文章编号: 1673- 9469(2011) 02- 0060- 04

基于信息分组的TDOA 安全定位算法

吴开兴, 张荣华
(河北工程大学 信息与电气工程学院, 河北 邯郸 056038)

摘要: 将信息分组的方法应用于定位过程中, 以方差的无偏估计是否符合误差假设作为定位参照集选取依据, 提出一种能抵抗轻量级攻击的 AR- TDOA 定位算法。将该算法与基于 TDOA 测距的定位算法和 SeRLoc 安全定位算法在定位误差、计算开销与稳定性方面进行比较。结果表明, 相同攻击强度下三者定位误差大小顺序依次为 TDOA> SeRLoc> AR- TDOA。虚假锚节点数量越大, 基于 TDOA 测距和 SeRLoc 的定位误差也越大, 而基于 AR- TDOA 算法的定位误差则能保持在较小程度内。因此在增加少量计算复杂度的情况下, AR- TDOA 算法能够改善定位的稳定性。

关键词: 信息分组; TDOA; 安全定位; WSN
中图分类号: TP309 文献标识码: A

TDOA secure localization algorithm basing on grouping information

WU Kai-xing, ZHANG Rong-hua
(College of Information and Electronic Engineering, Hebei University of Engineering, Hebei Handan 056038, China)

Abstract: The attack resistant- time difference of arrival (AR- TDOA) was put forward by using grouping information method in the positioning process, with the selection standard of positioning reference that the unbiased estimation variance according to the error assumption. By comparing the TDOA localization algorithm with the SeRLoc safety localization algorithm on positioning error, computing cost and stability, the results show that the sequence of their positioning error is TDOA> SeRLoc> AR- TDOA under the same attack strength. The greater the number of anchor node is, the larger positioning errors of both TDOA localization algorithm and SeRLoc safety localization algorithm are, while the AR- TDOA algorithm could keep the positioning error within a smaller range. Accordingly the AR- TDOA algorithm can improve the stability of positioning with a little increase in computing complexity.

Key words: grouping information; TDOA; secure localization; WSN

无线传感器网络(wireless sensor network, WSN) 是一种新型的低功耗、自组织、短距离的无线传输网络, 可以实时监测网络分布区域内各种监测对象的状态信息。在 WSN 的各种应用中, 大多数需要确定事件发生的位置, 或者需要对目标进行跟踪。随着 WSN 应用研究的不断深入, 对定位技术提出了更高需求。其中, 安全定位已经与定位精度和能耗一起成为 WSN 中评价定位算法性能的三个主要标准之一。安全定位技术是 WSN 节点定位的关键技术, 是定位过程有效性的重要保障[1]。

现有针对基于 TDOA 测距提出的安全定位算法, 或者依赖于节点的密度[2], 或者计算复杂性过高[3], 或者只针对某种特定的攻击[4], 具有局限性。由于 WSN 受到的攻击种类可能多种多样, 不可能对每种可能出现的特定攻击行为采取一一防范的措施[5]。本文将针对基于 TDOA 测距的定位提出一种抵抗轻量级攻击的定位算法 AR- TDOA (Attack Resistant- Time Difference Of Arrival), 采用

收稿日期: 2011- 04- 22
作者简介: 吴开兴(1962-) 男, 陕西澄城人, 教授, 从事自动化、计算机教学与研究工作。

信息分组方法隔离可疑数据, 目的是在存在攻击的情况下, 保证节点的可靠定位, 属于被动式的安全定位思想。

1 AR- TDOA 算法

节点定位过程中, 为了提供初始的定位参照, 需要在初始化阶段预先部署一定比例的锚节点(beacon node), 锚节点可通过GPS 或预设等方式实现定位, 配有大功率无线发射设备, 向未知节点发送包含位置信息的信标报文。

1.1 TDOA 测距原理

TDOA 是一种适用性较强的定位算法, 通过记录信号的到达时间差来测量距离, 降低了对时间同步的要求, 测距精度可达到厘米级, 被广泛应用于WSN 定位系统。

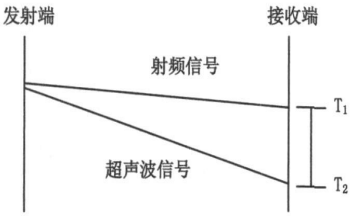

图1 TDOA测距原理

Fig. 1 Principle of TDOA

TDOA 测距原理如图 1 所示, 发射节点同时发射无线射频信号和超声波信号, 接收节点记录两种信号到达的时间 T_1、T_2, 已知无线射频信号和超声波的传播速度分别为 c_1、c_2, 那么两点之间的距离为

$$d = (T_2 - T_1) \times \frac{c_1 \times c_2}{c_1 - c_2} \tag{1}$$

1.2 坐标计算

本文计算坐标采用的是多边测量法的极大似然估计法。此方法在测距存在一定误差的情况下仍然能够达到相当高的定位精度。在进行坐标求解时, 采用多边测量法(multilateration), 它是三边测量法的变形, 如图 2 所示。

