一种有效防御虫洞攻击的方法①

吕 振[1]，林振杨[1]，张晓红[2]

[1](辽宁工程技术大学 电气与控制工程学院，葫芦岛 125105)
[2](辽宁工程技术大学 应用技术学院，阜新 123009)

摘 要：由于无线传感器网络节点位置信息对网络的应用起着重要的作用，且传感器网络的资源有限，因此，针对 DV-Hop 定位算法的安全性能较差，定位过程中极易受到破坏性极大的虫洞攻击等缺点，提出了一种有效防御 DV-Hop 中的虫洞攻击的方法，在 DV-Hop 算法中引入了检测虫洞攻击及有效防御虫洞攻击的 EPWDV-Hop 算法，通过 Matlab 仿真软件进行模拟仿真。仿真结果表明，修改后的算法不仅提高了定位精度，而且很好地预防了算法中的虫洞攻击。

关键词：无线传感器网络；DV-Hop 算法；虫洞攻击；EPWDV-Hop 算法

Effective Defense Method for Wormhole Attack

LV Zhen[1], LIN Zhen-Yang[1], ZHANG Xiao-Hong[2]

[1](Faculty of Electrical and Control Engineering, Liaoning Technical University, Huludao 125105, China)
[2](Institute of Technology, Liaoning Technical University, Fuxin123009, China)

Abstract：The information about node location of wireless sensor network plays an important role to the application of network, however, it's limited of sensor network resources, therefore, this paper puts forward a kind of effective defense method to the wormhole attack of DV-Hop, which is directed to the short comings of that the safety performance of DV-Hop algorithm poor, and the location process easily attacked by the destructive worm hole and so on. The method is that introducing EPWDV-Hop algorithm which is an effective detection defense algorithm against the wormhole attack into the DV-Hop algorithm. According to the simulation test of Matlab software, it shows that the modified algorithm can not only improve the precision of location, but also is very good to prevent the wormhole attack in algorithm.

Key words：wireless sensor network; DV-Hop algorithm; wormhole attack; EPWDV-Hop algorithm

目前，绝大多数已有的定位系统或者定位算法的前提均是在安全可信的网络环境下实施的，忽略了无线传感器网络在定位过程中安全性的脆弱问题。由于节点定位过程很容易收到各种攻击，导致错误、无效的定位结果，将这个定位结果应用在一些重要的场合，如战场监视，则会导致网络功能局部或整个网络的瘫痪，从而造成难以估计的重大损失。因此，在资源受限的无线传感器网络中，如何安全、有效地获取节点的物理位置信息，是一个极具挑战性的安全问题。

文献[1]采用特殊硬件如方向天线来实现对虫洞攻击的检测；文献[2]引入了基于邻居信任评估的方法实现对虫洞攻击的防御；文献[3-4] 基于前提测试的邻居数测试和所有距离测试的方法来防御虫洞攻击。然而这些方法需要借助外界的特殊硬件支持或者以增加算法的开销为代价，对依赖于数据包传递来实现准确定位的 DV-Hop 算法显然是不合适的。本文根据前人的工作，通过对 DV-Hop 算法中的虫洞攻击进行详细的分析，进而，提出了一种有效的防御虫洞攻击的算法 EPWDV-Hop(Effective Prevention Wormhole Attack in DV-Hop)，该算法通过检测节点之间的跳数 $HopSize$ 与最小跳数 $Hop_{\min}$ 相比较，从而判断是否存在虫洞攻击。最后通过 Matlab 仿真表明，该改进后的算法既提

① 收稿时间:2011-10-12;收到修改稿时间:2011-11-25

高定位精度，也很好地预防了虫洞攻击，进而实现了预期的目标。

1　DV-Hop算法及虫洞攻击

1.1 DV-Hop 算法的基本定位过程

基本的 DV-Hop 定位算法的过程可分为三个基本阶段[5-7]：

① 计算未知节点与每个锚节点的最小跳数。

② 假设网络中节点的通信半径相同，平均每跳距离为节点的通信半径，未知节点计算到每个锚节点的跳段距离。

③ 利用三边测量法或极大似然估计值法计算未知节点的自身位置。然后根据下面公式可估算平均每跳的实际距离。

$$HopSize_i = \frac{\sum_{j\neq i}\sqrt{(x_i-x_j)^2+(y_i-y_j)^2}}{\sum_{j\neq i} h_j} \quad (1)$$

