# 基于Hilbert填充曲线的海洋无线传感网源节点位置隐私保护方法

李攀攀*[①] 谢正霞[②] 周志刚[③] 乐光学[①] 郑仕链[④] 杨小牛[①④]

[①](嘉兴学院数理与信息工程学院 嘉兴 314001)

[②](嘉兴学院建筑工程学院 嘉兴 314001)

[③](山西财经大学信息管理学院 太原 030006)

[④](通信信息控制和安全技术重点实验室 嘉兴 314033)

**摘 要**：节点位置保护对于海洋无线传感器网络(MWSNs)至关重要，尤其是对于无人值守的环境。然而，由于大多数静态部署，传感器的能量、存储和通信能力的限制，MWSNs容易受到各种位置(和衍生)攻击的影响。该文从攻击和防御两个方面研究节点位置隐私保护问题。首先，针对两种重要节点(包括基站和源节点)提出了一种新的二相定位攻击，它可以在少量的本地无线传输监视中找到基站节点，反向跟踪源节点的位置。与现有方法不同，提出的攻击根据传输方向确定节点位置，从而突破现有的防御。然后，为了抵御这种攻击，该文设计了一种基于Hilbert填充曲线的传感器网络路由节点位置隐私保护方法(HLPS)。攻防理论分析与对抗实验表明，该方法能够保护目标节点的位置隐私，具有较小的通信和计算开销。

**关键词**：海上无线传感网；网络安全；网络位置隐私保护；Hilbert填充曲线

**中图分类号**：TN915.08; TP393.08 **文献标识码**：A **文章编号**：1009-5896(2020)06-1510-09

**DOI**: 10.11999/JEIT190364

# A Source-location Privacy Preservation Method Based on Hilbert-filling-curve Routing Protocol in Marine Wireless Sensor Networks

LI Panpan[①] XIE Zhengxia[②] ZHOU Zhigang[③] YUE Guangxue[①]

ZHENG Shilian[④] YANG Xiaoniu[①④]

[①](*College of Mathematics and Information Engineering*, *Jiaxing University*, *Jiaxing* 314001, *China*)

[②](*College of CML Engineering and Architecture*, *Jiaxing University*, *Jiaxing* 314001, *China*)

[③](*College of Information Management*, *Shanxi University of Finance and Economics*, *Taiyuan* 030006, *China*)

[④](*Science and Technology on Communication Information Security Control Laboratory*, *Jiaxing* 314033, *China*)

**Abstract**: Source node location protection is critical to the Marine Wireless Sensor Networks (MWSNs), especially for unattended environment. However, due to most of the static deployment and the limitations in energy, storage and communication capabilities of the sensors, MWSNs are vulnerable to various location (and derivative) attacks. In this work, the node location privacy protection issues are studied from both aspects of attacks and defenses. First, a new two-phase location attack is proposed for two important types of nodes (including base station and source node). It can locate a base station node within few amounts of local wireless transmission monitoring, and then reversely traces the location of the source node. Different from existing methods, the proposed attack determines the node location based on the transmission direction, which can break through existing defenses. Then, to defend against such attack, a Hilbert-filling-curve-based Location-privacy Protection Scheme (HLPS) is designed for MWSNs. The theory analysis and confrontation experiment of attack and defense show that the proposed scheme owns capable of protecting the location privacy of the target node with moderate communication and computation overhead.

收稿日期：2019-05-22；改回日期：2020-03-05；网络出版：2020-04-17

*通信作者： 李攀攀 pli0311@aliyun.com

基金项目：国家自然科学基金(U19B2015, 61902226)，浙江省教育厅一般科研项目(Y201840356)

Foundation Items: The National Natural Science Foundation of China(U19B2015, 61902226), The General Research Projects of Zhejiang Provincial Education Department(Y201840356)

**Key words**: Marine Wireless Sensor Networks (MWSNs); Network security; Location privacy preservation; Hilbert-filling-curve

