



(12)发明专利申请

(10)申请公布号 CN 105873065 A

(43)申请公布日 2016.08.17

---

(21)申请号 201610184752.7

(22)申请日 2016.03.28

(71)申请人 南京邮电大学

地址 210023 江苏省南京市栖霞区仙林大学城文苑路9号

(72)发明人 李鹏 余笑天 王汝传 徐鹤  
王晓艳 董璐 谢慧 彭徽  
陈艺婷

(74)专利代理机构 南京知识律师事务所 32207

代理人 汪旭东

(51)Int.Cl.

H04W 12/12(2009.01)

H04W 64/00(2009.01)

H04W 84/18(2009.01)

---

权利要求书2页 说明书8页 附图3页

(54)发明名称

基于信任度评估的无线传感网安全定位方法

(57)摘要

本发明提供一种基于信任度评估的无线传感网安全定位方法,为信任实体做出评估行为提供了定位属性集,定位属性集通过量化节点定位过程的关键行为表现从而得以用数值的形式给出信标节点的可信度,同时对阈值加以确定确保在滤除攻击节点的同时不至于影响正常节点的工作。当攻击节点侵入该系统时,随着信任关系的建立该攻击节点便被滤除不参与正常节点的定位过程。

1. 一种基于信任度评估的无线传感网安全定位方法,其特征在于,包括以下步骤:

步骤1:未知节点N<sub>1</sub>发出定位请求Loc\_req,其通信范围内的信标节点B<sub>1</sub>收到请求之后向未知节点发送回应Loc\_ack,N<sub>1</sub>成为模型中的源节点,收到Loc\_req信息的信标节点B<sub>1</sub>成为目标节点;

步骤2:B<sub>1</sub>收到节点N<sub>1</sub>的定位请求之后,向未知节点发送形如{id,(B\_x,B\_y),Distance\_BN}的信息包,其中id表示信标节点的id号,(B\_x,B\_y)表示该信标节点的坐标位置,Distance\_BN为该信标节点通过RSSI计算模型算得的信标节点距未知节点的距离信息;

步骤3:根据步骤1中信标节点提供的id号、坐标位置、距离信息,生成评价定位效果的标准即定位属性集,该定位属性集内有距离测量值、定位效果、信标节点位置检测、传输时间检测四大属性;

距离测量值函数p<sub>1</sub>为:

$$p_1(d) = \begin{cases} \frac{d}{d_0} & d \leq d_0 \\ \frac{d-d_0}{d_0} & d > d_0 \end{cases}$$

无线传感网WSN定位过程中,未知节点距离测量值与实际距离值的差值近似服从正态分布,且误差可由函数 $\sigma_N(d) = ae^{-\frac{(d-d_0)^2}{b^2}}$ 拟合, $\sigma_N(d)$ 是关于距离d的误差高斯函数,参数a、d<sub>0</sub>、b为常数,其中当d=d<sub>0</sub>时,在安全环境下的测量误差值达到最大;

定位效果属性值p<sub>2</sub>为:

$$p_2 = \begin{cases} \rho & \rho \leq \zeta \\ \zeta & \rho > \zeta \end{cases}$$

其中, $\rho^2 = \frac{\sigma_{sum}^2}{n} \leq \zeta^2$ , $\rho^2$ 表示均残差平方,n为参与节点定位的信标节点个数, $\zeta$ 为阈值, $\sigma_{sum}$ 为总定位残差;

信标节点位置检测的表达式为:

$$p_3 = \begin{cases} \frac{|diff(p, q, r, s, t)|}{\tau} & |diff(p, q, r, s, t)| \leq \tau \\ 1 & |diff(p, q, r, s, t)| > \tau \end{cases}$$

其中, $\tau$ 为常数,diff(p,q,r,s,t)=MAX(diff<sub>tn</sub>(p,q,r,s,t)),(n=1,2,3),表示不同时刻测量的关于函数diff<sub>tx</sub>(p,q,s)绝对值之差的最大值,diff<sub>tx</sub>(p,q,s)表示在tx时刻接收方p与发送方s之间的RSSI值与接受方q与发送方s之间的RSSI值之差的绝对值;

传输时间检测的可信度为:

$p_4 = \omega_1 \times p_{4\_1} + \omega_2 \times p_{4\_2}$ ,其中 $\omega_1$ 、 $\omega_2$ 分别为p<sub>4\\_1</sub>、p<sub>4\\_2</sub>的权重,p<sub>4\\_1</sub>为目标节点的处理时间观测值的评价函数,p<sub>4\\_2</sub>为源节点到目标节点的实测距离的可信度;

步骤4:确定阈值问题:

(1)在步骤3的定位效果属性值计算过程中,需确定最大定位误差, $MAX|d_i - \sqrt{(x_i-x)^2 + (y_i-y)^2}| \leq \varepsilon$

表示最大定位误差,其中( $x, y$ )表示未知节点的测量位置坐标,( $x_i, y_i$ )表示信标节点坐标, $d_i$ 表示信标节点*i*到未知节点的距离测量值; $\epsilon$ 表示为最大测距误差,通过多次取节点的实测距离值和RSSI计算值之间的最大偏差确定;

(2)在步骤3中用式 $\rho^2 = \frac{\sigma_{sum}}{n} \leq \zeta$ 量化信任模型属性集中的定位效果,对于阈值 $\zeta$ ,保证

正常节点的误差均方差落在阈值区间内,同时避免阈值过大使得恶意节点通过检测;

步骤5:未知节点收到信标节点信息包的同时,邻居节点根据步骤3中的定位属性集及其计算方法计算对信标节点的信任度并将该信任度广播到其他节点,未知节点分别根据邻居节点的信任度以及定位属性集的自身的计算方法计算间接可信度和向其发送数据包的信标节点直接信任度;

步骤6:根据式 $C = \alpha D_{index} + \beta M_{index}$ 计算未知节点对信标节点的综合信任度,其中 $D_{index}$ 、 $M_{index}$ 分别为源节点对目标节点的直接推荐度和推荐节点对目标节点的间接推荐度, $\alpha$ 、 $\beta$ 分别为直接推荐度、间接推荐度的权重系数;最后将信标节点的综合信任度进行排序并选取其中综合信任度最高的三个信标节点进行定位。

