doi: 10.3969/j.issn.1006-1576.2012.03.014

一种基于 RSSI 的无线传感网络安全定位算法

马梁，彭保
（西南科技大学信息工程学院，四川 绵阳 621010）

摘要：为防止在不可靠环境中传感节点被捕获，提出一种与范围无关的算法来解决节点的定位问题，即基于接收信号强度(received signal strength indication，RSSI)的安全定位算法。介绍了通过估计各个锚节点的环境参数，用加权的最小均方法计算未知节点的位置，提高位置计算过程的鲁棒性和恶意攻击的防御性能。该方法既不用增加参考点的数量，也不用增加每个参考点或节点硬件的复杂性，就能够使传感器被动且高可靠地确定其自身位置。同时，在串谋和非串谋的攻击模式下，分析该算法对不同攻击模式的安全定位的性能。仿真结果表明：该算法可以得到更低的平均定位误差，同时达到恶意攻击对定位影响最小。

关键词：RSSI；安全定位；恶意攻击
中图分类号：TP393.08 **文献标志码**：A

A Security Localization Algorithm Based on RSSI in Wireless Sensor Networks

Ma Liang, Peng Bao
(*School of Information Engineering*, *Southwest University of Science &Technology*, *Mianyang* 621010, *China*)

Abstract: For sensing nodes not to be captured in unreliable environment, put forward a range-independent algorithm to solve node location problem, that is received signal strength indication (RSSI) security location algorithm. Through estimating anchor node environment parameters, use weighted minimum equal partition method to calculate the unknown node positions, improve the position calculation process robust and anti-attack defense ability. The method allows sensors to passively determine their location with high reliability, without increasing the number of reference points, or the complexity of the hardware of each reference point or node. At the same time, in the joint and non-joint attack modes, analyze the algorithm security location performances under different attack modes. The simulation result shows that the algorithm can get lower average location error, meanwhile reduces attacks influence have little side effects to location performance.

Key words: RSSI; security localization; malicious attacks

0 引言

无线传感器网络(wireless sensor network，WSN)可简单描述为：知觉+CPU(计算)+无线通信技术=成千上万的潜在应用。在这些应用中，大多数要求有节点相关的位置信息。但是 WSN 通常采用自组织组网的模式，节点不可能提前知道其自身位置。因此，在网络的初始化阶段需要通过定位来确认节点的位置，同时，在实际的无线传感网络中，由于环境的复杂性使得节点很可能遭到攻击，而且会不同程度地影响定位的准确性，这样就使节点的整个位置信息无效。因此，定位的过程非常重要[1-3]。基于此，笔者介绍一种新的 WSN 的安全定位方法，使得传感器能被动确定其位置，并具有高精度。

1 定位算法

1.1 安全定位问题的描述

假设在 WSN 网络中有一些恶意攻击锚节点，它们的目标就是增加实际位置和估计位置间的偏差，使得未知节点不能够正确估计自身位置[4-6]。在此，笔者不分析容易被发现的攻击以及基于 DOS(disk operating system)[7]之类的网络协议。恶意节点的攻击模式分为串谋攻击和非串谋攻击。串谋攻击是指所有的攻击锚节点都朝同一方向移动一定的距离。非串谋攻击是指攻击锚节点沿随机的方向移动一定的距离。

用 (x_i, y_i)、(x_j, y_j) 和 d_{ij} 分别表示未知节点 i 和锚 j 的真实坐标，d_{ij} 为它们之间的距离。在存在虫洞攻击，西比尔攻击和位置监测信息等[8-11]情况下，为了实现安全定位，可将公式优化为

$$\min f(x_i, y_i) = d_{ij} - \sqrt{(x_i - x_j) + (y_i - y_j)} \quad (i = M+1, M+2, \cdots, N) \tag{1}$$

这里，d_{ij} 是通过 RSSI 测距获得的。由于无线信道里有反射、多径和环境干扰，存在各种各样的传输

收稿日期：2011-09-13；修回日期：2011-10-09
基金项目：基于语义的物联网信息标引、计算及智能管理机制研究(10zg2116)
作者简介：马梁(1986—)，男，安徽人，硕士研究生，从事无线传感网络安全定位的研究。

损耗，因此需要将高斯噪声 x^{σ} 添加到仿真里。其计算公式为：

$$P_r(d)=P_r(d_0)-10n\lg\left(\frac{d}{d_0}\right)-X_{\delta},d>d_0 \quad (2)$$

这里，$P_r(d)$ 是接收功率，$P_r(d_0)$（距离为 d_0 的路径损耗）在自由空间可以被忽略，$n\in[2,5]$（信号传播衰减因子）为基于指定路径的损耗因子，X_{σ} 为高斯标准偏差，均值为 0，$\delta\in[4,10]$（标准偏差）。当 $d_0=1\,\mathrm{m}$，式 (2) 可以简化为式 (3)：

$$P_r(d)=A-10n\lg(d) \quad (3)$$

$$\text{当 } A=\overline{P_r}(d_0)-X_{\delta} \quad (4)$$

$$\text{同理 } d=10^{(A-RSSI)/(10n)} \quad (5)$$

从式 (3) 可得到结论：常数 A 和 n 的值取决于接收信号强度和信号传输距离间的关系。

1.2　安全定位算法

笔者全面考虑了每个锚节点的可靠性因子和锚节点的剩余能量，以及由锚节点与未知节点间距离关系对未知节点位置的确定和整个网络性能的影响。通过安全定位算法确定未知节点的准确的位置。

