基于约束总体最小二乘的泰勒级数定位算法

陆剑锋[1] 谢胜东[2]

[1](泰州职业技术学院信息技术学院 江苏 泰州 225300)

[2](南京信息工程大学计算机与软件学院 江苏 南京 210044)

摘 要 目前基于到达时间差(Time Difference of Arrival,TDOA)的无线定位算法既不能在基于距离平方差(Squared Range-Difference,SRD)的误差平方和最小模型中获得总体最小二乘准则下的全局最优解,也不能在基于距离差(Range-Difference,RD)的误差平方和最小模型中获得普通最小二乘准则下的全局最优解。将泰勒级数法与约束总体最小二乘法(Constraint Total Least Square,CTLS)相结合,提出一种基于约束总体最小二乘的泰勒级数定位算法(CTLS-Taylor)。利用 CTLS 方法获得目标节点的粗估计位置,并将该位置作为泰勒级数展开法的初始点,通过迭代,获得目标节点的精估计位置。仿真结果表明,CTLS-Taylor 算法不仅能够获得与 QCLS-Taylor 算法相同的定位精度,而且迭代次数有了明显减少;同时与 CTLS 定位算法相比,当测量噪声较高时,CTLS-Taylor 算法的定位精度更高。

关键词 无线定位 泰勒级数 约束总体最小二乘准则 到达时间差

中图分类号 TP393 **文献标识码** A DOI: 10.3969/j.issn.1000-386x.2019.12.041

TAYLOR SERIES LOCATION ALGORITHM BASED ON CONSTRAINED TOTAL LEAST SQUARES CRITERION

Lu Jianfeng[1] Xie Shengdong[2]

[1](*Institute of Information Technology, Taizhou Polytechnic College, Taizhou 225300, Jiangsu, China*)

[2](*Computer and Software Institute, Nanjing University of Information Science and Technology, Nanjing 210044, Jiangsu, China*)

Abstract At present, the wireless location algorithm based on the time difference of arrival(TDOA) can neither obtain the global optimal solution under the global least squares criterion in the least squares error sum model based on SRD(Squared Range-Difference), nor obtain the global optimal solution under the ordinary least squares criterion in the least squares error sum model based on RD(Range-Difference). Combining the Taylor series with the Constraint Total Least Square(CTLS), we propose a Taylor series localization algorithm based on CTLS, which is called CTLS-Taylor. We used CTLS to obtain a coarse estimated coordinate of the target node, and took the coordinate value as the initial point of Taylor series method. Through iteration, the refined coordinate of the target node could be obtained. The simulation results show that CTLS-Taylor can obtain the same positioning accuracy as QCLS-Taylor, and the number of iterations can be significantly reduced. Compared with CTLS, CTLS-Taylor can achieve higher positioning accuracy when the measurement noise is higher.

Keywords Wireless location Taylor series Constrained total least squares criterion Time difference of arrival

0 引 言

无线定位是指利用无线信号的物理参数估计目标节点在某一坐标系统中的位置,最初是为了满足航海导航以及精确制导等方面要求,其典型代表为 20 世纪 70 年代的全球定位系统(GPS)。自 1996 年美国联邦通信委员会要求无线蜂窝系统必须能够对发出紧急呼

收稿日期:2019-02-11。江苏省自然科学基金项目(BK20160955)。陆剑锋,副教授,主研领域:信息安全,信号处理。谢胜东,副教授。

叫的移动用户实现准确定位后,无线定位便引起了众多学者的广泛关注[1]。目前,无线定位除了应用于蜂窝网络中的紧急呼叫外,还可以用于智能交通、数字城市以及现代化农业、医疗等领域中,以实现目标跟踪、资源调度和导航等为目的,因此具有广泛的应用范围。

根据物理量的不同,现有定位算法可以分为基于信号强度(Received Signal Strength,RSS)的定位[2]、基于信号到达时间(Time of Arrival,TOA)的定位[3]、基于信号到达时间差(Time Difference of Arrival,TDOA)的定位[4]以及基于信号到达角度(Angle of Arrival,AOA)的定位[5]四种基本类型。由于 RSS 定位精度低、AOA 实现复杂以及 TOA 需要目标节点与源节点之间时间同步[6],在无线定位系统中,现阶段使用最为广泛的就是 TDOA 算法。例如,在 GSM 和 LTE 系统中,均采用该类算法进行位置估计。

