# ZigBee 网络容忍恶意攻击的安全定位算法

郁 滨 刘子清*
(信息工程大学 郑州 450001)

**摘 要**：该文提出一种基于进化思想的容忍恶意攻击安全定位算法(ELAMP)。依据最大似然估计概率模型，结合接收信号强度(RSS)标准差与距离的分布关系，建立 ZigBee 网络安全定位模型。进一步，设计进化算法对模型进行求解，并分析了算法的收敛性和时间复杂度。实验结果表明，当恶意节点比例不超过 50%的情况下，所提算法的定位精度明显优于已有定位算法。

**关键词**：安全定位；ZigBee；进化算法；接收信号强度；恶意攻击
**中图分类号**：TP393 **文献标识码**：A **文章编号**：1009-5896(2018)07-1676-08
**DOI**: 10.11999/JEIT170962

# Malicious Attack-resistant Secure Localization Algorithm for ZigBee Network

YU Bin LIU Ziqing
(*PLA Information Engineering University*, *Zhengzhou* 450001, *China*)

**Abstract**: A malicious attack-resistant secure localization algorithm Evolutionary Location Algorithm with the Maximum Probability value (ELAMP) based on evolutionism is proposed. According to the maximum likelihood estimation probability model and the distribution of Received Signal Strength (RSS) standard deviation and the distance, a secure location model of ZigBee network is established. Furthermore, the evolutionary algorithm is designed to solve the model, and the convergence and the time complexity of the algorithm is analyzed. Experimental results show that the proposed algorithm has better positioning accuracy than the existing positioning algorithm when the proportion of malicious nodes is not more than 50%.

**Key words**: Secure location; ZigBee; Evolutionary algorithm; Recived Signal Strength (RSS); Malicious attack

## 1 引言

ZigBee 是一种短距离、低速率无线网络技术，它在医疗健康监视、战场环境监测、生态环境数据收集等领域具有广泛应用[1]。节点定位技术是许多 ZigBee 网络应用得以实现的基础，如基于地理信息的路由协议、目标跟踪、火灾报警等。目前，诸多定位方法被提出，如基于到达时间[2](Time of Arrival, ToA)，到达时间差[3](Time Difference of Arrival, TDoA)，到达角度[4](Angle of Arrival, AoA)和接收信号强度[5](Received Signal Strength, RSS)。其中，基于 RSS 的定位方法由于实现简单且不需要增加额外的硬件设施，被广泛应用于 ZigBee 节点定位[6]。

基于 RSS 的定位算法主要有最大似然估计法[7](Maximun Likelihood estimator, ML)、线性最小二乘法[8](Linear Least Squares, LLS)、凸优化[9]和位置指纹[10]等。这些算法虽然具有较好的定位性能，但对恶意攻击的考虑尚不全面。ZigBee 网络具备开放性且常常部署在无人值守的非合作环境中，因此攻击者不仅可以通过俘获节点伪造、重放或插入数据报文，而且会采用故意阻挡、遮盖等方式削弱信号强度，使节点获得的接收信号强度值与参考坐标不一致，从而导致 ZigBee 网络定位功能失效。

文献[11]提出一种最小中值二乘法安全定位算法，通过迭代加权的方法过滤恶意数据，但是该算法的计算复杂度较高。文献[12]提出一种基于梯度下降法的安全定位算法，以梯度值为评估对象滤除恶意节点，但算法滤除恶意节点的方法太过简单，其准确度较低。文献[13]提出一种分散式的 DPC 安全定位算法，利用测量和计算一致性原理滤除恶意节点，然后基于簇平面完成定位，但方案要求节点的发射功率可调。文献[14]提出基于网络投票法的安全定位算法，利用投票机制过滤恶意节点，但算法需要将网络划分为网格并多次迭代，计算量过大。文

收稿日期：2017-10-19；改回日期：2018-03-22；网络出版：2018-04-21
*通信作者：刘子清 13223091632@163.com
基金项目：信息保障技术重点实验室开放基金(KJ-15-104)
Foundation Item: The Key Laboratory of Information Assurance Technology Open Fund (KJ-15-104)

献[15]指出机械地将过滤恶意节点与位置估计分开会额外增加算法的时耗，从而提出一种无需过滤恶意信标节点的安全定位算法 RSRSL。该算法将信号发射功率和待估算坐标一同作为未知量，建立最大似然估计定位模型，然后将其转化为半定规划问题。但当待定位节点数量大时，算法的复杂度甚至比线性最小二乘法还大，并且定位精度相对较低。上述算法均对恶意节点过滤和位置估计两个环节进行相对独立地处理，导致算法复杂度和定位精度都不太理想。目前，进化算法已经被用于解决无线传感器网络定位问题[16]。进化算法可以有机融合恶意节点过滤和位置估计两个环节，其中选择算子可以同时完成恶意节点过滤和位置坐标估计两个过程，不仅具有较高的计算效率，而且可以通过设计交叉和变异算子来提高定位精度。

基于此，本文提出一种基于进化思想的 ZigBee 网络容忍恶意攻击的安全定位算法。首先，结合 RSS 标准差与距离的关系建立最大似然估计概率模型；其次，针对该模型的概率乘积形式无法抵御恶意攻击的问题，使用对数函数对其进行改造；然后，设计进化算法估算节点位置，并分析算法的收敛性和时间复杂度；最后，基于公开数据集进行仿真实验获取算法理想的边界条件，并在自主设计的 ZigBee 定位系统上进行实测实验。

