Location of Sybil Attack Source under Heterogeneous IWSN*

SUN Ziwen[1,2*], *ZHU Ying*[1]

(1.*School of Internet of Things, Jiangnan University, Wuxi Jiangsu* 214122, *China*; 2.*Engineering Research Center of Internet of Things Technology Applications Ministry of Education, Wuxi Jiangsu* 214122, *China*)

Abstract: An RSSD-based location estimation algorithm is adopted to against the problem of Sybil attack source location in industrial wireless sensor networks. First, use DV-Hop algorithm to estimate the coordinates of unknown reference nodes and preprocess the RSSI value. Then, transform the attack node position estimation problem into a solution to the nonlinear equations. The attack nodes are located by using the least square method and the Taylor series expansion method. MATLAB simulation results show that the localization algorithm can effectively reduce the noise interference, solve the problem that the attack source does not cooperate with positioning and the number of beacon nodes is too, and significantly improve the node positioning accuracy.

Key words: industrial wireless sensor networks; attack source location; received signal strength difference; Taylor series expansion method

EEACC: 6150P **doi**: 10.3969/j.issn.1004-1699.2019.02.019

异构 IWSN 下对 Sybil 攻击源的定位*

孙子文[1,2*], 朱 颖[1]

(1.江南大学物联网工程学院, 江苏 无锡 214122; 2.物联网技术应用教育部工程研究中心, 江苏 无锡 214122)

摘 要: 针对工业无线传感器网络中女巫攻击源定位问题, 采用一种基于 RSSD 的定位估计算法。首先, 利用 DV-Hop 算法估计出未知参考节点的坐标并对 RSSI 值预处理。其次, 将攻击节点位置估计问题转化为对非线性方程组的解算问题, 分别利用最小二乘法和泰勒级数展开法对攻击节点进行定位。MATLAB 仿真结果表明该定位算法可以有效地减少噪声的干扰, 解决攻击源不配合定位和信标节点数量少的问题, 显著提高节点定位精度。

关键词: 工业无线传感器网络; 攻击源定位; 接受信号强度差; 泰勒级数展开法

中图分类号: TP393 **文献标识码**: A **文章编号**: 1004-1699(2019)02-0276-07

工业无线传感器网络 IWSN(Industrial Wireless Sensor Networks)[1]中, 为节约成本, 除少量节点带有自定位的 GPS 模块, 大部分传感器节点则被随机分布在特定的检测区域, 即节点的位置是未知的。IWSN 在实际工作过程中会受到各种攻击和安全威胁, 其中 Sybil 攻击是一种危害巨大, 容易发起的基础攻击类型。受到 Sybil 攻击后, 恶意节点违法地以多个身份出现, 并发送错误信息, 误导用户管理中心的决策。因此, 在检测出 Sybil 攻击之后, 对恶意节点及时进行定位是至关重要的。

IWSN 中根据是否需要测距将定位算法分为基于测距定位算法和基于非测距定位算法[2]。基于测距的定位算法包括: 信号到达角度 AOA(Angle of Arrival)、到达时间 TOA(Time of Arrival)、基于接收信号强度指示 RSSI(Received Signal Strength Indication)等。非测距的定位算法主要包括: 质心定位算法, 距离矢量跳 DV-Hop(Distance Vector-Hop)算法, 近似三角形内点测试法 APIT(Approximate Point-in-Triangulation Test)定位算法, 多维比例图 MDS-MAP(Multidimensional Scaling-Map)算法等。其中基于 RSSI 的定位技术具有定位精度高且无需额外的硬件设备等优点, 使得 RSSI 定位算法成为一大研究热点。目前 RSSI 定位算法常用的是 RSSI 指纹定位算法[3]和基于 RSSI 测距的三边定位算法。Zhang G 等人[4]采用 RSSI 指纹定位算法, 在离线阶段, 建立 RSSI 指纹数据库, 在在线阶段, 利用 K-近邻 KNN(K-Nearest Neighbor)匹配算法将采集到的 RSSI 值与指纹数据库中 RSSI 值进行匹配, 最终选择出 K 个参考节点进行

项目来源: 国家自然科学基金项目(61373126); 中央高校基本科研业务费专项资金项目(JUSRP51510); 江苏省自然科学基金项目(BK20131107)

收稿日期: 2018-07-19 **修改日期**: 2018-11-14

目标节点的质心定位算法。何青春等人[5]运用 RSSI 测距技术测量目标节点与已知参考节点之间的距离,随后利用三边测量定位算法得到目标节点坐标信息。然而 RSSI 易受环境影响,尤其在恶劣的工业环境下,测距误差较大,因此文献[6]进一步的改进,建立卡尔曼滤波器模型,在基于 RSSI 的定位算法进行测距时利用卡尔曼滤波器模型对通信节点之间的 RSSI 值进行平滑优化,使优化过的 RSSI 值更接近于理想测量值,从而来降低测距算法在测距过程中的误差,提高定位精度。在文献[7]中对采集到的 RSSI 值进行均值滤波,并基于 RSSI 进行泰勒级数展开定位算法,但在泰勒级数展开定位算法中初始值的选取未进行讨论。文献[8]中采用基于混合接收信号强度差 RSSD(Received Signal Strength Difference)和到达时间差 TDOA(Time Difference of Arrival)的最小二乘法定位算法,但对硬件要求高,且计算量大,定位精度不高。同时由于 Sybil 节点会篡改自身的信息来达到难以被定位的效果,导致大多数定位算法都不适用于直接定位攻击节点。如改进的 RSSI 指纹定位算法中,Sybil 节点篡改接收到的 RSSI 值,使得无法与指纹数据库进行正确匹配。