## 1　引言

随着海事活动的日趋频繁，海上无线传感网(Marine Wireless Sensor Networks, MWSNs)因其布设速度快，方式灵活、成本低等特点，被广泛应用于国防军事、环境监测、海洋灾害预警、海洋油气勘探等领域[1]。海上无线传感网络大多采用无线多跳的通信方式，容易受到各种位置攻击。在MWSNs中，节点位置保密技术是保护网络中某些重要节点(如源节点、基站等)的位置信息的方法。定位源节点意味着攻击者可以发现源节点附近有价值的目标[2]；在定位基站时，意味着攻击者可以攻击基站并窃取重要信息[3]；匿名通信技术通过隐藏通信过程中节点的标识来保护源节点或基站的位置[4,5]。但是，与陆地环境不同，在海洋环境下的MWSNs源节点位置隐私保护面临着新的挑战。

首先，传感器节点在海域上静态部署，海洋环境导致网络施工、维护困难，特别是空旷海域环境下，网络覆盖范围缺少遮蔽物和可供隐藏的位置，节点位置信息更容易被定位，使得源节点位置隐私被暴露的风险陡增。

其次，海上传感网中涉及到海洋环境监测、军事等领域的大量敏感数据，关涉国家信息安全，源节点位置隐私一旦暴漏或被攻击者捕获，会由此带来较多的衍生攻击，如海洋敏感数据窃取、军事目标情报收集等，因此，需要轻量级的、高安全的源节点位置隐私保护方法。

第三，传统单一、固定的源节点位置隐私保护模式难以抵御大样本下的知识关联攻击，如基于随机游走或多路径的路径伪装方案、陷阱诱导策略等。在海洋环境下，攻击者可以轻易使用资源优良的监听设备，监听传感网中大规模数据样本数据集，通过关联分析、神经网络等大数据挖掘与分析技术，能大概率地识别出相对精确的位置隐私保护的模式，进而威胁到节点的位置隐私的安全。

当前的位置隐私保护策略主要分为路径伪装技术、陷阱诱导技术和访问控制技术三大类。

(1) 在路径伪装技术研究领域中，PU SBRF方法[2]能够产生远离真实源节点且地理位置多样性的幻象源节点，增加攻击者回溯追踪的成本，能有效抵御局部流量攻击。LPMS方法[6]使用随机的数据接收方案实现动态的Sink节点，隐私保护强度高，但是对端到端的通信质量影响较大。文献[7]采用伪装数据包和真实包随机游走策略，真实数据包在特定阶段进行随机游走以隐藏传输方向，同时伪装数据包被注入到两个或更多最短路径的相交节点中，使攻击者无法确定真实路由，MoRF[3]和Fclique[8]也是采用类似的策略。

(2) 在陷阱诱导技术研究领域中，文献[9]提出了基于环路的路由方案，网络拓扑由多个路由环和路由路径组成，数据经由就近的路由环再发送到接收节点，从而保护基站的位置隐私。SRCRR方法[10]中数据在路由过程中随机存储在中间节点中，Sink节点在半圆形的圆周移动过程中间歇性地收集中间节点发送的数据，达到防止攻击者预测和追踪其位置及移动模式的目的。文献[11]利用伪造的虚假数据均衡网络中的流量密度。

(3) 在访问控制技术研究领域中，STAP方法[12]使用联合层的分组转发策略，在节点位置未知的情况下实现数据转发和分组，能抵御局部和全局攻击，但是该方法需要布置存储节点，通信质量不稳定。MQA方法[4]采用加密技术实现节点ID的匿名，但是加解密过程过多导致系统效率低。PPSNC方法[13]采用GEVs(Global Encoding Vectors)对数据流进行同态加密，由于密文数据流具有不可检测性，有效地阻止流量分析攻击，但是该方法计算复杂度较高。

针对上述问题，本文提出了基于Hilbert填充曲线的节点位置隐私保护方法(Hilbert-filling-curve-based Location-privacy Protection Scheme, HLPS)，采用泰森多边形划分规则对无线传感器网络中各个基站进行部署，通过数据环绕式路由，增强隐私保护的强度；为了抵御大数据采样攻击，传感器不定期地生成并发送伪消息以扰乱攻击者，进一步地提升了整个网络中源节点位置隐私抗攻击的能力。