2. 如权利要求1所述的基于信任度评估的无线传感网安全定位方法,其特征在于,所述步骤2中,信标节点距未知节点的距离信息Distance\_BN为信标节点发送信息到未知节点的时间与信号传输速度的积。

3. 如权利要求1所述的基于信任度评估的无线传感网安全定位方法,其特征在于,所述步骤3中,通过误差高斯函数将实际误差值与安全环境下的理论最大误差值对比,初步排除含有攻击节点的无线传感网WSN里产生的具有较大误差的定位结果。

4. 如权利要求1所述的基于信任度评估的无线传感网安全定位方法,其特征在于,所述步骤3中,当均残差平方不大于阈值时,则认定此次定位效果是一致的,若超过阈值,则认定此次定位存在攻击节点。

5. 如权利要求1所述的基于信任度评估的无线传感网安全定位方法,其特征在于,所述步骤3中,任意两个接收端节点与发送端距离比值和RSSI比值的关系式为: $\frac{d_r^i}{d_r^j} = 10^{\frac{RSSI(d_r^i) - RSSI(d_r^j)}{10\lambda}}$ ,

其中,RSSI( $d$ )表示接收端距发送端 $d$ 处的信号强度, $C_0$ 为接收端距发送端单位距离处的信号强度参考值, $\lambda$ 是路径损失因子, $d_r^i$ 表示接收端节点*i*与发送端节点*r*的距离, $d_r^i$ 值恒定的情况下 $RSSI(d_r^i) - RSSI(d_r^j)$ 的差值稳定,如果该差值不稳定,则无线传感网WSN遭受女巫攻击。

6. 如权利要求1所述的基于信任度评估的无线传感网安全定位方法,其特征在于,所述步骤3中,如果未知节点到信标节点的信息传递时间超过预设值,则信标节点被入侵成为恶意节点,无线传感器WSN遭受攻击。

## 基于信任度评估的无线传感网安全定位方法

### 技术领域

[0001] 本发明涉及一种基于信任度评估的无线传感网安全定位方法,用于解决在无线传感网环境下的各种类型定位攻击问题,属于信息安全领域问题。

### 背景技术

[0002] 随着传感器技术、嵌入式技术、无线通信技术的快速发展迭代,由大量具有微处理能力的微型传感器节点组成的无线传感器网络(WSN)使得快速便捷地获取陆、海、空三位一体化信息成为可能。传统的传感器系统早在越战时期就已经走向了实用进程。美越双方在该时期丛林密布的“胡志明小道”战况焦灼,美军对当时的“胡志明小道”进行了多轮轰炸,却都收效甚微。之后,美军改而空投了2万多个“热带树”传感器。“热带树”型传感器实质上是震感以及声感两部分传感器构成的传感器系统,美军战机从半空予以投放,并最终触地插入泥土中,外界只能看到露在地表经过伪装的无线传感器天线,因此称其为“热带树”。当敌方车辆路过时,传感器节点采集到车辆经过造成震感和声音信息,该信息被传送到美军指挥中心,美军战机根据消息传送位置立即展开追杀,总共炸毁或炸坏4.6万辆卡车。

[0003] 早在上个世纪末,美国率先对无线传感网络进行了深入研究,发展至今无线传感网及周边相关技术已然成为目前学术界的一大研究热点。美国《商业周刊》和《技术评论》在一份针对现有技术在未来的发展前景报告中,同时将无线传感器网络评估为本世纪最有影响的技术及改变世界的技术之一。就目前来说,无线传感器网络已经引起了国防部门、商业界和学术界越来越多的关注。2005年8月,美国计算机学会(ACM)开始出版《ACM Transactions on Sensor Networks》,专门研究无线传感器网络问题。2007年的《IEEE Communications magazine》发表专辑,论述无线传感器网络的安全问题,同时,2007年的《IEEE Transactions on mobile computing》、《软件学报》和2008年的《通信学报》等国内外很多高水平杂志也出版专辑,论述WSN的相关问题。可以预计,WSN的发展和广泛应用,将对人们的社会生活和产业变革带来极大的影响并产生巨大推动。

[0004] 同时无线传感器网络在战场监督、目标跟踪、环境监测、燃料探测和智能交通系统等众多应用中,都存在一个共同特征,即对传感器节点位置信息的需求。因此在任何无线传感器网络中,节点的位置信息对理解应用背景都是至关重要的。并且由于无线传感器网络具有部署随机、网络拓扑易变化、自组网的特点,使得其定位过程更容易遭受各种攻击。事实上,缺乏有效的安全机制已经成为传感器网络应用的主要障碍。在传统网络中,网络安全需要解决信息的机密性、完整性、消息认证、入侵监测以及访问控制等问题,同样在无线传感器网络中,我们面临着相同的问题。但传感器网络自身的特点也决定了其安全研究的复杂性和独特性。其中就包括:资源受限我们很难将非对称密码体制应用到无线传感网中,存在一些多跳的无线通信方式增加了被攻击的几率,俘获攻击直接威胁到网络内部的安全通信。节点定位作为无线传感器网络应用的基础,其安全性与整个网络系统的安全性密切相关。

[0005] 安全定位技术的目的是保障节点获得高精度的位置信息,设计安全的节点定位机

制是节点完成定位任务的前提。

## 发明内容

[0006] 技术问题：定位作为无线传感器网络的关键支撑技术已被广泛研究，然而针对节点的定位问题研究还不够完善，并且这些方法多数关注于定位算法的能源有效性和定位精度，而对于定位算法另一项重要的性能评价标准—安全性，研究的较少。本发明针对无线传感网下的各类定位攻击提出一种基于信任度评估的安全定位方法，从而达到防御攻击的效果。

[0007] 技术方案：本发明的设计方案利用信任评估，提出无线传感器网络下的安全定位方法。该信任评估模型通过构建安全定位中所需的属性集，并明确了每个属性的具体定义、计算方法以及阈值选择问题，保证该模型能够有效抵御无线传感网下的多种攻击手段。