目前关于如何提高 TDOA 算法定位精度的研究主要可以分为三大类:(1) 最小二乘类定位算法。这类算法基于目标节点到达不同锚节点距离平方之差的误差 2-范数最小原则,将位置估计描述为一个空间的向量仿射变换问题,基于普通最小二乘(Least Square,LS)准则,使用拉格朗日算子法[7]、广义信任域法[8]或半正定规划法[9]即可求得该准则下的全局最优解。然而,使用 LS 准则求解原问题本身就是存在偏差[10],因此,上述全局最优解未必是原问题的全局最优解。(2) 凸规划类定位算法[11]。这类算法基于目标节点到达不同锚节点距离之差的误差 2-范数最小原则,将估计量的最优值表示成求解一个非凸非线性函数的最小值问题,进而通过松弛技术,将原问题转化成一个非线性凸函数最小化问题,以该问题的最优解作为目标节点坐标的最优估计值。然而,原问题与转换后的问题之间并不等价,因此,转换后问题的最优值未必是原问题的最优值。(3) 泰勒级数类定位算法[12]。与第二类算法的准则相同,这类算法也是基于目标节点到达不同锚节点距离之差的误差 2-范数最小原则,将估计量的最优值描述成求解一个非线性最小二乘函数的最小值问题,进而使用泰勒级数展开法,将到达时间差函数用某个初始坐标点的一阶泰勒级数近似,实现了非线性最小二乘函数到线性最小二乘函数的转变。在获得修正步长的最小二乘解后,更新原初始坐标点。如此不断迭代,从而逐渐逼近真实坐标点。由于忽略了泰勒级数的高次项,因此迭代解未必是原始非线性最小二乘问题的最优解。很显然,上述三类算法均无法获得各自所对应的原始问题的全局最优解。

本文主要研究第三类,即泰勒级数类定位算法。对于该类算法,初始坐标点的选择是一个重要环节,它直接决定了此类算法的性能。现有算法中,常见的初始点选择方法主要包括最小二乘法[4]、最速下降法[13]、残差加权法[14]以及二阶锥松弛法[15]等。事实上,几乎所有最小二乘类和凸规划类定位算法所获得的位置估计值均可以作为泰勒级数类算法的初始坐标点,区别主要在于算法的收敛性、迭代次数以及估计精度的不同。当初始坐标点与实际位置值越接近时,算法的收敛性越能得到保障,迭代次数也将越少,定位精度也将越高。

由于总体最小二乘(Total Least Square,TLS)准则弥补了 LS 准则不能解决观测矩阵的元素中误差的影响,且基于 TLS 准则的约束总体最小二乘定位算法[10]能够取得较好的定位精度,因此,本文提出了一种基于约束总体最小二乘的泰勒级数定位算法(CTLS-Taylor)。该算法首先使用 CTLS 方法获得目标节点位置的粗估计坐标值,接着基于泰勒级数展开法,通过迭代过程,对粗估计坐标值不断进行改善,从而得到目标节点位置的精估计坐标值。仿真结果表明,CTLS-Taylor 算法不仅能够获得与 QCLS-Taylor 算法[4]相同的定位精度,而且迭代次数有了明显减少;同时与 CTLS 定位算法相比,当测量噪声较高时,CTLS-Taylor 算法的定位精度更高。

1　定位模型

考虑到二维坐标系统中的定位算法经简单扩展后便可适用于三维坐标系统,因此本文以二维坐标系统为研究环境。假设在二维坐标系统中,存在某个位置未知的目标节点,其坐标记为(x,y),同时还存在 N 个不在同一条直线上位置已知的普通锚节点,它们的坐标分别记为(x_i,y_i),$i=1,2,\cdots,N$,以及一个位于坐标系统原点的参考锚节点。