## 2　问题定义

### 2.1　网络模型

海上无线传感网中由大量的传感器节点和部署在监控区域中的若干个基站组成，传感器节点部署在岛礁、浮标、船舶上。传感器节点通过无线多跳自组织网络系统，旨在对网络覆盖区域内的对象信息进行感知、采集、处理后，发送给基站节点。如图1所示，传感器网络监测海上舰艇的活动和位置，一旦发现舰艇，最近的传感器将作为源节点，将立即或定期以消息的形式发送给观测基站，基站通过Internet或卫星向用户发送信息。

本文方法的核心设计目标是如何在低网络开销的情况下大幅提高攻击者定位源节点的成本，包括

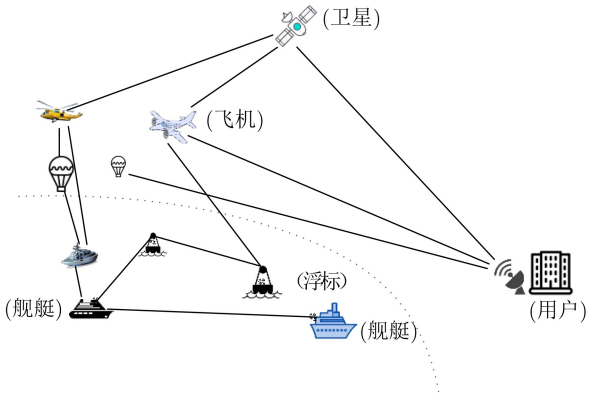



图 1 海上无线传感器网络示意图

计算成本、通信成本等。本文首先对整个MWSNs作如下假设：(1)传感器节点在目标海域全网内均匀分布，并且网络中的任何两个节点都可以通过一跳或多跳进行通信；(2)假设每个传感器节点都有一个传输范围$r$，它与最近邻居节点的距离相同；(3)整个网络可以有多个基站，且基站的位置是随机的；(4)在同一时刻，网络可能存在多个源节点，这些源节点可能同时发送数据；(5)传感器节点和基站外观不可区分，但传感器在计算、存储和能量方面均受限，而基站在这些方面不受限制。

### 2.2 攻击模型

本文在攻击者能力假设的基础上，进一步提出海洋环境下更具普适性和现实性的攻击模型。

#### 2.2.1 攻击者能力假设

本文假定攻击者有强大的硬件配置，并且具备有目的性攻击的能力。具体来讲，攻击者的攻击能力具有以下特征：

(1) 被动攻击：每个攻击者都可以侦听其通信范围内的节点发送的消息，攻击者的侦听半径与节点的通信半径相同，均为$r$；

(2) 局部流量监听：MWSNs中节点部署在广泛的海域，覆盖面积广泛，攻击者难以对如此巨大的MWSNs进行全局流量监控；

(3) 节点定位：攻击者可以通过现有定位技术在其有效监听区域内定位节点；

(4) 合谋攻击：攻击者为了实现对源节点的定位，$m$个攻击者$A=\{A_i|1\le i\le m\le i\le m\}$能够共同合作并进行消息的共享，其中$A$表示攻击者集合，$A_i$表示网络中的第$i$个攻击者。