[0008] 本发明提供的基于信任度评估的无线传感网安全定位方法，包括以下步骤：

[0009] 步骤1：未知节点N<sub>1</sub>发出定位请求Loc\_req，其通信范围内的信标节点B<sub>1</sub>收到请求之后向未知节点发送回应Loc\_ack，N<sub>1</sub>成为模型中的源节点，收到Loc\_req信息的信标节点B<sub>1</sub>成为目标节点；

[0010] 步骤2：B<sub>1</sub>收到节点N<sub>1</sub>的定位请求之后，向未知节点发送形如{id,(B\_x,B\_y),Distance\_BN}的信息包，其中id表示信标节点的id号，(B\_x,B\_y)表示该信标节点的坐标位置，Distance\_BN为该信标节点通过RSSI计算模型算得的信标节点距未知节点的距离信息；

[0011] 步骤3：根据步骤1中信标节点提供的id号、坐标位置、距离信息，生成评价定位效果的标准即定位属性集，该定位属性集内有距离测量值、定位效果、信标节点位置检测、传输时间检测四大属性；

[0012] 距离测量值函数p<sub>1</sub>为：

$$[0013] p_1(d) = \begin{cases} \frac{d}{d_0} & d \leq d_0 \\ \frac{d-d_0}{d_0} & d > d_0 \end{cases}$$

[0014] 无线传感网WSN定位过程中，未知节点距离测量值与实际距离值的差值近似服从正态分布，且误差可由函数 $\sigma_N(d) = ae^{-\frac{(d-d_0)^2}{b^2}}$ 拟合， $\sigma_N(d)$ 是关于距离d的误差高斯函数，参数a、d<sub>0</sub>、b为常数，其中当d=d<sub>0</sub>时，在安全环境下的测量误差值达到最大；

[0015] 定位效果属性值p<sub>2</sub>为：

$$[0016] p_2 = \begin{cases} \rho, & \rho \leq \zeta \\ \zeta, & \rho > \zeta \end{cases}$$

[0017] 其中， $\rho^2 = \frac{\sigma_{sum}^2}{n} \leq \zeta^2$ ， $\rho^2$ 表示均残差平方，n为参与节点定位的信标节点个数， $\zeta$ 为阈值， $\sigma_{sum}$ 为总定位残差；

[0018] 信标节点位置检测的表达式为：

$$[0019] \quad p_3 = \begin{cases} \frac{|diff(p, q, r, s, t)|}{\tau} & |diff(p, q, r, s, t)| \leq \tau \\ 1 & |diff(p, q, r, s, t)| > \tau \end{cases},$$

[0020] 其中,  $\tau$  为常数,  $diff(p, q, r, s, t) = \text{MAX}(diff_{tn}(p, q, r, s, t))$ , ( $n=1, 2, 3$ ), 表示不同时刻测量的关于函数  $diff_{tx}(p, q, s)$  绝对值之差的最大值,  $diff_{tx}(p, q, s)$  表示在  $tx$  时刻接收方  $p$  与发送方  $s$  之间的 RSSI 值与接受方  $q$  与发送方  $s$  之间的 RSSI 值之差的绝对值;

[0021] 传输时间检测的可信度为:

[0022]  $p_4 = \omega_1 \times p_{4\_1} + \omega_2 \times p_{4\_2}$ , 其中  $\omega_1, \omega_2$  分别为  $p_{4\_1}, p_{4\_2}$  的权重,  $p_{4\_1}$  为目标节点的处理时间观测值的评价函数、 $p_{4\_2}$  为源节点到目标节点的实测距离的可信度;

[0023] 步骤4: 确定阈值问题:

[0024] (1) 在步骤3的定位效果属性值计算过程中, 需确定最大定位误差,

$MAX \left| d_i - \sqrt{(x_i - x)^2 + (y_i - y)^2} \right| \leq \epsilon$  表示最大定位误差, 其中  $(x, y)$  表示未知节点的测量位置坐标,  $(x_i, y_i)$  表示信标节点坐标,  $d_i$  表示信标节点  $i$  到未知节点的距离测量值;  $\epsilon$  表示为最大测距误差,  $\epsilon$  通过对  $d_0$  处多次取节点的实测距离值和 RSSI 计算值之间的最大偏差来确定;

[0025] (2) 在步骤3中用式  $\rho^2 = \frac{\sigma_{sum}}{n} \leq \zeta$  量化信任模型属性集中的定位效果, 对于阈值  $\zeta$ ,

保证正常节点的误差均方差落在阈值区间内, 同时避免阈值过大使得恶意节点通过检测即可;

[0026] 步骤5: 未知节点收到信标节点信息包的同时, 邻居节点根据步骤3中的定位属性集及其计算方法计算对信标节点的信任度并将该信任度广播到其他节点, 未知节点分别根据邻居节点的信任度以及定位属性集的自身的计算方法计算间接可信度和向其发送数据包的信标节点直接信任度;

[0027] 步骤6: 根据式  $C = \alpha D_{index} + \beta M_{index}$  计算未知节点对信标节点的综合信任度, 其中  $D_{index}, M_{index}$  分别为源节点对目标节点的直接推荐度和推荐节点对目标节点的间接推荐度,  $\alpha, \beta$  分别为直接推荐度、间接推荐度的权重系数; 最后将信标节点的综合信任度进行排序并选取其中综合信任度最高的三个信标节点进行定位。

[0028] 所述步骤2中, 信标节点距未知节点的距离信息  $Distance\_BN$  为信标节点发送信息到未知节点的时间与信号传输速度的积。

[0029] 所述步骤3中, 通过误差高斯函数将实际误差值与安全环境下的理论最大误差值对比, 初步排除含有攻击节点的无线传感网 WSN 里产生的具有较大误差的定位结果。

[0030] 所述步骤3中, 当均残差平方不大于阈值时, 则认定此次定位效果是一致的, 若超过阈值, 则认定此次定位存在攻击节点。

[0031] 所述步骤3中, 任意两个接收端节点与发送端距离比值和 RSSI 比值的关系式为:

$$\frac{d_r^i}{d_r^j} = 10^{\frac{RSSI(d_r^i) - RSSI(d_r^j)}{10\lambda}}, \text{ 其中, } RSSI(d) \text{ 表示接收端距发送端 } d \text{ 处的信号强度, } C_0 \text{ 为接收端距发}$$