我们可以使用时延估计法[16]获得电磁波或声波从目标节点到达普通锚节点 i 与参考锚节点之间的时间差 t_{i0},然后乘以它们的传播速度,即可获得目标节点到达两节点之间的距离差 d_{i0}。由此可见,TDOA 定位算法可以看成是基于距离差的定位算法。因此,在本文中,我们将以距离差来代替时间差。

目标节点到达普通锚节点 i 与参考锚节点距离差的真实值 $f_{i0}(x,y)$ 可分别表示为:

$$f_{i0}(x,y)=\sqrt{(x-x_i)^2+(y-y_i)^2}-\sqrt{x^2+y^2}\quad(1)$$
$$i=1,2,\cdots,N$$

由于我们事先并不知道目标节点的坐标值,因此不能通过式(1)来计算距离差,而只能通过测量得到

距离差 d_{i0}的值:

$$d_{i0}=f_{i0}(x,y)+n_{i0}\quad i=1,2,\cdots,N \tag{2}$$

式中: n_{i0}为测量误差,我们假设它们之间独立同分布。

采用测量误差平方和最小化准则,根据式(2),可以得到目标节点位置的坐标估计量的最优估计值 $(\hat{x},\hat{y})$ 的表达式为:

$$(\hat{x},\hat{y})=\min_{(x,y)}\sum_{i=1}^{N}(f_{i0}-d_{i0})^2=\min_{(x,y)}\left\|\begin{matrix}d_{10}-\sqrt{(x-x_1)^2+(y-y_1)^2}+\sqrt{x^2+y^2}\\ d_{20}-\sqrt{(x-x_2)^2+(y-y_2)^2}+\sqrt{x^2+y^2}\\ \vdots\\ d_{N0}-\sqrt{(x-x_N)^2+(y-y_N)^2}+\sqrt{x^2+y^2}\end{matrix}\right\|_2^2 \tag{3}$$

式中: $\|\cdot\|_2$表示向量的 2-范数。

式(3)是求解一个非线性最小二乘函数的最小值问题,这类问题因存在多个极值点,故一般不存在或难以求得其全局最优解,而只能通过某种优化算法,如牛顿法、最速下降法等方法获得它的局部最优解。

2 定位算法

如果能够求得式(3)的全局最优解,那么该解即可作为节点的位置坐标最优估计值,但如前所述,函数的非凸性使其成为一件较为困难的事情,牛顿法、最速下降法等搜索算法只能获得函数的局部最优解。如果我们可以对非凸函数进行线性近似,那么就能获得近似后函数的全局最优解,尽管其未必是原函数的全局最优解,但其性能可能会优于原函数的局部最优解。一方面,泰勒级数分解使得这种线性近似成为可能,另一方面,CTLS 算法利用了牛顿法获得了 SDR 模型中的局部最优解。因此,我们将这两种方法结合,提出一种基于完全约束最小二乘的泰勒级数定位算法(CTLS-Taylor),以期望能够获得更好的定位效果。CTLS-Taylor 包含两个方面的内容:(1) 泰勒级数的线性近似原理;(2) 利用 CTLS 算法进行目标节点位置坐标初始点的选择。

2.1 泰勒级数线性近似原理

设存在某个初始点 (x_0^o,y_0^o),那么 $f_{i0}(x,y)$ 的一阶泰勒级数展开表达式为:

$$f_{i0}(x,y)\approx f_{i0}(x_0^o,y_0^o)+\alpha_i(x-x_0^o)+\beta_i(y-y_0^o) \tag{4}$$

式中: $\alpha_i=\left.\frac{\partial f_{i0}(x,y)}{\partial x}\right|_{x=x_0^o}$; $\beta_i=\left.\frac{\partial f_{i0}(x,y)}{\partial y}\right|_{y=y_0^o}$。对于某一确定坐标点 (x_0^o,y_0^o),α_i、β_i以及 $f_{i0}(x_0^o,y_0^o)$ 的取值均可以通过计算获得。尽管泰勒级数展开无需考虑确定坐标点 (x_0^o,y_0^o) 的选择,但由于式(4)忽略了高次项,因此只有当 (x,y) 与 (x_0^o,y_0^o) 较为接近时,才能取得较好的近似效果。本文中,(x,y) 为目标节点的位置坐标值,在进行确定坐标点选择时,应让其尽可能地接近目标节点的实际位置。