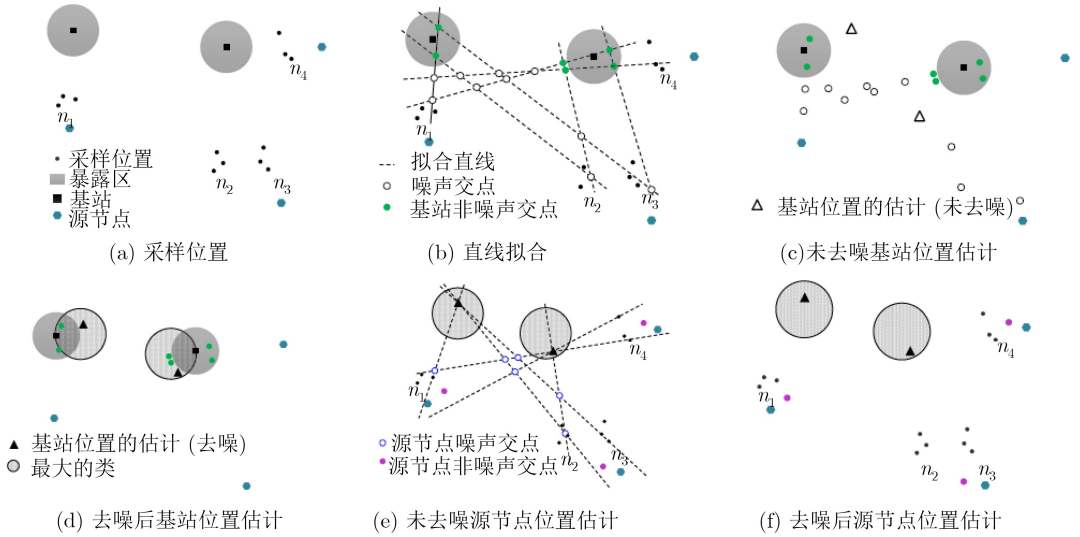
#### 2.2.2 攻击者二相定位攻击模型

根据攻击者的能力，下面给出攻击者的二相定位攻击模型，如图2所示，其中灰色区域表示基站的暴露区，若攻击者估计的基站位置位于暴露区，则攻击者可以发现基站。二相定位攻击模型具体如下：

(1) 多个攻击者的合谋攻击，对多个监听域中进行位置采样：根据前文对攻击者攻击能力的假设，攻击者具备优良的计算能力和存储能力，攻击者$A_i$能在一定范围内监听网络，如图2(a)所示，攻击者分别位于$n_1$, $n_2$, $n_3$和$n_4$附近，攻击者可以根据位置采样获得数据，得到$n_i$和$h$个样本位置的集合，位置信息标记为$(x_i, y_i)$ $(1\le i\le N)$。

(2) 基站位置的估计：$A_i$根据位置采样信息，采用最小二乘法将位置拟合成一条直线$l$:$y$=a$x$+$b$, $a$和$b$可以表示为

$$a=\frac{N\sum_{n=1}^{N}x_n\cdot y_n-\left(\sum_{n=1}^{N}x_n\right)\left(\sum_{n=1}^{N}y_n\right)}{N\sum_{n=1}^{N}(x_n)^2-\left(\sum_{n=1}^{N}x_n\right)^2} \tag{1}$$




(a) 采样位置 (b) 直线拟合 (c)未去噪基站位置估计

(d) 去噪后基站位置估计 (e) 未去噪源节点位置估计 (f) 去噪后源节点位置估计

图 2 攻击者攻击策略示意图

$$b=\frac{\left(\sum_{n=1}^{N}y_n\right)}{N}-a\cdot\frac{\left(\sum_{n=1}^{N}x_n\right)}{N} \tag{2}$$

(3) 位置采样集合进行拟合，并去除噪声，定位基站[2]：假设$k$个估计点的位置集合为LS，使用聚类的方法清洗LS中的噪声点，去噪过程的主要步骤分为：(a)攻击者首先对LS集合进行层次化聚类；(b)根据聚类结果，找到最大的类$C_{\max}$；(c) Loc$(C_{\max})$即为去噪后基站的估计位置，如图2(c)和图2(d)所示。

(4) 在攻击者定位基站的基础上，可以再次依靠数据采集及拟合的方式反向回溯定位源节点，如图2(e)所示。

(5) 根据回溯的含噪声的源节点，同理，攻击者再次使用步骤(3)的聚类清洗方法，可得到去噪的源节点位置信息，如图2(f)所示，这样，攻击者就能大概率地对源节点进行定位。

针对二相定位攻击模型，本文提出了基于Hilbert填充曲线的环绕式节点位置隐私保护方法。

## 3　基于Hilbert填充曲线的随机混淆式源节点位置隐私保护方法

在本文提出的攻击模型中，攻击者主要通过对其探测范围内传感器信息传递的路径进行回溯式拟合，从而定位信息的来源(即源节点的位置)。通过观察易知，对信息传输方向的攻防是传感器网络节点位置攻防中敌我双方争夺的焦点。为此，在由源节点到基站构成的所有路径集合中，寻求位置隐私保护与通信代价相平衡的“最优”路径成为传感器网络研究人员关注的焦点。