送端单位距离处的信号强度参考值,  $\lambda$  是路径损失因子,  $d_r^i$  表示接收端节点  $i$  与发送端节点  $r$  的距离,  $d_r^i$  值恒定的情况下  $RSSI(d_r^i) - RSSI(d_r^j)$  的差值稳定, 如果该差值不稳定, 则无线传感网 WSN

遭受女巫攻击。

[0032] 所述步骤3中,如果未知节点到信标节点的信息传递时间超过预设值,则信标节点被入侵成为恶意节点,无线传感器WSN遭受攻击。

[0033] 有益效果:本发明利用对属性集中各属性的定义及计算为信任实体对另一实体的主观评价提供了量化途径,并通过对属性计算中的阈值问题研究确保该发明有效抵御攻击节点的同时不至于剔除正常节点参与定位过程。下面进行具体说明。

[0034] 安全性:通过仿真实验验证该方法的抵御攻击节点能力,将实验场景设置为 $100m \times 100m$ 正方形场景,将100个未知节点布置于该场景内,其中20为信标节点,通信半径为20m,通信模型:Regular Model,网络的平均连通度为11.14,网络的邻居信标节点平均数目为:2.28。图5为正常节点分布图,其中红色\*表示信标节点,蓝色0表示未知节点。图6为含有攻击节点的分布图,其中红色\*表示信标节点,黑色\*表示攻击节点,蓝色0表示未知节点。图7是遭受攻击情况下的误差图,其中信标节点不存在定位误差用红色\*表示,攻击节点用黑色\*表示,蓝色0表示未知节点的估计位置,蓝色-表示这些节点的估计位置到真实位置的误差。图8是基于信任关系的安全定位方法下的误差图,且各个节点的标示与图7相同。

[0035] 通信开销:在网络初始化时,由于各节点之间的信任关系并不确定,各节点之间的信息包发送比较频繁。随着定位的进行,各未知节点对信标节点的信任度逐渐确定,通信开销逐渐下降,当网络中所有信标节点信任度全部确定之后,该方法的信任度计算方面通信开销降为0。当有新节点加入网络,其附近区域的局部通信开销重复上述过程。因此本发明保证了网络的大部分时间下的低通信开销。

[0036] 定位精度:本发明中,未知节点评价信标节点信任度中存在距离测量值以及定位效果这两项属性值。这两项内容不仅保证了未知节点剔除攻击节点同时保证节点优先选择距离本地近以及定位效果好的信标节点,同时,针对一些将已定位的未知节点转换为信标节点的定位算法来说,对于新信标节点的这两项属性值的计算可界定该信标节点是否参与定位计算,从而保证了定位误差不会累积扩散。

## 附图说明

- [0037] 图1是信任关系链;
- [0038] 图2是Sybil攻击下的WSN定位模型;
- [0039] 图3是节点信息通信过程;
- [0040] 图4是基于信任评估的定位框架示意图;
- [0041] 图5是正常节点分布图;
- [0042] 图6是加入攻击节点的分布图;
- [0043] 图7是遭受攻击情况下的误差图;
- [0044] 图8是基于信任关系的安全定位方法下的误差图。

## 具体实施方式

[0045] 由于传感器节点的自身限制决定了安全定位算法本身不可能有像传统网络里的攻击防御手段具有的完备性,同时针对攻击手段的多样性,针对无线传感网的安全定位算法要兼具可用性和完整性。目前根据这些特征,安全定位算法分为三大类:(1)基于鲁棒观

测计算的安全定位策略;(2)基于恶意信标节点隔离的安全定位策略;(3)基于位置校验的安全定位策略。

[0046] 本发明采用了第一类算法下的基于容忍攻击的安全定位算法,该算法较之其余算法有以下几点优势:(1)基于容忍攻击的安全定位算法有应对的攻击类型较广,防御成功率及最大攻击节点数量容忍度高的特点。其它类型算法普遍存在仅针对特定攻击方式有效,难以抵御合谋攻击,漏检或误将正常节点定为攻击节点等情况。(2)该算法能够有效防御内部攻击,其它算法针对内部攻击不具备或者具备较低的防御攻击能力。

[0047] 本发明所提出的基于信任度评估的无线传感网安全定位方法依赖于信任计算模型,该模型中的信任指的是一个实体依据各类属性的计算得出的关于另一对等实体的主观意见,其中的主观意见包括数据以及路径可靠性判断、节点处理能力评估等对各类影响无线传感网服务质量的因素的评价。目前的信任计算模型包括两大类分别是:(1)基于策略的信任管理,(2)基于声誉的信任管理。第一类信任模型的建立需要安全策略和安全证书因此该类模型需要完全可信的第三方发布证书和密钥,这对于资源和计算能力的传感器节点而言很难胜任并且由于其集中式的信任管理同时带来了安全隐患。因此本发明采用第二类信任关于方式,实体通过计算其他实体的声誉值来判断该实体节点是否可信,其中可信度包括直接可信以及间接可信两大类组成。

[0048] 对于信任评估模型,本发明先给出了一些针对信任度以及模型中各类节点的描述性定义:

[0049] 定义1 综合信任度:在无线传感网中,信任是待测节点根据信标节点的定位误差、定位耗时等行为表现,而对其定位所需信标节点提供的定位信息的采纳程度。

[0050] 定义2 直接信任度:在一定的上下文环境中,未知节点通过信任评估模型给予直接参与定位之信标节点的信用评价。

[0051] 定义3 间接信任度:在一定的上下文环境中,表示未知节点通过第三者实体节点的间接推荐形成对目标信标节点的信任评价。

[0052] 定义4 间接可信度:在一定的上下文环境中,间接信任度评估中所涉及的第三者实体节点自身的信任度。

[0053] 定义5 源节点:无线传感网中的待测节点。

[0054] 定义6 目标节点:无线传感网中待测节点定位所需的信标节点。

[0055] 定义7 推荐节点:信任评估模型中信任度计算过程中除去源节点和目标节点之外的其他节点。

[0056] 节点各类信任度之间的关系如图1所示。

[0057] 本发明提供的基于信任度评估的无线传感网安全定位方法具体流程如下:

[0058] 步骤1:未知节点N<sub>1</sub>发出定位请求Loc\_req,其通信范围内的信标节点B<sub>1</sub>收到请求之后向未知节点发送回应Loc\_ack,N<sub>1</sub>成为模型中的源节点,收到Loc\_req信息的信标节点B<sub>1</sub>成为目标节点。

[0059] 步骤2:B<sub>1</sub>收到节点N<sub>1</sub>的定位请求之后,向未知节点发送形如{id,(B\_x,B\_y),Distance\_BN}的信息包。其中id表示信标节点的id号,(B\_x,B\_y)表示该信标的坐标位置,Distance\_BN为该信标节点通过RSSI计算模型算得的信标节点距未知节点的距离信息。Distance\_BN可通过信标节点发送信息到未知节点的时间与信号传输速度的积计算得到。

[0060] 步骤3:根据上一步骤中信标节点提供的标号、位置、距离等信息,该信任评估模型生成评价定位效果的标准即定位属性集,如下所示:

[0061] (1)距离测量值

[0062] 因无线传感网WSN定位过程中,未知节点距离测量值与实际距离值的差值近似服从正态分布,且该误差可由函数  $\sigma_N(d) = ae^{-\frac{(d-d_0)^2}{b^2}}$  拟合,  $\sigma_N(d)$  是关于距离  $d$  的误差高斯函数,参数  $a, d_0, b$  为常数,可由多次试验仿真训练所得。其中当  $d=d_0$  时,在安全环境下的测量误差值达到最大,由此,我们定义属性  $p_1$  是关于距离测量值的函数如下所示:

$$[0063] p_1(d) = \begin{cases} \frac{d}{d_0} & d \leq d_0 \\ \frac{d-d_0}{d_0} & d > d_0 \end{cases}$$

[0064] (2)定位效果

[0065] 定义8 令集合  $R = \{(x_1, y_1, d_1), (x_2, y_2, d_2), \dots, (x_i, y_i, d_i), \dots, (x_n, y_n, d_n)\}$  为未知节点定位参考集,  $(x_i, y_i)$  表示信标节点  $i$  的坐标,  $d_i$  表示信标节点  $i$  到未知节点的距离测量值。

[0066] 定义9 总定位残差:表示一次定位过程中,每个信标节点的定位残差总和。残差指的是在选定一个定位参考集  $R$  的环境下,信标节点  $x_i$  的距离测量值与定位距离值的偏差。总定位残差定义如下式所示:

$$[0067] \sigma_{sum} = \sum_{i=1}^n \left| \sqrt{(x-x_i)^2 + (y-y_i)^2} - d_i \right|,$$

[0068] 将定位效果的一致性以残差的形式表现出来,这为信任模型属性集中的定位效果属性值提供了量化的途径,为此我们定义式  $\rho^2 = \frac{\sigma_{sum}}{n} \leq \zeta$ , 其中  $\rho$  表示均残差,  $\rho^2$  表示均残差平方,  $n$  为参与节点定位的信标节点个数,  $\zeta$  为阈值。当均残差平方不大于阈值时,可以认为此次定位效果是一致的,若超过阈值,则可认为此次定位存在攻击节点。定义定位效果属性值  $p_2$  为:

$$[0069] p_2 = \begin{cases} \frac{\rho}{\zeta}, & \rho \leq \zeta \\ 0, & \rho > \zeta \end{cases};$$

[0070] (3)信标节点位置检测

[0071] 根据以上属性值计算出的节点综合信任度可以过滤大部分的攻击形式,但是对于 Sybil 攻击,以上属性值的检测手段并不足以排除攻击节点。

[0072] 在无线传感网WSN定位过程中,若信标节点遭受Sybil攻击,则将会以不同ID身份向未知节点发送定位信息,以此扰乱定位过程从而出现定位结果频繁刷新或与实际位置误差巨大等问题,Sybil攻击下的定位模型如图2所示。令RSSI( $d$ )表示接收端距发送端  $d$  处的信号强度,  $C_0$  为接收端距发送端单位距离处的信号强度参考值,  $\lambda$  是路径损失因子。

[0073] 根据该衰减模型推导出任意两接受端节点与发送端距离比值和RSSI比值符合如下的关系式:

$$[0074] \quad \frac{d_r^i}{d_r^j} = 10^{\frac{RSSI(d_r^i) - RSSI(d_r^j)}{10\lambda}},$$

[0075] 其中  $d_r^i$  表示接收端节点 i 与发送端节点 r 的距离, 根据该值稳定可得出等式右边保持稳定, 所以理论情况下在接收端与发送端节点的距离位置不变的情况下 RSSI 差值保持稳定。可根据实际环境下该差值是否恒定判断该 WSN 是否遭受女巫攻击。因此令  $diff(p, q, r)$  表示接收方 p 与发送方 r 之间的 RSSI 值与接受方 q 与发送方 r 之间的 RSSI 值之差的绝对值。在 t1 时刻我们选取源节点 p 作为接收方, 任意选择 p 附近另两个未知节点 q 和未知节点 r 作为另一接收方。同时选取两信标节点 s, t 作为发送方。在之后的 t2, t3 时刻同样选取这些节点并检测 RSSI 值。其中  $|diff_{t1}(p, q, s) - diff_{t1}(p, q, t)|$  表示在 t1 时刻, 节点 p、节点 q 分别与节点 s 的 RSSI 差值和节点 p、节点 q 分别与节点 t 的 RSSI 差值之间的绝对值。

[0076] 同时令:

[0077]  $diff_{t1}(p, q, r, s, t) = \max(|diff_{t1}(p, q, s) - diff_{t1}(p, q, t)|, |diff_{t1}(q, r, s) - diff_{t1}(q, r, t)|, |diff_{t1}(p, r, s) - diff_{t1}(p, r, t)|)$  且  $diff_{t2}(p, q, r, s, t) = \max(|diff_{t2}(p, q, s) - diff_{t2}(p, q, t)|, |diff_{t2}(q, r, s) - diff_{t2}(q, r, t)|, |diff_{t2}(p, r, s) - diff_{t2}(p, r, t)|)$ 、 $diff_{t3}(p, q, r, s, t) = \max(|diff_{t3}(p, q, s) - diff_{t3}(p, q, t)|, |diff_{t3}(q, r, s) - diff_{t3}(q, r, t)|, |diff_{t3}(p, r, s) - diff_{t3}(p, r, t)|)$ 。