令 $\Delta x=(x-x_0^o)$ 以及 $\Delta y=(y-y_0^o)$,并将式(4)代入式(3),可以得到:

$$(\hat{x},\hat{y})\approx\min_{(x,y)}\left\|\begin{matrix}d_{10}-f_{10}(x_0^o,y_0^o)-\alpha_1\Delta x-\beta_1\Delta y\\ d_{20}-f_{20}(x_0^o,y_0^o)-\alpha_2\Delta x-\beta_2\Delta y\\ \vdots\\ d_{N0}-f_{N0}(x_0^o,y_0^o)-\alpha_N\Delta x-\beta_N\Delta y\end{matrix}\right\|_2^2 \tag{5}$$

式(5)等价于求解如下线性方程式在普通最小二乘准则下的最优解:

$$\boldsymbol{AX}=\boldsymbol{b} \tag{6}$$

式中: 矩阵 $\boldsymbol{A}=\begin{bmatrix}\alpha_1&\beta_1\\ \alpha_2&\beta_2\\ \vdots&\vdots\\ \alpha_N&\beta_N\end{bmatrix}$; $\boldsymbol{X}=\begin{bmatrix}\Delta x\\ \Delta y\end{bmatrix}$; $\boldsymbol{b}=\begin{bmatrix}d_{10}-f_{10}(x_0^o,y_0^o)\\ d_{20}-f_{20}(x_0^o,y_0^o)\\ \vdots\\ d_{N0}-f_{N0}(x_0^o,y_0^o)\end{bmatrix}$。

在测量噪声 n_i之间独立且服从同一分布的情况下,$\boldsymbol{X}$ 的最优解为 $(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{b}$。

由于忽略了泰勒级数的高次项,利用 X 的最优解,结合 (x_0^o,y_0^o),可以得到一个新的坐标点 (x_0^n,y_0^n)。尽管该坐标点是式(5)的最优解,但未必是式(3)的最优解。然而只要 (x_0^n,y_0^n) 更加接近式(3)的最优解,我们就可以将 (x_0^n,y_0^n) 作为新的确定点,再次利用泰勒级数展开法进行函数线性近似,如此迭代循环,可以使式(5)的最优解不断逼近式(3)的最优解。上述过程的正常执行依赖于迭代过程的收敛性。文献[12]指出,选择合适的初始点 (x_0^o,y_0^o),让其接近真实值,则能够保证迭代过程的收敛。因此,对于基于泰勒级数展开法的目标定位,初始点的选择就显得尤为重要,这也是目前此类算法研究的重点。

2.2 初始点的选择

很显然,初始点越接近式(3)的最优解,则不仅能够保证迭代过程的收敛,而且能够减少迭代的次数,提高位置估计的速度。考虑到最小二乘类定位算法中的 CTLS 算法[10]能够获得较高的位置估计精度,本文采用 CTLS 算法来获取目标节点的初始位置。

基于目标节点到达普通锚节点与参考锚节点的距离平方值之差的误差平方和最小原则,目标节点的坐标可以通过下式进行描述:

$$\boldsymbol{A\theta}=\boldsymbol{b} \tag{7}$$

式中: 矩阵 $\boldsymbol{A}=\begin{bmatrix} x_1 & y_1 & d_{10} \\ x_2 & y_2 & d_{20} \\ \vdots & \vdots & \vdots \\ x_N & y_N & d_{N0} \end{bmatrix}$; $\boldsymbol{\theta}=\begin{bmatrix} x \\ y \\ d_0 \end{bmatrix}$; $\boldsymbol{b}=\frac{1}{2}\begin{bmatrix} x_1^2+y_1^2-d_{10}^2 \\ x_2^2+y_2^2-d_{20}^2 \\ \vdots \\ x_N^2+y_N^2-d_{N0}^2 \end{bmatrix}$;