## 2　安全定位模型

考虑一个 2 维 ZigBee 网络，其包含 1 个待定位节点和 $n$ 个信标节点，信标节点发送携带自身坐标的报文，其坐标用 $L_i=(x_i,y_i),i=1,2,\cdots,n$ 表示，待定位节点坐标未知，用 $s=(x,y)$ 表示。待定位节点测量到第 $i$ 个信标节点发送报文的 RSS 用对数正态分布模型表示为式(1)：

$$\mathrm{RSS}=P_0-10n\lg\frac{d}{d_0}+\nu \tag{1}$$

其中，RSS 表示在距离 $d$ 处获得的信号强度值，单位为 dBm；$P_0$ 表示在参考距离 $d_0$ 处的 RSS，一般取 $d_0$ 为 1 m；$n$ 表示路径衰减因子；$\nu$ 表示为环境噪声，它是一个均值为 0，方差为 $\sigma^2$ 的高斯随机变量。当待定位节点与信标节点间的真实物理距离为 $d$ 时，RSS 的条件概率分布表示为式(2)：

$$P(\mathrm{RSS}\mid d)=\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{\nu^2}{2\sigma^2}\right) \tag{2}$$

用 $P(d)$ 表示节点间真实物理距离为 $d$ 的先验概率，$P(\mathrm{RSS})$ 表示接收信号强度的先验概率，$P(d\mid\mathrm{RSS})$ 表示在接收信号强度为 RSS 条件下真实物理距离为 $d$ 的概率，由式(1)和式(2)可得式(3)：

$$\begin{aligned}P(d\mid\mathrm{RSS})&=P(\mathrm{RSS}\mid d)P(d)/P(\mathrm{RSS})\\&=\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{\nu^2}{2\sigma^2}\right)\cdot P(d)/P(\mathrm{RSS})\\&=\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left\{-\frac{(\mathrm{RSS}-P_0+10n\lg d)^2}{2\sigma^2}\right\}\\&\quad\cdot P(d)/P(\mathrm{RSS})\end{aligned} \tag{3}$$

RSS 标准差与测量距离的变化关系接近正态分布[16]，可以用高斯函数 $\sigma(d)=a\exp\left(-\frac{(d-d_0)^2}{b^2}\right)$ 进行拟合，其中的参数 $a,b,d_0$ 在后续实验中将给出具体取值方法。

假设待定位节点接收到 $n$ 个信标节点的信号强度为 $\mathrm{RSS}_1,\mathrm{RSS}_2,\cdots,\mathrm{RSS}_n$，且与各个信标节点的欧式距离分别是 $d_1,d_2,\cdots,d_n$，$d_i=\|L_i-s\|$，根据式(3)得到最大似然估计定位模型如式(4)所示：

$$\begin{aligned}(x^*,y^*)&=\arg\max_{x,y}L(\mathrm{RSS}_1,\mathrm{RSS}_2,\cdots,\mathrm{RSS}_n;s)\\&=\arg\max_{x,y}\{F(x,y)\},\\F(x,y)&=\prod_{i=1}^{n}F_i(x,y)=\prod_{i=1}^{n}P(d_i\mid\mathrm{RSS}_i)\\&=\prod_{i=1}^{n}\left(\frac{1}{\sqrt{2\pi\sigma_{d_i}^2}}\exp\left\{-\frac{(\mathrm{RSS}_i-P_0+10n\lg d_i)^2}{2\sigma_{d_i}^2}\right\}\right.\\&\quad\left.\cdot P(d_i)/P(\mathrm{RSS}_i)\right)\end{aligned} \tag{4}$$

在正确的待定位节点位置处，恶意信标节点 $L_i$ 提供的定位概率值 $P(d_i\mid\mathrm{RSS}_i)$ 几乎接近于 0。由于有几乎为 0 的连乘因子存在，模型式(4)相乘结果也就几乎为 0，定位失效。为此，对最大似然估计定位模型取对数，得到连加形式的安全定位模型，避免单个恶意信标节点影响定位模型的有效性。去掉常数项，得到安全定位模型为式(5)：

$$\begin{aligned}(x^*,y^*)&=\arg\min_{x,y}\{F(x,y)\},\\F(x,y)&=\sum_{i=1}^{n}F_i(x,y)=\sum_{i=1}^{n}\left(\frac{(\mathrm{RSS}_i-P_0+10n\lg d_i)^2}{2\sigma_{d_i}^2}\right.\\&\quad\left.-\ln P(d_i)+\ln\sigma_{d_i}\right)\end{aligned} \tag{5}$$

其中，$P(d_i)$ 表示半径为 $d_i$ 的环形区域占节点通信范围的比重[17]，计算方法如式(6)所示。其中 $R$ 表示节点通信半径，$m(d_i)\approx\begin{cases}2\pi\cdot d_i, & d_i\le R\\0, & d_i>R\end{cases}$。

$$P(d_i)=\frac{m(d_i)}{\int_0^R m(d_i)\,\mathrm{d}\,d_i} \tag{6}$$

## 3 ELAMP 算法

本文利用进化思想的迭代寻优能力，并结合无线射频信号辐射特点，设计了求解安全定位模型式(5)的算法，称为概率值最大进化定位算法(Evolutionary Location Algorithm with The Maximum Probability value, ELAMP)。算法步骤如下：

