计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2019.20170660
56(6): 1231-1243, 2019

无线传感器网络节点位置验证框架

苗春雨[1] 陈丽娜[2] 吴建军[2] 周家庆[2] 冯旭杭[1]
[1](杭州安恒信息技术股份有限公司 杭州 310051)
[2](浙江师范大学网络应用安全研究中心 浙江金华 321004)
(Crain.miao@dbappsecurity.com.cn)

Node Location Verification Framework for WSN

Miao Chunyu[1], Chen Lina[2], Wu Jianjun[2], Zhou Jiaqing[2], and Feng Xuhang[1]
[1](*Hangzhou Anheng Information Technology Co. LTD, Hangzhou* 310051)
[2](*Research Center of Network Application Security, Zhejiang Normal University, Jinhua, Zhejiang* 321004)

Abstract Localization is one of the pivot technologies in wireless sensor networks. The traditional node localization schemes consider that the locations of anchors are reliable, which makes these schemes are invalid in some scenarios with unreliable anchors such as drifted anchors, fake anchors and malicious anchors. Aiming at solving this problem mentioned above, a distributed and lightweight node location verification framework (NLVF) is proposed. NLVF offers location verification service as an underlying technic for the traditional localization algorithms, including range-based localization algorithm and the range-free localization algorithm. NLVF can filter out these unreliable anchors by which the application area of traditional localization algorithms is enlarged. UNDA (unreliable node detection algorithm) is the key algorithm of NLVF. It constructs location reputation model based on mutual distance observation between neighbors in WSN. UNDA algorithm improves the localization reliability by filtering out these anchors with inferior location reputations. Extensive experiments are conducted to evaluate the performance of UNDA. Results show that NLVF is adapted to both of range-based and range-free localization schemes. It works better in the presence of three kinds of unreliable anchors. So, it yields general applicability. In addition, UNDA relatively has high accuracy, and the average success rate of detection is more than 95%, so NLVF yields significant practicability.

Key words wireless sensor network (WSN); node localization; reliable localization; node location verification; distributed reputation model

摘 要 节点定位是无线传感器网络(wireless sensor network, WSN)关键支撑技术之一,传统的定位算法均假设信标节点位置是可靠的,导致其无法应用于存在信标漂移、虚假信标和恶意信标的场景.针对上述问题,提出一种分布式轻量级的节点位置验证框架(node location verification framework,

收稿日期:2017-09-12;**修回日期**:2018-11-13
基金项目:国家自然科学基金项目(61502431,61379023);浙江省计算机科学与技术重中之重学科(浙江师范大学)基金项目(ZC323014074);浙江省科技厅公益性技术应用研究计划基金项目(2015C33060)
This work was supported by the National Natural Science Foundation of China (61502431, 61379023), the Opening Fund of Zhejiang Provincial Top Key Discipline of Computer Science and Technology at Zhejiang Normal University (ZC323014074), and the Zhejiang Provincial Science Technology Department Public Welfare Technology Application Research Project (2015C33060).
通信作者:冯旭杭(colin.feng@dbappsecurity.com.cn)

NLVF),作为底层框架为传统的2类定位算法(基于测距的定位算法与非测距定位算法)提供信标位置验证服务,以过滤位置不可靠的信标扩展传统定位算法的应用范畴.节点位置验证的核心算法UNDA (unreliable node detection algorithm)是基于节点相互距离观测结果建立位置信誉模型,在定位过程中排除位置信誉较低的信标,以提高定位结果的可靠性.实验结果表明,NLVF可服务于基于2类测距技术的定位算法,且适用于存在3种不可靠信标的场景,具有普适性;UNDA算法具有较高的检测性能,平均检测成功率在95%以上,NLVF具有较高的可用性.

关键词 无线传感器网络;节点定位;可信定位;节点位置验证;分布式信誉模型

中图法分类号 TP391

无线传感器网络(wireless sensor networks, WSNs)是物联网(Internet of things, IOT)的重要组成部分[1].节点定位技术则是WSN中重要的支撑技术之一,大量场景中缺少位置的感知数据是无意义的[2],且诸如基于地理位置的路由、拓扑控制和节点部署等技术均以节点的相对或绝对位置为基础[3-4].学者们从不同的方法论角度出发,提出了大量的WSN节点定位算法[5],这些算法通常由网络中的信标节点为普通节点的定位过程提供位置参考,以估算其绝对地理位置.最常见的节点定位技术分类方法是按照定位过程是否需要测量节点间的距离分为测距(range-based)算法和非测距(range-free)算法2类[6].在实际应用场景中,信标节点提供的位置参考并不总是可靠的[7],而传统的定位算法不考虑信标提供的位置参考信息可靠性问题,导致众多性能表现优异的节点定位算法无法适用于信标位置不可靠的场景[8].为解决位置不可靠的信标节点带来的定位精度下降导致网络服务质量降低的问题,提出一种适用于2类定位算法的轻量级信标位置验证方法,作为底层框架(无须采集原定位算法所需的额外参数,同时具有可重用性),对传统定位算法提供不可靠信标过滤服务,以扩展传统算法的应用范畴.据作者所知,在节点位置验证方面的已有工作,很少在纵向上将3类不可靠信标和横向上的2种测距技术进行统一考虑.

本文的主要贡献有3方面:

1) 提出了一种适用于多种不可靠信标节点共存的节点位置验证框架,为实现可靠的定位提供底层服务;

2) 提出的框架支持测距和非测距2类传统节点位置算法,具有较好的普适性;

3) 节点可信定位框架利用了群智感知信誉模型,具有轻量级分布式的特点,适合大规模的、计算能力有限的无线传感器网络应用场景.

1 相关工作

针对信标位置不可靠问题展开的WSN节点位置验证方法可分为2类:1)漂移信标和恶意信标方面的研究;2)针对定位过程的重放攻击(以虫洞攻击为代表)方面的研究.

以漂移信标和恶意信标为主要研究目标的研究工作分为可容忍测距异常值的算法[9]及带有可靠信标选择的定位算法[10].前者比较适用于存在测距信息干扰和信标移动距离较小的场景.这类算法的主要思想是降低不可靠信标的定位参考作用,但当参考位置误差较大时,算法的定位精度严重下降.可靠信标选择即对位置不可靠的信标进行过滤,以排除其对定位过程的影响.文献[11]提出一种可以应用于任何测距技术的点对点位置验证算法,但需要配备GPS的节点作为校验节点,文献[12]也采用类似的方法,由AP节点进行集中式的节点位置校验,以实现可信的定位.文献[13]提出基于Huber损失函数的恶意信标节点检测算法,具有高效且轻量级的特点,属于可信的测距定位算法.He等人[14]则提出一种应用于到达时间(time of arrival, TOA)测距技术的、可排除异常测距值的可信定位算法;而文献[15]中提出的恶意信标过滤机制也是基于TOA或到达时间差(time difference of arrival, TDOA)测距技术,采用每个节点在自己的视角通过准确地测距构建局部坐标一致集,通过对局部坐标一致集的合并,排除恶意信标.而对接收信号强度指标(received signal strength indication, *RSSI*)测距技术,由于其测距本身的误差,对可信定位算法的设计带来更大的挑战.Kuo等人[16]提出的信标移动检测算法(beacon movement detection, BMD),主要用来识别网络中的部分位置发生被动改变的信标节点.其思路为:在网络中设置一个BMD引擎来收集

全网络的 *RSSI* 信息并进行处理,在一定容错范围内能够识别出信标节点的位置是否已发生移动.但集中式的算法因其计算量较大,且在信息收集阶段产生大量的通信开销,不适用于由随机撒播部署的网络连通度较高、规模较大的 WSN 网络;也有一些集中式的算法,采用隐藏的位置校验节点对信标位置进行验证[17],由于需要额外的可信节点作为检验者,导致其普适性不高.文献[18-19]运用图论中的刚性理论作为节点间相互位置的基本原理,用于排除定位过程中的位置参考异常值,确保节点定位的可信性,但此类方法运算量较大,且刚性理论对节点间测距精度有很高的要求.Garg 等人[20]采用识别和排除在节点定位算法收敛过程中提供了较大下降梯度的信标节点,提高定位结果的可信性,但由于算法只依赖信标节点,缺少对普通节点位置的参考,不太适用于信标节点稀疏的 WSN,且也存在计算开销较大的问题.Ansari 等人[21]也采用了相似的方法,并存在同样的问题.文献[22]采用分布式的信誉模型设计可信定位算法,但对网络的变化需要较长的反应时间.Wei 等人[23]根据邻居节点间的相互观测信息建立了位置验证概率模型,并取得较好的效果,但也只适用基于测距的定位算法.文献[24]运用分布式的基于 RSSI 变化的邻居节点评分机制来识别位置被动改变的信标节点,但不能运用于信标节点被诱捕的情况.文献[25]则通过凸优化方法,对主动提供不可信位置参考的信标进行识别,但也存在集中运算导致计算量过大的问题.