d_0 为目标节点到达参考锚节点的距离。

对于式(7),我们可以求得它在普通最小二乘准则下的最优值[7]。但该准则是建立在矩阵 $\boldsymbol{A}$ 中所有元素均不存在误差的基础上,而事实上,$\boldsymbol{A}$ 中最后一列的所有元素均为测量所得,必然存在着测量误差,因此采用普通最小二乘准则获得的最优值显然是不准确的。此时,可以采用总体最小二乘准则[17],它不仅考虑了向量 $\boldsymbol{b}$ 中的误差,同样考虑到了矩阵 $\boldsymbol{A}$ 中元素的误差,其目的是在最小化所有误差平方和的情况下,使得式(7)有唯一确定解。于是在该准则下,式(7)的最优值 $\boldsymbol{\theta}$ 等价于式(8)的最优解:

$$\min_{\theta,n} \|n\|^2 \quad \text{s.t.} \quad \boldsymbol{A\theta}-\boldsymbol{b}=\boldsymbol{G}n \tag{8}$$

式中:

$$\boldsymbol{G}=d_0\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}_{N\times N}+\begin{bmatrix} d_{10} & 0 & \cdots & 0 \\ 0 & d_{20} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & d_{N0} \end{bmatrix}_{N\times N}$$

利用牛顿迭代法,我们可以很容易地求得式(8)的一个局部最优解 $\boldsymbol{\theta}$,并将其中的 x 和 y 作为目标节点位置坐标的粗估计值。

2.3　CTLS-Taylor 算法

这里,我们给出 CTLS-Taylor 算法的完整过程:

Step 1　利用 sCTLS 算法获得目标节点的一个位置估计值 $\begin{bmatrix} x_0^o \\ y_0^o \end{bmatrix}$。

Step 2　将 $\begin{bmatrix} x_0^o \\ y_0^o \end{bmatrix}$ 作为初始点,利用泰勒级数近似法,获得 $\begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix}$,并令 $\begin{bmatrix} x_0^n \\ x_0^n \end{bmatrix}=\begin{bmatrix} x_0^o \\ y_0^o \end{bmatrix}+\begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix}$。

Step 3　如果 $\left\|\begin{matrix} \Delta x \\ \Delta y \end{matrix}\right\|_2 \geqslant \varepsilon$,则用 $\begin{bmatrix} x_0^n \\ x_0^n \end{bmatrix}$ 来代替 $\begin{bmatrix} x_0^o \\ y_0^o \end{bmatrix}$,跳转到 Step 2,否则用 $\begin{bmatrix} x_0^n \\ x_0^n \end{bmatrix}$ 作为最终的目标节点位置坐标的估计值。其中 ε 为一个事先确定好的较小值。

3　仿真分析

本文的仿真环境为 MATLAB 7.0,仿真参数来自文献[18]: 在一个 100 m×100 m 的 2 维坐标系统中,存在一个实际坐标(42,12) m 的目标节点,同时存在 9 个普通锚节点,它们的坐标依次为(16,42) m、(34,52) m、(58,30) m、(78,18) m、(66,48) m、(30,-12) m、(22,12) m、(57,-3) m、(12,-28) m,另外还存在一个参考锚节点,其坐标为(0,0) m。TDOA 的测量噪声服从均值为 0,方差为 δ^2 的高斯分布。为了评价 CTLS-Taylor 算法的性能,将其与 CTLS 算法、QCLS 算法以及 QCLS-Taylor 算法[4]进行比较,并从定位误差和泰勒级数迭代次数两个角度进行衡量。本文中定位误差 e 的计算公式为:

$$e=\sqrt{\frac{\sum_{i=1}^{N}\left((\hat{x}_i-42)^2+(\hat{y}_i-12)^2\right)}{N}} \tag{9}$$

式中: N 为仿真次数。

图 1 和图 2 为普通锚节点数目分别为 5 个和 9 个时,不同算法的定位误差。可以看出: (1) 随着测量噪声方差的增加以及普通锚节点数目的增多,泰勒级数类算法的定位误差要优于非泰勒级数类算法,这表明使用泰勒级数法有助于提高定位精度。(2) 本文的 CTLS-Taylor 算法与 QCLS-Taylor 算法的定位误差几乎相等,不受测量噪声与普通锚节点数目的影响。这意味着单纯从定位误差的角度看,本文算法与 QCLS-Taylor 算法的性能相当。(3) CTLS 算法的定位误差要优于 QCLS 算法,这是因为 CTLS 算法是基于总体最小二乘准则,而 QCLS 算法是基于普通最小二乘准则的原因。

