A Label-Based MMCL Algorithm Against Wormhole Attack

BAO Lu, DENG Ping *

(*Key Lab of Information Coding and Transmission, Southwest Jiaotong University, Chengdu* 610031, *China*)

Abstract: To solve the problem of secure localization in MWSN, this paper analyzes the effect of wormhole attack on MMCL algorithm. In order to resist wormhole attacks and improve localization performance, a secure LB-MMCL algorithm was proposed. Based on the abnormal nodes neighbor-lists when wormhole attack occurs, LB-MMCL can label and detect two kinds of wormhole link nodes according to distance-astrict property and packet uniqueness property, break wormhole links to mitigate the impact of wormhole attacks and enhance the node localization accuracy. The simulation results show that LB-MMCL can efficiently against the wormhole attack without extra-hardware, improve the node localization accuracy and the percentage of localizable nodes.

Key words: MWSN; wormhole attack; MMCL; secure localization

EEACC: 7230 **doi**: 10.3969/j.issn.1004-1699.2018.07.024

一种基于标签的抗虫洞攻击 MMCL 算法

鲍 露, 邓 平*

(西南交通大学信息编码与传输重点实验室, 成都 610031)

摘 要: 针对移动传感器网络节点定位算法的安全性问题, 分析了虫洞攻击对 MMCL 算法的影响。为抵御虫洞攻击, 改善定位性能, 提出了一种基于标签的抗虫洞 MMCL 算法 LB-MMCL(Label-Based Multi-hop Monte Carlo Localization)。该算法基于节点邻居列表中的异常, 依据距离约束机制和消息唯一性原则, 标记并区分虫洞两端受攻击的节点, 断开虚假链路, 以减轻虫洞攻击的影响, 达到抵御攻击的目的。仿真结果表明, 在无需额外硬件辅助下, LB-MMCL 算法能有效抵御虫洞攻击, 改善节点定位精度和定位率。

关键词: 移动无线传感器网络; 虫洞攻击; MMCL; 安全定位

中图分类号: TP393 **文献标识码**: A **文章编号**: 1004-1699(2018)07-1118-06

无线传感器网络[1]发展至今, 已在理论上基本解决静态和安全环境下的节点定位问题。但对于移动无线传感器网络 MWSN(Mobile Wireless Sensor Networks)来说, 移动网络环境的复杂性和多样性使定位系统更容易遭受网外攻击和网内干扰, 造成节点无法自定位或定位精度不达标。因此, MWSN 定位技术的安全性是一项亟待解决的关键问题。

到目前, 国内外对 MWSN 定位技术[2-4]的研究主要集中在假设网络安全的前提下, 缺乏抵御攻击能力。对 MWSN 安全定位问题的研究报道还相对较少。蒙特卡洛(MC)方法作为 MWSN 定位的一种主要方法被广泛研究, 多跳蒙特卡罗定位算法[5] MMCL(Multi-hop-based Monte Carlo Localization)作为其中一种典型算法, 结合了 DV-Hop 和 MC 方法的优点, 有较高的定位精度和定位覆盖率, 但抗攻击能力差。为了提高 MMCL 算法的安全性, 本文针对抵御虫洞攻击的 MMCL 算法展开研究。

1 相关工作

受攻击情况下的移动节点定位问题, 近年来仅有一些分散的研究: 2009 年, Zeng 等人首次讨论蒙特卡罗定位算法的安全性, 提出了一种抵御欺骗攻击的安全定位算法 SecMCL[6], 该算法通过非对称密钥和扩大采样来抵御欺骗攻击。当定位过程由于欺骗攻击无法获得足够的合法样本时, 降低样本点的要求进行扩大采样, 仅要求样本点与尽可能多的锚节点观测信息一致。2012 年, Garg 等人通过纯代数方法解决欺骗攻击下的安全移动定位问题, 该算法[7]包括代价函