即有 $n(n > 3)$ 个参考节点 $P_1(x_1, y_1)$, $P_2(x_2, y_2)$, …, $P_n(x_n, y_n)$ 到未知节点M 的距离分别为 $d_1, d_2, \cdots, d_n$, 设M 的坐标为(x, y), 则满足

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = d_1^2 \\ \vdots \\ (x - x_n)^2 + (y - y_n)^2 = d_n^2 \end{cases} \tag{2}$$

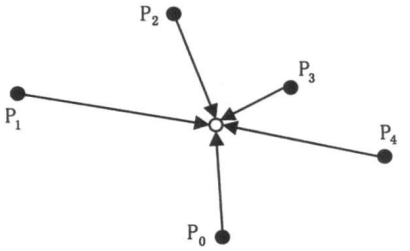

图2 多边测量法的极大似然估计图示

Fig. 2 Multilateral measuring method of maximum likelihood estimation

采用极大似然估计法(Maximum Likelihood Estimation, MLE) 求解, 从第一个方程开始分别减去最后一个方程, 得

$$\begin{cases} x_1^2 - x_n^2 - 2(x_1 - x_n)x + y_1^2 - y_n^2 - 2(y_1 - y_n)y = d_1^2 - d_n^2 \\ \vdots \\ x_{n-1}^2 - x_n^2 - 2(x_{n-1} - x_n)x + y_{n-1}^2 - y_n^2 - 2(y_{n-1} - y_n)y = d_{n-1}^2 - d_n^2 \end{cases} \tag{3}$$

用线性方程组表示为

$$AX = b$$

其中: $A = \begin{bmatrix} 2(x_1 - x_n) & 2(y_1 - y_n) \\ \vdots & \vdots \\ 2(x_{n-1} - x_n) & 2(y_{n-1} - y_n) \end{bmatrix}$, $b = \begin{bmatrix} x_1^2 - x_n^2 + y_1^2 - y_n^2 + d_n^2 - d_1^2 \\ \vdots \\ x_{n-1}^2 - x_n^2 + y_{n-1}^2 - y_n^2 + d_n^2 - d_{n-1}^2 \end{bmatrix}$, $X = \begin{bmatrix} x \\ y \end{bmatrix}$ (4)

使用标准的最小均方差估计法可以得到节点M 的坐标为

$$\hat{X} = (A^T A) A^T b \tag{5}$$

1.3 抵抗攻击的安全定位算法设计

提出的AR- TDOA 算法主要针对安全敏感的无线传感器网络应用。AR - TDOA 算法是在TDOA 测距技术基础上增加安全机制, 充分利用节点定位系统中大都存在冗余参照信息的特性, 以方差的无偏估计是否符合误差假设为安全性检验依据, 对采集来的定位信息进行数据分组过滤, 目的是在存在攻击的条件下仍能有效的计算正确的定位结果, 降低攻击对定位的影响。

本论文拟采用两步对采集来的信息进行过滤。

首先, 对采集来的定位信息三元组进行初步过滤, 考虑基于 TDOA 测距技术定位的特点, 利用

待定位节点与锚节点之间的距离 d 必定在节点的通信范围之内的特性, 粗略滤掉 $d > R$ 的定位数据, 为第二步信息分组做铺垫。

其次, 综合分析、比较了多种信息分组方法的时间复杂度和定位误差之后, 选择复杂度和定位精度达到平衡的 4NP 算法[9] 作为 AR- TDOA 中使用的信息集分组算法, 对其进行改进, 利用信息的一致性对定位信息进行分组。

正常的定位信息集其定位误差或均方差满足一定规律, 因此正常的定位信息集中的定位信息三元组(x_i, y_i, d_i)之间满足某种关联特征。存在攻击的定位信息集中, 恶意信标发出的定位信息三元组(x_i, y_i, d_i)与正常定位信息之间不存在关联特征, 这些恶意三元组(x_i, y_i, d_i)在整个定位信息集中是奇异点。正常的定位信息可以根据数据之间的一致性进行数据分类, 从而很容易排除这些奇异点。