Sybil 攻击源的定位以攻击源的检测为基础,目前 Sybil 攻击检测方法中基于 RSSI 的检测方法凭借对节点硬件要求低,通信能耗少等优点,成为 Sybil 攻击检测的主流方法。文献[9]利用 RSSI 与节点 ID 的关联性,检测 Sybil 攻击。但改变节点发射功率则改变 RSSI,所以仅利用关联性检测存在漏检问题。文献[10]利用不同节点接收的 RSSI 比值来解决 RSSI 的不可靠性,一个节点需要四个节点作为监测节点来进行检测,但监测节点会消耗大量能量,影响网络的生命周期。文献[11]采用一种基于异构 IWSN 的高能节点级、基站级的双层 Sybil 攻击检测方案,高能节点基于 RSSI 二次差值检测普通节点,基站根据高能节点的成功及不成功交互数量计算出信任值进行高能节点的检测。保证较低虚警率和漏警率的同时提高检测准确率,减少节点能耗,延长网络寿命。

文章借鉴 TOA 定位算法转化为 TDOA 定位算法的思想,在 RSSI 定位算法的基础上进行改进,实现了一种基于 RSSD 的定位算法[12],该算法可以定位具有未知传输信息的攻击节点的位置,适用于 Sybil 攻击源定位。通过参考节点采集攻击节点的 RSSI 值,并采用卡尔曼滤波对 RSSI 值进行预处理,先利用 DV-Hop 算法估计出未知参考节点的坐标;再根据 RSSD 测量值得到非线性方程组,因此对攻击节点定位问题转化为对非线性方程组的解算问题,通过最小二乘法估计方程组中攻击节点的初始值,利用泰勒级数展开法对攻击节点进行精确定位。

1　定位模型

假设整个网络分为普通节点和信标节点,其中信标节点通过 GPS 定位系统或者人工亲自部署等方法获取自身的位置信息,普通节点则是随机部署,因此位置是未知的。由于攻击源会篡改自身的信息,因此需要选取攻击节点通信范围内的部分节点作为参考节点参与定位。若被攻击的是信标节点,则节点位置已知,可以直接定位;若 Sybil 攻击发生在普通节点中,则需要进行攻击源定位。

在工业无线传感器网络中,假设需要定位的攻击节点的坐标为 $\boldsymbol{X}=(x,y)$,参考节点的坐标为 $\boldsymbol{X}_i=(x_i,y_i)$,$i=1,2,\cdots,N$,$N$ 为参考节点数。如图 1 所示的攻击节点定位模型中,参考节点数 $N=4$,在攻击节点的通信范围内选取出参考节点 X_1,X_2,X_3,X_4,其中参考节点 X_2 是信标节点,另外三个参考节点 X_1,X_3,X_4 是普通节点,此三个节点自身的位置也待估计。

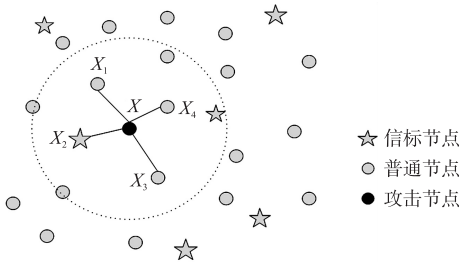

图 1　攻击节点定位模型

2　基于 RSSD 的攻击节点定位总体框架

当利用双层 Sybil 攻击检测方案[11]检测出攻击节点,攻击节点的 ID 会被发送至基站,基站接收到信息后,向整个网络发起对该攻击节点定位的命令。

基于 RSSD 的攻击节点定位主要分为三部分。第一部分,基站对参考节点的选择及位置估计。基站在攻击节点的所有邻居节点范围内选择出合适的参考节点参与定位,并对本身不是信标节点的参考节点利用 DV-Hop 算法进行位置估计。第二部分,参考节点对 RSSI 值的采集与预处理阶段。参考节点采集攻击节点发送数据包时的 RSSI 值后发送给基站,由基站采用卡尔曼滤波对所采集的 RSSI 值进行预处理。第三部分,基于 RSSD 的攻击节点的位置估计。根据接收信号强度差与传播距离之间的数学关系构建非线性方程组,采用最小二乘算法对攻击节点进行初步估计,再利用泰勒级数展开法进行精确定位。