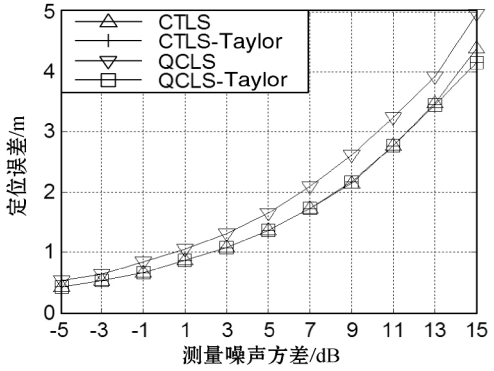

图 1　普通锚节点数目 5 个的定位误差

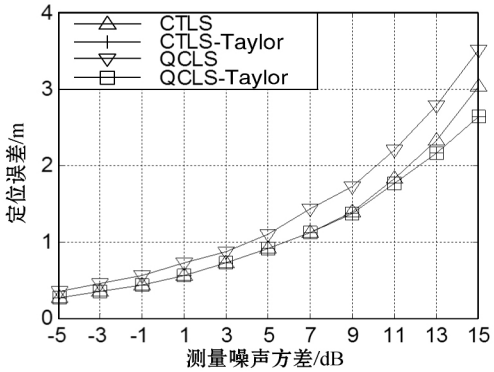

图 2　普通锚节点数目 9 个的定位误差

图 3 与图 4 为普通锚节点数目分别为 5 个和 9 个时，两种泰勒级数类算法所需要的迭代次数。可以看出：(1) 当测量方差较低时，尤其是当信噪比低于 -1 dB 时，CTLS-Taylor 算法几乎只要迭代一次即可，且与普通锚节点的数目无关，而 QCLS-Taylor 算法的平均迭代次数均大于 1.5 次，这与 CTLS-Taylor 算法的初始点更为接近真实坐标点有关。(2) 当测量方差逐渐增大时，两个泰勒级数算法的迭代次数均出现不同程度的增加，但 CTLS-Taylor 算法的迭代次数始终小于 QCLS-Taylor 算法。

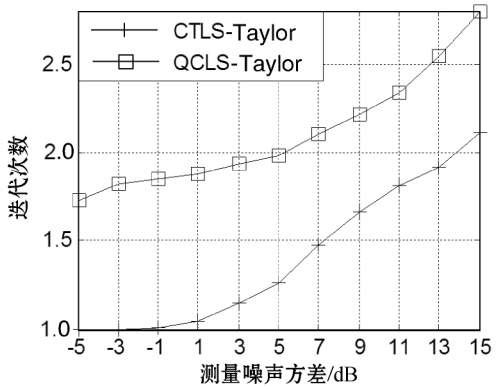

图 3 普通锚节点数目 5 个的迭代次数

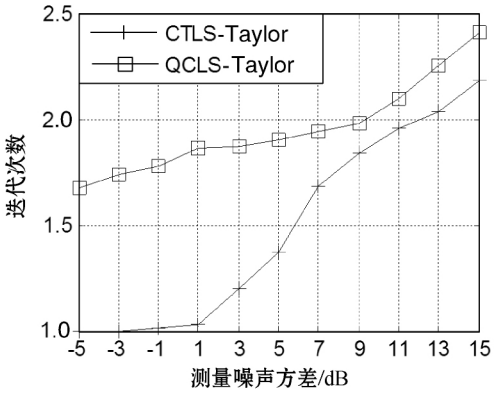

图 4 普通锚节点数目 9 个的迭代次数

上述结果表明，尽管从定位误差的角度看，CTLS-Taylor 算法的性能与 QCLS-Taylor 算法相当，但前者的迭代次数却小于后者，也就意味着前者的定位速度优于后者。