收稿日期: 2017-12-21 修改日期: 2018-03-13

数构造和最小化两个阶段:首先利用锚节点定位参考信息构造代价函数,在第 2 阶段通过迭代梯度下降法将代价函数最小化并剔除残差较大的矢量值,提高节点的定位精度。Vennam 等于 2014 年分析了虫洞攻击对 MCL 的影响,提出的 WRMCL 算法[8]采用锚盒子重置检测方案发现伪锚节点,利用节点间距离和通信半径的距离约束关系剔除虫洞范围中的锚节点,达到抵御虫洞攻击的目的。次年,池玉辰等人提出了一种抵御虫洞攻击的 DewormMCL 算法[9],该算法利用移动节点连续定位特点进行虫洞攻击检测,识别并剔除伪锚节点,改善定位算法的抗攻击能力。2017 年,曹璐等人提出一种 DWMCB 安全定位算法[10],通过计算普通节点侦听到的锚节点的质心,比较锚节点到质心的距离,识别并剔除伪锚节点提高虫洞攻击下的节点定位精度。

以上针对移动定位算法安全性的研究中,大都要求传感器节点有较强的存储计算能力,算法计算量较大。SecMCL 算法需要进行循环采样,直到获得足够的合法样本,这个过程对节点计算和存储能力要求较高,计算量大,且对定位误差的改善并不明显;WRMCL、DewormMCL 和 DWMCB 3 种抵御虫洞攻击的定位算法在识别和剔除伪锚节点信息时,提高了算法的计算量。除此之外,3 种算法都仅考虑两跳范围内的锚节点信息,无法满足多跳式定位算法抵御虫洞攻击的需求。

虫洞攻击具有很好的隐藏性,对定位系统性能有极大的影响。近几年虫洞攻击被广泛关注[11-12]。这些抵御虫洞攻击的安全定位算法大多以节点静态为前提,对虫洞攻击下节点跳数偏差的特征参数提取没有与移动网络特性相关联。基于蒙塔卡罗的定位算法充分利用节点移动性和和历史定位信息,得到较高的定位精度,其中 MMCL 是作为一种典型 MWSN 定位算法,定位精度和定位率都远高于 MCL 和 MCB,但当前还没有关于 MMCL 算法的安全性研究,且动态、多跳式的节点定位算法受虫洞攻击的影响更大。基于此,本文针对 MMCL 算法在虫洞攻击下的定位性能展开研究。

2　虫洞攻击的影响

2.1　MMCL 算法

MMCL 算法的定位过程主要分为两个阶段:

①计算锚节点平均跳距:锚节点在全网内洪泛信标信息,当锚节点 i 获取与其他锚节点间的跳数 h_i 和坐标信息后,按式(1)计算平均跳距 C_i,并在下一时刻锚节点洪泛信标信息时一起广播出去,以节省网络中的通信量。

$$C_i = \sum \sqrt{(X_i - X_j)^2 + (Y_i - Y_j)^2} / \sum h_i \quad (1)$$

②蒙特卡罗定位:MMCL 算法假设每个待定位节点与锚节点间的距离 d_i 满足条件:

$$C_i\alpha \leqslant d_i \leqslant C_i\beta \quad (2)$$

式中:$\alpha = h_i \times 0.4$,$\beta = h_i + 2$,C_i 为平均跳距。

基于此假设,在预测阶段,结合上一时刻样本集合与节点运动模型,建立采样区域如下:

$$x_{\min} = \max[\max_{i=1}^{n}(x_i - C_i\beta), x_{t-1} - v_{\max}] \quad (3)$$

$$x_{\max} = \min[\min_{i=1}^{n}(x_i + C_i\beta), x_{t-1} + v_{\max}] \quad (4)$$

$$y_{\min} = \max[\max_{i=1}^{n}(y_i - C_i\beta), y_{t-1} - v_{\max}] \quad (5)$$

$$y_{\max} = \min[\min_{i=1}^{n}(y_i + C_i\beta), y_{t-1} + v_{\max}] \quad (6)$$

若上一时刻没有合法样本,采样区域则不考虑速度约束条件。

过滤阶段,仅保留满足式(2)要求的样本,不满足要求的样本点丢弃掉。过滤表达式如下:

$$\text{filter}(l_t) = \forall a \in A, \quad C_a\alpha \leqslant d(l_t, a) \leqslant C_a\beta \quad (7)$$

式中:A 为锚节点集合,$d(l_t, a)$ 表示锚节点 a 与当前时刻样本点之间的距离。

不断重复预测和过滤过程,直到获得足够的合法样本。普通节点的位置估计坐标为所有合法样本坐标的平均。

2.2　虫洞攻击对 MMCL 的影响

本文假设虫洞攻击由 W_1、W_2 两个位于网络不同区域的攻击节点协同发起,攻击节点之间建立一条双向对称的虫洞链路。攻击节点从一端侦听周围节点的数据包,并通过虫洞链路在另一端传输。本文参考文献[9]部署虫洞攻击节点,考虑虫洞链路长度大于 2 倍节点通信半径的情况。