而另外一些工作则将可信定位的重点放在抵抗攻击的安全定位方面,最典型的是抗虫洞攻击的定位算法,代表了信标节点信息被重放的外部攻击类型(恶意节点属内部攻击)[26].文献[27-28]对 WSN 节点定位方面的安全威胁和安全算法进行了综述.文献[26]对常见的攻击方法进行了分类,并将现有的安全定位算法进行分类比较;而文献[27]则重点描述了威胁的类型;文献[28]不但将安全定位算法进行了综述,同时将节点位置验证的方法进行了介绍.Lazos 等人[29]的工作分析了虫洞攻击、女巫攻击和捕获信标节点的攻击对定位过程的影响,采用方向天线和加密等技术提供安全可信的非测距定位方法.文献[30]提出的安全定位算法则适用于基于测距的定位场景,能够通过距离约束完成恶意节点检测和抵抗虫洞攻击,但属于集中式的算法.Dong 等人[31]的工作则阐明由于虫洞攻击改变局部的网络拓扑结构,则可利用拓扑结构信息检测虫洞攻击;而文献[32]的工作与其类似,利用网络连通度的一致性检验来检测虫洞攻击.Che 等人[33]针对安全定位(主要考虑虫洞攻击引起的信标重放问题)做了连续的工作,包括提出利用节点间的距离约束抵抗虫洞攻击,属于基于测距技术的安全定位算法.在文献[34-35]中分别提出利用节点间的 3 种数据传输特征:1)发送数据自我排斥特性;2)邻居数据接收唯一性;3)传输距离约束,进行测距定位技术下和非测距定位技术下的虫洞攻击检测算法.Bao 等人[36]则运用证据理论进行节点可信值计算,采用博弈论算法按节点可信等级进行分类,排除对定位影响较大的恶意信标节点,以抵抗信标重放攻击提高定位精度.

目前的研究工作虽然在非测距 WSN 节点定位算法的信标位置验证问题上取得的进展较少,还是对解决由信标位置不可靠引起的定位质量下降问题提供了借鉴.存在 3 方面问题:1)研究成果无法同时适用于基于测距和非测距的定位算法,不具备通用性;2)集中式算法能够提供全局视野,但不符合大规模 WSN 分布式计算的需求;3)现存的大量节点位置验证方法均只针对某种特定场景进行研究,可谓各自为战,并没有将存在 3 类不可信的信标进行统一考虑和解决,因此,提出的方法缺少普适性.

2 问题描述与解决思路

2.1 相关定义

WSN 部署到特定场景后,出于成本的考虑,往往只给部分节点配备 GPS 或预先定义其位置,使其成为信标,其他节点依靠信标广播的位置作为参考,通过特定的算法估算自身位置.因节点位置可能因为外界原因而发生改变,在每个时间周期 T 重新定位,即可完成位置校准,但在校准过程中,若信标提供的位置参考是不可靠的,则定位质量会严重降低.我们定义 3 类位置不可靠的信标.

定义 1. 漂移信标.在某些应用场景中,网络部署并完成节点定位后可能发生节点自身位置发生被动的改变(如被动物影响等),这种现象叫作节点漂移,发生漂移的信标称为漂移信标.

定义 2. 虚假信标.信标节点广播的 Beacon 信息被通过某种方式在网络的另外区域重放,使得原来不能接收到该 Beacon 信标的节点误以为有 1 个可用信标,这种被信息重放影响而多出来的信标节点称为虚假信标.

定义 3. 恶意信标.信标节点因为内部软件错误

或硬件故障,造成其广播的位置参考信息与其实际位置信息不一致;或在敌对环境中(如战场环境),某些信标节点可能被敌方捕获,而故意广播虚假的位置参考信息.这种主动或被动地提供错误位置信息的信标节点,均被认为是恶意信标.

定义 3 的场景可由虫洞攻击而出现,如图 1 所示.图 1 中 A_1 和 A_2 为 2 个信标节点,相互间的距离大于通信半径,S_1 和 S_4 处于 A_1 的通信范围之内,而 S_2,S_3 处于 A_2 的通信范围之内;通过 S_1 与 S_2 这 2 个节点实施虫洞攻击,将各自听到的 Beacon 信息通过特殊的链路(可以是有线连接[37])双向重放,使得 S_3 和 S_4 分别收到来自 A_1 和 A_2 的 Beacon 信息,使得各自的通信范围内存在 1 个虚假信标节点.

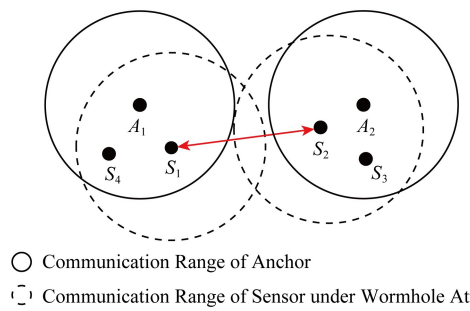

Fig. 1 False beacon suffered from worm-hole attack

图 1 受虫洞攻击而出现的虚假信标

可见,漂移信标、恶意信标和虚假信标均是位置不可靠的信标,其中恶意信标属于内部攻击,另外 2 种属于外部攻击[37],恶意信标相对来讲更加难于检测,因其不会以合作的态度参与到检测过程.

2.2 问题建模

在 2 维空间部署的无线传感器网中,共有 N 个传感器节点,组成 ad hoc 网络.其中 m 个信标节点 $A=\{a_i:i=1,2,\cdots,m\}$,n 个普通节点 $S=\{s_i:i=1,2,\cdots,n\}$,$m+n=N$,$m\ll n$.信标节点自身位置已知,坐标为 $C_{\text{anchor}}=\{c_i:i=1,2,\cdots,m\}$,$c_i=[x_i,y_i]$.普通节点的位置未知,但假设它们的实际位置为 $C_{\text{normal}}=\{c_i:i=1,2,\cdots,n\}$,$c_i=[x_i,y_i]$.信标节点主动或被动地广播自己的位置信息(称为 beacon packet),以提供给普通节点完成定位.网络部署完成后(普通节点定位成功),所有节点均可能发生漂移或被捕获,所有信标节点也均有可能受到虫洞攻击.假设发生漂移、被捕获和受虫洞攻击的信标节点比例较低,数量为 t,由集合 $A_{\text{d}}=\{a_k:k=1,2,\cdots,t,t\ll m\}$ 表示,A_{d} 中的信标自身位置改变为 C'_{anchor},其广播的自身位置 $C_{\text{anchor}}\neq C'_{\text{anchor}}$,普通节点利用 C_{anchor} 重新定位时导致定位误差变大.通过位置验证算法 $g(\cdot)$ 对信标节点位置进行验证 $g(A)=A'_{\text{d}}$,A'_{d} 为算法确认的 $C_{\text{anchor}}\neq C'_{\text{anchor}}$ 的信标节点集合.研究目标为设计位置验证算法 $g(\cdot)$,使 A'_{d} 尽量接近 A_{d},即 $\min|A_{\text{d}}-A'_{\text{d}}|$.