2.1　基于 RSSD 的攻击节点定位架构图

如图 2 所示,是由参考节点的选择及位置估计、

RSSI 值的采集与预处理阶段、基于 RSSD 对攻击节点的初步定位及精准定位三个部分组成的攻击节点定位架构图。

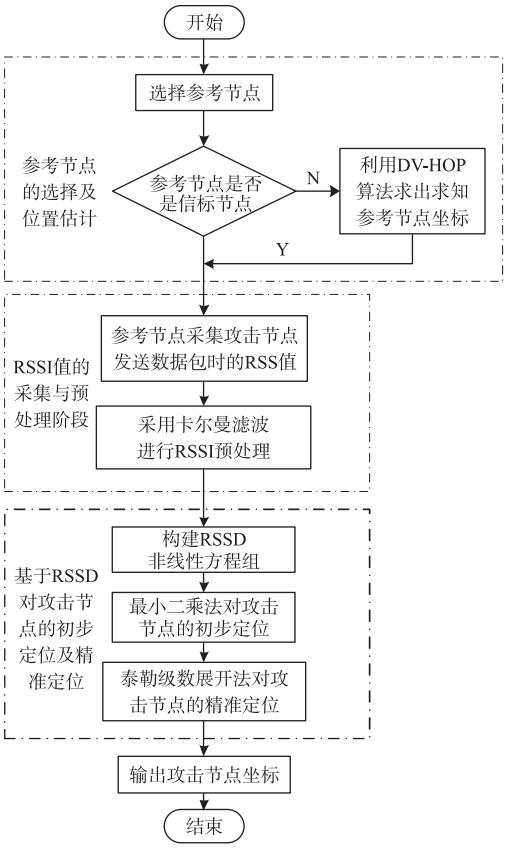

图 2 攻击节点定位架构图

2.2 参考节点选择及位置估计

参与定位的参考节点数量越多,定位精确度越高,但所需的能量消耗也就越大,同时定位的时间也会增加,因此为了节约节点能耗以及减少定位时间,同时保证定位精度要求,需要选择出一些合适的参考节点来参与定位。

2.2.1 参考节点选择原则

在选取参考节点时遵循以下原则[13]:

①选取的节点应尽量均匀分布在攻击节点四周,也就是参考节点不能集中分布在攻击节点的一侧。理想状态下,所有参考节点连接起来所构造的区域应该以攻击节点为中心[14]。

②在节点同等均匀分布下,为了减少节点间传播过程中能量消耗,应选取距离攻击节点较近的参考节点,即所选参考节点到攻击节点的距离和最小[15]。

③所选择的参考节点的剩余能量不低于所有邻居节点的平均剩余能量。

根据构建的 RSSD 非线性方程组可以得到所需要的最少参考节点数量为 4 个。

2.2.2 基于 DV-Hop 算法对参考节点进行位置估计

DV-Hop 算法是目前非测距定位算法中使用最广泛的定位算法之一,它具有实现简单、通信开销和计算量较小等优点,所以本文选用 DV-Hop 算法[16]对位置未知的参考节点进行位置估计。DV-Hop 算法的基本思想是:用平均跳距乘以跳数,计算出信标节点到未知参考节点之间的距离,随后通过极大似然估计解出未知参考节点的坐标。位置未知的参考节点的坐标位置估计过程分为 3 个阶段。

第一阶段:获得最小跳数信息。每个信标节点将数据包{ID,位置,跳数(初始化为 0)}发送给通信范围内的邻居节点,当邻居节点收到此数据包时,记录下到信标节点的跳数,然后跳数值加一继续转发给邻居节点。第二阶段:计算信标节点与未知节点之间距离。每个信标节点根据其到其他信标节点的最少跳数和自身坐标,计算出信标节点的平均跳距。所有信标节点将其平均跳距广播至整个网络中,未知参考节点将距离最近的信标节点的平均跳距作为自己的平均跳距。最后将平均跳距和跳数信息相乘获得未知参考节点到信标节点的距离。

第三阶段:求解未知参考节点的位置信息。根据未知参考节点已经记录了到各个信标节点的距离,利用极大似然估计计算出未知参考节点的坐标。

2.3 RSSI 值的采集与预处理

攻击节点将数据包发送给通信范围内所有节点,其中参考节点就会采集接受数据包时的 RSSI 值,并将所采集到的 RSSI 值发送至基站,由基站采用卡尔曼滤波进行 RSSI 预处理。

2.3.1 参考节点对攻击节点 RSSI 值的采集

攻击节点到参考节点的距离可表示为:

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

不考虑测量误差的理想环境下,根据阴影衰落模型,各参考节点接收到攻击节点的 RSSI 值可表示为:

$$R_i=K_0\frac{P_t}{(d_i)^{\gamma}},i=1,2,\cdots,N \quad (2)$$

式中:P_t 是节点发送信号功率,γ 是传播路径损耗指数,根据实际环境选取不同的值,K_0 是影响接收信号强度所有因素的总效应,如天线高度、天线增益和传输干扰等。将式(2)表示成对数正态分布形式

$$10\log_{10}(R_i)=10\log_{10}(K_0P_t)-10\gamma\log_{10}(d_i),\ i=1,2,\cdots,N \quad (3)$$

根据 dB=10lg(X),在考虑噪声引起的测量误差情况下,RSSI 值表示为[17]:

$$R_i(\mathrm{dB})=P_t(\mathrm{dB})+K_0(\mathrm{dB})-10\gamma\log_{10}(d_i)+e,\ i=1,2,\cdots,N \quad (4)$$

式中:e 是高斯噪声,$e\sim N(0,\sigma^2)$。

2.3.2　运用卡尔曼滤波对 RSSI 预处理

由于复杂的工业环境,存在电磁信号的多径效应和非视距传播以及大型工业设备的影响,RSSI 信号强度并不稳定,存在一定的波动性,因此,不能将 RSSI 信号强度的一次测量值直接作为参考值,必须对 RSSI 值进行一定的预处理。