虫洞攻击对 MMCL 算法的两个阶段都有严重的影响。第 1 阶段中,虫洞攻击导致节点间跳数小于真实值,从而影响锚节点计算平均跳距。如图 1 所示,锚节点 S_1 到 S_2 间的真实路由为 $S_1 \rightarrow N_5 \rightarrow N_6 \rightarrow N_7 \rightarrow S_2$,跳数为 4;在虫洞的影响下,$S_1$ 的数据包被攻击节

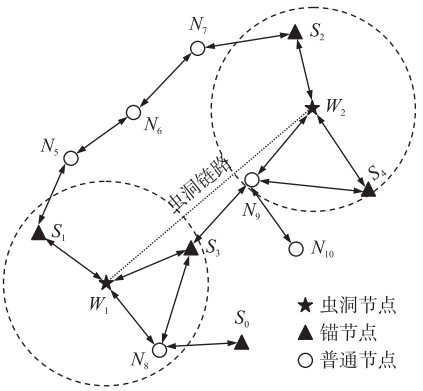

图 1　虫洞攻击对跳数的影响

点 W_1 捕获,并在 W_2 端重放,此时的路由为:S_1→虫洞链路→S_2,跳数为 1,跳数信息小于真实值。在此基础上,锚节点由式(1)计算平均跳距时导致平均跳距结果偏大,使计算结果出现偏差。

在 MMCL 算法的第 2 阶段,需要利用满足式(2)约束条件的锚节点构建锚盒子和采样盒子。若存在虫洞攻击,锚盒子的约束条件也会出现较大偏差,严重影响蒙特卡罗定位过程,导致定位误差进一步增大,甚至出现锚盒子无法建立的情况影响节点定位率。

因此,虫洞攻击能对 MMCL 算法各阶段造成严重的破坏,影响定位算法的有效性和可靠性。

3 抵御虫洞攻击的安全定位算法

针对虫洞攻击的攻击特性和对 MMCL 算法的影响,本文受文献[11]启发,依据锚节点距离约束条件和节点邻居关系,发现并区分受攻击的传感器节点,断开虚假链路,从而保证 MMCL 算法在第 1 阶段得到更准确的锚节点平均跳距,减小虫洞攻击的影响,提高定位精度。

3.1 网络模型与基本假设

本文假设虫洞节点 W_1、W_2 范围内的传感器节点集合分别为 V_{W1}、V_{W2},V_{W1}和 V_{W2}中的节点通过虫洞链路与彼此相连,互为邻居节点。如图 1 所示,普通节点 N_9 的真实邻居节点为{S_3、S_4、N_{10}},受虫洞攻击影响,为邻居节点为{S_1、N_8}。

所有节点在定位周期初始向相邻节点广播 HELLO 消息,建立自己的邻居节点列表,HELLO 消息包括节点类型、节点 ID,锚节点还包括节点位置坐标。虫洞攻击导致在建立邻居节点列表过程中出现异常现象。

因此,本文的研究目标是通过邻居节点列表异常检测找到受虫洞影响的传感器节点,并区分得到集合 V_{W1}、V_{W2},断开虫洞建立的虚假链路,使邻居节点列表接近未受攻击时的情况。

为标记区分节点,本文将未受攻击的节点标记为'N',受攻击的节点标记为'S',其中,集合 V_{W1}中的节点标记为'S_1',集合 V_{W2}中的节点标记为'S_2'。所有节点在定位初始都被标记为'N'。

3.2 LB-MMCL 安全定位算法描述

当节点运动到虫洞范围中,数据包通过虫洞链路与另一端虫洞范围中的节点建立邻居关系,影响 MMCL 算法的定位过程。因此,最简单直接的方法就是找到虫洞两端受攻击的节点,并断开虚假链路。

LB-MMCL 安全定位算法分为锚节点标记、普通节点标记和安全定位 3 个阶段。

①锚节点标记

初始时,所有节点标记为'N',假设节点未受到攻击。锚节点检测的基本思想是:距离约束机制(BL1)——节点数据包的传输范围不能超过通信半径 r,若锚节点在构建邻居列表时,检测到与邻居锚节点的距离大于 r,则判断该锚节点受到攻击,标记为'S'。如图 1,锚节点 S_1 和 S_4 因虫洞链路建立邻居关系,但通过锚节点坐标计算出两节点间的距离 d 大于 r,则将 S_1 和 S_4 标记为'S'。对于未检测到异常的锚节点,保持原来的标记'N'。

