文章编号:1671-4598(2024)12-0178-06 DOI:10.16526/j.cnki.11-4762/tp.2024.12.026 中图分类号:TP393 文献标识码:A

节点网络参数掩盖安全定位算法

王子豪[1], 胥 玲[2]
(1. 北京智慧城市网络有限公司, 北京 100176;
2. 中国电子科技集团公司 第15研究所, 北京 100083)

摘要: 对无线传感器网络的安全定位服务问题进行了研究, 采用了无线传感器网络的参数掩盖安全定位算法; 该方法将网络定位区域划分均匀分布的网格相位, 对存在恶意节点参与定位的多跳节点网络设计参数掩盖通信信号, 该信号中包含跳数和位置信息; 将网络中每跳参数掩盖信号沿多跳路径叠加, 产生多跳路径叠加信号的索引相位, 通过逐跳解算掩盖信号的相角, 并将其与相位索引矩阵匹配, 恶意节点转发叠加的多跳掩盖信号使得估计的位置和跳数信息难以与相位索引矩阵匹配, 从而筛选出恶意节点攻击的多跳路径; 利用网络中节点的身份信息提取恶意节点, 并对合法节点重新定位; 经实验测试实现了多跳叠加的参数掩盖信号消除恶意节点对网络的攻击, 有效抑制了恶意节点对合法节点定位精度的影响。

关键词: 无线传感器网络; 安全定位; 参数掩盖; 叠加信号; 索引相位

Secure Localization Algorithm with Parameter Masking for Note Network

WANG Zihao[1], XU Ling[2]
(1. Beijing Smartcity Network Co., Ltd., Beijing 100176, China;
2. The 15th Researach Institute, China Electronics Technology Group Corporation, Beijing 100083, China)

Abstract: The parameter masking secure localization algorithm for wireless sensor network (WSN) is used to study the issue of secure localization service in WSN. A parameter masking secure localization algorithm for wireless sensor network is proposed. The network localization area is divided into evenly distributed grid phases, and the parameter masking communication signal is designed for the multi-hop node network with malicious nodes participating in the localization, which contains the number of hops and position information. Each hop parameter masking signal in the network is superimposed along the multi-hop path to generate the superimposed signal index phase with the multi-hop path. The phase angle of the parameter masking signal is solved hop by hop and matched with the phase index matrix. The malicious node forwards the superimposed multi-hop masking signal, which makes the estimated position and hop information difficult to match with the phase index matrix, so as to screen out the multi-hop path attacked by the malicious node. The identity information of nodes in the network is used to extract malicious nodes, and relocate legitimate nodes. Through experimental testing, the parameter masking signal with multi-hop superposition eliminates the attack of malicious nodes on the network and effectively suppresses the influence of malicious nodes on the positioning accuracy of legitimate nodes.

Keywords: WSN; secure localization; parameter masking; superimposed signal partition; index phase

0 引言

无线传感网络 (WSN, wireless sensor network) 是由大量传感器节点通过无线自组网方式构成的无线节点感知网络。无线传感网络主要用于监测、检测和采集区域中的各类感知信息。在无线感知的节点网络中, 作为交换信息的多个小型设备称为传感器节点[1-2]。现有的 WSN 主要应用于军事和民用领域, 包括环境监测, 医疗救援, 目标跟踪侦查等[3-5]。由于无线传感器通常在大规模节点网络中工作, 因此, 它们容易受到恶意攻击[6-9]。在无线感知的节点网络的基本应用中, 未知节点的定位是传感器网络的关键组成要素, 节点定位主要应用于目标的状态检测、监测、追踪、传感器网络节点间的流量负载平衡及自动配置节点网络拓扑等。无线传感网络可以使物联网在任意时间、地点获取任何想要得到的监测信息, 而在无线传感网络中监测信息的采集节点的真实位置是至关重要的, 没有准确位置信息的监测信息毫无意义, 只有已知位置的监测信息才有理论研究意义和实际应用价值, 因此在无线传感网络中能够正确监测信息采集位置的定位技术成为无线传感网络研究的关键问题之一, 也是目前国内外的研究重点。目前, 国内外学者针对无线传感器网络定位性能的优化提出大量改进方法, 所提的改进算法根据网络类型和硬件性能指标的不同而不同, 定位算法依据的主要参考因素包括同构及异构网络、硬件型号、传感器的时效性、信号样式、室内及室外环境的信号传播特性、信号同步处理、网络通信开销、节点定位精度、节点灵活性等。其中, 误差要求是判断节点网络工作有效性的重要指标之一, 从而使得正确定位传感器节点成为无线传感网络应用的重要组成部分。例

收稿日期:2023-09-19; **修回日期**:2023-11-30。

作者简介:王子豪(1991-),男,硕士,工程师。

引用格式:王子豪,胥 玲. 节点网络参数掩盖安全定位算法[J]. 计算机测量与控制,2024,32(12):178-183.