其中，$(x_i, y_i), (x_j, y_j)$ 是参考节点 i、j 的坐标，h_j 是参考节点 i 与 j $(j \neq i)$ 之间的跳段数。最后结合前面的两个阶段，在利用三边测量法或者极大似然估计值法即可计算出自身坐标。

下面用一个小型传感器网络来说明 DV-Hop 定位算法的过程，图 1 是一个 9 个节点的 WSN 结构图，已知参考锚节点的 L_1、L_2、L_3，A 为未知节点，每个锚节点估计的平均每跳距离分别为：

$HS_1^D = \frac{d_1+d_3}{2+6}$、$HS_2^D = \frac{d_1+d_2}{2+5}$、$HS_3^D = \frac{d_3+d_2}{5+6}$。

对未知节点 A，首先接收到 L_2 发出的平均每跳距离，A 到 L_1、L_2、L_3 的估计距离分别为：$d_1 = 3*HD_2^D$，$d_2 = 2*HD_2^D$，$d_3 = 3*HD_2^D$，最后利用三边测量法或者极大似然估计值法即可计算出 A 自身坐标。

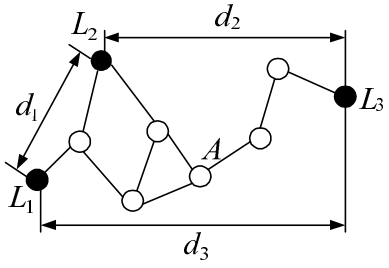


图 1　小型传感器网络结构图

1.2 虫洞攻击的常见类型[8,9]

所谓的虫洞攻击是一种针对网络的路由协议，破坏网络路由机制的攻击，它是两个物理位置之间的专用链接，是无线传感器网络的最大安全威胁。虫洞攻击的常见类型有：

① 数据包被篡改：该攻击类型是最简单的一种攻击，常规密码学机制就可以有效的防御此种类型的攻击。

② 大功率重放攻击：攻击节点不篡改数据包中的信息，只是以大功率重放该数据包。

③ 使用带外隐藏信道攻击：如果虫洞连接由带外隐藏信道构成，那么跳数必会减少。

本文只对第三种情况下的攻击进行检测及防御。

1.3 DV-Hop 算法中的虫洞攻击及危害

1.3.1 虫洞攻击的危害[10]：

虫攻击的主要危害有以下两个方面：

① 能量的大量消耗：由于虫攻击，造成节点发送大量重复的数据包，因而消耗过多的能量，且不考虑节点的能量补给问题，从而造成节点失效而不能正常工作。

② 定位不准确：由于虫攻击，得不到正确的跳数，未知节点点也就得不到正确距离，也就不能正确计算出平均跳距，从而确定出来的坐标也是不准确的。

1.3.2 DV-Hop 算法中的虫洞攻击

带外隐藏信道攻击有两种情况：一是攻击锚节点，如图 2 所示；二是攻击未知节点，如图 3 所示。在图 2 中，恶意节点 C_1、C_2 通过虫洞进行通信，L_2 接收恶意节点 C_2 关于 L_3 信息，从而使 L_2 与 L_3 之间的跳数变为 1，此时，L_2 估计的平均每跳距离为 $HS_2^{D'} = (d_1+d_2)/(2+1)$（正常情况 $HS_2^D = (d_1+d_2)/(2+5)$），对于未知节点 A 来说，到参考节点 L_1、L_2、L_3 的估计距离分别为：$d_1 = 3*HS_2^{D'}$、$d_2 = 2*HS_2^{D'}$、$d_3 = 1*HS_2^{D'}$，正常情况 $(d_3 = 1*HS_2^D)$。在图 3 中，由于存在恶意节点的攻击，A 与 L_3 之间的跳数变为 1，L_2 与 L_3 之间的跳数因此变为 3，则 L_2 估计的平均每跳距离 $HS_2^{D'} = (d_1+d_2)/(2+3)$（正常情况 $HS_2^D = (d_1+d_2)/(2+5)$），对于未知节点 A 来说，到参考节点 L_1、L_2、L_3 的估计距离分别为 $d_1 = 3*HS_2^{D'}$、$d_2 = 2*HS_2^{D'}$、$d_3 = 1*HS_2^{D'}$。