直观地，在所有平面坐标系中，Hilbert填充曲线在欧式直角坐标系下具有以下3点特性：

(1) 将平面进行格状划分，Hilbert填充曲线能够遍历其上任意单元子结构；

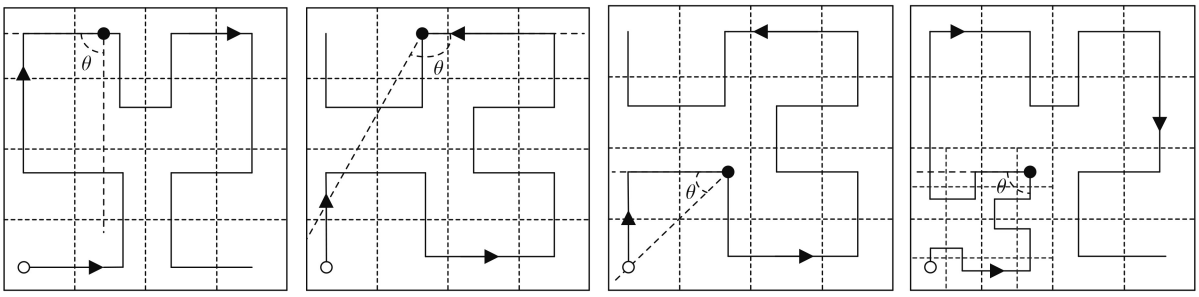
(2) 平面网络可以进行无限细化，曲线理论上可以遍历其上任意一点；

(3) Hilbert填充曲线线序相近的单元区域其地理位置也具有近邻性。

此外，不似含有圆环的选路策略[10](需要选择每一跳路径的路由方向)，基于Hilbert填充曲线的选路策略实现更为高效节能，更适于海上无人值守的环境；进一步地，该曲线的填充特性所形成的路由路径又与圆环选路策略所形成的路径有相近性，即由基站到所有路由点所构成的最大张角(称为可探测角)相近。因此，使用Hilbert填充曲线的选路策略在理论上天然地平衡了路由效率与位置隐私保护两大需求。

图3形象地展示了基于Hilbert填充曲线选路策略在隐私保护方面的特性。令源节点为$x_1$，基站为$x_2$，假设敌人的探知域为$D$($D$不包含$x_1$所在的子区域)，比较图3中的4个子图可知，攻击者对源节点的探知域$D$的大小取决于Hilbert填充曲线的线序和空间划分粒度。例如由图3(a)和3(b)可知，Hilbert填充曲线的线序不同，路由路径所形成的最大张角也不同。图3(a)所形成的最大张角小于图3(b)所形成的最大张角，但其所需的路由路径要高于后者；又如由图3(c)和3(d)可知，当源节点与基站的相对位置固定，空间划分的粒度越细，其所形成的最大张角也越大。图3(d)所形成的最大张角大于图3(c)所形成的最大张角，但图3(c)所需的路由路径更长。在现实场景中，由于对通信开销的限制，导致空间划分的粒度受到相应限制；而$\theta$的值与攻击者的可能监听域$D$呈正相关，从通信开销的限制看，对于线序的选择往往也受到限制，从而导致$\theta$的值受限。因此，现有的传感器网络位置隐私保护方案无法实现理想环境下节点位置隐私保护与通信开销的最优化信息路由策略。

基于上述观察，与文献[2]所针对单基站的无线传感网络应用场景不同，本文针对多基站的现实无线传感器网络场景，提出一种基于Hilbert填充曲线的环绕式节点位置隐私保护路由方法。如图4所示，