如，环境监测、军事和民用跟踪都需要了解特定事件发生的地点。在无线传感网络定位技术中，基于发送和接收来估计节点间的距离时，传感器根据无线信号传播时间、信号强度等信息来估计距离。若所有传感器节点都配合组网，在网络中存在行为恶意节点的情况下，节点允许收发虚假的位置和距离信息，从而干扰节点的实际定位性能。因此，在无线传感网络应用中，传感器的定位能力起着关键作用，若定位过程中不包括安全措施，则无线传感网络将遭受敌对场景下的位置威胁[10-12]。例如，采用随机部署的无线传感网络的侦查和跟踪人员，当节点网络中存在恶意攻击的非法节点参与定位和信息传输时，恶意节点参与的定位会导致节点报告错误地理区域，恶意节点发送错误信息使得汇聚节点接收到虚假信息。因此，为了保证无线传感网络节点位置的准确性，安全的定位算法至关重要。

WSN 中的节点定位易受到两种攻击场景的攻击：内部攻击和外部攻击[13-15]。为了防御内部攻击，可以设计了位置验证方案，将可疑锚的定位结果与其他锚的定位结果进行比较，以检查节点定位一致性，从而排除恶意攻击的定位结果。文献［16］采用轻量级的位置验证系统，该系统同时执行现场和区域内位置验证，现场验证旨在验证传感器声称的位置是否远离其真实位置超过一定距离。通过探索传感器声称的位置与其邻域观测之间的不一致性来检测异常位置。区域内验证验证传感器是否在特定于应用程序的验证区域内。与现场验证相比，只要传感器的位置不会导致应用程序出现故障，区域内验证就可以容忍较大的误差。通过推导不同应用的验证区域，并采用概率算法来计算每个传感器的区域内置信度，以高检测率和低误报率来验证传感器的位置。文献［17］在能量受限的 WSN 中提出了轻量级的位置验证系统，利用基于密度的空间聚类来获取异常聚类，并通过序列概率比检验对异常聚类进行进一步检验，从而确定危害网络的恶意节点。上述方案需要传感器在网络中分布的先验知识，因此，文献［17］在没有此类先验知识的情况下利用聚类算法来检测受损的锚节点。为了防御外部攻击，利用低检测概率策略可防御外部攻击的方案，该方案要求攻击者无法检测到合法发射器和接收器之间的通信[18]。

以上安全定位方法主要利用节点网络的先验知识和安全通信策略抵御恶意节点的攻击。对于安全通信策略，文中根据混沌参数掩盖的思想，对 WSN 的节点设计与位置信息相关的传输信号，检测恶意节点对通信和定位的攻击，避免采用节点网络的先验知识。

在混沌安全系统的应用中，主要采用的技术包括混沌伪随机数技术的信号发生器产生序列密码、前向与反向混沌迭代的密码分组技术、散列函数的混沌技术等。混沌系统的密码序列是利用非线性动态系统产生非周期伪随机序列。混沌序列的确定性依赖于系统初值和参数的设定。混沌序列所具有的确定性及不可预测性是由不收敛和有界混沌序列的产生过程而导致，同时依赖于系统初值和参数设定。因此，混沌系统因其良好的密码序列特性被广泛应用于密钥构建、信号加密和安全通信等领域。其中，提高通信系统的可靠性和安全性可基于混沌信号安全传输技术的混沌序列特性实现。目前，在无源光网络系统和相干光正交频分复用系统的应用中，混沌信号传输技术主要采用基于正交频分复用的混沌重排序安全符号传输方法、基于时频域二维置换物理层混沌加扰的安全传输方法、基于物理层混沌系统传输序列及混沌系统反向迭代的信号调制方法，以上方法可有效阻止外界非合作方对传输系统的恶意攻击[19]。

文献［19］采用混沌旋转数据相位及混沌映射信号子载波的方法设计混沌序列安全传输方案。在处理正交频分复用信号发射系统的基带信号时，信号星座图相位随机畸变，同上随机干预并选择信号子载波的对应法则，从而得到以混沌初始参数作为对应法则的传输密钥，接收机采用传输密钥产生的相反过程解调出通信信号。当窃听者截获混沌传输信号时，混沌对应法则使得窃听者难以解调出加密信号所传输的原始信息。该方案能够有效地对信息进行混沌安全传输，增强输出信号的随机特性，窃听方无法通过信号的统计特性估计出发送信息，从而保证通信的安全性。文献［20］采用直接调制方案将半导体激光二极管驱动到混沌区域，并采用混沌信息掩蔽方案添加光纤无线电信号，混沌屏蔽信号通过光通信链路传输，从而完成接收器处混沌的传播问题和同步，当传输的混沌在接收器处被同步时，通过使用减法规则来解掩蔽信号。

在混沌安全通信技术中，混沌参数掩盖方法是物理层安全通信技术的重要方法之一[19]，该方法是在发射端以加乘方式产生混沌信号，并将该信号作为载体来隐藏所要传送的信息，接收端可利用系统参数恢复出有用信息。