2.3 解决思路

节点位置验证框架(node location verification framework, NLVF)的实现思路是将每个节点对其邻居的位置观察结果与其他节点的观察进行综合,得到某一特定节点位置可靠性的判断;用带有直接和间接信誉的模型来表征这 2 种观察结果,并依靠 2 种信誉值计算综合信誉值来表征节点位置的可靠程度.计算过程中通过带有可信度更新机制的间接信誉计算方法克服恶意评价的影响.为使其适用于基于测距和非测距的 2 类定位算法,在直接信誉值计算过程屏蔽 2 类算法的距离表达差异.NVLF 结构如图 2 所示:

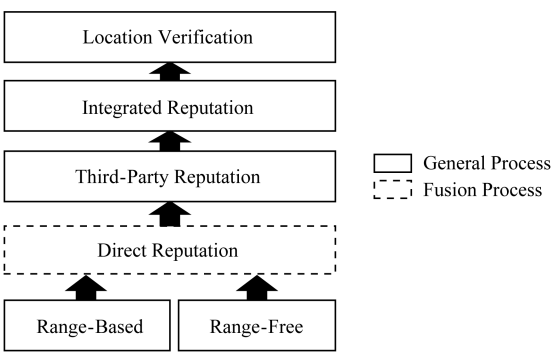

Fig. 2 Framework of location verification

图 2 位置验证框架结构图

3 分布式位置信誉模型

3.1 距离的定义

NLVF 以节点间的相互位置观测结果作为分布式信誉模型的构建基础,而节点间的位置相互观测则以距离作为度量,对于测距技术的定位算法,节点 i 可测量与其能够直接通信的信标节点 j 之间的信号特征计算 2 点间的距离 δ_{ij},比如在基于 $RSSI$ 的定位算法中,可计算测量距离 δ_{ij}[38]:

$$\delta_{ij}=10^{\frac{RSSI-E}{10n}}, \tag{1}$$

其中,E 为基础信号强度,通常取 1 m 距离上的接收信号强度;n 为损耗系数,取值范围为[2,4](真空中取 2,干扰较大的环境取 4).

本文的信誉模型,对于其他的 TOA 或 AOA 测距技术,同样适用.而对于非测距定位算法,传统方法是网络中的普通节点 i 通过特定方式获得到达信标点集合 A 的最小跳数集 $H=\{h_{ij}:j=1,2,\cdots,m\}$,并计算出网络的平均每跳距离 D_{hop},通过 $H\cdot D_{\text{hop}}$ 计算到达信标节点的距离 δ'_{ij}.但仅采用"跳数"这一普遍被传统非测距定位算法作为输入的参数.传统的非测距定位算法中有 2 种对"跳数"的定义:1)能够通信,即 1 跳;2)为了提高定位精度,将跳距定义为实数.本文采用后一种方法,但具体的实现并不是将跳数归一化为(0,1]内的实数,只要有利于描述节点对位置的判断即可(因定位算法对跳数的定义可能是采用第 1 种方法).相关文献的工作中验证了 *RSSI* 测距虽存在较大误差,但也能用于表现节点间的相互距离"远近"[39],通过对 MICZ 节点的 *RSSI* 进行收集和分析,我们进一步验证了可以用 *RSSI* 表现节点"远近"关系的可行性.实验过程中首先在空旷的室外场地对同一节点在不同方向上(按 45°为分隔,采样方向为 8 个)的 *RSSI* 值进行收集,结果如图 3 所示.其中,2 条平滑的区线是采用经典的测距模型,取信道传播衰减指数为 2.0 和 2.2,本文仿真阶段引入的 *RSSI* 测量误差就是采用随机改变信道传播衰减指数的方法.图 4 展示的是不同节点(3 个)在同一方向上的 *RSSI* 与距离的关系,可以看出 MICZ 节点在 *RSSI* 表现上的个体差异很小.

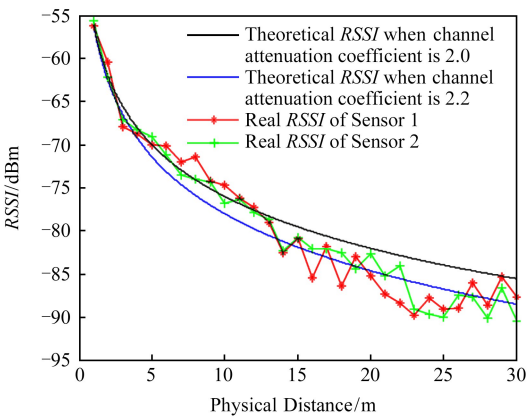

Fig. 3 *RSSI* vs. distance under ideal condition

图 3 理想情况下 *RSSI* 与距离的关系

图 5 则是在行人和车辆随机经过实验场景的情况下,经过高斯过滤后的 3 个节点的 *RSSI* 平均值曲线.可以看出 *RSSI* 受到较大的影响,当节点间距较近时,*RSSI* 基本上反映出这种距离的远近关系;但当节点相距较远时,表现则不明显.这也为基于分级制的跳数划分提供了依据.

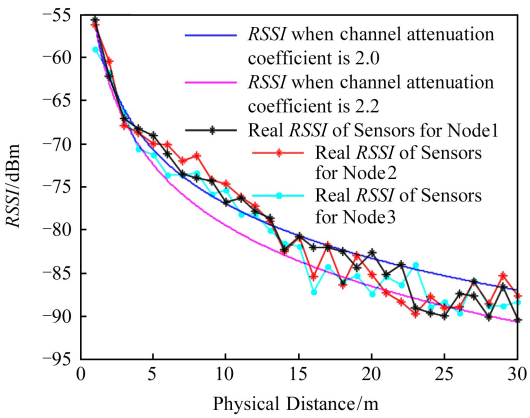

Fig. 4 *RSSI* vs. distance under ideal condition with identical orientation of different nodes

图 4 理想情况下不同节点在同一方向上 *RSSI* 与距离的关系

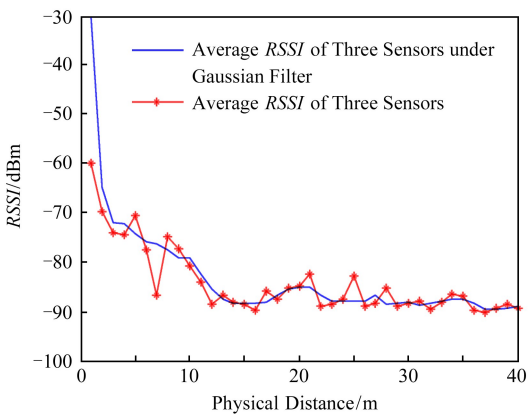

Fig. 5 *RSSI* vs. distance under severe interferences

图 5 严重干扰情况下 *RSSI* 与距离的关系

因此,本节用 log 函数定义节点间跳数:

$$hop_{ij}=1+\lfloor \text{lb}\lceil \|RSSI_{ij}-RSSI_{(i,m)\min}\| \rceil \rfloor,\quad (m\in S_j(t)\cap m\neq i), \tag{2}$$

其中 $RSSI_{(i,m)\min}$ 为节点 i 接收到其邻居的所有 *RSSI* 值中的最小值.式(2)没有采用固定的 *RSSI* 作为基准而是采用节点接收到的 *RSSI* 最小值,有效地表达了局部观测结果,本算法的分布式特性与这种局部表达高度吻合.

采用式(2),相当于将节点间的距离进行了等级划分,克服了采用 0-1 模型带来的输入过于简单的问题;而对数形式的节点间距离划分,又较好地表达了 *RSSI* 与距离之间的关系.假设 1 对节点 S_i,S_j 之间传递了若干数据包,采用 Dixion 准则进行异常值的过滤后按式(2)进行计算,对应的距离等级集合表达为 $V_i=\{v_1,v_2,v_3,v_4,v_5\}$,$i=1,2,\cdots,n$,表示对节点之间的距离的等级划分,其中 $v_1,v_2,v_3,v_4,$

v_5 可看作表示近、较近、较远、远、很远.

假设 $U_i=\{u_1,u_2,u_3,u_4,u_5\}$, $i=1,2,\cdots,n$, 表示 2 节点间收发的 $RSSI$ 强度, 我们用模糊评价矩阵 $\boldsymbol{M}$ 表示 U 和 V 之间的模糊关系, 其形式为

$$\boldsymbol{M}=\begin{pmatrix} r_{11} & \cdots & r_{15} \\ \vdots & & \vdots \\ r_{51} & \cdots & r_{55} \end{pmatrix}, \tag{3}$$

假设 SA 节点向 SB 节点发送 n 个 $RSSI$ 数据报, r_{ij} 表示在当 $|SA,SB|\in v_i$ 时其 $RSSI$ 数据报中在 U_j 对应的 $RSSI$ 值范围的个数为 m, $r_{ij}=m/n$.

