。为了避免频繁的选取簇头节点， α 与 β 设为可调变量，一般情况下 α 取较小值， β 取较大值，随着节点信任值的增加， α 取较大值，而 β 取较小值。

然后选择重心周围 M_j 最大的节点作为簇头节点 C_i' ： $M(C_i') = \max\{M(s_j) | s_j \in \delta(X, r_1)\}$ ，其中 r_1 表示这个邻域的半径大小，随着时间的推移，节点个数变少， r_1 相应的变大。

(3) 选择中继节点：在所有能量大于 E_y 的节点中选择 P_j ，满足 $T(P_j') = \max\{T(S_j) | S_j \in \delta(C_i', r_2)\}$ ，其中与 r_1 相似，随着时间的推移，节点个数变少， r_2 相应的变大。

4 分析

4.1 性能分析

(1) 模型通过改进快速聚类算法对节点进行分类，避免了以往简单的矩形分区时边界上的节点分区

不明的情况出现。算法主要是通过距离为标准进行分类，目的就是使簇中其它节点到簇头节点的距离和尽可能小，这样从节点总的传输距离方面使节点的总能耗较小。若网络中节点分布疏密不一致、分布不均匀，如图 3 所显示的是网络中小块区域。若以矩形的分区方式，很可能把距离较远的分在一个节点簇中，簇中节点两两间相互交往，获取信任证据，都会较多资源和能量。图 4 是利用改进的快速聚类算法进行的分类，使相近的节点在一个节点簇中，较远的节点不需要频繁的交往，在传输数据的时候，在节点簇中先对数据进行融合，再由簇头节点和簇头节点相互交往进行数据传递。

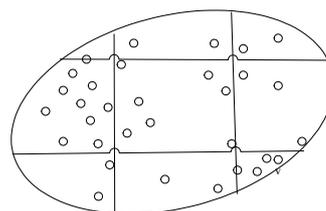


Figure 3. Matrix of small regions of the network partition
图 3. 网络中小块区域的矩阵分区

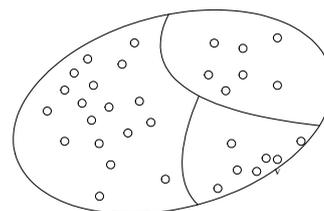


Figure 4. Small-area network fast clustering algorithm partitions
图 4. 网络中小块区域的快速聚类算法分区

(2) 模型把信任值和能量值结合在一起，考虑到能量的限制对节点工作的影响，根据节点能量剩余的多少选择节点担任何种任务，同时选取动态的变量 α 和 β ，在能量较少的情况下对信任值的增长速度起到一定的抑制作用，使节点得到更有效的利用。算法通过信任值反应了节点可信赖的程度，加强无线传感器网络的安全保证。

4.2 仿真分析

传感器网络中，评价网络分层算法好坏的一个重要参数就是网络生存时间。在不考虑其它外界可能破坏因素的前提下，当一个传感器节点的能量小于 0 时，就认为这个节点死亡；当网络中出现节点能量小于 0 时，定义该时刻为网络生存时间。

我们在 Windows 系统下利用 C 语言编程进行仿真，试验参数如表 1 示。

Table 1. Simulation parameters
表 1. 仿真试验参数表

节点数	区域面积/m ²	节点初始能量/J	处理器能耗 E_{elec} nJ/bit	放大器消耗能量 ϵ_{fs} pJ/bit $t \times m^2$	数据包大小 bit
200	100×100	0.5	50	100	50

若两节点间距离为 d ，通信能量消耗与 d^2 成正比，则节点传送 k bit 数据到与之距离为 d 的另外一个节点所消耗能量可表示为： $E_{rx}(k, d) = kE_{elec} + k\epsilon_{fs}d^2$ ，其中 k 表示数据包大小， E_{elec} 表示处理相应数据所消耗的能量， $k\epsilon_{fs}d^2$ 为根据通信距离所消耗的能量， ϵ_{fs} 为信号放大器耗能参数。