文中提出 WSN 参数掩盖安全定位算法，该方法将存在恶意节点参与定位得到的估计位置对应到定位区域所划分的网格，通过对网格划分信号相位，利用叠加信号中隐含的跳数信息和节点位置信息对网络节点设计参数保密信号。通过信号的相位索引提取存在恶意节点攻击的多跳路径，从而消除邻居节点中存在的恶意节点，完成 WSN 的节点安全定位。

1　参数掩盖安全定位算法设计

参数掩盖安全技术是将发送的信息隐藏在系统参数内，利用发送端所传输的信号来调制系统参数，在参数掩盖安全传输系统中采用多个参数进行信号调制，接收端利用参数掩盖安全信号提取出相应的系统参数，进而恢复所传输的信号。

传统的加密技术只能抵御外部攻击，攻击者通过俘获和破解正常节点，其伪造的恶意节点发动的内部攻击很难防御。恶意节点在 WSN 中获取节点传输信息，并洪泛虚假信息，从而破坏网络信息传输，并降低未知节点的定位精度。结合参数掩盖安全技术，将系统参数调制到传输信号

中，通过参数掩盖方式保护节点间的传输信息。

1.1 网格相位划分法

在多跳的无线传感器网络中，节点以洪泛的方式广播锚节点信息，此时，汇聚节点接收到的锚节点坐标信息中可能包含恶意节点发送的虚假信息。当无线传感器节点网络完成对未知节点的定位后，由于恶意节点的攻击，使得汇聚节点接收到的采集信息包含虚假信息，且完成定位的未知节点是由真实的锚节点坐标和恶意节点的虚假信标共同定位，使得未知节点定位误差增大。

设计网格相位法用于剔除恶意锚节点，如图 1 所示，将定位区域网格化，网格边长为 l，在存在恶意节点攻击的网络中，节点坐标为 $(x_{n,i}, y_{m,i})$，i 表示第 i 跳的节点标号，则在定位区域内的节点坐标与网格的关系满足：

$$(n-1)l \leqslant x_{n,i} \leqslant nl \tag{1}$$

$$(m-1)l \leqslant y_{m,i} \leqslant ml \tag{2}$$

其中：n 和 m 为正整数，分别表示网格化定位区域分割长和宽所对应的网格编号，如图 1 所示。

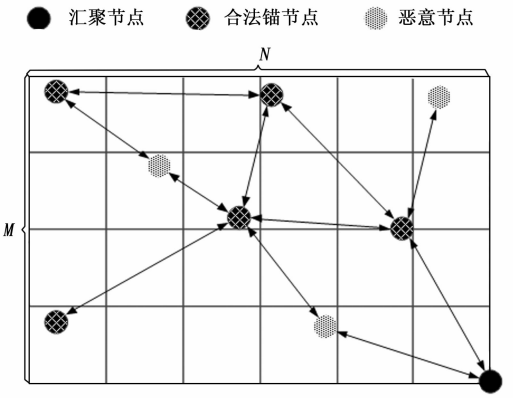

图 1 网格划分示意图

由式（1）和式（2）可得节点横纵坐标的索引号分别为式（3）和式（4）：

$$\left|\frac{x_{n,i}}{l}+1\right| \leqslant n \leqslant \left|\frac{x_{n,i}}{l}\right| \tag{3}$$

$$\left|\frac{y_{m,i}}{l}+1\right| \leqslant m \leqslant \left|\frac{y_{m,i}}{l}\right| \tag{4}$$

由式（3）和式（4）中节点坐标与网格编号的关系可将 $x_{n,i}$，$y_{m,i}$ 与 n，m 建立对应关系。通过该对应关系可将横纵坐标对应的网格在 γ 到 δ 内划分相位，其中，γ 到 δ 表示相位范围，即相位范围为 (γ, δ)，则横纵坐标对应的网格相位分别为：

$$\theta(x_{n,i}) = \left[\gamma \quad \cdots \quad \frac{\gamma-\delta}{N}n \quad \cdots \quad \delta\right]_{1\times N} \tag{5}$$

$$\theta(y_{m,i}) = \left[\gamma \quad \cdots \quad \frac{\gamma-\delta}{N}m \quad \cdots \quad \delta\right]_{1\times M} \tag{6}$$

其中：$\theta(x_{n,i})$ 和 $\theta(y_{m,i})$ 表示横纵坐标值 $x_{n,i}$ 和 $y_{m,i}$ 对应的网格相位。通过对网络中的节点进行网格相位划分使得信标节点自定位后产生具有相位信息的位置估计，即，位置坐标包含相位信息。当网络中存在恶意节点时，恶意节点未知预设的 γ 到 δ 及节点坐标与网格编号的关系，则恶意节点在洪泛广播自身位置信息时无法携带对应的网格相位。