Kalman 滤波是一种高效的滤波方法,它以最小均方误差为最佳估计标准,采取无线信号和环境噪声的状态空间模型,利用在上一状态下对现在的预测值和现状态下的测量值来代替对现状态的最佳估计,求出现在时刻的估计值。为了从一系列有噪声干扰的 RSSI 数据中用 Kalman 滤波估计出理想 RSSI 值,首先,必须建立 RSSI 值系统模型并且用如下的线性微分方程来描述该模型:

$$\boldsymbol{R}_i(k|k-1)=\boldsymbol{A}\cdot\boldsymbol{R}_i(k-1|k-1) \tag{5}$$

式中:$R_i(k|k-1)$表示根据 $k-1$ 时刻的 RSSI 的预测值来预测 k 时刻的 RSSI 预测值,$R_i(k-1|k-1)$表示 $k-1$ 时刻的最佳估计 RSSI 值,$\boldsymbol{A}$ 和 $\boldsymbol{B}$ 是系统参数。

当系统模型更新后,用 T 来表示更新的协方差:

$$\boldsymbol{T}(k|k-1)=\boldsymbol{A}\cdot\boldsymbol{T}(k-1|k-1)\cdot\boldsymbol{A}'+\boldsymbol{Q} \tag{6}$$

式中:$\boldsymbol{T}(k|k-1)$是 $\boldsymbol{R}_i(k|k-1)$对应的协方差,$\boldsymbol{T}(k-1|k-1)$是 $\boldsymbol{R}_i(k-1|k-1)$对应的协方差,$\boldsymbol{A}'$是 $\boldsymbol{A}$ 的转置矩阵,$\boldsymbol{Q}$ 为系统过程噪声的协方差。

计算卡尔曼增益:

$$K_g(k)=\boldsymbol{T}(k|k-1)\boldsymbol{H}'|[\boldsymbol{H}\cdot\boldsymbol{T}(k|k-1)\boldsymbol{H}'+\boldsymbol{V}] \tag{7}$$

式中:$\boldsymbol{H}$ 是系统模型参数,$\boldsymbol{H}'$为 $\boldsymbol{H}$ 的转置,$\boldsymbol{V}$ 为测量噪声的协方差。结合预测 RSSI 值和实际测量 RSSI 值,得到 k 时刻下最佳估计 RSSI 值 $\boldsymbol{R}_i(k|k)$:

$$\boldsymbol{R}_i(k|k)=\boldsymbol{R}_i(k|k-1)+\boldsymbol{K}_g(k)[\boldsymbol{R}_i(k)-\boldsymbol{H}\cdot\boldsymbol{R}_i[k|k-1)] \tag{8}$$

式中:$\boldsymbol{R}_i(k)$是 k 时刻的实际 RSSI 测量值,$K_g(k)$是卡尔曼增益。

为了得到所有时刻下的最佳估计 RSSI 值,需要更新 k 状态下最佳估计 RSSI 值 $\boldsymbol{R}_i(k|k)$的协方差 $\boldsymbol{T}(k|k)$,并将新的协方差代入下个迭代中,即将式(9)中的 $\boldsymbol{T}(k|k)$代入式(6)中。

$$\boldsymbol{T}(k|k)=[\boldsymbol{I}-\boldsymbol{K}_g(k)\cdot\boldsymbol{H}]\cdot\boldsymbol{T}(k|k-1) \tag{9}$$

式中:$\boldsymbol{I}$ 为 1 的矩阵,对于单模型单测量,$\boldsymbol{I}=1$。假设 $k=2,3,\cdots,k_{\max}$,当运行至 $k_{\max}$时,所有时刻都得到最佳 RSSI 估计值,迭代结束。经过卡尔曼滤波,可有效地削弱由噪声等因素造成的 RSSI 的测量误差,达到提高测量精度的目的。

2.4　基于 RSSD 的攻击节点定位

基于 RSSD 的定位算法是通过测得攻击节点信号到达不同参考节点之间的信号强度强差,根据信号在空间传播的模型获得接收信号强度差与传播距离之间的数学关系构建非线性方程组,并对方程组进行解算估计攻击节点的位置坐标。泰勒级数展开法由于求解精度高,收敛速度快等优点是求解非线性方程组的有效方法,该算法对初始值有很强的依赖性,只有在初始值有一定的准确性的情况下才能有较快的收敛速度。因此文中采用最小二乘算法估计攻击节点坐标的初始值,再利用泰勒级数展开法进行精确定位,保证初始值的合理性,从而减少泰勒级数展开算法的复杂度。

2.4.1　基于最小二乘法的攻击节点初步定位

在式(4)RSSI 值的表达式的基础上,参考节点之间的接收信号强度差 RSSD 可表示为[18]:

$$\Delta R_{1i}(\mathrm{dB})=R_1(\mathrm{dB})-R_i(\mathrm{dB})=10\gamma\log_{10}(d_1)-10\gamma\log_{10}(d_i)+e_{1i}=10\gamma\log_{10}(d_i/d_1)+e_{1i}\quad i=2,\cdots,N \tag{10}$$