1.4 一致性检验原则

由于存在测距误差, 定位系统大都采用最小二乘法(least square, LS) 进行估算。LS 的回归模型和估算函数分别为

$$d^2 = (x - x_0)^2 + (y - y_0)^2 + \varepsilon,\ \varepsilon \sim U(-e, e) \tag{6}$$

$$(\hat{x}_0,\ \hat{y}_0) = \arg \min_{(x_0, y_0)} \sum_{i=1}^{n} \left(\sqrt{(x_i - x_0)^2 + (y_i - y_0)^2} - d_i\right)^2。 \tag{7}$$

LS 算法简单易行, 但由于其代价函数采用求总和方式, LS 算法对局外点非常敏感, 单个干扰数据就足于导致参数估计严重偏差。针对 LS 算法的脆弱性, 采用统计方法对定位结果进一步分析。根据经典回归理论可知, 如果测距误差的分布是已知的, 则通过分析残差可以检验所给参照数据是否服从误差分布, 利用这个规律可以检验定位参照集是否满足一致性检验。

假如$(\hat{x}_0, \hat{y}_0)$是基于 L 的定位估算, 则定位残差平方和 δ^2 定义为

$$\delta^2 = \sum_{i=1}^{n} \left(d_i - \sqrt{(\hat{x}_0 - x_i)^2 + (\hat{y}_0 - y_i)^2}\right)^2 \tag{8}$$

假设参照集 L 的测量误差 $\varepsilon \sim U(-e, e)$, 则 L 的定位残差平方和 δ^2 满足$\frac{3\delta^2}{(n-2)e^2} < t$, 其中 $n = |L|$, t 为常数。根据实验统计规律寻找合适的 t 值, 依据文献[7] 可得如果$\frac{3\delta^2}{(n-2)e^2} < 4$, 则可以判定 L 中不存在恶意攻击, 即 L 通过了一致性检验。

1.5 改进后的 4NP 信息分组算法

改进后的 4NP 信息分组算法步骤如下:

步骤 1: 生成安全定位信息集。利用蒙特卡方法从 L 中随机抽取$K(K \geq 3)$个元素形成集合 L_1, 对集合 L_1 进行一致性检验, 直到集合 L_1 通过一致性检验为止。

步骤 2: 集合划分。从剩余的$L - L_1$中取出元素(x_i, y_i, d_i)放入 L_1 中, 对 L_1 进行一致性检验, 若满足则将元素(x_i, y_i, d_i)取出, 放入 L_3; 不满足则将元素取出, 放入 L_2。直至 l 中所有元素取完, 将 L_3 元素并入 L_1 中, 若 L_1 不满足一致性校验则继续转到步骤 1。

步骤 3: 生成新簇 L_1, 利用 L_1 中的元素采用极大似然估计法进行定位求解。

2 仿真结果

本节通过仿真来验证以上理论结果的正确性及检测算法的有效性, 比较基于 TDOA 的定位算法, SeRLoc 安全定位算法和 AR- TDOA 在受到攻击时的定位性能。在 100m × 100m 区域内部署 4 个锚节点, 坐标分别为(0, 0), (0, 100), (100, 0) (100, 100)。系统参数参照MIT 开发的室内定位系统 Cricket[8] 取典型值, 节点平均侦听到锚节点数为 4, 节点间通信距离为 R, 锚节点通信距离与 R 的比值为 10, 节点数 $N = 500$, 未知节点随机放置, 测距误差满足 $\varepsilon \sim U(-e, e)$。

实验考察了不同虚假锚节点数量情况下对定位的影响, 仿真中锚节点通信半径 $R = 150$m, 模拟敌方虚假锚节点, 向定位场景中广播错误的位置信息。整个实验重复 1 000 次, 并取平均值。

图 3 为 3 种定位算法在不同攻击强度下的定位比较, 其中 c 为虚假锚节点数量, d_a 为攻击强度, 即虚假锚节点声称的坐标与真实坐标的偏差距离, d_e 为平均定位误差, 即定位结果偏离未知节点真正坐标的平均距离。由图 3 可以看出, 攻击强度 d_a 从 0 逐渐增大到 100m 的过程中, 3 种定位算法的定位误差明显不同。d_a 增大, 基于 TDOA 测距的定位算法的定位误差明显增大, SeRLoc 安全定位算法因扇形区域面积而忽略攻击强度小的