1.2 参数掩盖的信号设计

在无线传感器网络中对节点位置估计和定位区域进行网格相位划分后，结合位置的相位信息 $\theta(x_{n,i})$ 和 $\theta(y_{m,i})$ 中包含的相位范围参数 γ 和 δ 及位置编号参数 n 和 m，设计参数掩盖的信号用于网络合法节点间的安全通信。

在无线传感器网络中，汇聚节点可以收集网络中的合法和非法节点的跳数信息，移动的节点相对于汇聚节点的跳数为 $h_{mn,i}(t)$，且 $h_{mn,i}(t) \neq 0$，汇聚节点可以将所有节点的跳数信息以洪泛广播的方式回传给网络中所有的节点。此时，合法节点将设计的网格相位索引信号再次洪泛广播通信信息。

为使得通信信号中包含相位信息中的参数，设计网格相位索引的激励信号 $s_1(t)$ 为：

$$s_1(t) = e^{j2\pi ft}(c_1 e^{j\alpha_{n,i}} + c_2 e^{j\beta_{m,i}}) \tag{7}$$

其中：f 为载波频率，$f=2.4$ GHz，c_1 和 c_2 为信号的编码系数，取值为 ± 1。将式（7）中的信号相位设计为：

$$\alpha_{n,i} = \frac{\gamma-\delta}{Nh_{mn,i}(t)}n \tag{8}$$

$$\beta_{m,i} = \frac{\gamma-\delta}{Mh_{mn,i}(t)}m \tag{9}$$

式（8）和式（9）中的相位 $\alpha_{n,i}$ 和 $\beta_{m,i}$ 由相位范围参数 γ 和 δ、位置编号参数 n 和 m、节点跳数信息 $h_{mn,i}(t)$ 及定位区域的网格数 M 和 N 共同决定。因此，网格相位索引的激励信号 $s_1(t)$ 中包含了相位范围参数 γ 和 δ、位置编号参数 n 和 m、节点跳数信息 $h_{mn,i}(t)$ 及定位区域的网格数 M 和 N。

由式（8）和式（9）可知，当节点在节点网络中移动时，节点相对于汇聚节点的跳数可能发生变化，而恶意节点相对于汇聚节点的跳数难以与合法跳数总是保持一致。在移动设备的侦查过程中，可以通过 $\alpha_{n,i}$ 和 $\beta_{m,i}$ 映射节点的水平坐标和垂直坐标的变化，从而判断通信信号的合法性。

因此，节点之间的通信信息由相位范围参数 γ 和 δ、位置编号参数 n 和 m、节点跳数信息 $h_{mn,i}(t)$ 及定位区域的网格数 M 和 N 产生的相位 $\alpha_{n,i}$ 和 $\beta_{m,i}$ 进行掩盖。恶意节点难以使用的复杂的节点参数传输网络中所设计的参数掩盖信号。

进一步，根据节点跳数 $h_{mn}(t)$ 设计参数掩盖迭代的安全定位信号。此外，设备的移动速度远小于光速，则节点移出网格所需的时间远小于信号传播速度，因此，网络节点的实时信息传输不易受设备移动的影响。通过参数掩盖坐标的相位映射，产生参数保密的信号相位。采用正交调制思想，将式（7）信号的实信号形式写成：

$$Re[s_1(t)] = I_1\cos(2\pi ft) - Q_1\sin(2\pi ft) \tag{10}$$

其中：$Re[.]$ 表示取实部，得到式（10）的同相分量和正交分量分别为：

$$I' = c_1\cos\alpha_{n,i} + c_2\cos\beta_{m,i} \tag{11}$$

$$Q' = c_1\sin\alpha_{n,i} + c_2\sin\beta_{m,i} \tag{12}$$

设计网格相位索引的激励信号 $s_2(t)$ 为：

$$s_2(t) = -je^{j2\pi ft}(c_3 e^{j\alpha_{n,i}} + c_4 e^{j\beta_{m,i}}) \tag{13}$$

其中：c_3 和 c_4 的取值为±1。设计同相分量和正交分量的编码系数用于产生复基带信号的星座图形式，从而通过多跳路径产生参数掩盖信号星座图。由 $Re[s_1(t)] + Re[s_2(t)]$ 得到同相分量和正交分量分别为：

$$I = c_1\cos\alpha_{n,i} + c_2\cos\beta_{m,i} + c_3\sin\alpha_{n,i} + c_4\sin\beta_{m,i} \tag{14}$$

$$Q = c_1\sin\alpha_{n,i} + c_2\sin\beta_{m,i} - c_3\cos\alpha_{n,i} - c_4\cos\beta_{m,i} \tag{15}$$

对同相分量设计编码系数，则式（14）的同相分量编码系数可设计为 $c_1=1$，$c_3=1$，对正交分量设计编码系数，则式（15）的正交分量编码系数可设计 $c_1=1$，$c_3=-1$，则复基带信号 $Y_{n,i}$ 为：

$$Y_{n,i} = I + jQ = \sqrt{2}(1+j)\sin\left(\alpha_{n,i} + \frac{\pi}{4}\right) \tag{16}$$

