·安全技术· 文章编号：1000-3428(2016)10-0151-07 文献标志码：A 中图分类号：TP393

无线传感器网络中基于 RSSI 一致性的安全定位方法

朱青青[1]，杨玉斌[2]，刘 娜[1]，马秋环[1]

（1. 青岛黄海学院 机电工程学院，山东 青岛 266427；2. 中国电子科技集团公司第四十一研究所，山东 青岛 266580）

摘 要： 无线传感器网络通常部署在无人值守的敌对环境中，容易受到攻击节点的影响，给其应用带来较大挑战。针对该问题，利用移动信标节点，提出一种基于接收信号强度指示器（RSSI）一致性实现未知节点安全定位的方法。该方法通过计算未知节点接收到的数据包 RSSI 的方差，将方差较小的一组所对应的节点信息剔除，从而抑制虫洞攻击对定位的影响。仿真结果表明，该方法能有效消除虫洞攻击对节点定位的影响。

关键词： 接收信号强度指示器；无线传感器网络；虫洞攻击；移动信标节点；安全定位

中文引用格式： 朱青青，杨玉斌，刘 娜，等. 无线传感器网络中基于 RSSI 一致性的安全定位方法[J]. 计算机工程，2016，42(10)：151-157，163.

英文引用格式： Zhu Qingqing，Yang Yubin，Liu Na，et al. Secure Localization Method Based on Consistency of RSSI in Wireless Sensor Network[J]. Computer Engineering，2016，42(10)：151-157，163.

Secure Localization Method Based on Consistency of RSSI in Wireless Sensor Network

ZHU Qingqing[1]，YANG Yubin[2]，LIU Na[1]，MA Qiuhuan[1]

（1. School of Mechanical and Electrical Engineering，Qingdao Huanghai University，Qingdao，Shandong 266427，China；
2. The 41st Institute of China Electronics Technology Group Corporation，Qingdao，Shandong 266580，China）

【Abstract】 Wireless Sensor Network（WSN）is often deployed in hostile environments，in which malicious attackers can easily disrupt the nodes' localization procedure to challenge the WSN-based applications. A new method of secure unknown node localization is proposed on the basis of the consistency of Received Signal Strength Indicator（RSSI）by using mobile beacon node. The proposed secure localization scheme can counteract the impacts of wormhole attack by eliminating the group of beacon information with a smaller variance of RSSI. Simulation results show that this method can effectively eliminate the influence of wormhole attack on node location.

【Key words】 Received Signal Strength Indicator（RSSI）；Wireless Sensor Network（WSN）；wormhole attack；mobile beacon node；secure localization

DOI： 10.3969/j.issn.1000-3428.2016.10.027

1 概述

近年来，随着微机电系统和无线通信技术的快速发展和日趋成熟，无线传感器网络（Wireless Sensor Network，WSN）的研究得到了越来越多研究机构和学者们的关注，已经成为一个非常热门的研究领域。目前，无线传感器网络有着广泛的应用，包括移动目标追踪与定位、油气管道监测、医疗监护和智能家居等。然而，上述许多应用都是基于网络中的节点位置信息已知的条件下。例如油气管道监测过程中，一旦无线节点检测到油气泄漏，即可及时将该事件通过无线传输方式通知后台中心服务器，以便快速有效地做出响应。然而，检测到泄漏点的节点如果没有位置信息，整个响应过程将会大打折扣。因此，在这类无线传感器网络应用中，节点监测的事件与节点的物理位置信息有着密切的关系，两者同等重要，缺一不可。

无线传感器网络中的节点通常可分为 2 类：信标节点（Beacon）和未知节点（Unknown）。其中，信标节点可通过人工部署或者 GPS 获得其自身位置信

基金项目： 国家自然科学基金资助项目（61309023）；山东省自然科学基金资助项目（ZR2013FQ032）；山东省重点研发计划基金资助项目（2015GGX101045）。

作者简介： 朱青青（1984—），女，讲师、硕士，主研方向为故障诊断与信息处理；杨玉斌，硕士；刘 娜、马秋环，讲师、硕士。

收稿日期： 2015-09-28 **修回日期：** 2015-12-17 **E-mail：** zhuqq1225@163.com

息,未知节点则是位置信息未知,需要通过节点定位过程来获取其位置。无线传感器网络中节点的定位可分为基于距离的(Range-based)和距离无关的(Range-free)定位方法。基于距离的定位方法中,未知节点通过测量其与信标节点之间的距离信息或者角度信息,结合信标节点的坐标计算其自身坐标,包括到达时间差(Time Difference of Arrival, TDoA)[1]、接收信号强度指示器(Received Signal Strength Indicator, RSSI)[2]和达到角度(Angle of Arrival, AoA)[3]等。距离无关的定位方法则是利用网络特性,如跳数,常见的方法有距离向量算法(Distance Vector Hop, DV-Hop)[4]、近似三角形测试法(Approximate Point-In-Triangulation, APIT)[5]、Fingerprinting[6]等。

然而,无线传感器网络经常部署在无人值守的敌对环境中,攻击节点能够轻易地入侵到网络中,使网络的正常功能受到干扰。因此,无线传感器网络成功应用的前提之一是能够解决网络安全问题。在无线传感器网络中,攻击节点通常可分为外部攻击节点(external attackers)和内部攻击节点(internal attackers),其中,外部攻击节点无需获得系统的认可,即可对网络功能进行干扰和破坏,而内部攻击节点需要获得系统认证并获得相关的密钥信息。本文针对外部攻击节点(虫洞攻击),提出一种利用移动信标节点,基于接收信号强度指示器一致性的安全定位方法。