定位坐标, 但随着攻击强度的进一步增大, 定位误差随之大幅增大。AR- TDOA 算法的定位误差稍微增大到一个峰值后又回落到一个较小的稳定值, 这是因为较明显的定位攻击第一步就被滤掉。

从图 3 中的曲线对比中可以看出, 虚假锚节点数量 c 由 1 变为 2 时, 基于TDOA 测距的定位算法和 SeRLoc 安全定位算法的定位误差对应增大, 这是由于增加了的虚假定位信息影响了定位精度。AR- TDOA 算法定位误差变化相对缓和, 因其采用了一致性检验原则排除虚假数据, 利用符合条件的定位信息组进行定位计算。

改进前后的定位算法在计算开销与稳定性方面的比较见表 1, 可以看出改进后的 AR- TDOA 算法相对于基于TDOA 测距的定位算法和 SeRLoc 安全定位算法在计算开销方面有少量增加, 在稳定性方面优于前者。

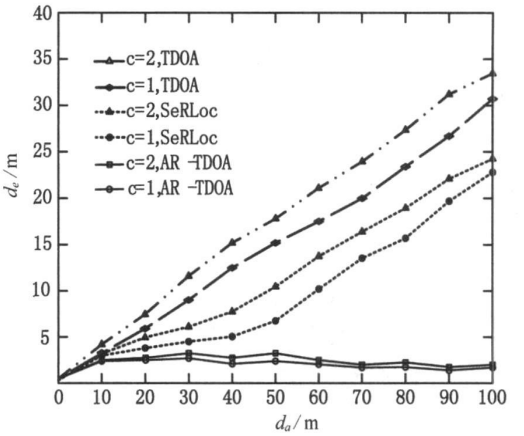

图3 攻击强度对定位误差的影响

Fig. 3 The influence of attack strength on the positioning error

表 1 虚假锚节点攻击条件下定位比较

Tab. 1 Positioning comparison with malicious beacon nodes

	TDOA	SeRLoc	AR- TDOA
计算开销	$(18k-17+2^3/3)*F+4AN$	$(18k-17+2^3/3)*F+4AN+3K$	$(18k-17+2^3/3)*F+4AN+16K$
稳定性	较差	一般	较好

3 结论

1) 攻击强度增大, 三种定位算法的平均定位误差随之增大, 其定位误差大小顺序依次为TDOA > SeRLoc> AR- TDOA。

2) 虚假锚节点数量越大, 基于 TDOA 测距和 SeRLoc 的定位误差越大, 但 AR- TDOA 算法的定位误差能保持在较小程度内。

3) AR- TDOA 算法在增加少量计算复杂度的情况下, 能够改善定位的稳定性。

参考文献:

[1] 曹晓梅, 俞 波, 陈贵海, 等. 传感器网络节点定位系统安全性分析[J]. 软件学报, 2008, 19(4): 879- 887.

[2] LAZOS L, POOVENDRAN R. SeRLoc: Secure range- independent localization for wireless sensor networks [C]// LAZOSL L, POOVENDRAN R. Proc. of the 2004 ACM Workshop on Wireless Security. New York: ACM Press, 2004: 196- 207.

[3] LIU D, NING P, DU W K. Attack- resistant location estimation in sensor networks[C]// ZHAO F, COZZENS J, ESTRIN D. Proc. of the Int' l Conf. on Information Processing in Sensor Networks. Washington: IEEE Computer Society Press, 2005: 178- 185.

[4] 任秀丽, 杨 威, 薛建生. 一种基于测距的无线传感网Sybil攻击检测方法[J]. 计算机应用, 2009, 29(6): 1628- 1631.

[5] BOUKERCHE A, OLIVEIRA H A, NAKAMURA E F, et al. Secure localization algorithms for wireless sensor networks [J]. IEEE Communication Magazine, 2008(4): 96- 101.

[6] 张起元. 无线传感器网络虚假数据检测排除机制研究[D]. 合肥: 中国科学技术大学, 2010.

[7] 叶阿勇. 无线传感器网络节点安全定位[D]. 西安: 西安电子科技大学, 2009.

[8] PRIYANTHA N B, CHAKRABORTY A, BALAKRISHNAN H. The cricket location- support system[C]// STEERE D C, BAPTISTA A, PU C, et al. Proc. of the 6th Annual Int' l Conf. on Mobile Computing and Networking. Boston: ACM Press, 2000: 58- 66.

(责任编辑　马立)