完成邻居列表创建后,对标记为'S'的锚节点按照地理位置关系区分为两类:W_1 攻击节点范围内、W_2 攻击节点范围内。区分方法为:比较两个标记为'S'锚节点的邻居节点列表,若邻居节点列表相同,则归为一类,若具有不同的邻居节点列表,则归为另一类,并假设标记为'S'且节点 ID 最小的锚节点受 W_1 攻击,另一类受 W_2 攻击。以图 1 中锚节点为例,锚节点 S_1、S_2、S_3、S_4 违反距离约束机制,标记为'S',S_1、S_3 具有相同的邻居锚节点列表{S_2、S_4}且 S_1 为 ID 最小,因此 S_1、S_3 假设受 W_1 攻击,重新标记为'S_1',同理,S_2、S_4 为另一类受 W_2 攻击的锚节点,重新标记为'S_2'。锚节点标记伪代码如图 2 所示。

Algorithm 1 Beacon Node Labeling

1: Each node B_i broadcasts a Hello Message to its neighbors and build its neighbor list.
2: if B_i detects the wormhole attack using scheme BL1 then
4: B_i is labeled with'S'.
5: end if
6: B_i builds the W_1 and W_2 based on its neighbor list which built in step 1.
7: B_i searches itself in both sets.
8: if B_i is found in the W_1 then
9: B_i is labeled with'S_1'.
10: else B_i is labeled with'S_2'.
11: end if

图 2 锚节点标记伪代码

②普通节点标记

仅断开锚节点间的虚假链路还不足以抵御虫洞攻击,还需要对普通节点进行虫洞检测标记区分。

遭受攻击的锚节点向邻居节点广播警报信息,警报信息包括受攻击的锚节点集合及锚节点的标记,收到警报消息的普通节点标记为'U',表示可能受到虫洞攻击的影响。再对标记为'U'的普通节点进行虫洞攻击检测,检测基本思想为:消息唯一性机制和距离约束机制。

消息唯一性机制(SL1):普通节点不可能收到

来自同一邻居锚节点的数据包两次。如图 1 所示,普通节点 N_9 收到两份来自 S_3 的消息:一份直接来自 $S_3 \rightarrow N_9$,另一份来自虫洞链路重放 $S_3 \rightarrow$ 虫洞链路 $\rightarrow N_9$。因此若违反消息唯一机制,则表明节点遭受虫洞攻击,将其标记为'S'。这种情况下,普通该节点进一步检测锚节点的标记,若锚节点标记为'S_1',则普通节点标记为'S_2',若锚节点标记为'S_2',则普通节点标记为'S_1'。例如,此时 N_9 检测到 S_3 标记为'S_1',则 N_9 标记为'S_2'。

距离约束机制(SL2):根据几何关系可知,普通节点的任意两个邻居锚节点间的距离小于 $2r$,若检测到异常情况,则判断普通节点受到虫洞攻击。以图 1 中 N_8 为例,其邻居锚节点为{S_0、S_2、S_3、S_4},其中根据锚节点坐标,计算得到 S_0、S_2 之间的距离大于 $2r$,则判断 N_8 受虫洞攻击,N_8 标记为'S'。这种情况下,进一步检测锚节点的标记,若其中一个锚节点标记为'N',检测另一个锚节点标记,若另一个锚节点标记为'S_1',则普通节点把自己标记为'S_2';若锚节点标记为'S_2',则普通节点标记为'S_1'。例中 N_8 检测到 S_0 标记为'N',则继续检测 S_2 的标记为'S_2',则 N_8 标记为'S_1'。

对于其他被标记为'S'的普通节点(SL3),对比其邻居锚节点列表和受攻击的锚节点集合,若受攻击的锚节点 S_j 不在邻居锚节点列表中,则以 S_j 的标记作为自己的标记。

Algorithm 2　Sensor Node Labeling

1:　sensor labels itself with 'U' if it receives an Alert message from neighbor beacon.
2:　if S_i is labeled with 'U' then
3:　S_i conducts the sensor nodes labeling schemes SL1, SL2 and SL3.
4:　end if