对式（14）的同相分量设计编码系数设计为 $c_2=1$，$c_4=1$，对式（15）的正交分量设计编码系数，则设计 $c_2=1$，$c_4=-1$，则得到复基带信号 $Z_{m,i}$ 为：

$$Z_{m,i} = \sqrt{2}(1+j)\sin\left(\beta_{m,i} + \frac{\pi}{4}\right) \tag{17}$$

由式（16）和式（17）的复基带信号可知，为避免正弦函数相位模糊导致的多值问题，将 γ 和 δ 分别设置为 $3\pi/4$ 和 $\pi/4$，从而使得式（16）和式（17）的复基带信号在 $[\gamma, \delta]$ 区间内取值唯一。

如图 2 所示，有恶意节点参与的多跳路径为非法多跳路径，合法节点组成的多跳路径为合法多跳路径。当恶意节点参与的节点网络的定位和通信时，恶意节点洪泛广播虚假位置坐标和虚假信息使得未知节点的位置估计误差增大，网络中传感器间传输的信息也存在错误。因此，恶意节点的参与使得节点网络难以正常工作。

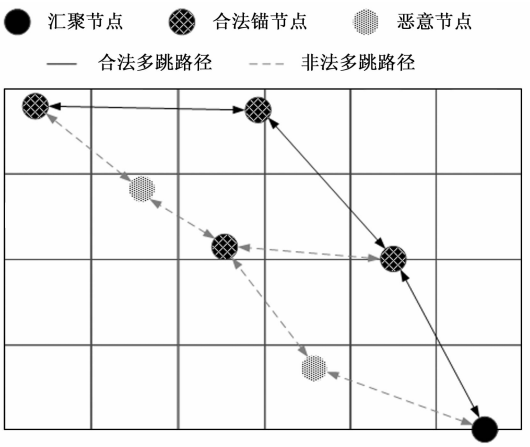

图 2　恶意节点参与的多跳路径示意图

为避免恶意节点的攻击使得节点网络无效工作，采用参数掩盖信号排除网络中的恶意节点。根据（16）和式（17），当节点 A_{mn} 的与汇聚节点进行多跳通信时，将多跳节点信号叠加，使得在节点网络中洪泛广播参数掩盖信号，则得到节点网络中汇聚节点的接收信号为：

$$W = \sqrt{2}(1+j)\sum_{i=1}^{h_{mn,i}(t)}\sin\left(\alpha_{n,i} + \frac{\pi}{4}\right) \tag{18}$$

$$X = \sqrt{2}(1+j)\sum_{i=1}^{h_{mn,i}(t)}\sin\left(\beta_{m,i} + \frac{\pi}{4}\right) \tag{19}$$

1.3　相位索引的安全定位算法设计

由式（18）和式（19）得到汇聚节点接收单跳节点传输的复基带信号 $Y_{n,1}$ 和 $Z_{m,1}$ 分别为 $VY_{n,1}$ 和 $VZ_{m,1}$，则汇聚节点接收信号后估计的相角为：

$$V\alpha_{n,1} = \arcsin\left(\frac{VY_{n,i}}{\sqrt{2}(1+j)}\right) - \frac{\pi}{4} \tag{20}$$

$$V\beta_{m,1} = \arcsin\left(\frac{VZ_{m,i}e^{-j\frac{\pi}{4}}}{\sqrt{2}}\right) - \frac{\pi}{4} \tag{21}$$

将估计的相角 $V\alpha_{n,1}$ 和 $V\beta_{m,1}$ 与式（5）和式（6）的相位索引矩阵进行匹配，从而判定相对于汇聚节点的单跳节点是否为恶意节点。当节点逐跳解调叠加信号时，对于第 i 跳的节点，其中 $i>1$，$h_{mn,i}(t)>1$，可以得到：

$$V\alpha_{n,i} = \frac{\arcsin\left[\dfrac{VY_{n,i} - VY_{n,i-1}}{\sqrt{2}(1+j)}\right] - \dfrac{\pi}{4}}{h_{mn,i}(t)} \tag{22}$$

$$V\beta_{m,i} = \frac{\arcsin\left[\dfrac{VZ_{m,i} - VZ_{m,i-1}}{\sqrt{2}(1+j)}\right] - \dfrac{\pi}{4}}{h_{mn,i}(t)} \tag{23}$$

同理，将估计的相角 $V\alpha_{n,i}$ 和 $V\beta_{m,i}$ 与相位索引矩阵进行匹配。当相角与相位索引矩阵映射的坐标无法与（$x_{n,i}$，$y_{m,i}$）匹配时，则判断该路径的传输信号是由恶意节点发送，即无法与（$x_{n,i}$，$y_{m,i}$）匹配的邻居节点为恶意节点，由该恶意节点参与的多跳路径为非法多跳路径，利用网络中节点的身份信息提取恶意节点。因此，通过非法路径估计的节点位置需要重新定位。当网络中的节点移动时，跳数的变化使得参数掩盖信号的复杂性更高，有利于抵御恶意节点的攻击。