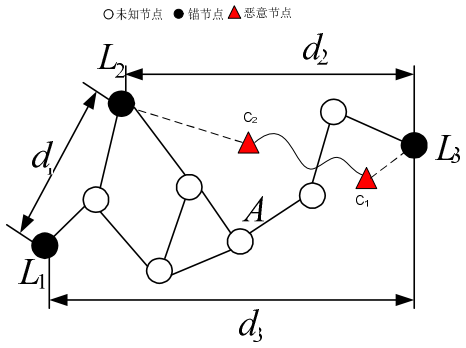


图 2 攻击锚节点情形

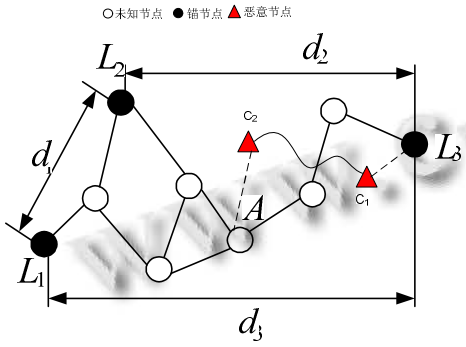
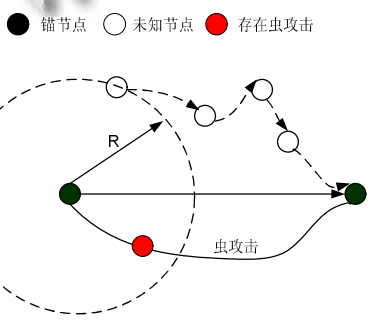


图 3 攻击未知节点情形

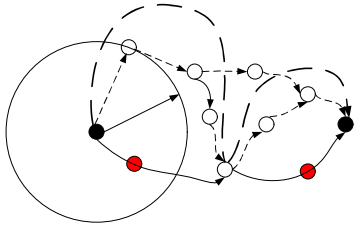
2 算法设计的步骤

2.1 算法的核心思想

虫攻击主要攻击原始 DV-Hop 算法的跳距，本算法提出了一种有效预防虫攻击的安全定位算法 EPW DV-Hop，通过检测到的跳数 $HopSize$ 与最小跳数 $Hop_{\min}$ 相比较，从而判断是否存在虫攻击。当 $HopSize < Hop_{\min}$ 时，则说明 $HopSize$ 是不符合的，即存在虫攻击，此时，利用最佳跳数 Hop_{opt} 替代检测受到虫攻击的跳数 $HopSize$。具体检测示意图如图 4 所示。



(a) 锚节点监测虫攻击



(b) 未知节点检测虫攻击

图 4 虫攻击检测示意图

2.2 算法设计的步骤

① 最小跳段 $Hop_{\min}$ 的计算。首先计算出某两个节点之间的跳数，并将位于这两个节点间的所有节点排成一条直线上，如图 5 所示。如果任意两个节点之间的通信半径都相等，则最小跳段 $Hop_{\min}$ 可以根据公式 2 计算出来，其中 int() 为取整函数。

$$Hop_{\min} = 1 + \text{int}\left(\frac{d_{(A,B)}}{R}\right) \tag{2}$$

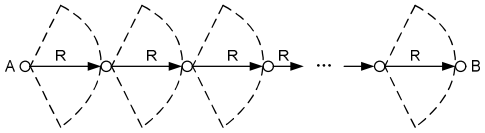


图 5 两个节点间的最小跳段

② 虫洞攻击的检测。如果获得一个 $HopSize$，锚节点就能够根据公式 2 检测出该跳数是否符合，如果公式 2 成立，即该 $HopSize$ 的路径中存在邻居节点的通信半径比 R 大，表明通信路径不符合且存在虫洞攻击。反之，说明网络中也有可能存在虫攻击，但是影响不大。某些节点获得了有效位置 EP。

$$HopSize < Hop_{\min} \tag{3}$$

③ 攻击下获取最小跳数的校正。如果 M 个节点在均匀分布的方正形 $(a*a)$ 区域内，则单个节点占整个网络的区域有公式 3 可以求出，若将该区域量化为边长 b 的正方形。