节点接受 k bit 长度数据所消耗的能量为： $E_{Rx}(k, d) = k \times E_{elec}$ 。

采用 LEACH 协议中的轮次方式，每个轮次分为建立阶段和稳定阶段，通过轮次的变化重新选择簇头节点。设定每轮稳定传输 30 次，将簇头百分比设定范围为 2%~20%，每次簇头数增加 2%，每种簇头比例进行 10 次仿真，求出生存轮数的平均值。新算法与 LEACH、DCHS 算法的比较结果如图 5 所示。

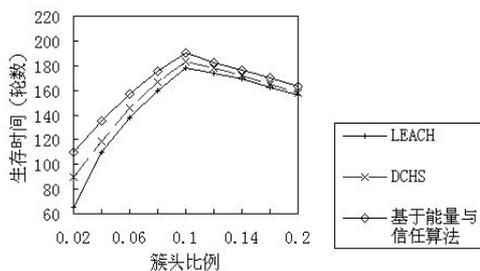


Figure 5. Survival time (Rounds) of three kinds of algorithms

图 5. 三种算法的生存时间 (轮数)

图 5 显示了三种算法在不同的簇头比例下的网络生存时间，显然本节中的算法较另外两种算法有更长的生存时间。在簇头比例较小是更为明显，当簇头比例为 10% 时，WSNs 生存时间最长。

5 结束语

本文所搭建的信任管理构架是一种由基站、簇头节点、中继节点和普通节点构成的层次构架，以信任值和剩余的能量作为各种节点选取的依据，为研究信任证据的获取，信任值的计算、传递和综合评价做基础。其中还有一些不足之处：如节点被捕获、信任值被伪造等情况都还没有考虑到。接下来，我们将进一步地探索信任证据的获取、信任值的计算以及无线传感器的其它信任问题。

References (参考文献)

- [1] Henzelman W., Chandrakasan A., Balakrishnan H. Energy-efficient Communication Protocol for Wireless Microsensor Networks[C]. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. Maui: IEEE Computer Society, 2005, 3005-3014.
- [2] Alkarkijn N., Ulmufafa R., Kamal A.E.. Data Aggregation in Wireless Sensor Networks exact and approximate Algorithms[C]. Proceedings of the IEEE Workshop on High Performance Switching and Routing. Phoenix: IEEE Communications Society, 2004, 241-245.
- [3] Youn I., Fahmy S.. Heed: a Hybrid, Energyefficient, Distributed Clustering Approach for Ad-hoc Sensor Networks[J]. IEEE Transactions on Mobile Computing, 2004, 3(4): 660-669.
- [4] Linc Gerlam. Adaptive Clustering for Mobile Wireless Networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 15(7): 1265-1275.
- [5] Handym J., Haasem G., Timmermann D.. Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster Head Selection [C]. Proceedings of the 4th IEEE Conference on Mobile and Wireless Communications Networks. Stockholm: IEEE Communications Society, 2002, 368-372.
- [6] Lei Huang, Lei Li, Qiang Tan. Behavior-based trust in wireless sensor network [C]//Advanced Web and Network Technologies, and Applications. 2006 International Workshops. 2006: 214-23.
- [7] Crosby, Garth V. Cluster-based reputation and trust for wireless sensor networks [C]//2007 4th Annual IEEE Consumer Communications and Networking Conference. 2007: 604-608.
- [8] Wei Zhang, Das S.K., Yonghe Liu. A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks [C]//2006 3rd Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks. 2006: 60-69.
- [9] Weifang Cheng, Xiangke Liao, Changxiang Shen.
- [10] A trust-based routing framework in energy-constrained wireless sensor networks [C]// First International Conference, Wireless Algorithms, Systems, and Applications. 2006. Proceedings. 2006: 478-489.
- [11] Su Wang et al. Wireless Sensor Networks Theory and Applications[M]. Beijing University of Aeronautics and Astronautics Press. 2007.
王殊等. 无线传感器网络的理论及应用[M]. 北京: 北京航空航天大学出版社, 2007.