获得模糊评价矩阵 $\boldsymbol{M}$ 后, 假设 S_1 接收到 S_2 的 n 个 $RSSI$ 数据时, 计算其在 u_1,u_2,u_3,u_4,u_5 对应 $RSSI$ 范围的概率分别为 a_1,a_2,a_3,a_4,a_5, 通过 $F(\wedge,\vee)$ 计算得到模糊评价向量 (b_1,b_2,b_3,b_4,b_5), 其计算为

$$(a_1,a_2,a_3,a_4,a_5)\begin{pmatrix} r_{11} & \cdots & r_{15} \\ \vdots & & \vdots \\ r_{51} & \cdots & r_{55} \end{pmatrix}= (b_1,b_2,b_3,b_4,b_5), \tag{4}$$

最终按照最大隶属度原则, 获得最终的距离评级 v_k.

算法 1. 基于 $RSSI$ 值的节点距离模糊划分算法.

输入: $RSSI$;

输出: 距离等级.

Step1. 通过实验获得 $RSSI$-距离模型以及通信范围;

Step2. 构建距离等级 V 和 $RSSI$-距离关系 U, 计算模糊评价函数;

Step3. 节点与邻居节点互相发送 n 个 $RSSI$ 值数据包;

Step4. 节点将收到的 $RSSI$ 值数据包计算得到对应 V 中距离等级的概率分布向量 $\boldsymbol{A}$;

Step5. 计算得到模糊评价向量 $\boldsymbol{B}=\boldsymbol{A}\cdot\boldsymbol{M}=(b_1,b_2,b_3,b_4,b_5)$;

Step6. 按照最大隶属度原则, 得到距离等级 $\boldsymbol{B}(v_k)=\max(b_1,b_2,b_3,b_4,b_5)$.

若要将算法 1 定义的跳数转化为传统非测距定位算法中以小于 1 的实数定义的跳数, 可计算为

$$hop'_{ij}=2^{v_{ij}}/2^{v_{\max}}, \tag{5}$$

其中 $v_{\max}$ 为跳数估算的广播阶段中节点收到的等级划分最大值.

3.2 直接信誉值

网络中的所有节点对能够直接通信的节点进行观测而计算出的信誉值称为直接信誉值, 节点 i 计算出对节点 j 的信誉值用 D_{ij} 表示. 在每个时间片, 每个节点都对其邻居节点进行直接信誉值的计算. 基于 $RSSI$ 测距定位的场景下, 直接信誉值依据节点之间的测距距离 δ 与按定位结果 C_e 计算得到的节点间计算距离 $\hat{d}_{ij}$ 进行计算, 第 t 个时间片的 D_{ij} 为

$$D_{ij}(t)=\begin{cases} 1-\dfrac{|\delta_{ij}(t)-\min(r,\hat{d}_{ij}(t))|}{\delta_{ij}(t)+\min(r,\hat{d}_{ij}(t))}, \\ \quad i \text{ 与 } j \text{ 曾经通信过}; \\ 0,\ i \text{ 与 } j \text{ 第 1 次通信}. \end{cases} \tag{6}$$

不同的测距技术使得 δ_{ij} 虽然包含一定的误差项(如采用超宽带技术下的 TOA 测距时误差较小), 但其能够反映相对真实的节点间距离. 但当节点进行相对较大位移的漂移或广播明显错误的位置参考时, 邻居节点对其的信誉值下降. 式(6)很好地体现了距离越接近的节点, 相互测距越准确的实际情况[38]; 同时, 对于新加入的邻居节点采用不信任原则.

而对于非测距技术来讲, 我们虽然将节点间的距离按 $RSSI$ 值表达成等级划分, 但带来的问题是当 2 节点本身相距较远时, 该距离等级对应的距离也较长, 又因节点通信半径较大, 会出现节点位置改变后仍处于同一等级的问题, 即距离变化不敏感的问题.

如图 6 所示, 假设节点 S_1 和节点 S_2 之间距离为等级 4, S_2 漂移到 S'_2 位置后, 与 S_1 间相互距离虽然变大, 但仍属于等级 4 对应的距离范围之内. 这种移动通过节点 S_1 的直接观测是不能发现的, 也就是说基于非测距的等级划分方法在距离越远时, 敏感度越低; 距离越近时, 敏感度越高. 因此, 在计算直接信誉值时, 引入共同邻居的观测情况, 如节点

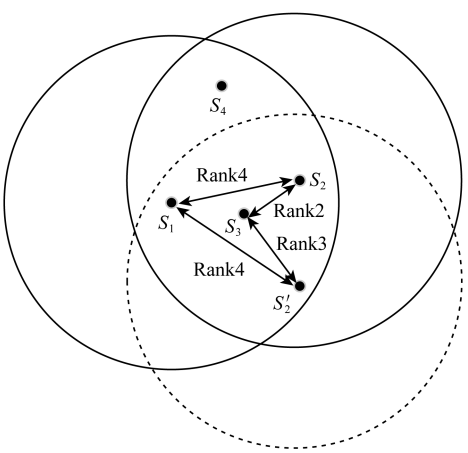

Fig. 6 Relationship between distance and rank

图 6 距离等级变化示意图

S_3 和节点 S_4 能够发现 S_2 的移动(S_4 在 S_2 漂移后,不能与其直接通信,而 S_3 与 S_2' 的距离等级由原来的 2 变成 3).

假设节点 i 和节点 j 之间在时刻 t 和 $t+1$ 的共同邻居集合分别为 $S^t(i,j)$和 $S^{t+1}(i,j)$,对应的节点 id 集合为 ID^t 和 ID^{t+1}.节点 m 属于这 2 个集合(也就是节点 m 一直能够与 i 和 j 通信),则 v_{mj}^t 和 v_{mj}^{t+1} 分别表示节点 m 在 2 个时刻对节点 j 的距离观测,在时刻 t 和 $t+1$,节点 i 的视角下,其与节点 j 的共同邻居(2 个时刻中任何 1 个时刻成为了 i 和 j 的共同邻居)对 j 的观测向量为 $\boldsymbol{V}_{mj}^t$ 和 $\boldsymbol{V}_{m'j}^{t+1}$,注意 m 与 m'不一定相等,取 $ID_{\text{com}}=ID^t\cup ID^{t+1}\cup\{i\}$,然后根据 ID_{com} 扩充 $\boldsymbol{V}_{mj}^t$ 和 $\boldsymbol{V}_{m'j}^{t+1}$,使 2 个集合中新增成员 $v_{mj}=0$.运用 Jaccard 系数法计算 2 个时刻下节点 i 和节点 j 的邻居观测相似度:

$$Sim(t,t+1)_{ij}=\frac{\boldsymbol{V}_{mj}^t\cdot\boldsymbol{V}_{mj}^{t+1}}{(\boldsymbol{V}_{mj}^t)^2+(\boldsymbol{V}_{mj}^{t+1})^2-\boldsymbol{V}_{mj}^t\cdot\boldsymbol{V}_{mj}^{t+1}},\quad(7)$$

Jaccard 系数法源于余弦定理,但能够克服除数为 0 的情况.

利用共同邻居相似性也可以识别产生漂移的信标,但其不具备更新收敛性,容易引起较高的误判率,而且不能用于检测恶意信标;假设恶意信标 j 在时刻 t 开始广播虚假位置参考 C_j^t,而上一个时刻其邻居节点 i 收到的其广播位置为 C_j^{t-1},若 $\|C_j^{t-1}-C_j^t\|\geqslant 0.5R$,则以 $1-Sim(t,t+1)_{ij}$ 作为信标 j 的直接信誉值.即在非测距情况下,节点 i 的视角下,节点 j 的直接信誉值计算过程为

$$D_{ij}(t+1)=\begin{cases}Sim(t,t+1)_{ij},\ i\text{ 与 }j\text{ 曾经通信过,}\\ \quad\text{且}\|C_j^{t-1}-C_j^t\|<0.5R;\\ 1-Sim(t,t+1)_{ij},\ i\text{ 与 }j\text{ 曾经通信}\\ \quad\text{过,且}\|C_j^{t-1}-C_j^t\|\geqslant 0.5R;\\ 0,\ i\text{ 与 }j\text{ 第 1 次通信.}\end{cases}\quad(8)$$

下文中可以看到,在信誉模型中,间接信誉值也是根据直接信誉值计算并迭代更新的,因此,采用不同的方法计算直接信誉值后,测距的和非测距的可信定位框架在其他运算过程均一致,体现了其普适性.