第 1 步 种群初始化： 在信标节点构成的定位平面内，随机生成 $\mu$ 个初始解 $\{s_1,s_2,\cdots,s_\lambda\}$，其中，$s_q=\left(x_q,y_q\right)^T$，$q=1,2,\cdots,\mu$。针对初始解中的任意个体 $s_q$，以信标节点 $L_i$ 为圆心，构造线段 $L_is_q$。在各线段上，求解适应度函数式(7)的最小值点，记为 $s_{iq}$，其中 $d_i=\sqrt{(x-x_i)^2+(y-y_i)^2}$，$x\in\left(0,x_q(0)\right]$，$y\in\left(0,y_q(0)\right]$。

$$F_i(x,y)=\left(\mathrm{RSS}_i-P_0+10n\lg d_i\right)^2\Big/\left(2\sigma_{d_i}^2\right)-\ln P(d_i)+\ln\sigma_{d_i} \tag{7}$$

这些最小值点和各自的信标节点的距离并不完全相同，它们构成以信标节点 $L_i$ 为圆心的一个圆环，记它们为初始种群 $A_0=\left\{s_{iq}\middle|i=1,2,\cdots,n,q=1,2,\cdots,\mu\right\}$，如图 1 所示。

第 2 步 子群体进化： 针对各圆环上的子群体，充分有效地扩充其数目，以提高位置估计的准确度和精度。开始时，令第 2 步进化代数 $k=0$。

(1)交叉：针对第 $i$ 个圆环上的子群体，任意取两个点作为 $s_{i1}(k)$，$s_{i2}(k)$，平分 $s_{i1}(k)$ $s_{i2}(k)$ 与圆心 $L_i$ 形成的夹角 $\theta=\angle s_{i1}(k)L_is_{i2}(k)$，产生两个新的个体 $s_{i1}^o(k)$，$s_{i2}^o(k)$，其计算公式如式(8)：

$$\left.\begin{aligned}x_i^o(k)&=x_i+\cos(\theta_{i2}+\theta/2)\left(\left|s_{i1}(k)L_i\right|+\left|s_{i2}(k)L_i\right|\right)/2\\ y_i^o(k)&=y_i+\sin(\theta_{i2}+\theta/2)\left(\left|s_{i1}(k)L_i\right|+\left|s_{i2}(k)L_i\right|\right)/2\end{aligned}\right\} \tag{8}$$

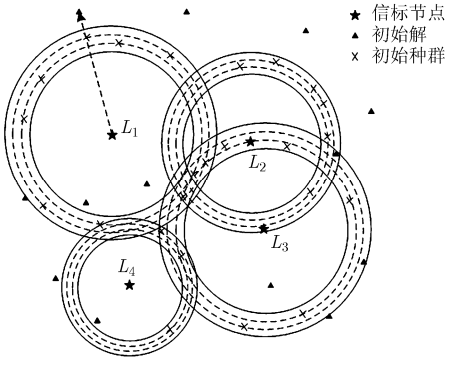


图 1 种群初始化示意图

其中，$x_i^o(k)$，$y_i^o(k)$ 代表 $s_i^o(k)$ 的横坐标和纵坐标，$\left|s_{i1}(k)L_i\right|$ 和 $\left|s_{i2}(k)L_i\right|$ 分别代表连线 $s_{i1}(k)L_i$ 和 $s_{i2}(k)L_i$ 的长度，$\theta_{i2}$ 为 $s_{i2}(k)L_i$ 的水平坐标夹角。另一个体用同样的计算方式可得到其坐标，如图 2 所示。

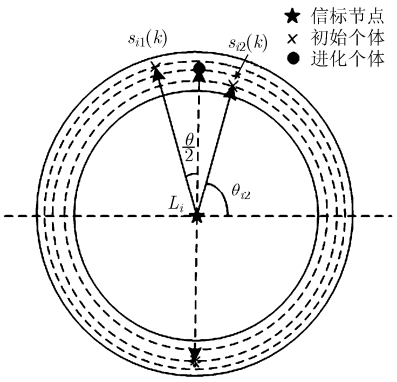


图 2 交叉算子示意图

(2)均匀变异： 对交叉后的子代，任取一个个体 $s_{iq}^o(k)$,，绕圆心 $L_i$ 顺时针随机转动角度 $\theta_r$，得到变异后的下一代个体 $s_{iq}^v(k)$，如图 3 所示。

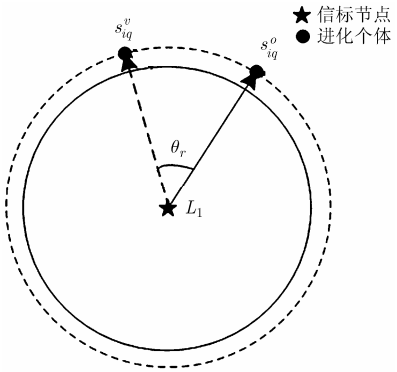


图 3 均匀变异示意图

(3)选择： 经过半角交叉和随机变异后，原子群体、交叉后子群体和变异后子群体构成定位平面上的新的种群为 $\left\{s_{iq},s_{iq}^o(k),s_{iq}^v(k)\middle|i=1,2,\cdots,n,q=1,2,\cdots,\mu\right\}$。以 $F(x,y)=\sum_{i=1}^n F_i(x,y)$ 为适应度函数，计算全部个体的适应度值，筛选出该圆环与其它圆环交叉区域内的 $\mu$ 个优良个体，如图 4 所示。每个圆环上有 $\mu$ 个个体，共有 $n$ 个圆环，它们组成下一代种群 $A_1$，$A_1=\left\{\bar{s}_{iq}\middle|i=1,2,\cdots,n,q=1,2,\cdots,\mu\right\}$，$k=k+1$。若 $k$ 大于事先给定的第 2 步进化代数 $G_1$，则进入第 3 步；否则，对此圆环的个体继续执行交叉、均匀变异算子。