2 相关工作

近年来,无线传感器网络安全定位技术得到了越来越多学者的关注,并且取得了一系列研究成果。无线传感器网络安全定位方法可分为 2 类:基于固定节点的安全定位方法[7-8]和基于移动节点的安全定位方法[9-10]。这 2 类方法都是通过估计未知节点与相邻节点的距离来进行定位,常见的测距方法包括 RSSI, AoA, TDoA[1]等。在文献[1]中,利用无线多跳网络时空特性与测距数据的一致性,提出一种针对基于 TDoA 定位中虫洞攻击的检测方法(Temporal Spatial Consistency based Detection, TSCD),能够有效地检测出虫洞攻击并且实现安全定位。

虫洞攻击通常是由 2 个相互合作的攻击节点共同发起,其对节点定位过程的影响不可忽视。目前,学者们提出了许多针对虫洞攻击的检测方法。文献[11]提出一种基于扇区唯一特性与通信距离违背特性的虫洞攻击检测方法,并通过对受攻击的信标节点的识别与剔除实现了抵御虫洞攻击的安全定位。文献[12]在文献[11]基础上考虑了天线的可旋转性以及功率等级的变化,利用更为丰富的信息来提高定位精度,并引入了原始加密法来确保 Beacon 传播的安全性。文献[13]分析虫洞攻击对 DV-Hop 定位过程的影响,通过异常节点的剔除,实现了无线传感器网络中抵御虫洞攻击的 DV-Hop 安全定位。文献[14]提出一种基于移动节点的定位算法,并且分析了 3 种不同的移动节点轨迹对定位精度的影响。文献[15]提出 2 种攻击检测方法,分别是采用一致性检测出异常的距离信息和采用网格投票选举的方法分离伪造的信息,在定位过程中将检测出来的异常距离信息剔除掉以实现安全定位的目标。文献[16]提出一种基于移动信标节点来检测虫洞攻击并且对虫洞攻击节点进行准确定位的方法,但该方法并没有考虑网络中未知节点的安全定位问题。

3 基于移动信标节点的节点定位过程

3.1 网络部署

无线传感器网络可以应用于检测网络中的特定事件。网络中随机部署一批传感器节点(Sensor),每个传感器节点的位置在网络部署完成后是固定不变的,但其自身并不能获得位置信息。为了让网络中的传感器节点获取自身位置信息,网络中专门部署了一个移动信标节点(Mobile Beacon),该信标节点可以通过 GPS 实时获取其位置信息。移动信标节点在网络中沿着特定轨迹移动,并且在移动过程中不断广播自身的位置信息。传感器节点通过接收来自移动信标节点的信息,运用特定的定位算法进行定位。由于网络经常部署在野外等敌对环境下,网络中还存在成对出现的虫洞攻击节点(Wormhole Attacker),每对攻击节点通过合作的方式共同发起虫洞攻击,对传感器节点的定位过程产生干扰。假设网络中的所有节点的通信半径均为 R,且不考虑通信范围之内的信息交互过程的丢包。

3.2 定位过程

为辅助传感器节点定位,移动信标节点可以在网络中进行“扫描式”移动。如图 1 所示,移动信标节点首先进行水平方向的扫描。假设整个网络部署在一个矩形区域,以网络部署区域的左下角为原点,建立坐标系(如图 1 中的 O 点)。移动信标节点从原点出发,以步长 L_p 沿 X 轴正方向移动,运动到网络部署区域的右边界后再以步长 L_h 沿 Y 轴正方向移动一个步长,然后沿 X 轴负方向移动,如图 1所示移动路径,移动信标节点完成对整个网络的水平扫描。

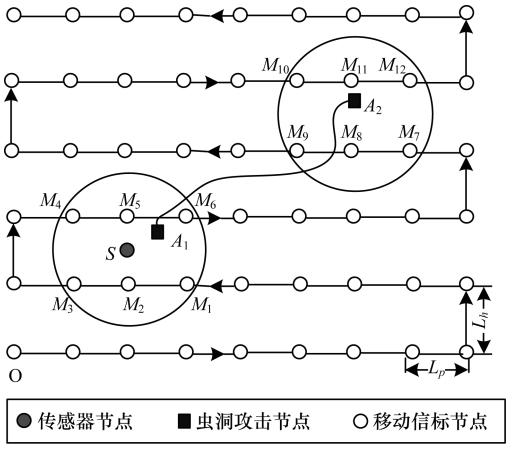

图 1　移动信标节点的水平扫描移动路径

移动信标节点每次移动到一个新的位置,都会通过 GPS 获取当前位置信息,并将其位置信息以及 ID 通过广播数据包的形式发送给邻居节点。邻居节点接收到广播信号后,即可保存发送端的位置信息以及接收数据包的信号强度,即 RSSI。如图 1 所示,当移动信标节点移动到 M_1 点时,传感器节点 S 能够接收到广播信号,同样的,当移动信标节点移动到 M_2 和 M_3 点时,S 也能够接收到信标节点的广播信号,之后,S 可以根据接收到的对应于不同位置的移动信标节点的位置信息,将$\overline{M_1M_3}$估计为 S 的传输区域的弦,根据圆心在弦的中垂线上这一规律,S 即可将$\overline{M_1M_3}$的中点的横坐标作为 S 的横坐标。因此,当移动信标节点以水平方向扫描完整个网络之后,网络中的所有位置未知的传感器节点都能够得到各自的横坐标。