(a) 示例情景1　(b) 示例情景2　(c) 示例情景3　(d) 示例情景4

● 基站　○ 源节点　→ 线序$\theta$可探测角

图 3 隐私保护策略与攻击者监听域关系示意图

每个节点将其感知范围内的其它节点划分为4个子节点集(分别为Next节点集、Prior节点集、向心节点集和离心节点集)，其中，向心节点集是指以基站为圆心，当前传感器节点到基站的距离为半径所成圆域与以当前传感器节点为圆心，其最大感知距离为半径所成圆域的交集中所含的节点集合；离心节点集是指以当前传感器节点为圆心，其最大感知距离为半径所成圆域的节点集合为论域，其是向心节点集的补集。在逐跳的信息路由中，每个节点以既定的概率及约定的线序从Next节点集或其它节点集选择相应的子节点集中的某个节点发送信息。需要注意的是，信息是加密传输的，且对于向心节点集和离心节点集的选择是由信息的加密状态位设定的。

因此，攻击者无法通过信息转发关系来推断中继节点与基站的相对位置关系。具体地，本文提出的路由方法主要包括网络初始化和信息发送两个阶段。

### 3.1 网络初始化描述

本文假定在网络初始化阶段，整个网络是安全的。根据泰森多边形划分规则[14]，无线传感器网络中各个基站以其各自位置信息对其部署域进行划分，使得：(1)每个被划分的子部署域Vcell中有且仅有一个基站；(2)给定一个Vcell$_i$及其覆盖的基站$q_i$，则其上任意一点$n_i$到$q_i$的距离小于等于其到其它基站的距离，当且仅当$n_i$位于区域边界点时，等号成立。

基于泰森多边形划分规则所进行的部署域划分建立了子部署域与基站的一一映射关系，其目的在于信息能够从给定的源节点发送到距离最近的基站，从而尽可能地减少通信开销。图5展示了一个区域划分实例，其中4个基站$q_1$, $q_2$, $q_3$, $q_4$基于泰森多边形划分规则分别被划分到$V_1$, $V_2$, $V_3$, $V_4$, 4个Vcell中。

给定源节点$n_i$位于$V_1$，能够得出$q_1$为与之最近的基站。此外，在采用泰森多边形划分规则对部署域进行划分的基础上，本文使用Hilbert空间填充曲线[15]对部署域进行迭代划分。给定待划分区域$\mathbb{G}$：

(1) 首先将$\mathbb{G}$划分为$N\times N$个大小均一的格状子区域Gcell，其中$N\in 2^n$ ($n$=1, 2, …)；

(2) 各传感器将其所属的泰森多边形划分域号Vcell$_i$记录于其相应的状态码中。

结合泰森多边形划分规则及Hilbert空间填充曲线，基站通过以下步骤对网络进行初始化：

(1) 部署域中的各个基站使用Hilbert空间填充曲线对其所在泰森多边形部署域进行排序。各传感器将其所属的Hilbert序号Gcell$_i$记录于其相应的状态码中。需要说明的是各个Vcell的在其所辖的区域内发布的Hilbert填充曲线的线序可以不同；

(2) 各个Gcell边界的传感器感知其覆盖范围内同属一个Vcell的最小上Gcell号传感器集及最大下Gcell号传感器集，并根据与其同属一个Vcell基站的相对位置将其分别标记为向心节点集和离心节点集；

(3) 各基站分别以自身为中心进行广播，而各个传感器仅接收其所属Vcell的基站的广播信息并将其标记在相应的状态位(包括基站ID、线序标识、相对于基站在当前线序下的位置标识(其中，“0”表示在当前线序下，目标传感器的线序编号先于基站；而“1”表示目标传感器的线序编号后于基站))，对于边界传感器，则需要使用列表记录所有包含它的基站信息；

(4) 各个传感器间感知其覆盖范围内是否有传感器被标记为“线序”传感器，若存在，则根据其与目标传感器的相对线序位置，将其记录在其Next节点集和Prior节点集中。

### 3.2 信息安全传输

为了保证信息的安全，信息需要加密传输。在预配置和初始化阶段，各传感器节点$q_i$预载入两个对称密钥$k_{i,B}$, $k_i$和一个哈希函数$F$。其中，$k_{i,B}$为$q_i$与基站共享的对称密钥。$k_i$为节点$q_i$与其邻节点共享的广播密钥。Wang等人[16]提出暴露域的概念，即攻击者容易从源节点附近的节点追踪至源节点的位置。为此，信息传输主要包括以下3个阶段：