3.3 间接信誉值

WSN 中因随机冗余部署的原因,每个节点都有多个邻居节点,$S_j(t)$表示在时刻 t 能够和节点 j 直接通信的节点集合.只要 $S_j(t)$中的节点将自己对 j 的信誉度局部广播给其 2 跳邻居,就能确保本集合之中所有节点均能相互交换对节点 j 的信任度,对节点 i 来讲,综合计算其收到的其他节点对 j 的信誉值,通过一定的计算可以得到反映其他邻居节点对节点 i 的定位精度的信任程度.计算方法为

$$I_{ij}(t)=\frac{\sum_m C_{im}(t)\cdot R_{mj}(t)}{\sum_m C_{im}(t)},\quad(9)$$
$$(m\in S_j(t)\cap m\neq i),$$

其中,$R_{mj}(t)$表示时刻 t 节点 m 对节点 j 的信任度,$C_{im}(t)$表示时刻 t 在节点 i 的视角上节点 m 的推荐可信度,$R_{mj}(t)$定义为

$$R_{mj}(t)=D_{mj}(t),\quad(10)$$

而 $C_{im}(t)$的计算相对复杂,无法从节点 i 的视角直接得到,因为要考虑到其他节点可能产生漂移而引起的间接可信度恶化的情况.如图 7 所示,时刻 t 节点 S_5 已经产生漂移,但节点 S_1 与节点 S_5 的相对距离并无改变,因此,可以获得较高的 $D_{S_1,S_5}(t)$,而节点 S_5 与节点 S_2,S_4 的距离变化将导致 S_1 来自 S_5 视角的对 S_2,S_4 的推荐度较低.而根据式(8),因节点 S_3 第 1 次能够与 S_5 通信,在 S_1 的视角上,S_3 获得的来自 S_5 的间接信誉值为 0,因此,必须采取一定的推荐可信度更新机制,使得节点间的相互观察能够收敛至稳定可信.

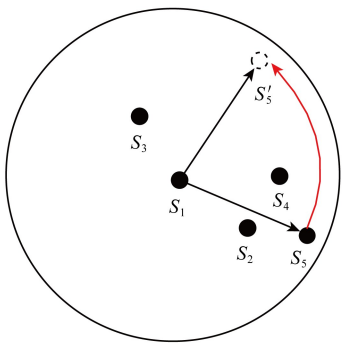

Fig. 7 Circumstance of identical direct reputation

图 7 直接信誉值不变的情况

为解决上述问题,我们引入信任度更新机制[40],首先计算节点信誉差 Dif 和相对信誉偏差 RTD 为

$$Dif_{i(m,j)}=\sum_{k\in S(j)}|R_{kj}-R_{mj}|/|S(j)|,\quad(11)$$

$$RTD_{i(m,j)}=Dif_{i(m,j)}/STD_j,\quad(12)$$

其中,$Dif_{i(m,j)}$表示在节点 i 的视角下,节点 m 对节点 j 的信誉值偏差;$|S(j)|$表示集合 $S(j)$的基;STD_j 表示 $S(j)$中所有节点对节点 j 信誉值的标准方差.当 $RTD_{i(m,j)}\leqslant 1$ 时,节点 i 认为节点 m 对

节点 j 的位置可信度判断与其他节点一致;否则,认为节点 m 产生了间接可信度恶化的现象.$C_{im}(t)$根据 $RTD_{i(m,j)}$ 进行更新的计算式为

$$C_{im}(t)=\begin{cases}C_{im}(t-1)+(1-C_{im}(t-1))\times\\ \quad(1-RTD_{i(m,j)}),\ 0\leqslant RTD_{i(m,j)}<1,\ t>0;\\ C_{im}(t-1)/RTD_{i(m,j)},\ RTD_{i(m,j)}\geqslant 1,\ t>0;\\ D_{im}(t),\ t=0.\end{cases}\tag{13}$$

信任度更新机制将降低节点漂移或不可靠信标节点对间接信任值计算的影响.

3.4 综合信誉值

在时刻 t,当节点 i 计算得到节点 j 的直接信誉值 $D_{ij}(t)$和间接信誉值 $I_{ij}(t)$后计算其综合信誉值 $T_{ij}(t)$:

$$T_{ij}(t)=\alpha D_{ij}(t)+(1-\alpha)I_{i,j}(t),\tag{14}$$

其中,α 为信誉值权重,其大小解决了对自己的判断和其他节点的推荐信誉值的依赖程度.当节点本身发生漂移或 2 节点同时漂移且相对距离变化不大时,如果 α 值较大时,易造成位置验证的性能下降;若 α 取值过小,则受到其他节点的误判影响较严重.关于 α 的取值将在第 5 节通过仿真实验进行讨论.

4 节点位置验证框架

基于分布式信誉模型的可信定位基本思路如图 8 所示,节点 i 通过其他节点信誉值所反映的位置可靠程度来判断其他节点是否可信;通过对直接信誉值和间接信誉值的一致性来判断自身是否产生了漂移.若节点 i 自身产生了漂移,则在排除了不可靠的信标节点后,通过重新调用定位算法进行位置验证,如果重定位过程中可用信标数小于定位算法的最低要求,则通过基于信誉值的临时信标择算法进行信标补充.因不可信信标的存在,网络部署后,位置验证和重定位是周期性进行的,因此以位置验证为目地收集到的 $RSSI$ 信息同样服务于重定位,因此,并没有额外的通信开销.下面按顺序对可信定位中的 2 个处理环节(即节点位置的验证与重定位)进行详细说明.

首先需要说明的是,节点对自身进行漂移检测时,假设自认信誉度为 1,并使用信誉相对偏差 $RTD_{i(m,i)}$ 进行判断,当 $RTD_{i(m,i)}>1$ 时,认为自身发生漂移.在如图 9 所示的场景中(只画出部分网络拓扑),网络部署且完成位置初始化后,传感器节点 S_6 发生了漂移,移动至位置 S_6' 处,信标节点 B_2 因

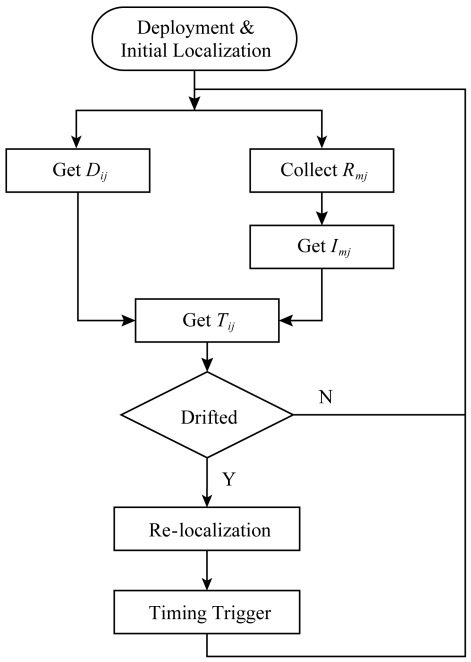

Fig. 8 Flow chart of NLVF

图 8 NLVF 工作流程图

被诱捕或故障成为不可靠信标节点,其广播的位置信息为 B_2'.假设判断阈值 $\omega=0.5$,节点 S_1 和 S_3 由于是首次能够和 S_6 通信,对 S_6 的直接信誉值计算结果为 0,而节点 S_4 与 S_6 的相对距离发生一定的变化,对 S_6 的直接信誉值计算结果为(0,1)范围内

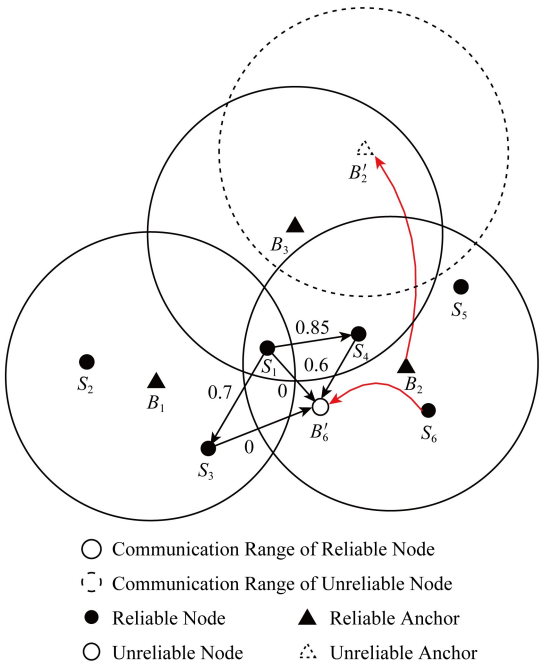

Fig. 9 Schematic diagram of reputation in reliable localization

图 9 可信定位过程信誉值示意图

的数字,假设为0.6,高于漂移检测的阈值,但由于借鉴了 S_1 和 S_3 对 S_6 的间接信誉值(0),对节点 S_6 的综合信誉值将大幅度低于0.6,从而成功地判断出 S_6 的漂移现象;而节点 S_6 也通过信誉偏差确认自身发生了漂移.基于同样的过程,信标节点 B_2 的错误位置也会被其周围的节点成功识别.我们将这一算法称为不可信节点检测算法(unreliable node detection algorithm, UNDA).而 ω 的取值与节点测距精度有关,将在第5节中进行讨论.