移动信标节点完成水平方向扫描后,重新回到原点,进行垂直方向扫描,其移动路径如图 2 所示,沿 Y 轴和 X 轴的移动步长分别为 W_h 和 W_p。

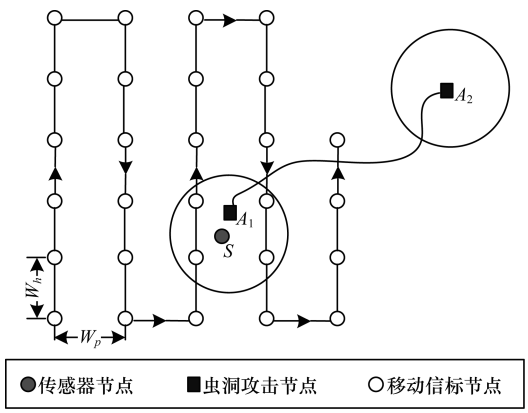

图 2　移动信标节点的垂直扫描移动路径

与上述过程类似,移动信标节点垂直扫描完整个网络后,所有位置未知的传感器节点均能够得到各自的纵坐标。因此,移动信标节点完成 2 次扫描,即可确保网络中的所有未知节点完成定位过程。本文所提出的安全定位方法是基于信标节点的移动辅助完成的,传感器节点需要在信标节点扫描完整个网络区域后才能完成自身定位,因此,本文所提出的方法只适用于对实时性要求不高的应用场景。

上述移动信标节点的移动过程中,移动步长必须要满足一定的关系才能使得定位过程正常进行。以水平扫描过程为例,为使移动信标节点穿过未知节点通信范围的过程中,在相应的弦上停留的位置的个数至少为 3,以降低横坐标的估计误差,下面研究移动步长 L_h 和 L_p 之间的关系分析。如图 3 所示,L_h 必须满足 $L_h<2R$。对于选定的 L_h,可以保证移动信标节点能够水平穿过未知节点 S 上下 $L_h/2$ 的区间。因此,为使得最坏情况下移动信标节点水平穿过未知节点 S 时,至少有一条弦上存在 3 个点,应满足:

$$2\sqrt{R^2-L_h^2/4}>4L_p$$

因此,对于移动信标节点的水平扫描过程,移动步长应满足式(1):

$$\begin{cases}L_h<2R\\ L_p<\sqrt{R^2-L_h^2/4}/2\end{cases}\tag{1}$$

类似地,移动信标节点的垂直扫描过程中,移动步长应满足式(2):

$$\begin{cases}W_p<2R\\ W_h<\sqrt{R^2-W_p^2/4}/2\end{cases}\tag{2}$$

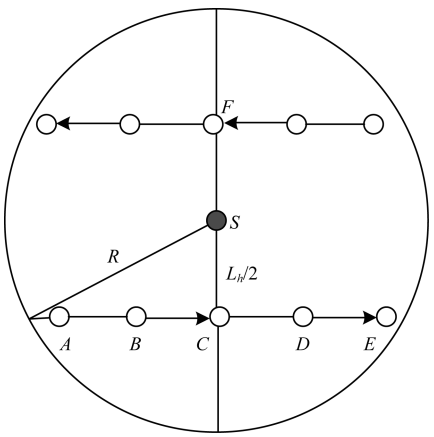

图 3　移动信标节点水平扫描过程中移动步长的确定

在传统定位过程中[1],一般是未知节点广播定位请求信号,邻居信标节点接收到请求信号后立即返回一个应答信号,以协助未知节点定位。然而,在这一过程中,未知节点需要在短时间内接收到多个邻居信标节点的应答信号,因此,不可避免会出现数据包冲突问题。然而,在本文所提出的基于移动信标节点的定位过程中,只有移动信标节点周期性地广播数据包,网络中的位置未知的传感器节点只需要接收数据包即可完成定位过程,即整个定位过程中只有移动信标节点发送数据包,其他节点都是接收数据包,因此,该定位方法能够有效地解决定位过程中的数据包冲突问题。同时,未知节点在估计其横坐标和纵坐标时,只需做简单的运算(计算 2 个点

的横坐标或者纵坐标的平均值),降低了节点定位过程的计算量,使得该定位方法尤其适用于计算能力有限的无线传感器节点。

4 基于 RSSI 一致性的安全定位方法

上述基于移动信标节点的定位过程,并没有考虑网络中可能存在攻击的威胁。当网络中存在虫洞攻击时,其定位过程将会受到严重的影响。本节首先分析了虫洞攻击对基于移动信标节点定位过程的影响,然后提出了一种基于 RSSI 一致性的安全定位方法,能够有效抵御虫洞攻击的干扰。

4.1 攻击模型

虫洞攻击是由一对相互协作的外部攻击节点共同发起,每个虫洞攻击节点都能监听其通信范围内的数据包,并且通过虫洞链路(Wormhole Link)将监听到的数据包发送给另一个虫洞攻击节点,再由该虫洞攻击节点将接收到的数据包广播给其邻居节点。每对虫洞攻击节点的虫洞链路是双向对称的,即数据包可以从任何一个攻击节点经由冲动链路转发给另外一个攻击节点。本文假设虫洞攻击节点的通信半径也是 R,但是由于虫洞攻击节点可以通过虫洞链路进行信息交互,它们之间的通信距离不受 R 的限制。虫洞攻击过程非常简单,但是其可以对定位过程产生严重的干扰,而且虫洞链路越长,其影响越严重。因此,本文所提出的安全定位方法只针对虫洞攻击对定位影响较为严重的条件,即虫洞链路长度大于 $4R$(对于虫洞链路长度小于 $4R$ 的条件,可以采用文献[17]方法解决)。