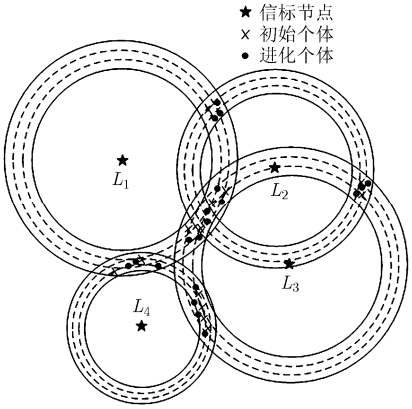


图 4 选择算子示意图

第 3 步　正常区域个体进化：

(1)正常区域筛选：　种群 $A_1$ 中，全部由正常信标节点的圆交叉所形成的区域是正常区域，包含恶意信标节点圆的区域是非正常区域。非正常区域内个体的适应度值远小于正常区域内个体的适应度值，由此可以筛选出正常区域。基于此，以 $F(x,y)=\sum_{i=1}^{n}F_i(x,y)$ 为适应度函数，选择出正常区域，记该区域内的个体为 $\bar{s}_q(t), q=1,2,\cdots,\lambda, G_2=0$ , $\lambda$ 是该区域个体数目，$t$ 代表第 3 步进化代数。

(2)凸组合交叉：　圆的交叉区域是一个凸区域，从中随机选取 3 个个体 $\bar{s}_1(t),\bar{s}_2(t),\bar{s}_3(t)$，利用公式 $\bar{s}_i^c(t)=\sum_{j=1}^{3}\omega_{i_j}\bar{s}_j(t)$ 计算获得一个新的个体，其中 $\omega_{i_j}$ 为在 0 和 1 之间的随机数，并且满足 $1=\sum_{j=1}^{3}\omega_{i_j}$ 。

(3)分量正态变异：　设计两个正态分布函数 $X_1\sim N_1\left(0,\sigma_1^2\right)$ 和 $X_2\sim N_2\left(0,\sigma_2^2\right)$，对交叉后的个体 $\bar{s}_i^c(t)$ 中的两个位置分量 $\bar{x}_i^c(t)$ 和 $\bar{y}_i^c(t)$ 分别进行高斯扰动，如式(9)所示。

$$\left.\begin{aligned}\bar{x}_i^n(t)&=\bar{x}_i^c(t)+X_1\\ \bar{y}_i^n(t)&=\bar{y}_i^c(t)+X_2\end{aligned}\right\}\tag{9}$$

得到新个体 $\bar{s}_i^n(t)$，$\bar{x}_i^n(t)$ 和 $\bar{y}_i^n(t)$ 分别是个体 $\bar{s}_i^n(t)$ 的横坐标和纵坐标。因为信道噪声近似服从正态分布，这里采用正态分布作为扰动量，有利于提高定位准确度。

(4)选择：　经过凸组合交叉和分量正态变异后，新个体为 $\bar{s}_i^c(t)$ 和 $\bar{s}_i^n(t)$，以 $F(x,y)=\sum_{i=1}^{n}F_i(x,y)$ 为适应度函数，从中选取 $\lambda$ 个个体作为下一代种群 $A_2$，$t=t+1$，$A_2=\left\{\bar{\bar{s}}_i(t+1)\middle|i=1,2,\cdots,\lambda\right\}$。若 $t$ 大于预先设置的第 3 步种群进化代数 $G_2$，算法终止，输出最优个体 $\left(x^*,y^*\right)=\arg\min_{x,y}F\left(\bar{\bar{s}}_i\left(G_2\right)\right)$。否则，转入第 3 步的凸组合交叉、分量正态变异算子步骤继续进化。

算法流程如图 5 所示，其中 $k$ 代表种群第 2 步进化的代数，$t$ 代表第 3 步进化的代数，$G_1,G_2$ 分别是第 2 步、第 3 步种群的最大进化代数。

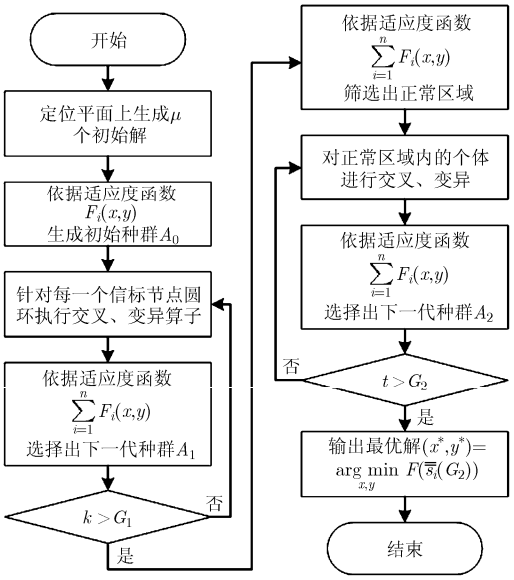


图 5 算法流程图

## 4 算法分析

### 4.1 算法收敛性

**定义 1**　对于可行解空间 $\Omega$，对充分小的 $\varepsilon>0$，如果 $\mathrm{Prob}\{\|x'-x\|\le\varepsilon\}>0$，其中 $x'$ 是 $x$ 通过交叉和变异后得到的点，$\mathrm{Prob}\{\cdot\}$ 代表事件 $\{\cdot\}$ 的概率，则称 $x'$ 由 $x$ 在 $\varepsilon$ -精度上可达。