$$t = (a*a)/M \quad b = \sqrt{t} \tag{4}$$

此时正方形 $(a*a)$ 被划分为多个小的正方形，假设各个小方形内的节点被分布在中心位置，根据工程数学上的覆盖定义，节点的通信半径要覆盖与该节点

的邻居的正方形，如图 5 所示。该方法能够得到较高的连通度。此时 R 具有最高的连通性，所以说是最优的拓扑结构。

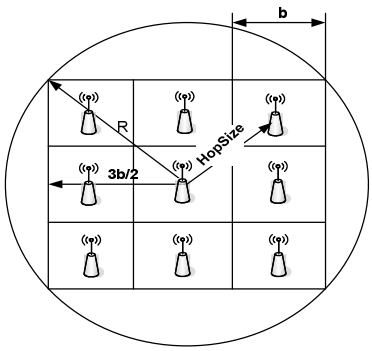


图 5　最佳通信半径及 *HopSize* 示意图

在水平或垂直方向上各个节点的距离都比 1/2*R 小，$HopSize_{opt}$ 由公式 5、公式 6 可以计算出来。

任意方向：$HopSize_{opt}=\sqrt{2}b$　　(5)

垂直或水平方向：$HopSize_{opt}=2b$　　(6)

两个网络节点之间间隔的最佳跳段可以通过下列公式 7 计算得到：

$$Hop_{opt}=\frac{d}{HopSize_{opt}} \tag{7}$$

3　仿真分析与结果评价

3.1 仿真环境

为了验证 EPWDV-Hop 算法的有效性，利用 Mat Lab/Simulink 仿真软件对基本的 DV-Hop 算法同本章的算法在防虫攻击方面进行了仿真比较，仿真实验的模拟区域假设将 225 个随机分布在 $100m\times100m$ 的正方形区域内，其中，在程序编写时将设置 R=15，网络连通度为 12，锚节点个数占网络中所有节点总数的 10%。但是由于在矩阵逆置过程中有可能导致仿真的失败，因此，在仿真过程中引入一个额外的合理检测，即利用已知给定的距离 d_i 和锚节点与估计位置间的距离之间的平均剩余值 R_{AV}，其计算如下公式 8：

$$R_{AV}=\frac{\sum_{k}^{m}\sqrt{(X_k-\tilde{x})^2+(Y_k-\tilde{y})^2}-d_k}{M} \tag{8}$$

式中 (X_k,Y_k) 为锚节点的坐标，$(\tilde{x},\tilde{y})$ 为估计位置的坐标，d_k 为给定的距离。如果 $R_{AV}>R$，那么位置 $(\tilde{x},\tilde{y})$ 被过滤，因此，并不是所有节点都能够得到估计位置坐标的。

3.2 仿真分析与结果评价

在仿真过程中，将无效位置率 $InPR$ 和均方误差 (Mean Squared Error，MSE)，如公式 9，当作评判该两种算法的性能。

$$MSE=\frac{1}{m}\frac{\sum_{k=1}^{m}\sqrt{(\tilde{x}_k-X_k)^2+(\tilde{y}_k-Y_k)^2}}{R} \tag{9}$$

其中，m—取得 EP 的节点个数。如果计算出来的 $MSE>1$，那么将这以位置的节点过滤掉。公式 10 是 $InPR$ 的计算公式。

$$InPR=\frac{l_{EP}}{l_{EP}+l_{InP}} \tag{10}$$

其中，l_{EP} —取得的节点个数。

l_{InP} —取得无效位置 InP 和公式 8 拒绝的节点个数。在不受到虫攻击时，两种算法的 MSE 都等于 0.34，$InPR$ 为 0.95。

下面对算法的性能进行仿真分析：

① 存在虫攻击，攻击节点随机布置，从表 1、表 2 可以看出，节点的物理位置和误差都发生了改变。对原始的 DV-Hop 而言，在其他参数一样的情况下，本文的算法在一定程度上降低了虫攻击下的误差，但是该算法引起了正常节点的误差增加，这是由于在算法执行的算过程中利用 Hop_{opt} 替代虫攻击下所产生的跳数造成的。如果存在严重的虫攻击，原始算法中的误差比 1 大，而本文算法使误差减少到小于 1。公式 8 能够处理不一致序列的情况，但是对虫攻击下 *HopSize* 的快速增加并不作任何的反应，所以，本文的算法可以有效地防御虫攻击。