虫洞攻击能够严重影响上述基于移动信标节点的定位过程。如图 1 所示,网络中存在一对虫洞攻击节点 A_1 和 A_2,且未知节点 S 位于 A_1 的通信范围之内。当移动信标节点分别经过点 $M_1 \sim M_6$ 时,未知节点 S 能够接收到移动信标节点的广播信息,这一过程并不受虫洞攻击影响。但是,当移动信标节点继续移动,进入攻击节点 A_2 的通信范围之后,如图 1 中的点 $M_7 \sim M_{12}$,移动信标节点在这些位置广播的数据包能够被攻击节点 A_2 监听,并且通过虫洞链路转发到达 A_1,然后由 A_1 广播。因此,未知节点 S 能够接收到来自点 $M_7 \sim M_{12}$ 的移动信标节点的广播数据包,使得 S 在估计其横坐标过程中,在有可能参考点 $M_7 \sim M_{12}$ 所在位置的横坐标,最终偏离 S 的真实位置。同理,当移动信标节点做垂直扫描时,也可能出现上述问题,使得未知节点 S 估计出错误的纵坐标。并且,位于虫洞攻击节点 A_1 和 A_2 通信范围之内的所有未知节点的定位过程都能够受到虫洞攻击的影响,而且虫洞链路越长,影响越严重。因此,虫洞攻击能够严重干扰本文提出的基于移动信标节点的定位过程。为此,提出一种简单有效的抵御虫洞攻击的安全定位方法。

4.2 虫洞攻击的检测

为了抵御虫洞攻击对节点定位过程的影响,未知节点在定位之前,首先检测其是否受到虫洞攻击,即是否有虫洞攻击节点位于其通信范围之内。对此,本文借鉴了文献[17]提出的空间特性,即无线传感器网络中,如果节点 A 和节点 B 都能够和节点 C 通信,则节点 A 和 B 之间的距离不能超过 $2R$。

正常情况下,网络中的通信不会违背空间特性。但是当未知节点位于虫洞攻击节点通信范围之内,就可能会出现异常情况,违背上述特性。如图 1 所示,M_3 和 M_{12} 之间的距离大于 $2R$。当移动信标节点移动到 M_3 时,立即广播当前位置信息,此时 S 能够接收到该广播信息。当移动信标节点移动至 M_{12} 时,其广播数据包同样能够被 S 接收到(通过虫洞链路)。因此,S 能够判断出接收到来自 2 个相互之间距离大于 $2R$ 的位置的移动信标节点的数据包(S 能够从接收到的广播数据包中获得 M_3 和 M_{12} 的位置信息),即其通信过程违背了空间特性。因此,S 能够判断当前存在虫洞攻击,进而执行相应的安全定位方法。具体的虫洞攻击检测方法可以参见文献[17]。

4.3 基于一致性的 RSSI 信息区分

对于一个位于虫洞攻击节点通信范围内的未知节点,它能够接收到 2 组广播数据包:(1)移动信标节点移动至未知节点通信范围之内广播的数据包,假设为 m 个,如图 1 中的点 $M_1 \sim M_6$;(2)移动信标节点移动至另一个虫洞攻击节点通信范围之内广播的数据包,假设为 n 个,如图 1 中的点 $M_7 \sim M_{12}$。很明显,第 1 组数据包对于未知节点是正常的,其信息有助于未知节点的定位,而第 2 组数据包则是由于虫洞攻击的存在而引入的,是异常的,其信息会干扰未知节点的定位。因此,当未知节点检测到虫洞攻击存在时,可以先将其接收到的来自移动信标节点的所有数据包分成 2 组。由于每组数据包所对应的移动信标节点的位置都在同一个节点的通信半径之内,因此任意 2 个点之间的距离不会超过 $2R$。如图 1所示,点 $M_1 \sim M_6$ 都在 S 的通信范围之内,因此,它们任意 2 点之间的距离都小于 $2R$,而点 $M_7 \sim M_{12}$ 都在 A_2 的通信范围之内,因此,它们任意 2 点之间的距离也小于 $2R$。然而,2 组数据包所对应的位置之间必然存在距离大

于 $2R$ 的情况(虫洞链路长度大于 $4R$),因此,未知节点可以采用如下方法对数据包进行分组:从 $m+n$ 个点中选出距离最大的 2 个点,即点 A 和 B(A 和 B 之间的距离必然大于 $2R$),然后将与 A 点的距离大于 $2R$ 的点归入 B 点所在的组,将与 B 点的距离大于 $2R$ 的点归入 A 点所在的组。

引理 1　受到虫洞攻击时,未知节点采用上述方法即可将其接收到广播数据的移动信标节点的所有位置分成 2 组,并且其中一组在未知节点通信范围之内,另一组则在另一个虫洞攻击节点(与未知节点通信范围之内的虫洞攻击节点成对的另一个攻击节点)的通信范围之内。