根据斯皮尔曼等级相关系数设计相关系数用于表示解算相位与相位索引矩阵的相关性，则相关系数 ρ 设计为：

$$\rho = \frac{\sum_i (V\alpha_{n,i} - \alpha_{n,i})(V\beta_{m,i} - \beta_{m,i})}{\sqrt{\sum_i (V\alpha_{n,i} - \alpha_{n,i})^2 \sum_i (V\beta_{m,i} - \beta_{m,i})^2}} \tag{24}$$

通过网格相位的相关系数来反映参数掩盖保密信号消除恶意节点的能力，$\rho\in[-1, 1]$。当 ρ 越接近于 1 时，表示参数掩盖信号消除恶意节点的能力越强，反之则越弱。实际上，受噪声影响的信号星座图使得式（24）中 $\rho\neq 1$。

在节点网络采用极大似然法估计节点位置，设未知节点的坐标为（$x_{0,i}$，$y_{0,i}$），未知节点与合法节点（$x_{ln,i}$，$y_{lm,i}$）的距离为 d_{li}，设恶意节点坐标为（$x_{en,i}$，$y_{em,i}$），当恶意节点参与距离测量，未知节点与恶意节点的距离为 d_{ei}，则根据极大似然定位算法原理可以得到：

$$\boldsymbol{HX} = \frac{1}{2}\boldsymbol{B} \tag{25}$$

其中：

$$\boldsymbol{H}=\begin{bmatrix}\vdots & \vdots\\ xl_{n,i}-xl_{n,1} & yl_{m,i}-yl_{m,1}\\ \vdots & \vdots\\ xe_{n,i}-xl_{n,1} & ye_{m,i}-yl_{m,1}\\ \vdots & \vdots\end{bmatrix} \tag{26}$$

$$\boldsymbol{B}=\begin{bmatrix}\vdots\\ xl_{n,i}^2+yl_{n,i}^2-dl_i^2-(xl_{n,1}^2+yl_{n,1}^2-dl_1^2)\\ \vdots\\ xe_{n,i}^2+ye_{n,i}^2-de_i^2-(xl_{n,1}^2+yl_{n,1}^2-dl_1^2)\\ \vdots\end{bmatrix} \tag{27}$$

$$\boldsymbol{X}=\begin{bmatrix}x_{0,i}\\ y_{0,i}\end{bmatrix} \tag{28}$$

由于恶意节点的参与，则 $\boldsymbol{H}$ 和 $\boldsymbol{B}$ 也可表示为：

$$\boldsymbol{H}=\begin{bmatrix}\vdots & \vdots\\ xl_{n,i}-xe_{n,1} & yl_{m,i}-ye_{m,1}\\ \vdots & \vdots\\ xe_{n,i}-xe_{n,1} & ye_{m,i}-ye_{m,1}\\ \vdots & \vdots\end{bmatrix} \tag{29}$$

$$\boldsymbol{B}=\begin{bmatrix}\vdots\\ xl_{n,i}^2+yl_{n,i}^2-dl_i^2-(xe_{n,1}^2+ye_{n,1}^2-de_1^2)\\ \vdots\\ xe_{n,i}^2+ye_{n,i}^2-de_i^2-(xe_{n,1}^2+ye_{n,1}^2-de_1^2)\\ \vdots\end{bmatrix} \tag{30}$$

由式（25）得到最小方差解为：

$$\boldsymbol{X}=\frac{1}{2}(\boldsymbol{H}^T\boldsymbol{H}^{-1})\boldsymbol{H}^T\boldsymbol{B} \tag{31}$$

由矩阵 $\boldsymbol{H}$ 和 $\boldsymbol{B}$ 可知，恶意节点会对未知节点的定位精度产生直接影响。当参数掩盖信号消除恶意节点后，可以得到：

$$\boldsymbol{H}=\begin{bmatrix}\vdots & \vdots\\ xl_{n,i}-xl_{n,1} & yl_{m,i}-yl_{m,1}\\ \vdots & \vdots\end{bmatrix} \tag{32}$$

$$\boldsymbol{B}=\begin{bmatrix}\vdots\\ xl_{n,i}^2+yl_{n,i}^2-dl_i^2-(xl_{n,1}^2+yl_{n,1}^2-dl_1^2)\\ \vdots\end{bmatrix} \tag{33}$$

将式（32）和式（33）代入式（31）得到的最小方差解为未知节点的位置估计。

2 数值分析

在 200 m×200 m 的定位区域内产生 100 次随机部署的节点网络，其中包含 80 个锚节点，120 个未知节点，节点通信半径为 30 m，网格边长为 5 m，测试环境的信噪比设置为 15 dB。在传感器节点网络中随机部署恶意节点，以无恶意节点攻击网络的平均定位精度为期望值（x_{pi}，y_{pi}），测试参数掩盖信号安全定位的性能。