[0078] 则可定义  $diff(p, q, r, s, t) = \max(diff_{tn}(p, q, r, s, t))$ , ( $n=1, 2, 3$ ), 其表示不同时刻测量的关于函数  $diff_{tx}(p, q, s)$  绝对值之差的最大值, 下式为该属性值的表达式:

$$[0079] \quad p_3 = \begin{cases} \frac{|diff(p, q, r, s, t)|}{\tau} & |diff(p, q, r, s, t)| \leq \tau \\ 1 & |diff(p, q, r, s, t)| > \tau \end{cases};$$

[0080] (4) 传输时间检测

[0081] 在无线传感网 WSN 定位环境下, 主要的攻击手段有: 重放攻击、Sybil 攻击、虫洞攻击等。在上述攻击手段中, 由于恶意节点需要篡改、重放信息以及更多的通信代价使得未知节点与恶意节点之间信息传输时间增加。在这个过程中如果目标节点被入侵成为恶意节点, 则恶意节点处理信息所耗费时间必然长于普通节点。因此可通过判别定位所需时间是否合理作为该节点是否遭受攻击的标准, 节点通信过程与时间的关系如图 3 所示。根据图 3 的模型可知目标节点的处理时间观测值为  $T_a = t_3 - t_2$ 。当我们观测  $T_a$  的时, 可以知道真实值  $T_b$  的概率密度分布是以  $T_b$  为均值,  $\sigma^2$  为方差的正态分布, 根据克拉美-罗界理论我们得出了目标节点的处理时间观测值的评价函数:

$$[0082] \quad p_{4-i} = \begin{cases} \frac{1}{-E\left[\frac{\partial^2 l(x)}{\partial^2 T_b^2}\right] \times \text{var}(\theta)} & \\ \end{cases},$$

[0083] 由图 3 可得信息从源节点发送至目标节点的时间为  $T_{time\_cost} = ((t_4 - t_1) - (t_3 - t_2)) / 2$ , 再由信号传输速度  $V_{RSSI}$  可得距离  $d_{acco\_to\_time} = T_{time\_cost} * V_{RSSI}$ 。由此我们得出了实测距离的可信度  $p_{4-i} = \frac{d_{acco\_to\_time}}{d}$ , 其中 d 表示为实测距离。

[0084] 根据 $p_{4\_1}$ 以及 $p_{4\_2}$ 的推导,我们相继得到了目标节点的处理时间观测值的评价函数和实测距离的可信度,这两组根据时间得出可信度综合起来成为基于时间检测的可信度如下式所示:

[0085]  $p_4 = \omega_1 \times p_{4\_1} + \omega_2 \times p_{4\_2}$

[0086] 其中 $\omega_1$ 、 $\omega_2$ 分别为 $p_{4\_1}$ 、 $p_{4\_2}$ 的权重。

[0087] 步骤4:确定阈值问题。

[0088] (1)定义10:节点的距离观察值与实际值之间的误差近似服从正态分布,在靠近信标节点处,随着距离的增大而增大。

[0089] 在步骤3的定位效果属性值计算过程中,需要确定最大定位误差问题,该问题中可用 $\text{MAX} |d_i - \sqrt{(x_i - x)^2 + (y_i - y)^2}| \leq \varepsilon$ 表达最大误差,其中 $(x, y)$ 表示未知节点的测量位置坐标, $(x_i, y_i)$ 表示信标节点坐标, $d_i$ 表示信标节点*i*到未知节点的距离测量值。这里我们需要讨论的是阈值 $\varepsilon$ , $\varepsilon$ 表示为最大测距误差。

[0090] 根据定义10可知定位误差服从正态分布即: $d_E \sim N(0, \sigma^2)$ ,对于正态分布第二参数的确定可由 $\sigma$ 与距离 $d$ 的关系近似于高斯函数得出 $\sigma(d) = ae^{-\frac{(d-d_0)^2}{b^2}}$ 。

[0091] 根据以上分析可知当未知节点距信标节点 $d_0$ 时,距离误差的标准差取得最大值。因此对于无障碍物的情况下阈值 $\varepsilon$ 的确定,可以对 $d_0$ 处多次取节点的实测距离值和RSSI计算值之间的最大偏差。

[0092] (2)同样在步骤3中用式 $\rho^2 = \frac{\sigma_{sum}}{n} \leq \zeta$ 量化信任模型属性集中的定位效果,对于阈值 $\zeta$ ,我们可根据莱维(Levy)一林德伯格(Lindeberg)中心极限定理结合标准正态分布表结合应用场景设置适当值,保证正常节点的误差均方差落在阈值区间内,同时避免阈值过大使得恶意节点通过检测。

[0093] 步骤5:未知节点收到信标节点信息包的同时邻居节点根据上一步骤中的属性集及其计算方法计算对信标节点的信任度并将该信任度广播到其他节点,未知节点根据邻居节点的信任度计算间接可信度。

[0094] 步骤6:未知节点根据属性集的计算方式给出向其发送数据包的信标节点直接信任度。

[0095] 步骤7:根据式 $C = \alpha D_{index} + \beta M_{index}$ 计算未知节点对信标节点的综合信任度,其中 $D_{index}, M_{index}$ 分别为源节点对目标节点的直接推荐度和推荐节点对目标节点的间接推荐度。 $\alpha, \beta$ 分别为两种不同推荐度的权重系数,信任度计算总体框架图如图4所示。