**定义 2**　对于可行解空间 $\Omega$，如果 $\mathrm{Prob}\{x'=x\}>0$，其中 $x'$ 是 $x$ 通过交叉和变异后得到的点，$\mathrm{Prob}\{\cdot\}$ 代表事件 $\{\cdot\}$ 的概率，则称 $x'$ 由 $x$ 可达。

ELAMP 算法主要由两个进化步骤组成，只要证明该两个步骤收敛，那么整个算法即收敛。

**引理 1**[18,19]　若进化算法满足以下两个假设条件，则该算法以概率 1 或在 $\varepsilon$ -精度上收敛于全局最优解，且与初始种群无关。

**假设 1**　进化种群中，对于任意两个个体 $a$ 和 $b$，个体 $b$ 由个体 $a$ 可达，或者以 $\varepsilon$ -精度可达。

**假设 2**　种群序列 $G(0),G(1),\cdots,G(k),\cdots$ 满足单调性，其中 $k$ 代表种群的代数。即 $\forall k$，满足 $\max(f(x)\mid x\in P(k+1))\ge\max(f(x)\mid x\in P(k))$。

**定理 1**　对于 ELAMP 算法第 2 步可行解空间的群体，按照交叉、均匀变异和选择算子进行进化，以概率 1 收敛于可行解空间的全局最优解，且与初始种群分布无关。

**证明**　第 2 步可行解空间群体是信标节点 $L_i$ 的

圆环群体 $s_{iq}, q=1,2,\cdots,\mu$。任取其中两个个体 $a$ 和 $b$，假设 $a$ 通过交叉后得到任一子代个体 $c$。由于交叉后个体 $c$ 被选中发生变异的概率是 $1/\left(\mu+C_\mu^2\right)$，显然大于 0。因此只需证明 $c$ 发生变异到 $b$ 的概率 $\text{Prob}\{c=b\}>0$，即可说明可行解空间内任意个体 $a$，$b$ 是可达的。记交叉后的子代为 $C_{iq}$，由于变异采用的是 $[0,2\pi)$ 的均匀旋转，$\forall c\in C_{iq}$ 变异到 $b$ 的概率 $\text{Prob}\{c=b\}=1/2\pi>0$，所以假设 1 成立。

又因为选择策略中以 $F(x,y)=\sum_{i=1}^{n}F_i(x,y)$ 为适应度函数，该函数在可行解空间内连续，上下有界，且采用保留 $\mu$ 个最好个体作为下一代种群，每次进化的下一代最好个体必定好于上一代，满足单调性，因此假设 2 成立。从而定理 1 得证。

**定理 2** 对于 ELAMP 算法第 3 可行解空间的群体，按照凸组合交叉、分量正态变异和选择进行进化，以概率 1 在 $\varepsilon$-精度上收敛于可行解空间的全局最优解，且与初始种群无关。

**证明** 第 3 步进化的群体是在正常区域筛选算子执行完毕后的正常区域内的群体，为 $\bar{s}_q, q=1,2,\cdots,\lambda$。对于任意两个个体 $a$，$b$，用 $c$ 表示 $a$ 通过凸组合交叉生成的下一子代个体。同理于定理 1 的证明过程，$c$ 被选中进行分量正态变异的概率是 $1/\left(\lambda+C_\lambda^3\right)$，显然大于 0。令 $x_c, y_c$ 分别是 $c$ 的横坐标和纵坐标，$x_c', y_c'$ 分别是经过分量正态变异后的横坐标和纵坐标，则 $\text{Prob}\left\{\left\|x_c'-x_b\right\|<\varepsilon\right\}=\dfrac{1}{\sqrt{2\pi}\sigma_1}\cdot\int_{-\varepsilon}^{\varepsilon}\text{e}^{-\frac{x^2}{2\sigma_1^2}}\text{d}x$，$\text{Prob}\left\{\left\|y_c'-y_b\right\|<\varepsilon\right\}=\dfrac{1}{\sqrt{2\pi}\sigma_2}\int_{-\varepsilon}^{\varepsilon}\text{e}^{-\frac{y^2}{2\sigma_2^2}}\text{d}y$。由于使用了两个相对独立的正态分布对个体 $c$ 的横坐标和纵坐标进行分别变异，得

$$\begin{aligned}&\text{Prob}\{\|b-a\|<\varepsilon\}\\&=\text{Prob}\left\{\left(x_c'-x_b\right)^2+\left(y_c'-y_b\right)^2<\varepsilon\right\}\\&\geq\text{Prob}\left\{\left(x_c'-x_b\right)^2<\varepsilon\right\}\cdot\text{Prob}\left\{\left(y_c'-y_b\right)^2<\varepsilon\right\}\\&=\frac{1}{\sqrt{2\pi}\sigma_1}\int_{-\sqrt{\varepsilon}}^{\sqrt{\varepsilon}}\text{e}^{-\frac{x^2}{2\sigma_1^2}}\text{d}x\cdot\frac{1}{\sqrt{2\pi}\sigma_1}\int_{-\sqrt{\varepsilon}}^{\sqrt{\varepsilon}}\text{e}^{-\frac{y^2}{2\sigma_1^2}}\text{d}y\end{aligned}$$

显然可知 $\text{Prob}\{\|b-a\|<\varepsilon\}>0$ 成立。因此，假设 1 成立。

又由于采取保留最优 $\lambda$ 个个体作为下一代，并且其适应度函数 $F(x,y)=\sum_{i=1}^{n}F_i(x,y)$ 在可行解空间内连续，所以每次进化的下一代最好个体肯定好于上一代的最好个体，满足单调性，假设 2 成立。从而定理 2 得证。