② 带外隐藏信道攻击：恶意节点的分布情况有两种：随机分布和部署在锚节点的通信半径以内。当恶意攻击节点是随机分布时，则从一个节点是以虫洞链接的形式向另一个节点发送数据包，节点间的最佳跳数减少了，从而导致平均条数减少。当恶意的攻击节点分布在通信半径之内，此时存在恶意攻击节点的两段节点可以直接进行通信，得到的平均跳距 *HopSize* 比正常情况要大，其仿真结果如图 6、7 所示。在图 6 中，恶意攻击节点随机分布下，与 DV-Hop 算法相比较，EPWDV-Hop 算法的 MSE 小，如果恶意攻击节点在通

信半径范围之内，DV-Hop 的 MSE 出现了比 EPWDV-Hop 算法要大的情况。从图 7 可以看出，两种算法的 *InPR* 都同时减少，网络中存在 10 个恶意攻击节点，此时，EPWDV-Hop 算法的 $InPR=0.23$，$MSE=0.64$，而原始 DV-Hop 算法的 $InPR=0.03$，$MSE=0.47$。总的来说，如果恶意攻击节点是随机分布，那么该情况下的误差就会更大，而恶意节点在通行范围内，由于额外的合理检测导致较多的节点不能够获取 *InP*，所以从图 6、7 可以看到，恶意节点在不同程度的攻击下 EPWDV-Hop 算法的 $MSE=0.5$ 左右，而原始 DV-Hop 算法的 $MSE=0.2$ 左右，因此说，EPWDV-Hop 算法能够有效地防御该虫洞攻击。

3.3 计算复杂度比较

通过对两种算法的分析比较得出，EPWDV-Hop 算法由于在第一阶段额外的附加了对跳数进行检测，增加了很小的计算开销，其他各个阶段与 DV-Hop 算法的计算开销一样。所以本章的 EPWDV-Hop 算法只需要额外的增加很小一部分的计算开销就能够达到有效预防虫洞攻击的效果，从而使更多的传感器节点获取有效的物理位置信息。

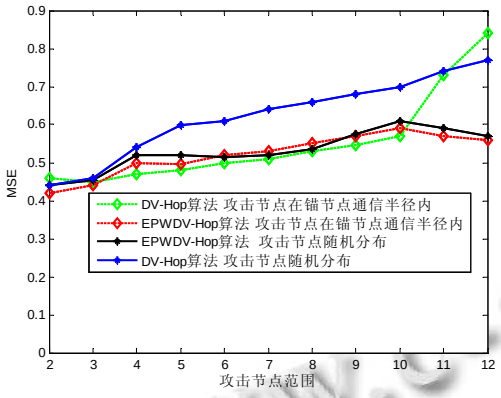


图 6 MSE 仿真比较

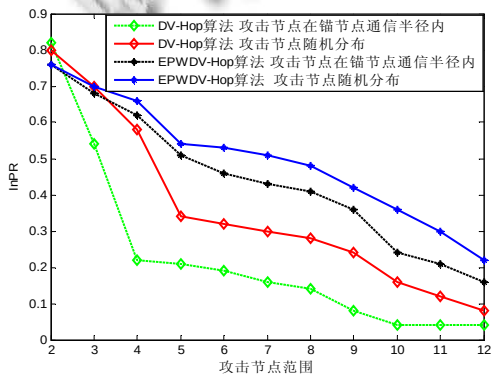


图 7 InPR 仿真比较

表 1 恶意节点在通信半径内

序号	实际位置	恶意节点在通信半径内			
		EPWDV-Hop		DV-Hop	
		估算位置	误差(%)	估算位置	误差(%)
x	24.88	30.19	35.4	23.33	13.4
y	17.85	16.69		20.05	
x	70.51	76.24	43.8	61.48	63.1
y	34.18	37.51		31.12	
x	92.95	10.02	24.9	108.35	108.9
y	36.80	36.48		30.99	
x	50.58	32.05	202.8	26.02	277.8
y	25.69	1.90		7.86	

表 2 恶意节点随机分布

序号	实际位置	恶意节点随机分布			
		EPWDV-Hop		DV-Hop	
		估算位置	误差(%)	估算位置	误差(%)
x	24.88	29.49	34.9	28.56	90.8
y	17.85	32.89		7.04	
x	70.51	81.98	76.9	67.51	37.2
y	34.18	33.45		35.62	
x	92.95	92.49	26.9	110.31	139.5
y	36.80	32.81		26.27	
x	50.58	76.11	229.8	75.49	293.9
y	25.69	3.02		9.98	