(1) 源节点$G(h)$跳有限洪泛：$G(h)$跳随机路由

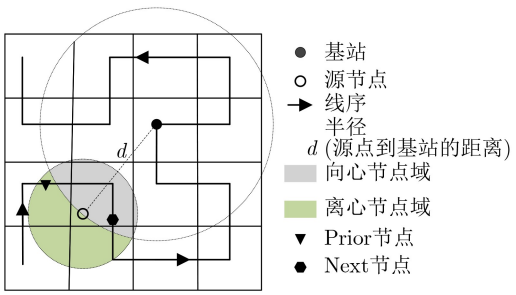



图 4 基于Hilbert填充曲线的节点位置隐私保护路由方法示意图

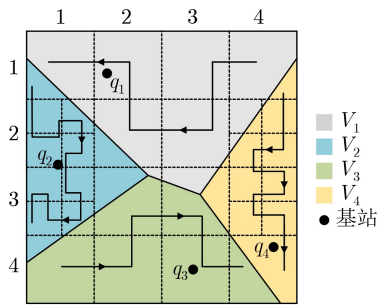



图 5 基于泰森多边形的多线序区域划分实例

的目的主要是为了防止攻击者对本文策略反向推导出随机扰动，其中，$G(h)$为一个随机函数；

(2) $(k, p)$-环路由：$k$表示路由所需选择经过的最大Hilbert填充曲线次数，该参数的设定旨在防止信息过度地在曲线上路由并能有效地降低通信开销。$p$为传感器节点以Next节点集(或Prior节点集)中节点为下一条中继的路由概率。相应地，$(1–p)$为节点以向心节点集(或离心节点集)中的节点为下一条候选中继的路由概率，其中，向心节点集或离心节点集的选择由信息的状态位决定，当信息未路由至基站时，相应的状态位为1(向心节点集)；当基站接收到信息后，将其相应的状态位改为0(离心节点集)。需要说明的是，在实际的MWSNs中，为了防止可探知角$\theta$过小而导致的位置泄露问题(类似于暴露域)或过大而导致的高额通信开销，参数$p$的取值往往不是定值，而是由一个与信息传播跳数$h$呈反向趋势的函数$Q(h)$来确定的；

(3) $G(h)$跳基站伪装：由于基站在信息传递的过程中仅负责接收信息，导致信息包的入度远大于出度。为此，需将其伪装成一个普通的“中继”节点。当信息被基站接收时，与阶段(1)相似，基站将该信息进行有限的$G(h)$跳转发。

### 3.3 伪信息混淆生成方法

此外，为了防止攻击者通过大数据采样技术分析信息的传播路由规律，传感器节点需要不定期地生成并发送伪消息以扰乱攻击者。为此，每一个传感器节点$q_i$在初始化时预载入两个随机数：$\lambda(0<\lambda<1)$和$h_{\text{fake}}$，其中，$\lambda$表示伪消息产生的概率，$h_{\text{fake}}$表示一个伪消息被转发的最大次数。然而，这将可能导致整个网络的信息拥塞。为此，本研究在伪信息混淆生成策略中加入了触发机制和抑制机制。

(1) 触发机制：每一个传感器含有一个计时器$T_i$，当传感器节点长时间没有作为源节点或中继节点传输信息时$(T_i>t)$，则伪信息混淆生成机制被触发，并将伪信息的相应状态值改为Fake，其自身节点的状态为也改为Fake。其中，每一个传感器节点所设定的计时器的值各异，传感器的状态值Fake将在其结束伪信息后的$m$个计时器周期后恢复为True。

(2) 抑制机制：当传感器节点感知到其覆盖范围内的其它节点的状态值为Fake时，其自身的计时器暂停；此外，当该节点正在传输信息状态值为True的信息时，若同时接收到状态值为Fake的信息，则忽略其$h_{\text{fake}}$参数的设置，直接将其丢弃。