图 3　普通节点标记伪代码

③安全定位

将网络中被标记为'S_1'、'S_2'节点间的虚假链路断开,移除虫洞攻击带来的伪邻居节点,以减小定位误差。即,对于标记为的'S_1'所有节点,断开与只收到 1 份数据包且标记为'S_2'的节点之间的链路;同样的,对于标记为的'S_2'所有节点,断开与只收到 1 份数据包且标记为'S_1'的节点之间的链路。

完成虚假链路移除工作后,即可按照原来的方法计算锚节点平均跳距,根据 MMCL 算法构建锚盒子和采样盒子,完成蒙特卡罗定位。

LB-MMCL 算法标记并区分受攻击的节点,断开虚假链路,虫洞攻击对定位过程的影响被降低。通过这种方法能够有效地抵御虫洞攻击的干扰,完成安全定位过程。

4　实验仿真与性能分析

本节对 MMCL 算法、受虫洞攻击的 MMCL 和安全定位算法进行实验仿真,分别从定位精度、定位率、锚节点密度、节点移动速度和样本数等多个角度分析算法性能,并与文献[9]中的算法进行比较。

实验中将 80 个节点随机部署在 500 m×500 m 的矩形区域内,节点通信半径为 r,最大移动速度为 V_{max},所有节点按照随机行走(Random WayPoint)模型沿任意方向随机移动。虫洞节点的位置坐标参考文献[9]进行设置。假设时间被分为离散的时间单位 T(s),在每个时间单位对移动的节点进行定位。具体默认仿真参数设置表 1 所示。

表 1　仿真参数典型值设置

参数名	参数值
节点通信半径 r	100 m
节点密度 N_d	10
锚节点密度 S_d	3
节点最大移动速度 V_{max}	20 m/s
样本数 N	50
虫洞节点坐标(W_1/W_2)	(150,150)/(350,350)
通信模型(DOI)	单位圆(DOI=0)

每种算法仿真随机运行 100 次,受虫洞攻击的算法称为 Wormhole-MMCL,定位误差为每个时刻定位均方误差的平均值。

图 4、图 5 分别为 MMCL、受攻击的 MMCL 和 LB-MMCL 3 种算法的定位误差和定位率随时间的变化曲线。

从图 4、图 5 可见,MMCL 利用网络中的全部锚节点信息,结合运动模型和历史定位信息,获得较高的定位精度和定位率。受虫洞攻击后,MMCL 算法定位误差从 0.14r 提高到 0.26r,增加一倍;同时,虫洞攻击导致在蒙特卡罗定位阶段锚盒子和采样盒子无法正常建立,使定位率从 98%下降到 96%左右。LB-MMCL 通过断开虫洞建立的虚假链路,有效抵御

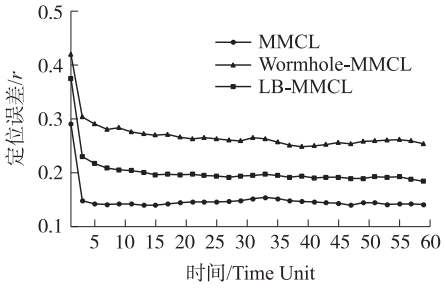

图 4　定位误差随时间的变化曲线

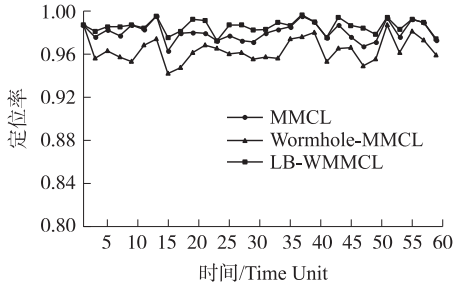

图 5 定位率随时间的变化曲线

虫洞攻击,明显改善定位误差至 0.2r 附近;在锚盒子建立过程中剔除伪锚节点,使定位率恢复到较高的水平。

平均定位误差随锚节点密度变化曲线如图 6 所示。随着锚节点密度的增大,网络中锚节点比例上升,可利用的定位参考信息增多,3 种算法的平均定位误差变小;因为 LB-MMCL 算法对普通节点攻击检测依赖于锚节点,因此,当锚节点密度 s_d<1 时,LB-MMCL 对定位误差的改善并不明显;但随着锚节点密度的继续增大,s_d>1 时,标记机制识别虫洞范围内的锚节点和普通节点数增加,LB-MMCL 定位误差不断减小,最终接近无攻击时的定位误差曲线。