5 实验结果与讨论

仿真环境在500 m×500 m的正方形区域内,随机部署 n 个普通传感器节点和 m 个信标节点(每对信标节点的间距不小于5 m).所有节点具有相同的通信半径 $r=50$ m.在网络成功部署及初始定位完成后,有 m' 个节点成为位置不可信节点,它们位置的改变大于20 m,其中被捕获的信标节点比例不高于50%.所有实验结果为50次实验的平均值.

5.1 算法参数选择

信誉值计算公式中权重参数 α 的取值难以利用封闭表达式进行描述,在产生漂移的节点和不可靠信标数量比重变化的场景中,对 α 不同取值情况的算法性能进行了仿真.因为节点的直接邻居数量对间接信誉值的准确性也有影响,故实验中也对平均网络连通度进行了调节,范围为[4,10],步长为2.信标节点占比10%,位置不可信节点数的比重从10%~40%变化,步长为10%.实验中将节点间的测距精度设定为 $0.1r$,对位置可信节点和位置不可信节点的平均信誉值 $average(T_{rel})$ 及 $average(T_{unr})$ 进行计算,结果如图10~13所示:

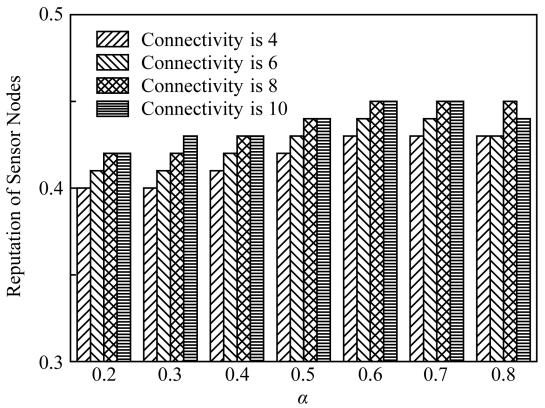

Fig. 10 Average mean variation with 10 percent unreliable anchor

图10 位置不可靠信标占比10%时信誉值平均偏差

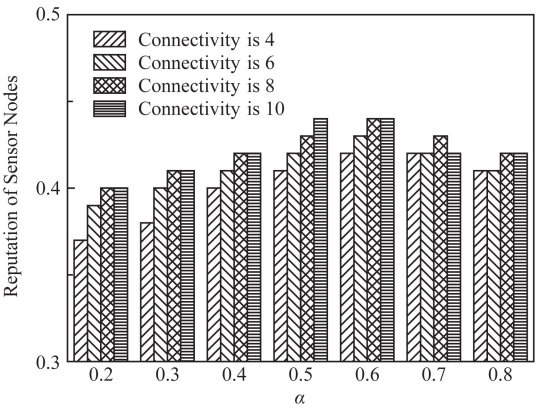

Fig. 11 Average mean variation with 20 percent unreliable anchor

图11 位置不可靠信标占比20%时信誉值平均偏差

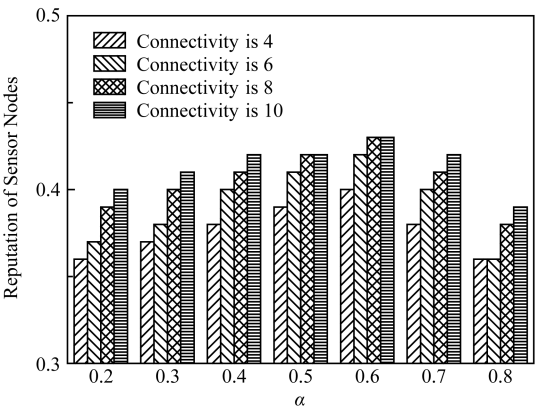

Fig. 12 Average mean variation with 30 percent unreliable anchor

图12 位置不可靠信标占比30%时信誉值平均偏差

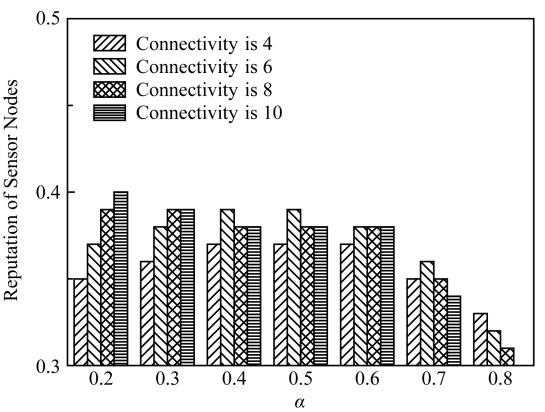

Fig. 13 Average mean variation with 40 percent unreliable anchor

图13 位置不可靠信标占比40%时信誉值平均偏差

图10~13中纵坐标为产生位置不可信节点3个时间片后 $average(T_{rel})-average(T_{unr})$ 的值,我们称之为 $Diff_{ave}$.可以看出,2种节点的信誉值

之间存在着明显的差异,当位置不可信的节点占比升高时,差异变小,但也足够明显,这也是采用分布式信誉模型进行位置验证的基础.这种差异随着网络连通度的提高也会变得明显,特别是当连通度大于 6,而$\alpha\in[0.4,0.6]$时.综合看来,$\alpha=0.6$ 时,$Diff_{ave}$的值始终大于 0.38,因此,实验中 $\alpha=0.6$.在不同的 *RSSI* 测量误差情况下对检测阈值ω 的取值进行了实验,仿真场景中网络平均连通度设置为 8,信标占比 10%,发生漂移的普通节点比例与不可靠信标的比例均为 20%,节点采集的 *RSSI* 数据噪音为[0.1,0.3],步长为 10%,结果如图 14 所示:

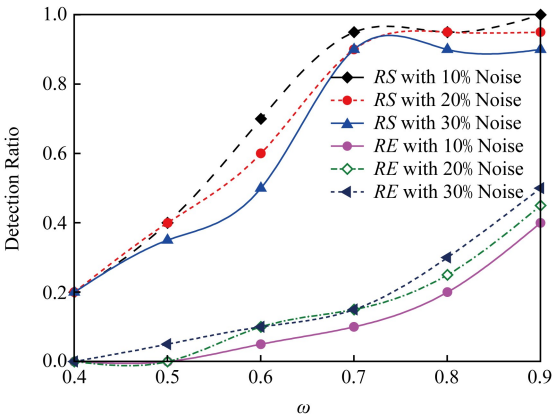

Fig. 14 Threshold vs. detection performance

图 14 检测阈值与检测性能的关系

我们用来衡量漂移检测算法性能的 2 个指标为:识别成功率及识别错误率,计算公式为

$$RS=|A_d\cap A'_d|/|A_d|, \tag{15}$$

$$RE=|A'_d-A_d|/|A_d|. \tag{16}$$

识别成功率为被正确判断为漂移节点的数量与实际漂移节点数量的比值,用来衡量算法能够成功识别位置不可信节点的概率;而错误率则是被错误地判断为不可信节点的数目与实际不可信节点数目的比值,用以衡量算法在检测漂移节点时产生误判的概率.实验结果显示的是实验过程中每个时间周期的检测成功率和错误率取平均值.非测距算法中 *RSSI* 的噪音由经典信号能量传播衰减模型为基础,衰减指数 $n=2.5$,上下随机产生百分比变化,如 20%的噪音,则 n 值变化范围是[2,3].

从图 14 中可以看出,当检测阈值增大时,检测成功率和检测错误率均呈上升状态,因为检测条件变得苛刻后,成功率必然升高,但由于误差的存在检测错误率也随之升高;综合来看,ω 取值为[0.7,0.8]之间时,算法性能较好,因此,后续实验中设置 $\omega=0.7$;另外,随着 *RSSI* 噪音的增加,检测错误率有很小的上升,检测成功率却影响不大,这也充分验证了 UNDA 的鲁棒性,*RSSI* 具有 30%的噪音情况下检测成功率能够达到 90%以上.