证明:利用虫洞链路长度大于 $4R$ 这一条件即可证明。证明过程略。

当未知节点将上述位置分成 2 组之后,由于一组位置在其通信范围之内,另一组在另一个虫洞攻击节点通信范围之内,因此未知节点只要能够对 2 组位置信息进行区分,挑选出其通信范围之内的位置信息来进行定位,即可消除虫洞攻击的影响。如图 1 所示,当移动信标节点移动至 M_1 并广播数据包时,未知节点接收到该数据包后,即可测得相应的 RSSI,即信号强度指示值。因此,M_1 的广播数据包的 RSSI 大小与 M_1 和 S 之间的距离相关。同理,$M_2 \sim M_6$ 的广播数据包的 RSSI 大小均与它们到 S 之间的距离相关。然而,当移动信标节点移动至 M_7 并广播数据包,该数据包能够经过虫洞链路最终由 A_1 广播给 S,因此,其对应的 RSSI 大小与 M_7 和 S 之间的距离无关,而是与 A_1 和 S 之间的距离有关。同理,$M_8 \sim M_{12}$ 的广播数据包的 RSSI 大小均与 A_1 和 S 之间的距离有关。也就是说,移动信标节点在虫洞攻击节点通信范围内不同位置广播的数据包的 RSSI 值变化不大。因此,可以基于 2 组位置所对应的数据包的 RSSI 的一致性对它们进行区分。

定义 1　RSSI 一致性指的是距离相近的多对节点之间传输的数据包的 RSSI 的方差小于距离差别较大的多对节点之间传输的数据包的 RSSI 的方差。

由定义 1 可知,移动信标节点移动至未知节点传输范围之内的各个点位置广播的数据包的 RSSI 一致性较差。假设未知节点受到虫洞攻击,移动信标节点经过其通信范围之内的点为 m 个,其广播数据包对应的 RSSI 值分别为:

$$\{RSSI_1, RSSI_2, \cdots, RSSI_m\}$$

移动信标节点经过另一个虫洞攻击节点的通信范围之内的点为 n 个,广播数据包对应的 RSSI 值分别为:

$$\{RSSI'_1, RSSI'_2, \cdots, RSSI'_n\}$$

未知节点采用上述区分方法将 $m+n$ 个位置分为 2 组,比较 $\frac{1}{m}\sum_{i=1}^{m}(RSSI_i - \overline{RSSI})^2$ 和 $\frac{1}{n}\sum_{i=1}^{n}(RSSI'_i - \overline{RSSI'})^2$ 的大小,其中,$\overline{RSSI} = \frac{1}{m}\sum_{i=1}^{m} RSSI_i$;$\overline{RSSI'} = \frac{1}{n}\sum_{i=1}^{n} RSSI'_i$。方差较大的 RSSI 所在的组的位置信息将被未知节点用于定位过程,估计其横坐标和纵坐标,另一组位置信息则被剔除掉。通过该方法,未知节点即可实现安全定位。

5　仿真结果与分析

本文首先通过仿真分析虫洞攻击对本文提出的定位过程的影响,接着通过仿真来验证上述针对虫洞攻击所提出的安全定位方法的有效性,最后分析了移动信标节点的移动步长对安全定位方法性能的影响。

仿真过程中采用如下参数配置:传感器网络部署在 1 500 m × 1 500 m 的正方形区域,包括 100 个未知节点(在网络中随机分布),节点的通信半径 R = 150 m,网络中存在一对虫洞攻击节点,移动信标节点的移动步长满足式(1)和式(2)。图 4 是仿真过程中存在虫洞攻击的传感器网络节点分布图,其中,实心圆表示网络中随机分布 100 个未知节点;正方形表示分布网络中的一对虫洞攻击节点。

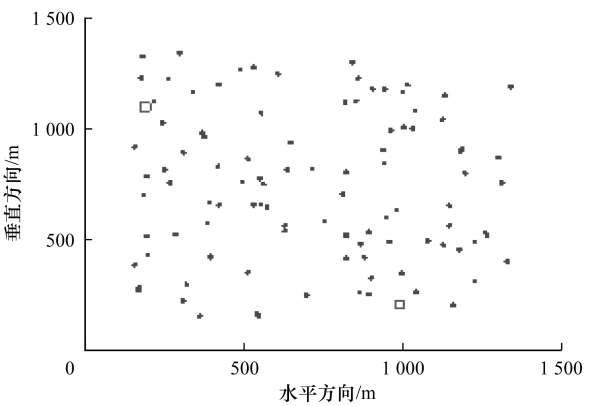

图 4　存在虫洞攻击的传感器网络节点分布

图 5 是不存在虫洞攻击的定位结果,实心圆表示的是未知节点的实际位置,圆圈表示的是本文提出的基于移动信标节点的定位方法所估计的未知节点的位置。从图 5 的结果可以看出,未知节点的估计位置和实际位置均比较接近,说明了本文提出的定位过程在没有虫洞攻击的条件下定位效果比

较好。

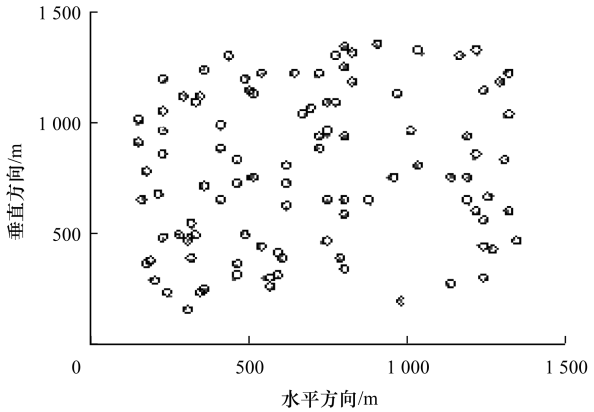

图 5 不存在虫洞攻击条件下基于移动信标节点的定位结果

图 6 是存在虫洞攻击但是未进行 RSSI 信息区分的定位结果，即不采用安全定位方法的定位结果。其中，实心圆表示网络中未知节点的实际位置；圆圈表示的是存在虫洞攻击条件下采用本文提出的定位方法的估计位置；直线的两端分别表示受到虫洞攻击的未知节点的实际位置和估计位置，因此，直线的长度显示了受到虫洞攻击影响的未知节点定位的误差大小。从图中可以看出，虫洞攻击对定位过程的直接影响是将未知节点的估计位置“拉伸”到另一个虫洞攻击节点附近，说明了虫洞攻击对本文提出的基于移动信标节点定位过程影响的严重性。