1) 首先，锚节点集 $\sum_{i=1}^{n}\mathrm{Anchor}_i(x_i,y_i)$ 中各个锚节点广播本锚节点的 ID 及坐标信息。然后，所有节点（包括锚节点与未知节点）接收并记录在其通信范围内的锚节点信息及 RSSI 值。

2) 每个锚节点含有一个信息表，记录了其通信范围内的锚节点坐标及 RSSI 值，利用这个信息表和式 (3)，并通过最小均方法计算锚节点 Anchor_i 的参数 A_i、n_i，使每个锚节点在其通信范围内有自己的环境参数。

3) 锚节点 Anchor_i 通过参数 A_i，n_i 及与通信范围内锚节点 Anchor_j 的 RSSI_{ij}，利用式 (5) 计算出锚节点 Anchor_i 与锚节点 Anchor_j 两者之间的估计距离 d_est_{ij}，同时通过锚节点 Anchor_i 的信息表计算出两者的坐标距离为 $d_{ij}=\sqrt{(x_i-x_j)^2+(y_i-y_j)^2}$，即可计算出锚节点 Anchor_i 的平均误差因子 W_i 与最大误差因子 $W\_\max_i$（误差因子=$d\_\mathrm{est}_{ij}/d_{ij}$，平均误差因子是将锚节点 Anchor_i 的 n 个误差因子从小到大排列，取第 $n/2$ 个为 W_i）。

4) 锚节点 Anchor_i 向未知节点广播本锚节点的 ID、坐标、A_i、n_i 及平均误差因子 W_i 与最大误差因子 $W\_\max_i$，未知节点接收并记录这些信息，建立信息表，未知节点同样通过参数 A_i、n_i 及 2 次接收的平均 RSSI_i，利用式 (5) 算出锚节点 Anchor_i 与未知节点的估计距离 d_est_i，同时计算 $x\_\max=\max(x_i),i\in[1,n]$，$x\_\min=\min(x_i),i\in[1,n]$，$y\_\max=\max(y_i),i\in[1,n]$，$y\_\min=\min(y_i),i\in[1,n]$，即可确定未知节点的可能存在区域为 $[x\_\max-R,x\_\min+R]$，$[y\_\max-R,y\_\min+R]$。

5) 未知节点利用信息表知道锚节点 Anchor_i 的最大误差因子为 $W\_\max_i$，可以估计未知节点与锚节点 Anchor_i 之间的距离在区间 $[\max(d\_\mathrm{est}_i-W\_\max_i*R,0),\min(d\_\mathrm{est}_i+W\_\max*R,R)]$ 内，则未知节点的可能存在区域为 $[x\_\max-R,x\_\min+R]$，$[y\_\max-R,y\_\min+R]$。

6) 以区域 $[x\_\max-R,x\_\min+R]$，$[y\_\max-R,y\_\min+R]$ 循环产生 m 个坐标节点集 $\mathrm{Unknow}_i(x_i,y_i),i\in[1,m]$，然后在其通信范围内的各个锚节点集对未知坐标节点集进行投票（投票方式为以各锚节点为中心，以 $[\max(d\_\mathrm{est}_i-W\_\max_i*R,0)$，$\min(d\_\mathrm{est}_i+W\_\max*R,R)]$ 为圆环半径，如果未知节点坐标在其范围内则投上一票，否则不投，每个未知坐标节点的初始投票数为 0）。

7) 待投票结束后，计算所有未知节点坐标集中各个坐标的投票数，选择投票最多的坐标节点集记为 $\mathrm{Unknow\_1}_i(x_i,y_i)$，并通过这些坐标集重新计算 $x\_\max=\max(x_i),i\in[1,m]$，$x\_\min=\min(x_i),i\in[1,m]$，$y\_\max=\max(y_i),i\in[1,m]$，$y\_\min=\min(y_i),i\in[1,m]$，确定新的未知节点可能存在区域为 $[x\_\max-R,x\_\min+R]$，$[y\_\max-R,y\_\min+R]$。

8) 按步骤 6、7 循环一定次数，记录所有投票最多的未知节点坐标集记录为 $\mathrm{Unknow\_max}_i(x_i,y_i),i\in[1,L]$（$L$ 表示未知节点坐标集投票最多的个数）。

9) 锚节点 Anchor_i 与未知节点的估计距离 d_est_i，与未知节点坐标集记录为 $\mathrm{Unknow\_max}_j(x_j,y_j)$ 中每个节点的距离为 d_{ij}，通过 $E_j=\sum_{i=1}^{k}W_i*(d_{ij}-d\_\mathrm{est}_i)^2,j\in[1,L]$ 计算出最小的 E，