式中:$e_{1i}\sim N(0,\sigma_i^2+\sigma_1^2)$,因此,RSSD 测量值与发射功率无关。由上式可得到参考节点 X_i 到攻击节点的距离 d_i 的表达式:

$$d_i=10^{\left(\frac{\Delta\bar{R}_{1i}(\mathrm{dB})}{10\gamma}\right)}d_1,\ i=2,\cdots,N \tag{11}$$

式中:$\Delta\hat{R}_{1i}(\mathrm{dB})$为 RSSD 的测量值。对式(1)左右两边同时平方,并代入左右两边同时平方的式(11)中,经过变换得到:

$$[10^{(\Delta\bar{R}_{1i}/(5\gamma)}-1]d_1^2=x_i^2+y_i^2-x_1^2-y_1^2+2x(x_1-x_i)+2y(y_1-y_i) \tag{12}$$

定义 $\xi_{1i}=10^{\Delta\hat{R}_{1i}(\mathrm{dB})/(5\gamma)}-1$,攻击节点的估计位置坐标假设为 $\hat{\boldsymbol{X}}=[\hat{x},\hat{y}]^{\mathrm{T}}$,则式(12)可以化简成矩阵的形式:

$$\boldsymbol{A}\hat{\boldsymbol{X}}=\boldsymbol{B} \tag{13}$$

式中:

$$\boldsymbol{A}=\begin{bmatrix}2(x_1-x_2) & 2(y_1-y_2)\\ 2(x_1-x_3) & 2(y_1-y_3)\\ \cdots & \cdots\\ 2(x_1-x_N) & 2(y_1-y_N)\end{bmatrix}$$

$$\boldsymbol{B}=\begin{bmatrix}\xi_{12}d_1^2-x_2^2-y_2^2+x_1^2+y_1^2\\ \xi_{13}d_1^2-x_3^2-y_3^2+x_1^2+y_1^2\\ \cdots\\ \xi_{1N}d_1^2-x_N^2-y_N^2+x_1^2+y_1^2\end{bmatrix}$$

最后通过最小二乘估计:

$$\hat{\boldsymbol{X}}=(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{B} \tag{14}$$

可以求出攻击节点的估计坐标位置 $\hat{\boldsymbol{X}}=[\hat{x},\hat{y}]^{\mathrm{T}}$。

最小二乘法的特性以最小化误差平方之和来作为目标,保证了基于最小二乘法的粗定位可以收敛

到真实位置附近,其次,将最小二乘法的值作为泰勒级数展开法的初始值之后,最终求出的目标位置估计值的门限值判定也保证了基于最小二乘法的粗定位可以收敛到真实位置。

2.4.2 基于泰勒级数展开法的攻击节点精准定位

泰勒级数展开法是一种迭代运算算法,根据参考节点之间的接收信号强度差 RSSD 建立非线性方程组,并转化成函数形式,将攻击节点的初始坐标代入,并在攻击节点处对其进行泰勒级数展开,获得最终攻击节点的位置估计[19]。

参考节点之间的接收信号强度差 RSSD 建立方程组如下所示:

$$\begin{cases}\Delta R_{1,2}=R_1-R_2\\ \Delta R_{1,3}=R_1-R_3\\ \cdots\\ \Delta R_{1,i}=R_1-R_i\end{cases} \tag{15}$$

将式(2)以及式(1)代入式(15)中,得到如下非线性方程组:

$$\begin{cases}\Delta R_{1,2}=K_0\dfrac{R_t}{[(x_2-x)^2+(y_2-y)^2]^{\gamma/2}}-K_0\dfrac{R_t}{[(x_1-x)^2+(y_1-y)^2]^{\gamma/2}}\\ \Delta R_{1,3}=K_0\dfrac{R_t}{[(x_3-x)^2+(y_3-y)^2]^{\gamma/2}}-K_0\dfrac{R_t}{[(x_1-x)^2+(y_1-y)^2]^{\gamma/2}}\\ \cdots\\ \Delta R_{1,i}=K_0\dfrac{R_t}{[(x_i-x)^2+(y_i-y)^2]^{\gamma/2}}-K_0\dfrac{R_t}{[(x_1-x)^2+(y_1-y)^2]^{\gamma/2}}\end{cases} \tag{16}$$

将上式定义成函数形式:

$$f_i(x,y)=K_0\frac{R_t}{[(x_i-x)^2+(y_i-y)^2]^{\gamma/2}}-K_0\frac{R_t}{[(x_1-x)^2+(y_1-y)^2]^{\gamma/2}} \tag{17}$$

式中:$i=1,2,\cdots,N$。

根据式(14)可以求得攻击节点的初始坐标为 $\hat{X}=[\hat{x},\hat{y}]^{\mathrm{T}}$,令 $x=\hat{x}+\Delta x$,$y=\hat{y}+\Delta y$。对上式进行泰勒级数展开,可得

$$f_i(x,y)=\Delta R_{1i}(x,y)=\Delta R_{1i}(\hat{x}+\Delta x,\hat{y}+\Delta y)\approx \Delta R_{1i}(\hat{x},\hat{y})+K_0R_t\gamma\left[\frac{x_i-\hat{x}}{d_i^{(\gamma+2)}}-\frac{x_1-\hat{x}}{d_1^{(\gamma+2)}}\right]\Delta x+K_0R_t\gamma\left[\frac{y_i-\hat{y}}{d_i^{(\gamma+2)}}-\frac{y_1-\hat{y}}{d_1^{(\gamma+2)}}\right]\Delta y \tag{18}$$