5.2 位置验证效果

为了验证可信定位模型中用于服务基于测距技术的不可信信标检测性能,我们用同样是分布式位置验证算法的文献[24]作为比较对象,简称为节点漂移检测(node drifting detection, NDD)算法.设置 40 个信标节点,仿真中每个时间段内均有随机数量(0~20%)的节点发生漂移或变为恶意信标,但漂移节点总数不变,随机出现 1~4 个虫洞(对应 2~8 个信标节点受到影响).首先固定漂移信标节点的数量,改变普通节点密度,当网络节点密度提高时,2 种算法的检测准确率都相应提高,误检率相应降低,如图 15 所示.这是各节点可参考的邻居节点数量增加引起的.但 UNDA 具有更好的检测性能,这是因为 UNDA 的节点间接信誉推荐信任度更新机制,可以更好地排除漂移节点对其他节点判断准确性的影响,而 NDD 算法每一轮的检测都是一个全新的算法执行过程,检测性能不会因为时间的累积而提高.

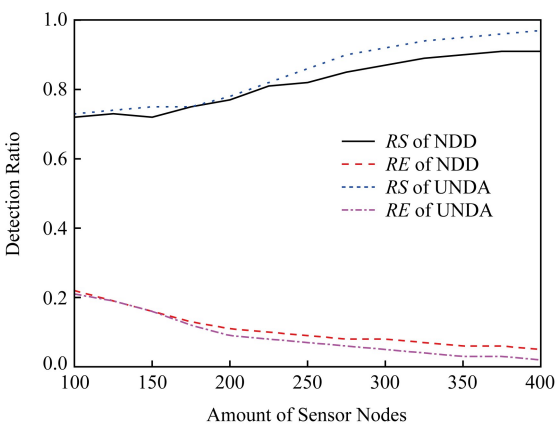

Fig. 15 Node density vs. detection performance

图 15 节点密度改变下的检测性能

图 16 展示的是固定节点数(300 个)的情况下,共 80 个信标节点,位置不可靠的信标数量范围[4,40]步长为 8,其中恶意信标占比 50%,同样数量的虫洞场景下的算法性能比较.随着漂移信标的增加 2 种算法的性能都有下降,但相比之下,UNDA 在漂移信标较多时,具有更高的检测成功率和较低的误检率,这同样是因为 UNDA 采用了间接信誉推荐可信度更新机制.

而 NLVF 用于非测距的定位技术中因缺少类似工作,我们将文献[24]的投票依据由测距值替换

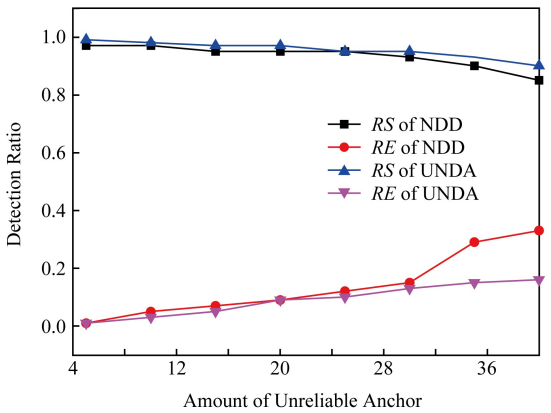

Fig. 16 Amount of unreliable vs. detection performance

图 16 不可信信标数量改变下的检测性能

为本文的分级跳距方法以移植到非测距定位场景,并简称为 RF-NDD(rank feed-NDD)算法,由于非测距定位算法应用场景中信标节点通常较少,我们固定其数量为 20 个,其中 8 个信标发生漂移,2 个信标受虫洞影响(2 个虚假信标),普通节点数量变化范围为[200,400],步长 50,*RSSI* 测量噪音为 10%.

实验结果如图 17 所示,与基于测距的场景相似,由于缺少相互观测的积累和投票可信性的更新,节点密度变大时,RF-NDD 性能并无明显的提升,而 NLVF 不但具有较好的检测性能,且随着节点密度升高,其性能也有显著提升,这对于节点密度较高的大型 WSN 来讲,具有实用性.设置 *RSSI* 噪音为 20%和 40%的 2 种情况以验证 NLVF 的鲁棒性.实验中共设置 20 个信标节点,网络平均连通度在[6,10]范围内变化,步长为 1,20 个信标节点全部成为不可信的信标,由于信标数量较少,故仿真结果采用节点个数代替比率,即检测成功的信标个数(number of detected anchor, NoD)和假阳性节点个数(number of false positive, NoFP).实验结果如图 18 所示,当 *RSSI* 噪音较大时,引起跳数等级划分不够准确,使得直接信誉值计算误差增大,但性能仍旧在可以接受的范围内,当网络平均连通度为 10 时,40%的 *RSSI* 噪音情况下,成功检测出 18 个不可信的信标,漏检 2 个;由假阳性引起的误检个数为 3.在 20%的 *RSSI* 噪音时,网络连通度达到 9 的情况下,误检率降为 0,只漏检了 1 个信标节点.由于 WSN 的节点部署冗余特性以及节点较大的通信半径,平均网络连通度达到 9 的假设是切合实际的.

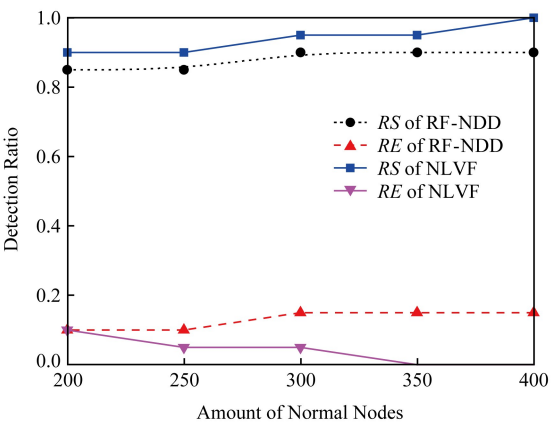

Fig. 17 Performance of NLVF in range-free scenario with variation of node amount

图 17 NLVF 在非测距场景中节点数量变化时的性能

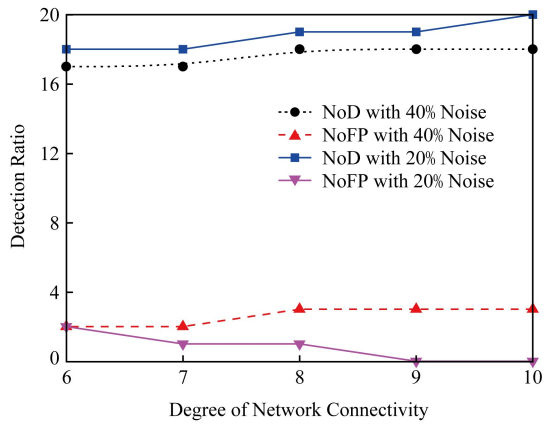

Fig. 18 Performance of NLVF in range-free scenario with variation of anchor amount

图 18 NLVF 在非测距技术场景下的性能

6 总结与展望

本文提出 NLVF 框架,服务于基于测距的定位算法和非测距定位算法,用以过滤位置不可靠的信标节点,NLVF 的核心算法 UNDA 以节点间的相互位置观测为基础,构建节点位置信誉模型,引入的间接信誉可信性更新机制,确保了算法收敛至稳定的判断结果.实验证明 NLVF 具有较高的检测率和较低的误检率,且具备轻量级的特点,适用于 WSN.未来的工作将围绕临时信标选择算法展开,以解决信标过滤后的后果定位过程中可用信标不足问题,进一步完善 NLVF 的服务能力,并通过实物实验床验证 NLVF 的扩展性和重定位性能.