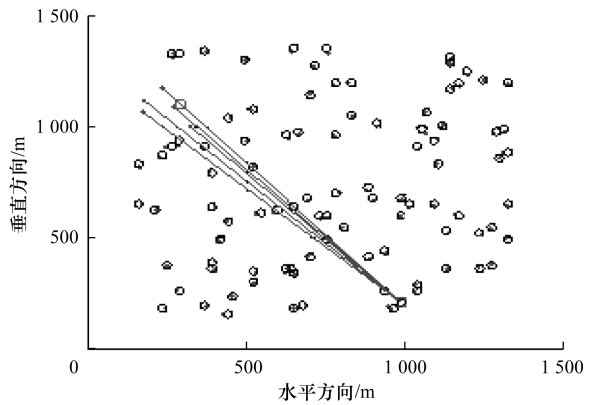

图 6 存在虫洞攻击条件下基于移动信标节点的定位结果

图 7 是存在虫洞攻击条件下采用本文所提出的基于移动信标节点的安全定位方法的定位结果。实心圆表示未知节点的实际位置，圆圈表示未知节点采用本文所提出的安全定位方法得到的估计位置。由图中的定位结果可以看出，采用本文所提出的安全定位方法得到的未知节点的估计位置与其实际位置比较接近，说明了该方法能够有效克服虫洞攻击对定位过程的影响。

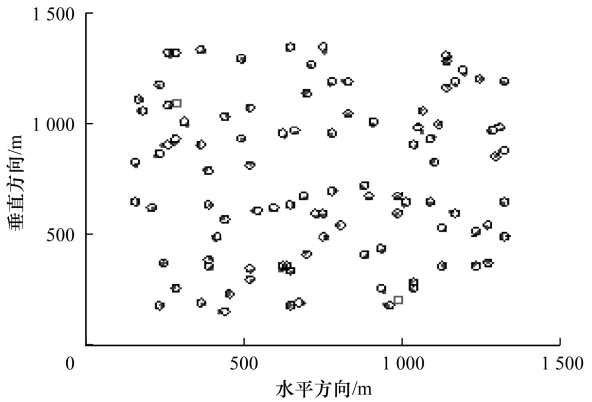

图 7 存在虫洞攻击条件下基于移动信标节点的安全定位结果

图 8 显示了 3 种不同的定位方法的定位误差，包括无虫洞攻击条件下的基于移动信标节点定位方法、存在虫洞攻击条件下的基于移动信标节点定位方法和存在虫洞攻击条件下的基于移动信标节点安全定位方法，随着移动步长 L_p 增大的变化趋势，其中，$L_p = W_h$。当移动步长 L_p 增大时，3 种方法的定位误差都增大。可知，本文所提出的基于移动信标节点的定位方法在虫洞攻击存在条件下，其定位误差将明显增大。同时，本文提出的安全定位方法定位误差与无虫洞攻击下的定位过程的定位误差基本一致，说明了本文提出的安全定位方法能够将虫洞攻击的影响基本消除。

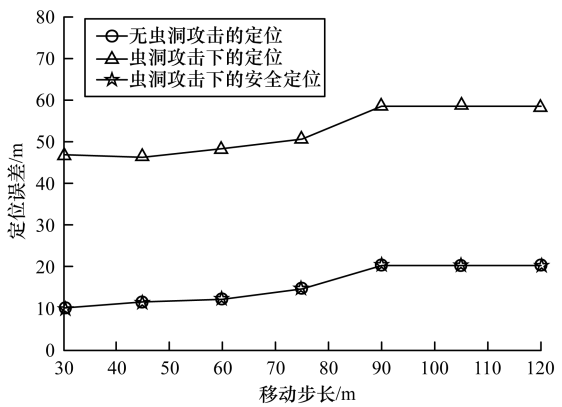

图 8 不同定位方法的性能比较

图 9 显示的是未知节点个数对本文所提出的安全定位方法的定位误差的影响。从图中曲线可以看出，当网络中未知节点数量改变时，安全定位方法的定位误差基本一致，说明了本文所提出的安全定位方法的性能不受未知节点密度影响。

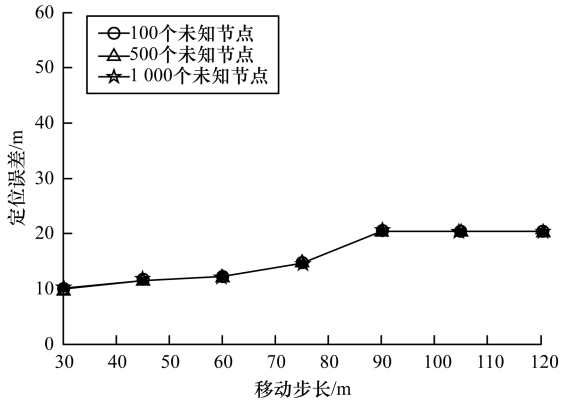

图 9　未知节点个数对定位结果的影响

图 10 反映了移动信标节点的移动步长 L_p 和 W_h 对所提出的安全定位方法定位误差的影响。如图所示,当 W_h 不变时,L_p 越大,其定位误差越大,这是由于 L_p 的增大将使得未知节点估计横坐标时的误差增大,进而增加定位误差。同样地,当 L_p 不变时,W_h 越大,其定位误差也越大,是由于 W_h 的增大使得未知节点估计纵坐标时的误差增大,进而增大定位误差。