节点网络中平均定位精度的误差为：

$$A=1-\frac{1}{u}\sum_{i=1}^{u}\frac{\sqrt{(x_{0,i}-xp_i)^2+(y_{0,i}-yp_i)^2}}{\sqrt{xp_i^2+yp_i^2}} \tag{34}$$

其中：u 为被定位的节点总数。

对节点网络采用多跳叠加的参数掩盖信号检测恶意节点时，解算相位与相位索引矩阵的相关系数如图 3 所示。由式（24）可知，由于相位解算受噪声影响，因此，相关系数难以始终保持为 1，随机部署 100 次节点网络的平均相关系数为 0.87，则解算相位与相位索引矩阵具有极强的相关性。如图 4 所示，恶意节点相位索引的相关系性较弱，平均相关系数为 0.03。由图 3 和图 4 中的数据可以表明，通过相位的索引和匹配可以筛选出恶意节点。

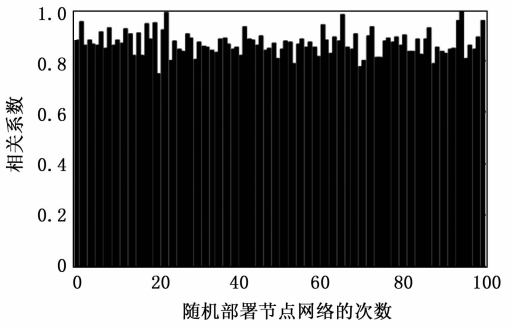

图 3 合法节点相位索引的相关系数

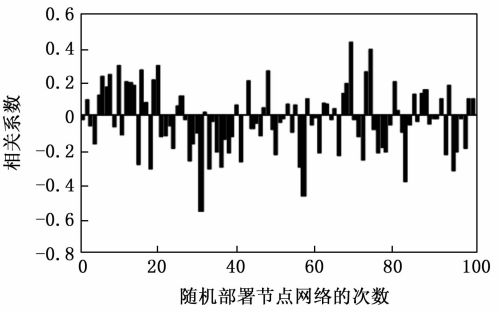

图 4 恶意节点相位索引的相关系数

在节点网络中存在随机部署的恶意节点，如图 5 所示，当网络中未消除恶意节点攻击时，平均定位精度的误差为 0.20，这表明恶意节点使得节点定位性能恶化。

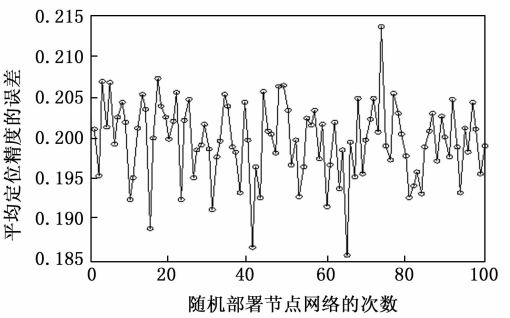

图 5 恶意节点攻击网络的节点定位性能

如图 6（a）所示，采用多跳叠加的参数掩盖信号消除恶意节点的攻击可以提高定位精度，平均定位精度的误差为 0.97。由式（5）和式（6）可知，当降低信噪比时，由

于受到噪声的影响变大，使得解算相位在精细的网格索引相位矩阵中可能匹配不准确，则通过增大网格边长扩大相位索引的覆盖区域，从而抑制噪声对相位匹配的影响。设置信噪比为 8 dB，网格为 8 m，如图 6（b）所示，网络中的节点可以保持较好的定位精度，平均定位精度的误差为 0.95。当忽略环境噪声对信号的影响时，平均定位精度的误差为 1，而实际环境需要考虑噪声影响，则平均定位精度的误差难以达到 1。