将上式转换成矩阵形式:

$$\boldsymbol{h}=\boldsymbol{WG} \tag{19}$$

式中

$$\boldsymbol{h}=\begin{bmatrix}\Delta R_{1,2}(x,y)-\Delta R_{1,2}(\hat{x},\hat{y})\\ \Delta R_{1,3}(x,y)-\Delta R_{1,3}(\hat{x},\hat{y})\\ \cdots\\ \Delta R_{1,N}(x,y)-\Delta R_{1,N}(\hat{x},\hat{y})\end{bmatrix},\ \boldsymbol{W}=\begin{bmatrix}\Delta x\\ \Delta y\end{bmatrix},$$

$$\boldsymbol{G}=K_0P_t\gamma\begin{bmatrix}\dfrac{x_2-\hat{x}}{d_2^{(\gamma+2)}}-\dfrac{x_1-\hat{x}}{d_1^{(\gamma+2)}},\dfrac{y_2-\hat{y}}{d_2^{(\gamma+2)}}-\dfrac{y_1-\hat{y}}{d_1^{(\gamma+2)}}\\ \dfrac{x_3-\hat{x}}{d_3^{(\gamma+2)}}-\dfrac{x_1-\hat{x}}{d_1^{(\gamma+2)}},\dfrac{y_3-\hat{y}}{d_3^{(\gamma+2)}}-\dfrac{y_1-\hat{y}}{d_1^{(\gamma+2)}}\\ \cdots\\ \dfrac{x_N-\hat{x}}{d_N^{(\gamma+2)}}-\dfrac{x_1-\hat{x}}{d_1^{(\gamma+2)}},\dfrac{y_N-\hat{y}}{d_N^{(\gamma+2)}}-\dfrac{y_1-\hat{y}}{d_1^{(\gamma+2)}}\end{bmatrix}$$

使用最小二乘估计得到 W 的值

$$\boldsymbol{W}=\begin{bmatrix}\Delta x\\ \Delta y\end{bmatrix}=[\boldsymbol{G}^{\mathrm{T}}\boldsymbol{G}]^{-1}\boldsymbol{G}^{\mathrm{T}}\boldsymbol{h} \tag{20}$$

攻击节点的初始坐标为 $\hat{\boldsymbol{X}}=[\hat{x},\hat{y}]^{\mathrm{T}}$,令 $x_0=\hat{x}+\Delta x$,$y_0=\hat{y}+\Delta y$。且直至 Δx,Δy 足够小并满足一个预先设定的门限值 ε[20],使得 $|\Delta x|+|\Delta y|<\varepsilon$。此时,得到最终攻击节点估计坐标 $\boldsymbol{X}_0=[x_0,y_0]^{\mathrm{T}}$。

3 仿真与结果

为了对所研究的 RSSD 定位算法进行仿真验证,采用 OPNET 和 MATLAB 软件进行仿真实验,OPNET 软件用于 RSSI 测量值的采集,MATLAB 软件用于定位算法的实现。选择均方根误差 RMSE(Root Mean Square Error)作为定位精度指标,将本文定位算法与文献[7-8]中的定位算法进行对比分析。

均方根误差 RMSE 的计算公式如下所示:

$$\mathrm{RMSE}=\sqrt{\frac{\sum L_n^2}{n}} \tag{21}$$

式中:n 为测量次数,$L_n=\sqrt{(x-x_0)^2-(y-y_0)^2}$ 测量值与真实值的偏差,即攻击节点的最终估计坐标与实际坐标的偏差。

对采用卡尔曼滤波对 RSSI 预处理的作用进行仿真验证。首先,在 OPNET 软件仿真区域为 150 m×150 m 的范围内随机部署一个攻击节点以及九个邻居节点,考虑噪声情况下,采集其中一个节点的 RSSI 值共 200 组。再在 MATLAB 仿真软件中运行卡尔曼滤波算法,对采集到的 200 组 RSSI 值作为卡尔曼滤波的输入值,对 RSSI 值进行预处理后。卡尔曼滤波处理前后对比情况如图 3 所示,由图 3 可知,卡尔曼滤波算法收敛速度较快,在第 100 组数据时滤波后的 RSSI 值开始稳定在 20 dBm 左右。其中选择了 150 组到 180 组期间

的 RSSI 值进行放大对比，滤波前，RSSI 值波动范围为 15 dBm~25 dBm，滤波后，RSSI 值波动范围为 19 dBm~21 dBm。可见，采用卡尔曼滤波对 RSSI 值进行预处理，对误差较大的值有很好的滤波作用，可以有效减少噪声干扰，达到去噪的效果，有利于提高定位精度。