[0096] 步骤8:计算信标节点的综合信任度并进行排序选取其中综合信任度最高的三个信标节点进行定位。

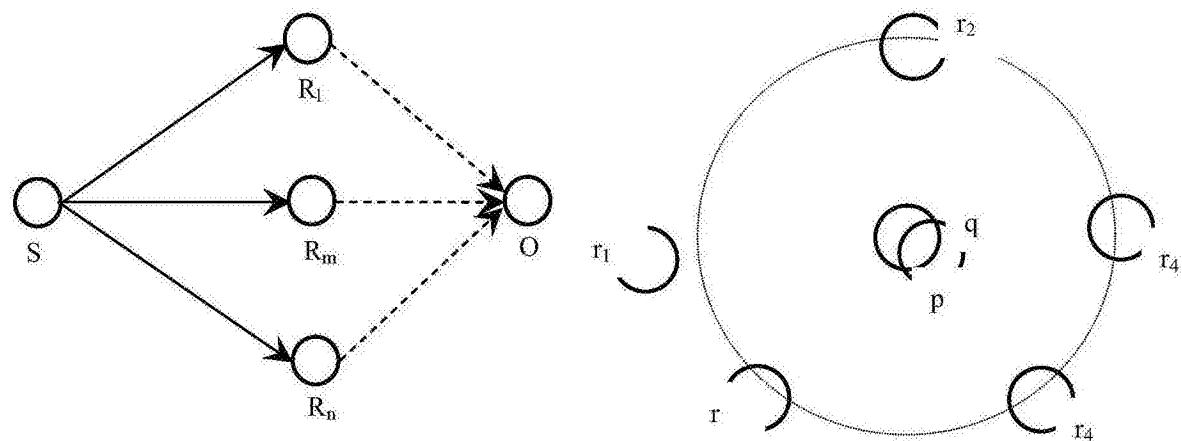


图1

图2

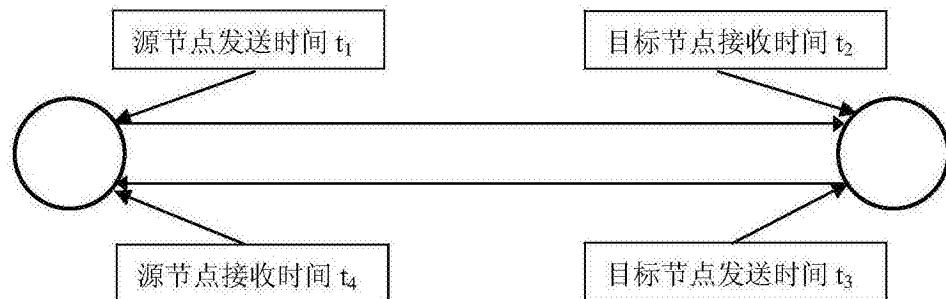


图3

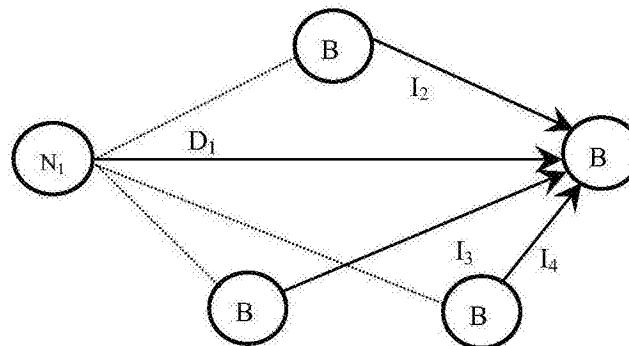