4 结 语

本文将泰勒级数法与 CTLS 算法相结合，提出了一种基于约束总体最小二乘的泰勒级数定位算法。该算法利用 CTLS 方法获得目标节点坐标位置的粗估计值，并将该值作为泰勒级数展开法的初始点，通过迭代，从而获得目标节点位置坐标的精估计值。仿真结果表明，CTLS-Taylor 算法不仅能够获得与 QCLS-Taylor 算法相同的定位精度，而且迭代次数有了明显减少；同时与 CTLS 算法相比，当测量噪声较高时，CTLS-Taylor 算法的定位精度更高。

参 考 文 献

[1] 孙宝山，刘晟源，刘骁骁. 基于 HDV-HOP 的无线传感器网络大型室内定位算法研究[J]. 计算机应用与软件，2018，35(3)：114－119，186.

[2] Wang Z，Zhang H，Lu T，et al. A grid based localization algorithm for wireless sensor networks using connectivity and RSS rank[J]. IEEE Access，2018，6(2)：8426－8439.

[3] Takayuki A，Masanori S，Hiromichi H. Time of arrival based smartphone localization using visible light communication[C]//2017 International Conference on Indoor Positioning and Indoor Navigation(IPIN)，2017：1－7.

[4] 熊瑾煜，王巍，朱中梁. 基于泰勒级数展开的蜂窝 TDOA 定位算法[J]. 通信学报，2004，25(4)：144－150.

[5] Zheng Y，Sheng M，Liu J Y，et al. Exploiting AoA estimation accuracy for indoor localization：A weighted AoA-based approach[J]. IEEE Wireless Communications Letters，2019，8(1)：65－68.

[6] 庞泳，李盛，巩庆超. 无线传感网时间同步技术综述[J]. 计算机应用与软件，2016，33(12)：1－5.

[7] Huang Y. T，Jacob B，Gary W. E，et al. Real time passive source localization：A practical linear correction least squares approach[J]. IEEE Transactions on Speech and Audio Processing，2001，9(8)：943－955.

[8] Amir B，Petre S，Li J. Exact and approximate solutions of source localization problems[J]. IEEE Transactions on Signal Processing，2008，56(5)：1770－1777.

[9] Heidari V，Sadeghi K，Pezeshk A M，et al. Exact solutions of time difference of arrival source localisation based on semi-definite programming and Lagrange multiplier：complexity and performance analysis[J]. IET Signal Processing，2014，8(8)：868－877.

[10] Yang K，An J. P，Bu X Y，et al. Constrained total least squares location algorithm using time difference of arrival measurements[J]. IEEE Transactions on Vehicular Technology，2010，59(3)：1558－1562.

[11] Zou Y B，Wan Q，Liu H P. Semidefinite programming for TDOA localization with locally synchronized anchor nodes[C]//2018 IEEE International Conference on Acoustics，Speech and Signal Processing(ICASSP)，2018：3524－2528.

[12] Wade H F. Position location solutions by taylor series estimation[J]. IEEE Transactions on Aerospace and Electronic Systems，1976，12(2)：187－193.

[13] 张令文，谈振辉. 基于泰勒级数展开的蜂窝 TDOA 定位新算法[J]. 通信学报，2007，28(6)：7－11.

(下转第 272 页)

单标签密钥生成算法中，标签一端在计算 $M1$ 的过程中，第一次进行“异或运算”。在步骤四中，计算 $M2 \oplus ID\_S\_L$ 与 $M3 \oplus ID$ 时，会进行第二次及第三次“异或运算”。同时计算共享密钥 KEY 时，涉及到 2 次的“与运算”。基于上述，标签端的计算量包含以下：3 次“异或运算”、2 次“与运算”，即 3ph + 2pm。

整个通信过程中，涉及到的传输消息有 $M1$、$M2$、$M3$，因此算法的通信量为 3pn。

标签一端需要存放如下信息：标签的标识符 ID、标签的假名标识符 ID_S，因此标签一端的存储空间为 2pn。

通过上面的分析可以得出：算法采用位运算进行加密，使得标签一端的计算量较低，能够满足标签低计算量的要求。产生随机数的操作放在读写器一端进行，使得标签一端不再产生随机数，从而可以减少实现功能的总的门电路数量，达到降低标签成本的目标。因此，本文算法具有低计算量、低成本的优势，且满足系统所需的安全需求。