依据引理 1，基于定理 1 和定理 2，ELAMP 算法以概率 1 在 $\varepsilon$-精度上收敛于全局最优解，所以算法具备收敛性。

### 4.2 时间复杂度分析

基于浮点运算的次数来评估算法的时间复杂度，并与投票法、LLS 和 RSRSL 进行对比。假设加减乘除以及平方根操作均可以通过一次浮点运算完成。$l$ 代表待定位节点数目，$n$ 代表信标节点的数目，$\mu$ 代表种群规模，$G_1$ 和 $G_2$ 分别表示第 2 步和第 3 步进化代数。算法分为 3 个步骤，第 1 步初始化种群为每个信标节点生成 $\mu$ 个初始个体，运算次数与 $n\cdot\mu$ 同数量级，因此时间复杂度可以用 $O(l\cdot n\cdot\mu)$ 表示；第 2 步中交叉共进行 $C_\mu^2$ 运算，变异进行 $2C_\mu^2$ 次运算，加上选择的运算次数，那么时间复杂度是 $O\left(l\cdot n\cdot G_1\cdot\mu^2\right)$；第 3 步与第 2 步类似，其时间复杂度用 $O\left(l\cdot n\cdot G_2\cdot\mu^2\right)$ 表示。那么算法的整体的时间复杂度可以用 $O\left(l\cdot n\cdot\left(\mu+(G_1+G_2)\cdot\mu^2\right)\right)$ 表示。

表 1 是各算法的时间复杂度对比表。从表 1 可知，当待定位节点数目增加时，LLS, RSRSL 算法的时间复杂度均呈指数增大，而本文算法和投票法的时间复杂度呈线性增大。同时，投票法定位精度依赖于网络区域内网格大小，网格数目越多，定位精度越高，时间复杂度越大。本文算法的定位精度主要依赖于初始种群数目和进化代数，与网络中信标节点数目、恶意节点数目无关，因此在大规模网络中本文算法时间复杂度比其余三者算法更具有优势。

## 5 实验及分析

为检验安全定位模型式(5)和ELAMP算法的性能，首先基于公开数据集进行仿真实验以获得算法理想的最大进化代数 $G_1$ 和 $G_2$，同时验证算法抗共谋攻击的能力，而后利用自主设计的 ZigBee 模块进行实测实验，并同 LLS[8]、投票法[14]、RSRSL 算法[15]进行比较。

### 5.1 仿真实验

为确定符合 ELAMP 算法的第 2 步和第 3 步的

**表 1 时间复杂度对比表**

| 算法 | 时间复杂度 |
|---|---|
| 投票法[14] | $O\left(k\cdot m^2\cdot(l+n)\right)$ |
| LLS[8] | $O\left(6\cdot l^3\cdot(n+l/2)^2\right)$ |
| RSRSL[15] | $O\left(k\cdot l^4\cdot(n+l/2)^2\right)$ |
| ELMAP | $O\left(l\cdot n\cdot\left(\mu+(G_1+G_2)\cdot\mu^2\right)\right)$ |

最大进化代数$G_1, G_2$，基于文献[20]提供的公开数据集进行仿真。该数据集由佛罗里达摩托罗拉通信实验室公布，总共采集了 44 个传感器的 RSSI 数据，它们的位置分布如图 6 所示。选择编号 2, 3, 10, 11, 35, 36, 44 节点为信标节点，对 15 号节点进行定位。

设估算出节点的位置为$\left(x^*, y^*\right)$，它的真实位置为 $(x, y)$，以两者欧式距离 $\mathrm{err}_i = \sqrt{\left(x^*-x\right)^2+\left(y^*-y\right)^2}$ 作为定位误差。根据文献[16]的分析，公开数据集中 RSSI 标准差与距离关系函数的参数设置为 $a=0.9, d_0=8.0, b=0.3$，初始解 $\mu=30$。图 7 是$G_1$分别取不同值时，算法的定位误差与$G_2$的关系。当$G_1=0$代表直接进入第 3 步进化，从图 7 可以看出算法的收敛缓慢，而随着$G_1$的不断增大，算法的收敛越来越快。并且当$G_1$大于 60 后，算法收敛速度基本趋于稳定。算法在$G_2$大于 80 时，定位误差基本保持在 0.8 m 左右。因此，最大进化代数$G_1$和$G_2$分别取 60 和 80，算法的定位精度比较理想。

为验证算法的抗共谋攻击的能力，共设置 3 个实验场景，第 1 个实验场景取 3 号作为恶意节点，坐标偏离实际位置$e$长度；第 2 个实验场景取 3, 12, 35 号作为恶意节点，它们独立使得自身坐标偏离实际位置$e$长度；第 3 个实验场景同样取 3, 12, 35 号作为恶意节点，不过它们实现共谋攻击，每个恶意节点都设置坐标在垂直向下的方向上偏离实际位置$e$长度。

图 8 为 3 种场景下的实验结果。从图 8 以看出，文献[15]的安全定位算法在一定程度上可以容忍恶意节点的攻击，但是随着恶意节点偏离距离的增大，其效果将会变差。本文算法在偏离距离的后期，误差基本趋于稳定，其容忍恶意节点攻击的性能明显优于文献[15]。从 3 个非共谋恶意节点与 3 个共谋恶意节点的曲线来看，两曲线差异不大，说明本文的安全定位算法对共谋攻击免疫。这是因为，在共谋恶意节点数目小于正常节点的情况下，算法中的第 3 步最优区域筛选结果是所有正常信标节点交叉的区域，所以对共谋攻击免疫。