4 结论

本文通过对改进前后的定位算法进行比较，利用 MATLAB/Simulink 仿真软件的仿真，得出本文算法无需其他外部的硬件支持，只在算法执行的第一阶段增加了额外的少量的计算开销，就可以达到有效地预防虫洞攻击的效果。通过仿真实验表明，在条件相同的情况下，与 DV-Hop 算法相比较，EPWDV-Hop 算法可以很好的防御虫洞攻击，如果网络中存在严重的虫攻击，那么 EPWDV-Hop 算法能够使得更多节点获得有效位置。同时，EPWDV-Hop 算法也为其他解决虫洞攻击问题提供了一个参考方案。抛弃来自于恶意节点的数据包以达到降低能量消耗的目的将是本文需要进一步研究的不足之处。

(下转第 122 页)

4 结论

模糊控制技术和 PID 控制技术在工业生产中的应用越来越多，但是各有自己的缺陷。本文通过实验分析表明，如果改常规 PID 控制为模糊自适应 PID 控制方式，则能够明显改善其动态性能，不仅较小了起动电流，缩短了起动时间，而且具有了更强的鲁棒性和自适应性从而可以更快地重新趋于稳定，提高了控制精度和起动性能。

参考文献

1 储岳中,陶永华.基于MATLAB的自适应模糊PID控制系统计算机仿真.安徽工业大学学报(自然科学版),2004,(1).

2 杨瑜,庄圣贤.异步电机的模糊 PID 矢量控制.电子元器件应用,2010,(10).

3 Astrom KJ, HagglundT, PIDcontrollers:theory, design and tuning. 2nd Edition. Research Triangle Park, North Carolina: Instrument Society of America. 1995.

4 Lu CH, Xu YW, Yang WM. Permanent magnet linear synchronous motor feed system for fuzzy PID control. Journal of Electrotechnics, 2007,22(9):59–63.

5 张化光,何希勤.模糊自适应控制理论及其应用.北京:北京航空航天大学出版社,2002.

6 陈志伟,杨向宇,申辉阳.无刷双馈电机专家自适应 PID 控制仿真研究.华南理工大学学报(自然科学版),2003(12):37–41.

7 杨白厚,杨超.模糊控制在工业中的应用阴.电气自动化.2005,89:17–21.

8 陶永华.新型 PID 控制及其应用.北京:机械工业出版社,2002.

9 张泾周,杨伟静,张安祥.模糊自适应 PID 控制的研究及应用仿真.计算机仿真,2009,(9).

10 刘金昆.先进 PID 控制及其 MATLAB 仿真.北京:电子工业出版社,2003.

(上接第 207 页)

参考文献

1 Hu L, Evans D. Using directional antenna to prevent wormhole attaeks. Network and Distributed System Seeurity Symposium. 2004. 131–141.

2 周启明,何勇.DV-Hop 中虫洞攻击的仿真及其抵御方法.计算机工程与应用,2010,46(14):88–90.

3 Buttyan L, Dora L, Vadja I. Statistical Wormhole Detection in Sensor networks. Second European Workshop on Security and Privacy in AdHoc and Sensor networks (ESAS2005). Visegrad, Hungary, July13–14, 2005.

4 程海青,王华,王芳,等.无线传感器网络节点定位中一种检测欺骗攻击的方法.太原理工大学学报,2011,42(5):510–513.

5 王晟.无线传感器网络节点定位于覆盖控制理论及技术研究.武汉理工大学,2006.

6 石为人,贾传江,梁焕焕.一种改进的无线传感器网络 DV-Hop 定位算法.传感技术学报,2011,24(1):83–87.

7 肖美华.无线传感器网络节点定位关键技术研究.南昌航空大学大学,2010.

8 杨姣,王东.基于 RTT 的统计分析方法检测与防御虫洞攻击.计算机系统应用,2011,20(6):65–68.

9 朱彤,唐俊国.无线传感器网络安全定位和位置检测.计算机工程与应用,2008,44(21):57–63.

10 刘方圆,严斌宇,张永齐,等.无线传感器网络的信任模型研究.计算机测量与控制,2011,19(5):1232–1235.