图4

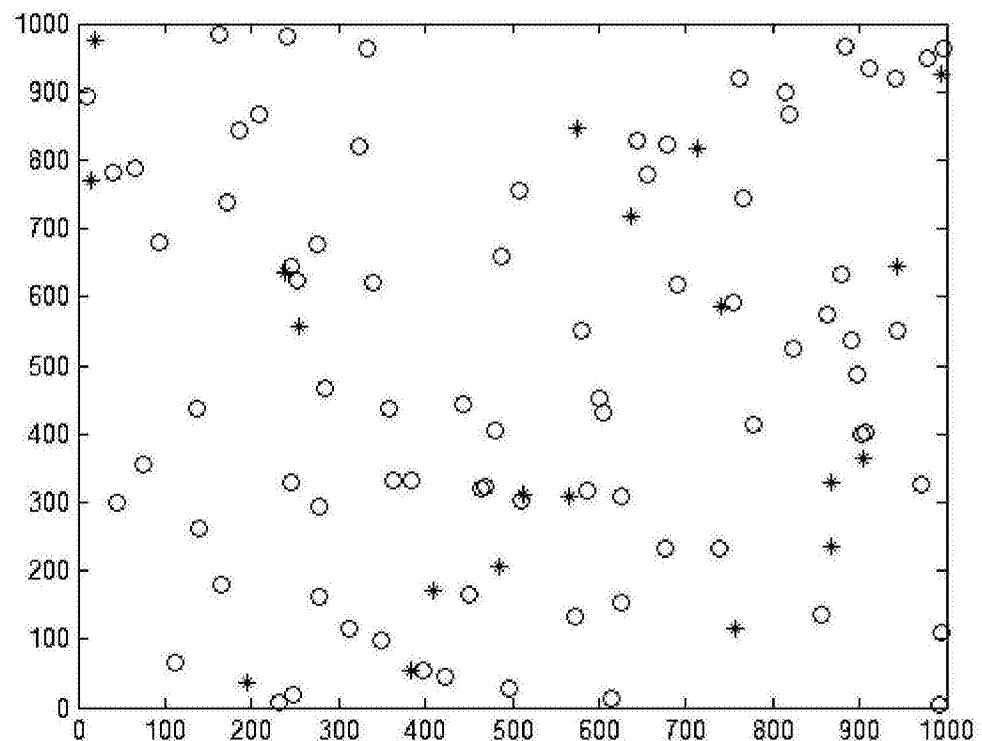


图5

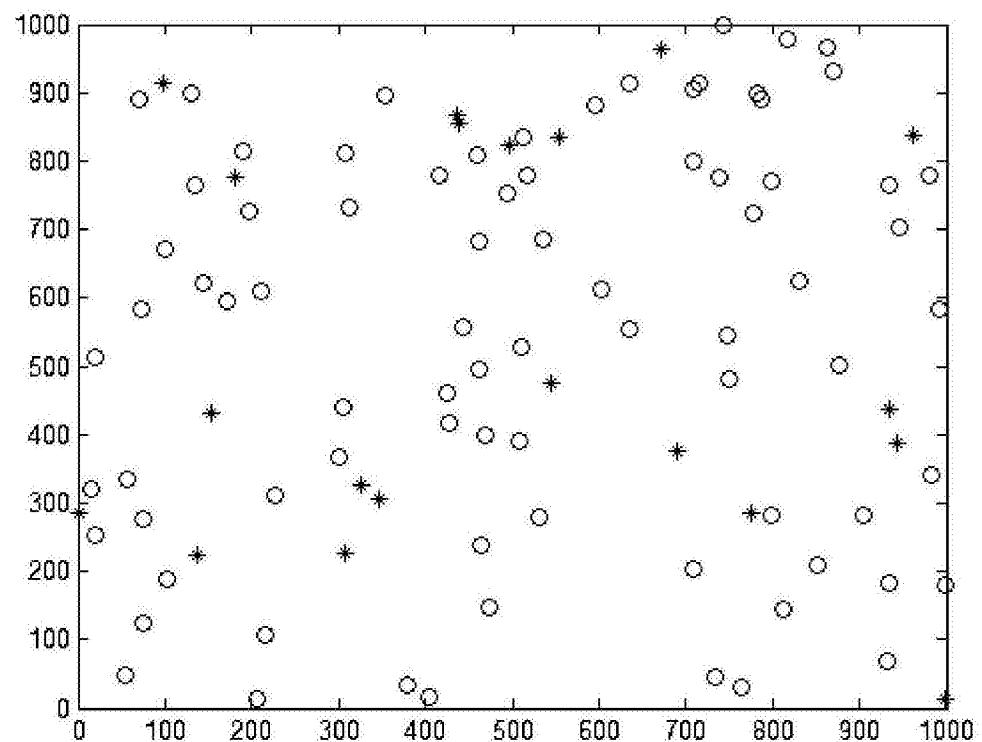


图6

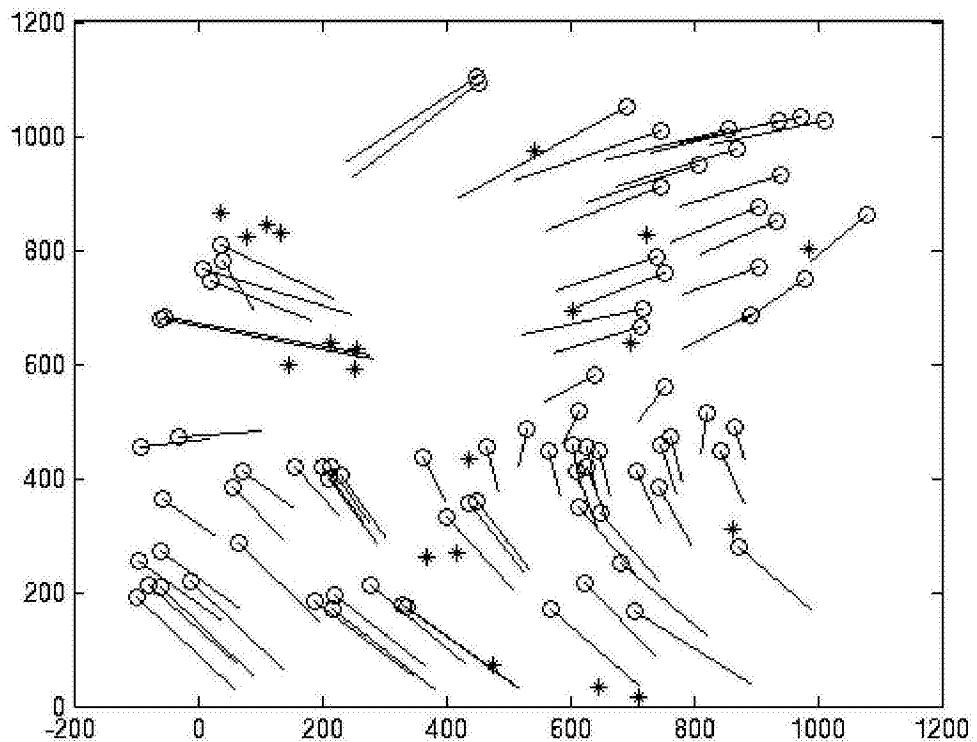


图7

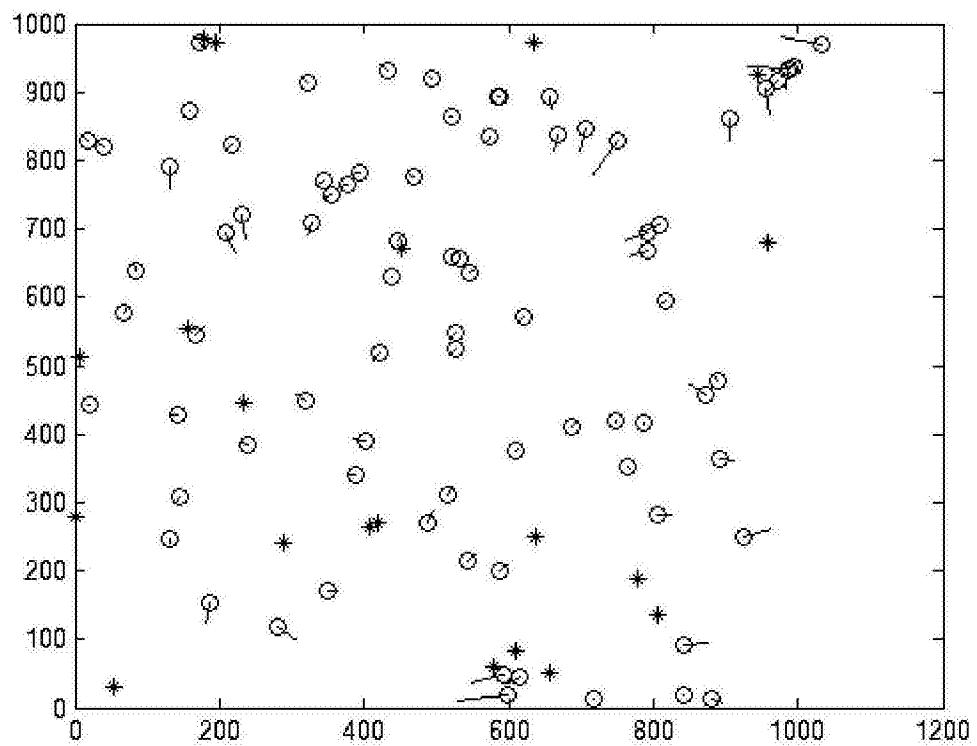


图8