### 5.2 实测实验

接下来，在 6 m×15 m 的室内实验室环境中，测试算法在恶意攻击背景下的定位精度。首先为确定该实验环境下，RSSI 标准差与测量距离的关系函数式参数，将两个 ZigBee 模块保持 15 dB 发射功率，多次改变两者的距离，每个位置上采集 1000 次 RSS 信号值，计算它们的标准差。对标准差取平方根，基于最小二乘法作其与距离之间的拟合曲线，得到拟合函数，如图 9 所示。

依据拟合函数，$a=1.21,\ b=6.21,\ d_0=4.54$，其余参数设置如表 2 所示。实验使用自主设计的 ZigBee 定位实验平台，其中部署了 10 个信标节点、1 个普通节点和 1 个协调器节点，协调器节点通过串口与实验机相连。每个节点都是基于 CC2530 芯片，信号发射功率设定为 15 dBm，路径衰减系数 $n=1.8$。

**表 2 实验参数设置**

| 参数 | 取值 |
|---|---|
| $P_0$ | 15 dBm |
| $n$ | 1.8 |
| $\mu$ | 30 |
| $G_1$ | 60 |
| $G_2$ | 80 |

图 10 是为不同恶意节点比例的情况下，不同算法的定位误差。由于本文算法利用了进化算法的迭代寻优能力，其定位误差与其余三者算法相比都较小。当恶意节点比例在 50%内时，除 LLS 算法外，其余算法均有较好的定位性能，定位误差没有出现强烈的波动。由于本文算法中设计的正常区域筛选算子是选择出全部为正常信标节点组成的区域，当恶意节点比例超过 50%时，算法分辨恶意节点构成的区域和正常信标节点构成的区域的能力减弱，所以定位误差逐渐变大。总体上来说，当定位区域内

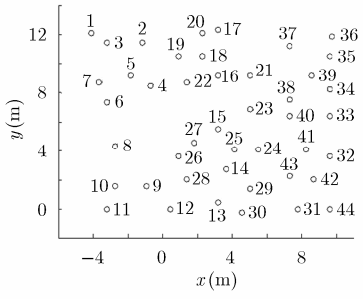


图 6 公开数据集节点分布图

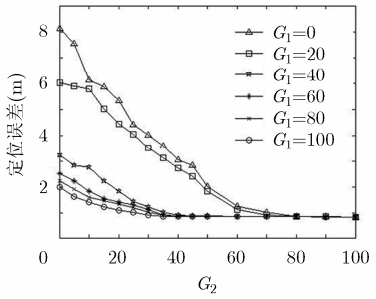


图 7 最大进化代数与定位误差关系图

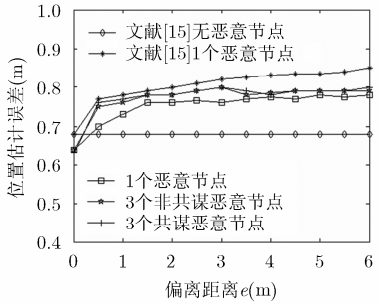


图 8 位置估计误差与偏离距离关系

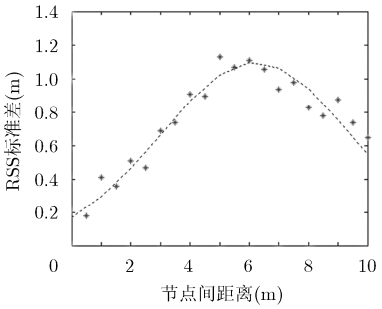


图 9 RSS 标准差与距离拟合曲线图

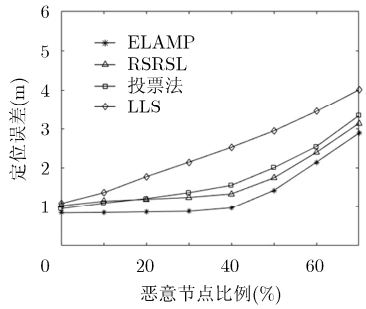


图 10 不同算法定位误差与恶意节点比例关系

正常信标节点的数目大于恶意节点的数目情况下，本文算法的定位误差基本趋于稳定，能够达到容忍恶意攻击的目的，并且有良好的定位精度。

## 6 结束语

本文针对恶意节点通过实施发送错误坐标、篡改信号发射功率等恶意攻击行为，破坏 ZigBee 节点正确定位的问题，提出一种基于进化思想的容忍恶意攻击安全定位算法。该算法将恶意节点过滤与位置估计结合起来，利用对数函数改进最大似然估计定位概率模型，并设计了新的进化算法 ELAMP 进行求解，提高了定位精度。理论分析表明 ELAMP 算法具有收敛性，并且时间复杂度比投票法、LLS 算法，RSRSL 算法都具有明显的优势。实验结果表明，本文算法在恶意节点比例不超过 50%的情况下能够实现安全定位，且具有较高的定位精度。

## 参 考 文 献

[1] KRISHNA K L, MADHURI J, and ANRADHA K. A ZigBee based energy efficient environmental monitoring alerting and controlling system[C]. IEEE International Conference on Information Communication and Embedded Systems, Chennai, India, 2016: 1–7. doi: 10.1109/ICICES.2016.7518849.

[2] SHALABY M, SHOKAIR M, and MESSIHA N W. Performance enhancement of TOA localized wireless sensor networks[J]. *Wireless Personal Communications*, 2017, 95(4): 4667–4679. doi: 10.1007/s11277-017-4112-8.