4 结 语

为解决通信实体之间认证所需的共享密钥不再事前设定好问题，本文给出一种通过无线方式动态生成共享密钥的算法。结合实际应用环境，给出适用于三种不同环境下的算法，使得所提算法具备广泛的应用范围。算法采用简单的“异或运算”、“与运算”对传输信息进行加密，一来可以不用明文直接传输，攻击者难以攻击；二来标签端的计算量较小，使算法适用于受限的低成本标签中。分析了算法安全性，表明其能够抵抗攻击者发起的常见的攻击方式，满足系统所需的安全要求。分析了算法性能，表明其对标签的计算量、标签的存储空间要求并不高，适用于低成本的受限制的标签中。结合基于 BAN 逻辑对算法进行形式化证明，分析了算法的正确性及可行性。

参 考 文 献

[1] Liu Z H, Fan Y Q. Provably secure searchable attribute-based authenticated encryption scheme [J]. International Journal of Network Security, 2019, 21(2): 177 - 190.

[2] 刘道微，凌捷. 一种改进的满足后向隐私的 RFID 认证协议 [J]. 计算机科学，2016，43(8)：128 - 130，158.

[3] Li C, Liu Z H. A secure privacy-preserving cloud auditing scheme with data deduplication [J]. International Journal of Network Security, 2019, 21(2): 199 - 210.

[4] Zhang X Q, Wang B P, Zhang W P. A robust authentication protocol for multi-server architecture using elliptic curve cryptography [J]. International Journal of Network Security, 2019, 21(2): 191 - 198.

[5] Gope P, Lee J, Quek T. Resilience of DoS attack in designing anonymous user authentication protocol for wireless sensor networks [J]. IEEE Sensors Journal, 2017, 17(2): 498 - 503.

[6] Liu H J, Chen Y H, Tian H, et al. A security and efficient data aggregation scheme for cloud-assisted wireless body area network [J]. International Journal of Network Security, 2019, 21(2): 243 - 249.

[7] Thokchom S, Saikia D K. Privacy Preserving and public auditable integrity checking on dynamic cloud data [J]. International Journal of Network Security, 2019, 21(2): 221 - 229.

[8] 鲁力. RFID 系统密钥无线生成 [J]. 计算机学报，2015，38(4)：822 - 832.

[9] 张朝晖，刘悦，刘道微. 基于标签 ID 的 RFID 系统密钥无线生成算法 [J]. 计算机应用研究，2017，34(1)：261 - 263.

[10] 黄琪，凌捷，何晓桃. 一种改进的基于标签部分 ID 的 RFID 密钥无线生成算法 [J]. 计算机科学，2017，44(1)：172 - 175.

[11] Liu Y J, Chang C C. A cloud-assisted passenger authentication scheme for Japan rail pass based on image morphing [J]. International Journal of Network Security, 2019, 21(2): 211 - 220.

[12] 朱宏峰，刘天华. 隐私保护安全协议研究 [M]. 科学出版社，2015.

(上接第 260 页)

[14] 周康磊，毛永毅. 基于残差加权的 Taylor 级数展开 TDOA 无线定位算法 [J]. 西安邮电学院学报，2010，15(3)：10 - 13.

[15] 陆文博，刘春生，周青松，等. 改进二阶锥松弛和泰勒级数展开在 TDOA 无源定位中的应用 [J]. 信号处理，2014，30(10)：1234 - 240.

[16] Hoda S H, Hassan R. Global time delay estimation in ultrasound elastography [J]. IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control, 2017, 64(10): 1625 - 1634.

[17] Sreedevi G, Manish B, Sandeep K. K, et al. Modeling errors compensation with total least squares for limited data photo acoustic tomography [J]. IEEE Journal of Selected Topics in Quantum Electronics, 2019, 25(1): 1 - 14.

[18] 谢胜东，胡爱群，黄毅. 基于达到时间差的两步最小二乘定位算法 [J]. 东南大学学报(自然科学版)，2013，43(6)：1157 - 1161.