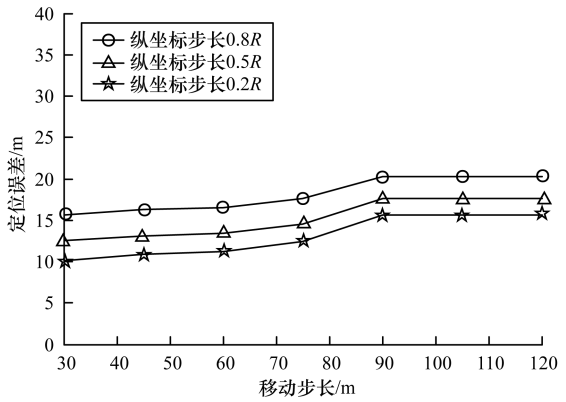

图 10　移动步长对安全定位方法定位误差的影响

图 11 说明了虫洞攻击节点对数对所提出的安全定位方法性能的影响。图中前 3 条曲线分别表示存在 3 对、2 对和 1 对虫洞攻击条件下,本文所提出的基于移动信标节点定位方法的定位误差。从中可以看出,在没有引入抵御虫洞攻击的策略下,虫洞攻击的对数越多,对定位过程的影响越大,使得整个网络的平均定位误差越大。而图中后 3 条曲线分别表示存在 3 对、2 对和 1 对虫洞攻击条件下,本文所提出的基于移动信标节点安全定位方法的定位误差。结果显示,本文所提出的安全定位方法不仅能够克服虫洞攻击对定位的影响,并且基本上不受虫洞攻击对数的影响,说明了该方法的有效性。

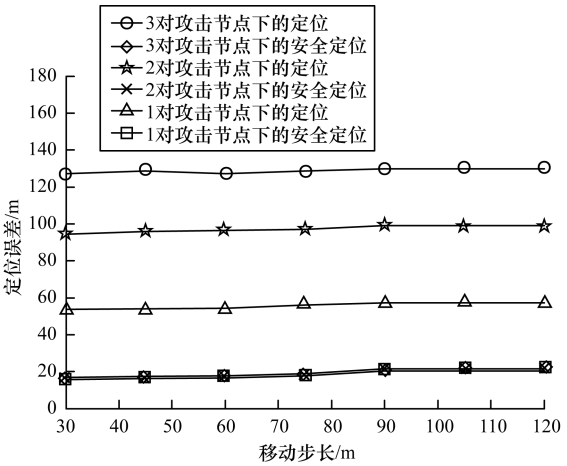

图 11　虫洞攻击对数对于定位性能的影响

6　结束语

本文针对无线传感器网络的节点定位问题,提出一种基于移动信标节点的定位方法。该方法主要利用未知节点和移动信标节点之间的通信链路来估计未知节点的位置,其计算复杂度小,适用于计算能力有限的无线传感器网络。同时,在定位过程中,只有信标节点广播数据包,能够有效解决节点定位过程中的数据包冲突问题。考虑虫洞攻击对该定位方法的影响,提出基于 RSSI 一致性的信息区分方法,以实现安全定位。仿真结果验证了本文方法的有效性。今后的研究方向是进一步将该方法扩展至适用于多组虫洞攻击的场景中。

参考文献

[1] 陈鸿龙,李鸿斌,王　智. 基于 TDoA 测距的传感器网络安全定位研究[J]. 通信学报,2008,29(8):11-21.

[2] Sichitiu M L, Ramadurai V. Localization of Wireless Sensor Networks with a Mobile Beacon [C]//Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems Conference. Washington D. C., USA:IEEE Press,2004:174-183.

[3] Priyanttha N, Miu A, Balakrisshman H, et al. The Cricket Compass for Context-aware Mobile Applications[C]// Proceedings of the 7th Annual International Conference on Mobile Computing and Networking. New York, USA:ACM Press,2001:1-14.

[4] Sit T, Liu Zheng, Ang M, et al. Multi-robot Mobility Enhanced Hop-count Based Localization in Ad-Hoc Networks[J]. Robotics and Autonomous Systems,2007, 55(3):244-252.

[5] He Tian, Huang Chengdu, Blum B, et al. Rang-free Localization and Its Impact on Large Scale Sensor Networks[J]. ACM Transactions on Embedded Computing System,2005,4(4):877-906.

[6] Bshara M, Orguner U, Gustafsson F, et al. Fingerprinting Localization in Wireless Sensor Network Based on Received Signal Strength Measurements: A Case Study on WiMAX Networks [J]. IEEE Transactions on Vehicular Technology,2010,59(1):283-294.