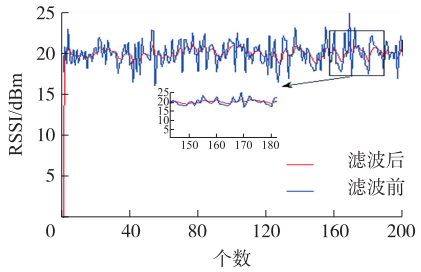

图 3　卡尔曼滤波处理前后 RSSI 值对比图

验证采用 DV-Hop 算法对未知参考节点位置估计的必要性以及 DV-Hop 算法的位置估计。在 MATLAB 中设仿真区域大小为 1 000 m×1 000 m，随机部署 300 个未知节点和 30 个信标节点；普通节点通信半径为 100 m，信标节点通信半径为 150 m。节点分布情况如图 4 所示。

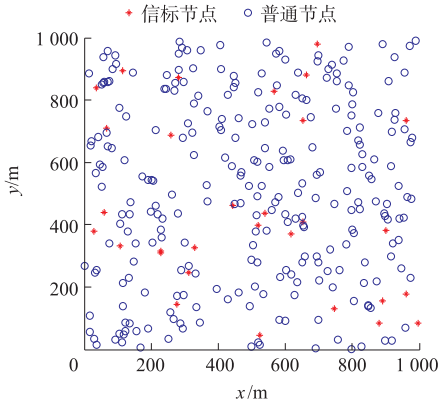

图 4　节点分布情况

节点间通信情况如图 5 所示。仿真计算出图 5 中未知节点通信区域内的信标节点平均数目为 2.044 4，未知节点通信区域内的未知节点平均数目为 8.592 6。可见，当需要对攻击节点进行定位时，攻击节点通信范围内的信标节点个数未达到定位时所需的参考节点个数最低要求 4 个，仅依靠信标节点来作为参考节点是不够的，为此，本文采用增加普通节点作为参考节点来对攻击节点进行定位，以有效地解决信标节点数量少的问题。

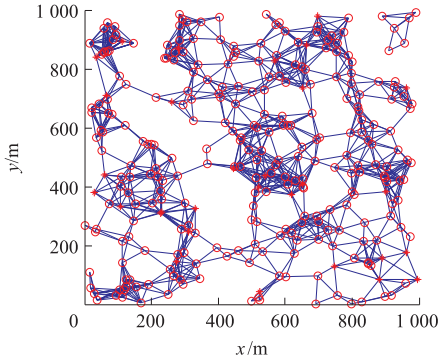

图 5　节点间通信情况

验证所选用的 DV-Hop 算法对位置未知节点的位置估计有很好的性能。假设在仿真区域内随机部署未知节点和信标节点，其中信标节点的密度为 10%。定义未知节点归一化的相对定位误差为：

$$\text{Error}=\frac{\sum_{i=1}^{M_T-M_B}\sqrt{(x_{\text{test},i}-x_{\text{real},i})^2-(y_{\text{test},i}-y_{\text{real},i})^2}}{(M_T-M_B)r} \tag{22}$$

式中：M_T 为总节点的个数，M_B 为信标节点的个数，r 为节点的半径，$(x_{\text{real},i},y_{\text{real},i})$ 为未知节点 i 的实际坐标，$(x_{\text{test},i},y_{\text{test},i})$ 为通过 DV-Hop 算法的估计坐标。表 1 为 DV-Hop 算法在不同总节数下的相对定位误差比较情况。

表 1　DV-Hop 算法相对定位误差情况

总节点的个数	相对定位误差
100	0.4268
200	0.3748
300	0.2578
400	0.2596
500	0.2614

由表 1 可以看出 DV-Hop 算法对未知节点位置估计时有较低的定位误差，较好的定位性能，且随着节点个数增多，定位误差越小，但当总节点数达到 300 以后，定位误差处于稳定状态。

MATLAB 软件仿真验证研究的 RSSD 定位算法的有效性。根据在 OPNET 软件中部署的一个攻击节点以及九个邻居节点的部署情况，在 MATLAB 中还原相同的部署，并在所有邻居节点中选择出四个最优参考节点。在相同条件下，不同门限值的选择会导致定位算法最终定位误差的差异，仿真中门限值设定为 1.5，此时定位误差最小[20]。如图 6 所示，根据选择的四个参考节点对攻击节点进行定位。

与文献[7-8]中的 Hybrid-LS 定位算法和 RSSI-TL 定位算法进行定位性能对比，主要比较了不同算法定位攻击节点的均方根误差，仿真结果如图 7 所示。

由图 7 可知，当噪声标准差越大时，三种定位算

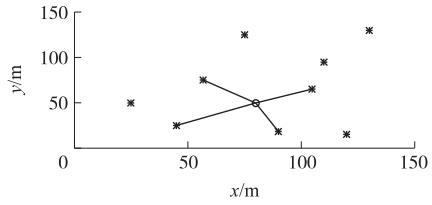

图 6　所选参考节点分布情况

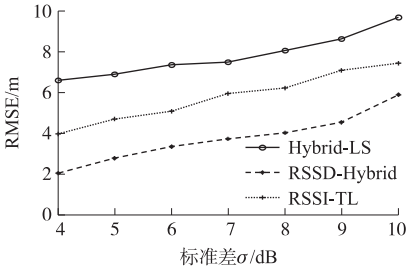

图 7 不同算法的定位误差情况

法的定位均方根误差 RMSE 越大。当标准差在 4 dB~10 dB 之间变化时,Hybrid-LS 定位算法[8]的 RMSE 在 6m~10m 之间变化;RSSI-TL 定位算法[7]的 RMSE 在 4 m~8 m 之间变化;RSSD-Hybrid 定位算法的 RMSE 在 2 m~5 m 之间变化。