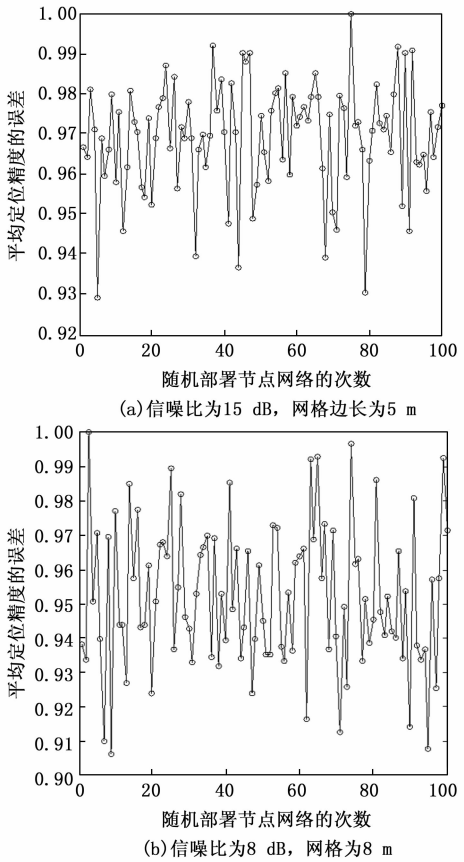

图 6　参数掩盖信号定位性能

文中在含有噪声环境下测试的数值可以表明，多跳叠加的参数掩盖信号可以消除恶意节点的攻击，抑制定位精度的误差。数值结果表明，与文献中的 WSN 安全定位策略相比，文中提出的算法无需节点网络的先验知识抵御恶意节点的攻击，为 WSN 节点安全定位提供新的设计思路。

3　结束语

文中针对 WSN 中存在恶意节点破坏节点定位精度的问题，提出了多跳叠加的参数掩盖安全定位算法。将网络中节点的跳数和位置信息作为掩盖参数，并将定位区域转换成网格相位的索引矩阵，通过将 WSN 参数调制到多跳叠加信号中，产生安全定位的参数信号，通过逐跳解算信号相位和相位索引矩阵匹配信号中携带的位置信息筛选出恶意节点，并对多跳路径中的未知节点重新定位，从而实现 WSN 的安全定位。

参考文献：

[1] MUNESH S，PABITRA M K. A range free geometric technique for localization of wireless sensor network（WSN）based on controlled communication range [J]. Wireless Personal Communications，2017（94）：1359－1385.

[2] 叶　贵，张林静. 基于 ZigBee 的室内空气质量感知系统的设计 [J]. 计算机测量与控制，2021，29（12）：161－165.

[3] 张　森，徐　亮. 基于 Android 与 ZigBee 无线传感器网络的档案库房智能管理平台设计 [J]. 电子设计工程，2020，28（20）：158－161.

[4] YUAN S. High-rise building deformation monitoring based on remote wireless sensor network [J]. IEEE Sensors Journal，2021，21（22）：25133－25141.

[5] 叶　贵，杨　洋，张林静，等. 基于 ZigBee 的养老院老人体征监测系统设计 [J]. 计算机测量与控制，2022，30（7）：56－61.

[6] XIE N，CHEN Y，LI Z，et al. Lightweight secure localization approach in wireless sensor networks [J]. IEEE Transactions on Communications，2021，69（10）：6879－6893.

[7] WEI S，MICHEL B，JEAN P C，et al. Secure localization in the presence of colluders in WSNs [J]. Sensors，2017，17（8）：1－15.

[8] 周伟伟，郁　滨. 基于不等簇半径和动态簇头的 WSN 能量空洞攻击抑制模型研究 [J]. 通信学报，2017，38（11）：93－102.

[9] 刘志锋，陈　凯，李　雷，等. 一种多种攻击并发下的 WSN 生存性评估模型 [J]. 计算机科学，2017，44（8）：129－133.

[10] 邓　平，张红江. 一种无线传感器网络抗虫洞攻击 DV-HOP 定位算法 [J]. 西南交通大学学报，2015，50（1）：51－57.

[11] 陈　宜，蒋朝惠，郭　春. 一种抗独立攻击的 WSN 三维安全定位算法 [J]. 传感技术学报，2015，28（11）：1702－1707.

[12] ZHANG Q，WAN J，WANG D，et al. Sparsty-incorporated secure localization for wireless sensor networks [J]. Electronics Letters，2017，53（9）：629－631.

[13] YAN S，MALANEY R，NEVAT I，et al. Optimal information-theoretic wireless location verification [J]. IEEE Transactions on Vehicular Technology，2014，63（7）：3410－3422.

[14] 张劭帅，袁津生. 基于集对分析的 WSN 安全态势感知模型的研究 [J]. 计算机工程与科学，2017，39（3）：505－511.

[15] 郭　蕊，芦天亮，杜彦辉. WSN 中基于目标决策的源位置隐私保护方案 [J]. 计算机科学，2021，48（5）：334－340.

[16] WEI Y，YONG G. Lightweight location verification algorithms for wireless sensor networks [J]. IEEE Transactions on Parallel and Distributed Systems，2013，24（5）：938－950.

[17] LIU X，SU S，FENG H，et al. A range-based secure localization algorithm for wireless sensor networks [J]. Nature reviews Cancer，2019，19（2）：785－796.

[18] SHIHAO Y，ZHOU X，HU J，et al. Low probability of detection communication：opportunities and challenges [J]. IEEE Wireless Communications，2019，26（5）：19－25.

[19] 王　颖，张晓忠，曾　娟，等. 基于二级混沌映射的 OFDM 安全传输方案 [J]. 通信学报，2016，37（7）：132－139.

[20] MAZHAR D A，SHAH S，ISLAM M K，et al. Design issues of digital and analog chaotic rof link using chaos message masking [J]. IEEE Access，2019，7：174042－174050.