那么其对应的坐标即是未知节点的估计坐标。

2 仿真分析

2.1 仿真环境的设置

实验采用Matlab 7.0。假设节点的通信半径为R，在未知节点的通信范围内总共有n=11个锚节点。

2.2 仿真标准

1) 定位误差E_n：通信范围内估计位置与实际位置间距离的比值。计算公式为：

$$E_n = \sum_{i=1}^{m} \sqrt{\left(x_i - \tilde{x}\right)^2 + \left(y_i - \tilde{y}\right)^2} \Big/ m$$

2) 算法的安全性：包含了抵制来自对锚节点的不同比例恶意攻击的实验。

2.3 仿真结果的分析

为研究在不同密度的恶意信标节点和攻击模式下安全定位的位置误差，仿真时在标准网络里只改变密度和攻击模式。为分析算法的效果，设置环境参数 $A\in[-50,-30]$ $n\in[2,5]$，仿真结果如图 1 和图 2。

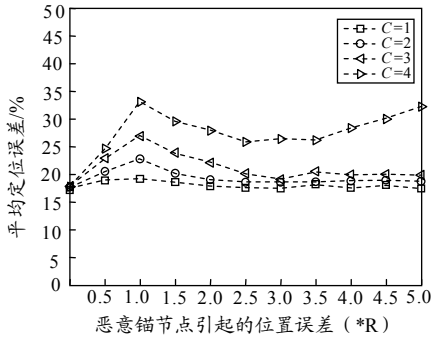

图 1 C=1:4 串谋攻击

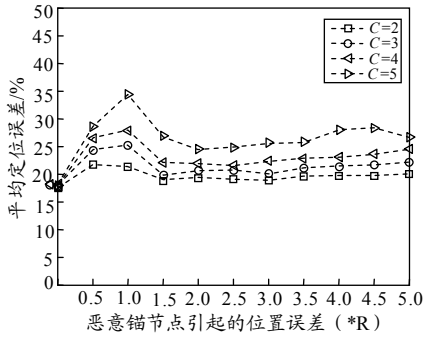

图 2 C=2:5 非串谋攻击

图 1 和图 2 分别演示了 RSSI 安全定位算法抵抗各种恶意信标节点串谋攻击和非串谋攻击的健壮性。很明显，在串谋攻击中由恶意信标节点产生的相对误差更大一些。在同一方向的串谋攻击产生的误差不会改变恶意信标节点间的相对距离，使得节点间仍然认为对方是良性的信标节点。因此，相同的恶性信标节点数，群攻可以导致更大的定位误差，即攻击更有效。但整体而言，对于不同的攻击模式，笔者提出的安全定位算法可以大大减少恶性攻击的定位误差，可以很好地防御恶性攻击。

3 结论

仿真结果表明：安全定位算法可以在攻击后接收较低的平均位置误差，而且其对有恶意攻击情况下的定位性能的影响不大。

参考文献：

[1] Fredric Newberg. Wireless sensor networks design and implementation[D]. Los Angeles: University of California, Los Angeles, 2002.

[2] C.-Y. Chong, Kumar S. Sensor networks: evolution, opportunities, and challenges[J]. Proceedings of the IEEE 2003, 91(8): 1247−1256.

[3] Donggang Liu. Security Mechanisms for Wireless Sensor Networks[D]. Raleigh: North Carolina State University PHD Thesis, 2005.

[4] Lazos L, Poovendran R. HiRLoc: High resolution Robust Localization for Wireless Sensor Networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 233−246.

[5] Li Z, Trappe W, Y. Zhang, et al. Robust Statistical Methods for Securing Wireless Localization in Sensor Networks[C]//Proc. of Proceedings of the Fourth International Conference on Information Processing in Sensor Networks(IPSN 05). UCLA: IEEE Signal Processing Society and ACM SIGBED, 2005: 91−98.

[6] 孙晓磊, 颜培玉, 解志斌, 等. 网络安全技术中的量子密码通信[J]. 四川兵工学报, 2010, 31(8): 97−99.

[7] Q. Wang, Y. Zhu, L. Cheng. Reprogramming Wireless Sensor Networks: Challenges and Approaches[J]. IEEE Network, 2006, 20(3): 48−55.

[8] Ayong Ye. Secure node positioning in Wireless sensor networks[D]. Xian: Xidian University PHD Thesis, 2009.

[9] Yang Feng. Research on the technique of countering malicious node in wireless sensor networks[D]. Hefei: University of science and technology of china PHD Thesis, 2009.

[10] Meiling Sun. Research on GA based self-localization algorithm in wireless sensor networks[D]. Dongying: China University of Petroleum Master Degree Thesis, 2009.

[11] Mudubai R, Barriac G, Madhow U. On the Feasibility of Distributed Beamforming in Wireless Networks[J]. IEEE Trans Wireless Communications, 2007, 6(5): 1754−1763.