参 考 文 献

[1] Bellavista P, Cardone G, Corradi A, et al. Convergence of MANET and WSN in IoT urban scenarios [J]. IEEE Sensors Journal, 2013, 13(10): 3558-3567

[2] Yang Zheng, Zhou Zimu, Liu Yunhao. From RSSI to CSI: Indoor localization via channel response [J]. ACM Computing Surveys, 2013, 46(2): 1-32

[3] Xu Ning, Huang Aiping, Hou Tingwei, et al. Coverage and connectivity guaranteed topology control algorithm for cluster-based wireless sensor networks [J]. Wireless Communications and Mobile Computing, 2012, 12(1): 23-32

[4] Jin Miao, Rong Guodong, Wu Hongyi. Optimal surface deployment problem in wireless sensor networks [C] //Proc of INFOCOM 2012. Piscataway, NJ: IEEE, 2012: 2345-2353

[5] Ghosh R K, Das S K. A survey on sensor localization [J]. Control Theory and Technology, 2010, 8(1): 2-11

[6] Han Guanjie, Xu Huiui, Duong T Q, et al. Localization algorithms of wireless sensor networks: A survey [J]. Telecommunication Systems, 2013, 52(4): 2419-2436

[7] Han Yunfeng, Zheng Cui'e, Sun Dajun. Localization of large scale underwater sensor networks based on recursive position estimation [C] //Proc of OCEANS 2015. Piscataway, NJ: IEEE, 2015: 1-4

[8] Perazzo P, Taponecco L, D'amico A A, et al. Secure positioning in wireless sensor networks through enlargement miscontrol detection [J]. ACM Transactions on Sensor Networks, 2016, 12(4): Article ID: 27

[9] Zhong Sheng, Jadliwala M, Upadhyaya S, et al. Towards a theory of robust localization against malicious beacon nodes [C] //Proc of IEEE INFOCOM 2008. Piscataway, NJ: IEEE, 2008: 2065-2073

[10] Hwang J, He Tian, Kim Y. Detecting phantom nodes in wireless sensor networks [C] //Proc of IEEE INFOCOM 2007. Piscataway, NJ: IEEE, 2007: 2391-2395

[11] Liu Dawei, Lee M C, Wu Dan. A node-to-node location verification method [J]. IEEE Transactions on Industrial Electronics, 2010, 57(5): 1526-1537

[12] Wu Di, Zhao Dongmei, Feng Weimiao, et al. SPIN: An active location verification scheme for wireless sensor networks [C] //Proc of 2016 Military Communications. Piscataway, NJ: IEEE, 2016: 120-125

[13] Wang Dexin, Yang Liuqing, Cheng Xiang. A low-complexity cooperative algorithm for robust localization in wireless sensor networks [C] //Proc of IEEE ICNC 2016. Piscataway, NJ: IEEE, 2016: 1-5

[14] He Daojing, Lin Cui, Huang Hejiao, et al. Design and verification of enhanced secure localization scheme in wireless sensor networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2009, 20(7): 1050-1058

[15] Xiao Bin, Chen Lin, Xiao Qingjun, et al. Reliable anchor-based sensor localization in irregular areas [J]. IEEE Transactions on Mobile Computing, 2010, 9(1): 60-72

[16] Kuo S P, Kuo H J, Tseng Y C. The beacon movement detection problem in wireless sensor networks for localization applications [J]. IEEE Transactions on Mobile Computing, 2009, 8(10): 1326-1338

[17] Miao Chunyu, Dai Guoyong, Ying Kezhen, et al. Collaborative localization and location verification in WSNs [J]. Sensors, 2015, 15(5): 10631-10649

[18] Yang Zheng, Jian Lirong, Wu Chenshu, et al. Beyond triangle inequality: Sifting noisy and outlier distance measurements for localization [J]. ACM Transactions on Sensor Networks, 2013, 9(2): 1-20

[19] Yang Zheng, Wu Chenshu, Chen Tao, et al. Detecting outlier measurements based on graph rigidity for wireless sensor network localization [J]. IEEE Transactions on Vehicular Technology, 2013, 62(1): 374-383

[20] Garg R, Varna A L, Wu Ming. An efficient gradient descent approach to secure localization in resource constrained wireless sensor networks [J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 717-730

[21] Ansari Z, Ghazizadeh R, Shokhmzan Z. Gradient descent approach to secure localization for underwater wireless sensor networks [C] //Proc of ICEE 2016. Piscataway, NJ: IEEE, 2016: 103-107

[22] Srinivasan A, Teitelbaum J, Wu Jie. DRBTS: Distributed reputation-based beacon trust system [C] //Proc of 2006 Dependable, Autonomic and Secure Computing. Piscataway, NJ: IEEE, 2006: 277-283

[23] Wei Yawen, Guan Yong. Lightweight location verification algorithms for wireless sensor networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(5): 938-950

[24] Xia Ming, Sun Peiliang, Wang Xiaoyan, et al. Distributed beacon drifting detection for localization in unstable environments [J]. Mathematical Problems in Engineering, 2013(7): 707-724

[25] Ren Ping, Liu Wu, Sun Donghong, et al. Node localization based on convex optimization in wireless sensor networks [C] //Proc of 2016 Fuzzy Systems and Knowledge Discovery. Piscataway, NJ: IEEE, 2016: 2169-2173

[26] Boukerche A, Oliveira H A B F, Nakamura E F, et al. Secure localization algorithms for wireless sensor networks [J]. IEEE Communications Magazine, 2008, 46(4): 96-101

[27] Sharma K, Ghose M K. Wireless sensor networks: An overview on its security threats [J]. International Journal of Computer Applications: Special Issue on MANETs, 2010, manets(1): 42-45

[28] Zeng Yingpei, Cao Jiannong, Hong Jue, et al. Secure localization and location verification in wireless sensor networks: A survey [J]. Journal of Supercomputing, 2013, 64(3): 685-701

[29] Lazos L, Poovendran R. Secure localization for wireless sensor networks using range-independent methods [M] // Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks. New York: Springer, 2007: 185-214

[30] Liu Donggang, Ning Peng, Du Wenliang. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks [C] //Proc of IEEE ICDCS 2005. Piscataway, NJ: IEEE, 2005: 609-619

[31] Dong Dezun, Li Mo, Liu Yunhao, et al. Topological detection on wormholes in wireless ad hoc and sensor networks [J]. IEEE/ACM Transactions on Networking, 2011, 19(6): 1787-1796

[32] Dimitriou T, Giannetsos A. Wormholes no more? Localized wormhole detection and prevention in wirelessnetworks [C] //Proc of IEEE DCOSS 2010. Piscataway, NJ: IEEE, 2010: 334-347

[33] Chen Honglong, Lou Wei, Sun Xice, et al. A secure localization approach against wormhole attacks using distance consistency [J]. EURASIP Journal on Wireless Communications and Networking, 2010: Article ID: 627039

[34] Chen Honglong, Lou Wei, Wang Zhi. On providing wormhole-attack-resistant localization using conflicting sets [J]. Wireless Communications & Mobile Computing, 2015, 15(15): 1865-1881

[35] Chen Honglong, Lou Wei, Wang Zhi, et al. Securing DV-Hop localization against wormhole attacks in wireless sensor networks [J]. Pervasive and Mobile Computing, 2015, 16 (PA): 22-35

[36] Bao Tianyue, Wan Jiangwen, Yi Kefu, et al. A game-based secure localization algorithm for mobile wireless sensor networks [J]. International Journal of Distributed Sensor Networks, 2015: Article ID: 642107

[37] Dong Dezun, Li Mo, Liu Yunhao, et al. Topological detection on wormholes in wireless ad hoc and sensor networks [J]. IEEE/ACM Transactions on Networking, 2011, 19(6): 1787-1796

[38] Jiang J, Zheng Xiangyao, Chen Yufan, et al. A distributed RSS-based localization using a dynamic circle expanding mechanism [J]. IEEE Sensors Journal, 2013, 13(10): 3754-3766

[39] Zhong Ziguo, He Tian. RSD: A metric for achieving range-free localization beyond connectivity [J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22 (11): 1943-1951

[40] Tian Chunqi, Yang Baijiang, Zhong Jidong, et al. Trust-based incentive mechanism to motivate cooperation in hybrid P2P networks [J]. Computer Networks, 2014, 73(c): 244-255

Miao Chunyu, born in 1978. PhD, assistant professor. Member of CCF. His main research interests include wireless network, security of IoT and application security.

Chen Lina, born in 1978. PhD, assistant professor. Her main research interests include wireless network and secure indoor localization.

Wu Jianjun, born in 1972. Master, lecturer. His main research interests include software engineering and cyberspace security.

Zhou Jiaqing, born in 1969. PhD candidate, assistant professor. His main research interests include network engineering and cyberspace security.

Feng Xuhang, born in 1982. Master, senior engineer. His main research interests include cyberspace security management and security risk assessment.