[3] MENG Wei, XIE Lihua, and XIAO Wendong. Optimal TDOA sensor-pair placement with uncertainty in source location[J]. *IEEE Transactions on Vehicular Technology*, 2016, 65(11): 9260–9271.

[4] TOMIC S, BEKO M, and RUI D. Distributed RSS-AoA based localization with unknown transmit powers[J]. *IEEE Wireless Communications Letters*, 2016, 5(4): 392–395.

[5] YIU S, DASHTI M, and CLAUSSEN H, *et al*. Wireless RSSI fingerprinting localization[J]. *Signal Processing*, 2017, 131: 235–244. doi: 10.1016/j.sigpro.2016.07.005.

[6] 叶阿勇, 许力, 林晖. 基于 RSSI 的传感器网络节点安全定位机制[J]. 通信学报, 2012, 33(7): 135–142.
YE Ayong, XU Li, and LIN Hui. Secure RSSI-based node positioning mechanism for wireless sensor networks[J]. *Journal on Communications*, 2012, 33(7): 135–142.

[7] ZEYTINCI M B, SARI V, HARMANCI F K, *et al*. Location estimation using RSS measurements with unknown path loss exponents[J]. *Eurasip Journal on Wireless Communications & Networking*, 2013, 12(1): 178–192. doi: 10.1186/1687-1499-2013-178.

[8] SO Hingcheung and LIN Lanxin. Linear least squares approach for accurate received signal strength based source localization[J]. *IEEE Transactions on Signal Processing*, 2011, 59(8): 4035–4040. doi: 10.1109/TSP.2011.2152400.

[9] WANG Chang, QI Fei, SHI Guangming, *et al*. A linear combination-based weighted least square approach for target localization with noisy range measurements[J]. *Signal Processing*, 2014, 94(1): 202–211. doi: 10.1016/j.sigpro.2013.06.005.

[10] 周牧, 蒲巧林, 田增山. 室内 WLAN 定位中位置指纹优化的接入点部署方法[J]. 通信学报, 2015, 36(s1): 30–41. doi: 10.11959/j.issn.1000-436x.2015279.
ZHOU Mu, PU Qiaolin, and TIAN Zengshan. Location fingerprint optimization based access point deployment in indoor WLAN localization[J]. *Journal on Communications*, 2015, 36(sl): 30–41. doi: 10.11959/j.issn.1000-436x.2015279.

[11] LI Zang, TRAPPE W, ZHANG Yanyong, *et al*. Robust statistical methods for securing wireless localization in sensor networks[C]. IEEE International Symposium on Information Processing in Sensor Networks, Los Angeles, USA, 2005: 12. doi: 10.1109/IPSN.2005.1440903.

[12] GARG R, VARNA A L, and WU M. An efficient gradient descent approach to secure localization in resource constrained wireless sensor networks[J]. *IEEE Transactions on Information Forensics & Security*, 2012, 7(2): 717–730. doi: 10.1109/TIFS.2012.2184094.

[13] 詹杰, 刘宏立, 刘大为, 等. 无线传感器网络中 DPC 安全定位算法研究[J]. 通信学报, 2011, 32(12): 8–17. doi: 10.3969/j.issn.1000-436X.2011.12.002.

ZHAN Jie, LIU Hongli, LIU Dawei, *et al.* Research on secure DPC localization algorithm of WSN[J]. *Journal on Communications*, 2011, 32(12): 8–17. doi: 10.3969/j.issn.1000-436X.2011.12.002.

[14] NIRMALA M B and MANMJUNATHA A S. Enhanced voting based secure localization for wireless sensor networks [J]. *International Journal of Computer Network and Information Security*, 2015, 7(12): 52–59. doi: 10.5815/ijcnis.2015.12.06.

[15] 徐琨, 刘宏立, 詹杰, 等. 容忍恶意攻击的无线传感网络安全定位算法[J]. 通信学报, 2016, 37(12): 95–102. doi: 10.11959/j.issn.1000-436x.2016276.

XU Kun, LIU Hongli, ZHAN Jie, *et al.* Malicious attack-resistant secure localization algorithm for wireless sensor network[J]. *Journal on Communications*, 2016, 37(12): 95–102. doi: 10.11959/j.issn.1000-436x.2016276.

[16] 叶苗, 王宇平. 基于变方差概率模型和进化计算的 WSN 定位算法[J]. 软件学报, 2013, 24(4): 859–872. doi: 10.3724/SP.J.1001.2013.04255.

YE Miao and WANG Yuping. Location estimation in wireless networks based on probabilistic model with variant variance and evolutionary algorithm[J]. *Journal of Software,* 2013, 24(4): 859–872. doi: 10.3724/SP.J.1001.2013.04255.

[17] CHANG C H and LIAO W. A probabilistic model for relative location estimation in wireless sensor networks[J]. *IEEE Communications Letters*, 2009, 13(12): 893–895.

[18] JOHN Galletly. Evolutionary algorithms in theory and practice[J]. *Complexity*, 1996, 2(8): 26–27.

[19] RUDOLPH G. Finite Markov chain results in evolutionary computation: A tour d'horizon[J]. *Fundamenta Informaticae*, 1998, 35(1/4): 67–89.

[20] PATWARI N. Wreless sensor network oalization measurement repository[OL]. http://www.eecs.umich.edu/~hero/Localize/, 2006.

郁　滨： 男，1964 年生，教授，博士生导师，研究方向为无线网络安全和视觉密码.

刘子清： 男，1993 年生，硕士生，研究方向为 ZigBee 和信息安全技术.