(下转第 163 页)

[5] 王　君,冀常鹏,汪　洋,等. P2P 网络中基于云模型的信任机制研究[J]. 计算机工程,2014,40(5):124-128.
[6] Sarat S,Terzis A. Measuring the Storm Worm Network:01-10-2007[R]. HiNRG Johns Hopkins University,2007.
[7] Kutzner K, Fuhrmann T. Measuring Large Overlay Networks——The Overnet Example[C]//Proceedings of the 14th Conference on Kommunikation in Verteilten Systemen. Berlin,Germany:Springer,2005:193-204.
[8] 黎梨苗,陈志刚,桂劲松,等. 基于优先权的 P2P 网络信任模型[J]. 计算机工程,2013,39(5):148-151.
[9] Starnberger G, Kruegel C, Kirda E. Overbot: A Botnet Protocol Based on Kademlia[C]//Proceedings of the 4th International Conference on Security and Privacy in Communication Networks. New York,USA:ACM Press, 2008:241-242.
[10] Wang Ping,Wu Lei,Aslam B,et al. A Systematic Study on Peer-to-Peer Botnets[C]//Proceedings of the 18th International Conference on Computer Communications and Networks. Washington D. C., USA: IEEE Press, 2009:1-8.
[11] Wang Ping, Aslam B, Zou C C. Peer-to-Peer Botnets: The Next Generation of Botnet Attacks[J]. Electrical Engineering,2010,24(4):1-25.
[12] 成淑萍,谭　良. 基于网络流量的僵尸网络动态检测模型[J]. 计算机工程,2014,40(11):106-112.
[13] Liu Xuejiao, Xiao Debao, Ma Nian, et al. A Scalable, Vulnerability Modeling and Correlating Method for Network Security[C]//Proceedings of the 4th International Conference on Scalable Information Systems. Washington D. C.,USA:IEEE Press,2009:217-227.
[14] Liu Xuejiao,Fang Chengfang,Xiao Debao,et al. A Goal-oriented Approach for Modeling and Analyzing Attack Graph[C]//Proceedings of International Conference on Information Science and Application. Washington D. C., USA:IEEE Press,2010:1-8.
[15] Stoica I,Morris R,Karger D,et al. Chord:A Scalable Peer-to-Peer Lookup Service for Internet Applications[C]// Proceedings of ACM SIGCOMM Computer Communication Review. New York,USA:ACM Press,2001:149-160.
[16] Rowstron A, Druschel P. Pastry: Scalable, Decentralized Object Location, and Routing for Large-scale P2P Systems[C]//Proceedings of International Conference on Distributed Systems Platforms. New York, USA: ACM Press,2001:23-29.
[17] Maymounkov P, Mazieres D. Kademlia: A Peer-to-Peer Information System Based on the Xor Metric[J]. Peer-to-Peer Systems,2002,32(2):53-65.
[18] Wang Binbin,Li Zhitang,Tu Hao,et al. Actively Measuring Bots in Peer-to-Peer Networks[C]//Proceedings of International Conference on Networks Security,Wireless Communications and Trusted Computing. New York, USA: ACM Press,2009:603-607.
[19] 邵秀丽,蒋鸿玲,耿梅洁,等. 基于关联关系和 Map Reduce 的僵尸网络检测[J]. 计算机工程,2014,40(5):115-119.

编辑　顾逸斐

(上接第 157 页)

[7] Doherty L D, Pister K S J P, Ghaoui L E. Convex Optimization Estimation in Wireless Sensor Networks[C]//Proceedings of the 20th Annual Joint Conference of IEEE Computer and Communications Societies. Washington D. C. , USA: IEEE Press, 2001: 1655-1663.
[8] So A M C,Ye Y. Theory of Semidefinite Programming for Sensor Network Localization[J]. Mathematical Programming,2007,209(2):367-384.
[9] Kushwaha M, Molnar K, Sallai J, et al. Sensor Node Localization Using Mobile Acoustic Beacons[C]//Proceedings of IEEE International Conference on Mobile Ad-hoc and Sensor Systems Conference. Washington D. C., USA:IEEE Press,2005:483-491.
[10] Priyantha B,Balakrishman H,Demaine E,et al. Mobile Assisted Localization in Wireless Sensor Networks[C]//Proceedings of the 24th Annual Joint Conference on IEEE Computer and Communications Societies. Washington D. C. , USA: IEEE Press, 2005: 172-183.
[11] Lazos L,Poovendran R. SeRLoc:Robust Localization for Wireless Sensor Network[J]. ACM Transactions on Sensor Networks,2005,1(1):73-100.
[12] Lazos L,Poovendran R. HiRLoc:High-resolution Robust Localization for Wireless Sensor Networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2):233-246.
[13] 陈鸿龙,王志波,王　智,等. 针对虫洞攻击的无线传感器网络安全定位方法[J]. 通信学报,2015,36(3):1-8.
[14] Jacques M, Makhoul B A, Mostefaoui A. A Mobile Beacon Based Approach for Sensor Network Localization[C]//Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. Washington D. C., USA:IEEE Press,2007:1-8.
[15] Liu D, Ning P, Du W. Attack-resistant Location Estimation in Sensor Networks[C]//Proceedings of the 4th International Symposium on Information Processing in Sensor Networks. Washington D. C., USA: IEEE Press,2005:99-106.
[16] Chen Honglong, Chen Wendong, Wang Zhibo, et al. Mobile Beacon Based Wormhole Attackers Detection and Positioning in Wireless Sensor Networks[J]. International Journal of Distributed Sensor Networks,2014(1): 1-10.
[17] Chen Honglong, Lou Wei, Wang Zhi. On Providing Wormhole Attack Resistant Localization Using Conflicting Sets[J]. Wireless Communications and Mobile Computing,2015,15(15):1865-1881.

编辑　刘　冰