表 2 列出了三种算法的时间复杂度,其中 N 表示样本数量,K 为特征的数量。可以看出三种算法复杂度都属于线性级,是同一数量级,在复杂度方面略微增加。

表 2 算法时间复杂度对比情况

算法	时间复杂度
Hybrid-LS 定位	$O(K^2N)$
RSSD-Hybrid 定位	$O(K^2N)+O(KN)$
RSSI-TL 定位	$O(KN)$

因此,RSSD-Hybrid 定位算法在复杂度方面略微增加,但定位精度要明显高于其他两种定位算法。

4 结论

根据工业无线传感器网络中被 Sybil 攻击的节点会篡改自身的信息导致难以被定位的问题,本文提出一种基于 RSSD 的定位估计算法。此方法中利用改进的 DV-Hop 算法估计出未知参考邻居节点的坐标,将攻击节点位置估计问题转化为对非线性方程组的解算问题,分别利用最小二乘法和泰勒级数展开法对攻击节点进行定位。整个定位算法可以有效地减少噪声的干扰,解决攻击源不配合定位和信标节点数量少的问题,显著提高节点定位精度。

参考文献:

[1] Salam H A, Khan B M. IWSN-Standards, Challenges and Future [J]. IEEE Potentials, 2016, 35(2): 9-16.

[2] Darakeh F, Mohammad-Khani G R, Azmi P. CRWSNP: Cooperative Range-Free Wireless Sensor Network Positioning Algorithm[J]. Wireless Networks, 2017, 24(1): 1-17.

[3] Yiu S, Dashti M, Claussen H, et al. Wireless RSSI Fingerprinting Localization[J]. Signal Processing, 2017, 131: 235-244.

[4] Zhang G, Zhan X, Dan L. Research and Improvement on Indoor Localization Based on RSSI Fingerprint Database and *K*-Nearest Neighbor Points [C]//International Conference on Communications, Circuits and Systems. IEEE, 2013: 68-71.

[5] 何青春,沈树群. 基于 RSSI 的无线传感器网络节点定位算法[J]. 计算机工程与设计,2010,31(2):291-294.

[6] 刘玉龙. 基于 RSSI 的无线传感器网络定位算法的研究与实现[D]. 沈阳:沈阳航空航天大学,2017.

[7] 陈金星. 基于泰勒级数的无线传感器网络定位算法研究[D]. 北京:北方工业大学,2017.

[8] Gemayel N E, Jakel H, Jondral F K. A Hybrid TDOA/RSSD Geolocation System Using the Unscented Kalman Filter [C]// Vehicular Technology Conference. IEEE, 2014: 1-5.

[9] Wang W. Anti-Sybil Attack MPRR-RSSI Localization Algorithm in Wireless Sensor Networks[J]. Journal of Electronic Measurement and Instrumentation, 2016, 30(10): 1599-1605.

[10] 钱秋雅. 无线传感器网络中的 Sybil 攻击防御与检测技术研究[D]. 南京:南京邮电大学,2014.

[11] 朱颖,孙子文. 异构工业无线传感器网络的双层 Sybil 攻击检测方案[J]. 信息与控制,2018,47(1):41-47.

[12] Lohrasbipeydeh H, Gulliver T A, Amindavar H. Unknown Transmit Power RSSD Based Source Localization with Sensor Position Uncertainty[J]. IEEE Transactions on Communications, 2015, 63(5): 1784-1797.

[13] 李敏,罗挺,徐华. 一种基于参考节点选择模型的无线传感器网络定位算法[J]. 传感技术学报,2011,24(2):264-268.

[14] 孙佩刚,赵海,张文波,等. 普适计算中定位服务的参考点布置及选择算法[J]. 电子学报,2006,34(8):1456-1463.

[15] 魏叶华,李仁发,罗娟,等. 基于动态网格划分的移动无线传感器网络定位算法[J]. 计算机研究与发展,2008,45(11):1920-1927.

[16] 刘三阳,胡亚静,张朝辉. 基于 RSSI 测距的 DV-Hop 算法[J]. 控制与决策,2017,32(10):1900-1904.

[17] Zou T, Lin S, Li S. Blind RSSD-Based Indoor Localization with Confidence Calibration and Energy Control[J]. Sensors, 2016, 16(6): 788-813.

[18] Lohrasbipeydeh H, Gulliver T A, Amindavar H, et al. Efficient RSSD-Based Source Positioning with System Parameter Uncertainties[C]// Vehicular Technology Conference. IEEE, 2014: 1-4.

[19] 林绪森,王红军,王伦文. 一种改进的目标位置协同解算算法[J]. 小型微型计算机系统,2017,38(10):2216-2220.

[20] 罗臻. 抵御恶意攻击的无线传感网络安全定位算法研究[D]. 长沙:湖南大学,2015.

孙子文(1968-),女,四川大竹人,博士,教授,主要研究方向为模式识别、人工智能、无线传感网络理论与技术、信息安全,sunziwen@jiangnan.edu.cn;

朱 颖(1993-),女,江苏无锡人,在读硕士研究生,研究方向为工业无线传感器网络。