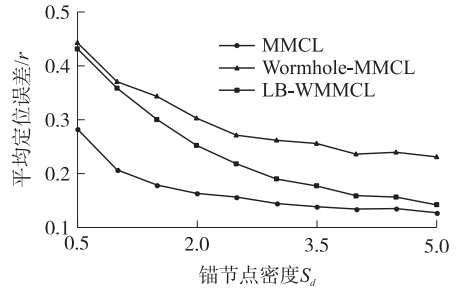

图 6 平均定位误差随锚节点密度的变化曲线

分析图 7,可以得出:随着节点移动速度的增大,3 种算法的定位误差逐渐增加。这是因为网络中锚节点密度决定了节点获得的定位参考信息保持不变,但单位时间内节点移动距离增大,上一时刻计算的锚节点平均跳距与当前时刻相比偏差变大,使采集的样本准确性降低,定位误差变大。LB-MMCL 算法对虫洞攻击情况下的 MMCL 定位误差改善明显,在相同节点移动速度的情况下,LB-MMCL 的定位精度始终高于受攻击的情况。

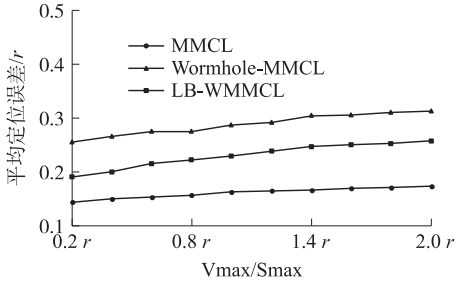

图 7 平均定位误差随节点移动速度的变化曲线

图 8 为算法平均定位误差随样本数的变化曲线,由图可知:MMCL 会随着样本数的增加定位精度逐渐提高。因为在蒙特卡罗定位阶段,利用带有权值的样本点集合来估计普通节点的位置坐标,增加样本数对定位精度提高有积极作用,但同时样本数增加会导致算法的计算量提高。样本数 N>50 时,定位精度提高缓慢,综合考虑定位误差和算法计算量,本实验中选取样本数为 50。

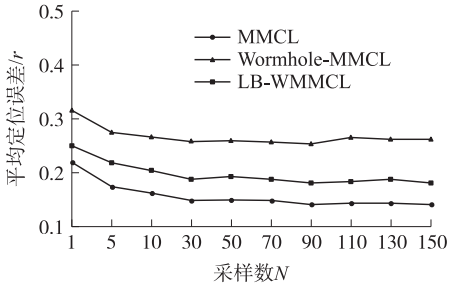

图 8 平均定位误差随样本数的变化曲线

为了进一步验证本算法在移动、受虫洞攻击情况下的定位误差和定位率改进效果,我们用文献[9]中的算法与本算法进行比较,文献[9]对受虫洞攻击情况下的 MCL 算法(图中表示为 Wormhole-MCL)进行改进,由图 9 和图 10 仿真结果可知,文献[9]算法仅利用了两跳范围内的锚节点信息,而 LB-MMCL 几乎利用了全网内所有的锚节点信息,因此 LB-MMCL 比文献[9]算法的定位精度和定位率在效果及收敛性方面要好得多;同时,LB-MMCL 需要在全网内洪泛锚节点信息,增加了网络通信量;

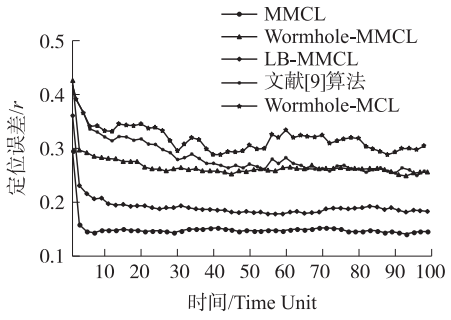

图 9 定位误差随时间的变化曲线

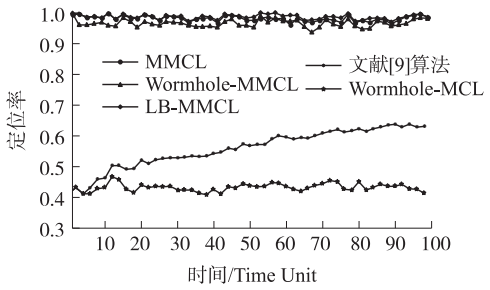

图 10 定位率随时间的变化曲线

虫洞检测时,文献[9]算法需要计算上一时刻所有样本点与两跳锚节点间的距离,此过程带来的计算量非常大;本算法为了抵御虫洞攻击,需要判断锚节点间的距离是否合理,但由于网络中锚节点比例较小,因此该过程计算量增加也较少;同时,受攻击的锚节点向外广播警报信息,需要增加网络通信量,这个增加量与受攻击的锚节点个数成正比;但网络中受到较少的虫洞攻击时,本算法计算量的增加还是较少。另一方面,本算法检测到虫洞攻击后,并不是简单的丢弃受攻击节点,而是针对节点邻居关系,断开虚假节点,较好的避免了因丢弃节点造成的网络连通度降低的现象,从而获得较高的定位精度和定位率,文献[9]算法利用节点移动性检测虫洞,导致算法收敛性低,定位率差。

总而言之,在受虫洞攻击时,本算法与文献[9]算法比,能获得更好的定位精度和定位率,实现虫洞攻击下的安全定位。

5　结论

本文总结了 MWSN 安全定位技术的研究现状,分析了虫洞攻击对 MMCL 性能的影响,并提出了一种抵御虫洞的安全移动节点定位算法 LBMMCL。本算法根据距离约束机制和消息唯一性原则,检测节点邻居列表中的异常,标记并区分两个虫洞范围内的节点,断开虚假链路以减轻虫洞攻击对锚节点平均跳距的不利影响,提高定位算法的抗攻击能力,在不需要额外硬件的基础上能有效抵御虫洞攻击对 MMCL 的影响。

参考文献:

[1] 王静,邓平. 一种基于边松弛的大规模 WSN 分簇定位算法[J]. 传感技术学报,2013,26(5):683-688.

[2] Tseng C L,Cheng C S,Chen C W,et al. A Localization Method Using the Bee Colony Algorithm for Mobile Wireless Sensor Networks[C]//International Automatic Control Conference,2016:194-199.

[3] Zhang Y,Cui L,Chai S. Energy-Efficient Localization for Mobile Sensor Networks Based on RSS and Historical Information[C]//Control and Decision Conference. IEEE,2015:5246-5251.

[4] Luan J,Zhang R,Zhang B,et al. An Improved Monte Carlo Localization Algorithm for Mobile Wireless Sensor Networks[C]//International Symposium on Computational Intelligence and Design. IEEE,2015:477-480.

[5] Yi J Y,Yang S W,Cha H J. Multi-Hop-Based Monte Carlo Localization for Mobile Sensor Networks[C]//Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor,Mesh and Ad Hoc Communications and Networks,2007:163-171.

[6] Zeng Y P,Cao J N,Hong J,et al. SecMCL:A Secure Monte Carlo Localization Algorithm for Mobile Sensor Networks[C]//IEEE 6th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS),2009:1054-1059.

[7] Garg R,Varna A,Wu M. A Gradient Descent Based Approach to Secure Localization in Mobile Sensor Networks[C]//IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP),2012:1869-1872.

[8] Kumari V R,Nagaraju A,Pareek G. Wormhole Attack Behaviour in Monte-Carlo Localization for Mobile Sensor Networks[J]. Journal of Sensor Technology,2014,4(2):48-58.

[9] 池玉辰,邓平. 一种移动无线传感器网络抵御虫洞攻击 MCL 算法[J]. 传感技术学报,2015,28(6):876-882.

[10] 曹璐,熊深文,李嘉俊. 基于 MCB 的移动节点安全定位算法[J]. 微型机与应用,2017(16):1-4.

[11] Wu J,Chen H,Lou W. Label-Based DV-Hop Localization Against Wormhole Attacks in Wireless Sensor Networks[C]//International Conference on Networking. IEEE Computer Society,2010:79-88.

[12] 陈立建,金洪波,毛科技,等. 抵御虫洞攻击的无线传感器网安全定位算法[J]. 传感技术学报,2016,29(12):1882-1887.

鲍　露(1993-),女,汉族,硕士研究生。主要从事移动无线传感器网络安全定位技术的研究;

邓　平(1964-),男,汉族,博士,教授。主要研究方向有无线网络定位技术,现代信号处理,无线传感器网络等。