## 4　实验结果对比及分析

仿真实验操作系统采用Ubuntu 16.04 LTS，利用NS2模拟仿真软件构建无线传感网络，其中10000个传感器节点随机部署在1000 m×1000 m的区域内，基站的位置固定，源节点的位置随机选择。每个节点的位置坐标添加一个随机扰动$\varepsilon$, $\varepsilon$服从高斯分布，即$\varepsilon\sim N(\mu, \varepsilon^2)$，所有节点的通信半径设置为100 m，攻击者在逆向追踪过程中的可视范围设置为300 m，此外，假设网络中没有数据分组冲突。本文提出的HLPS方法与PU SBRF[2], MoRF[3]以及PLAUDIT[11]进行对比验证，实验结果是多次实验所得的平均值。

### 4.1 通信开销对比与分析

通信开销是衡量隐私保护方法可用性的基础，本文中以数据传输的跳数为基准衡量本文方法的通信开销，在给定通信开销$d$=50(源节点到基站的跳数为50)的情况下，图6给出了HLPS方法在不同路由概率$p$下所经过的最大Hilbert填充曲线次数的通信开销，图7给出了HLPS方法在不同可探测角度下的通信开销。

从图6中可以看出，HLPS方法的通信开销随着路由路径所经历的最大Hilbert填充曲线次数的增加而增加，这表明消息传递途经的沿Hilbert线序路径次数愈多，路由路径愈长，所需要的跳数也就愈多，这与前文理论分析是一致的。另外，当$k$>8时，不同路由概率$p$情况下，路由跳数变化不大，这是由

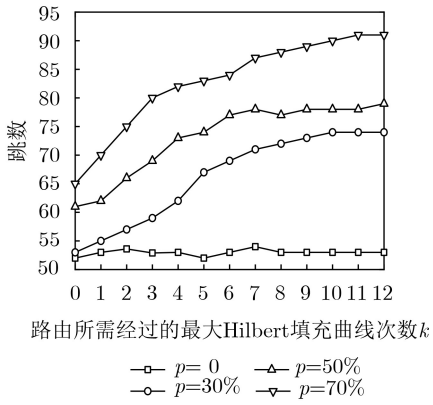



图 6 HLPS方法在不同沿Hilbert线上路由次数的通信开销

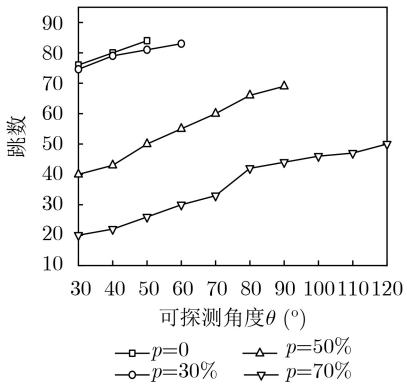



图 7 HLPS方法在不同可探测角度的通信开销

实验中设定的源节点和基站之间的距离跳数(50)决定的，在实际环境中，源节点和基站的距离不同将导致参数$k$的值能个性化设置，以平衡隐私保护与额外的通信开销。此外，根据HLPS方法的路由策略，当路由数据接近基站时，其路由路径将不仅仅局限于$k$，这种思路能够有效地降低数据在环中丢失的概率，同时也能降低通信开销。

结合图7，在路由概率$p$=70%的情况下，通过对比跳数、路由途经的最大Hilbert填充曲线次数和可探测角度3个指标可以看出，HLPS取得了较为优越的综合性能。此外，与{$p$=50%, $k$=5}和{$p$=30%, $k$=5}的情况相比，在{$p$=70%, $k$=5}的情况下，通信开销略有增加，但其可探测角度却大幅增加了30%。还可以看出，可探测角度的大小与路由早期经过的Hilbert填充曲线的跳数呈正相关。而随着从Next节点集中选择节点的路由概率$p$的增加，这种正相关性也趋于显著。

除了数据路由所需经过的最大Hilbert填充曲线次数影响隐私保护方法的通信开销外，源节点距离基站的跳数同样影响其通信开销，图8给出了源节点距离基站不同跳数情况下HLPS方法的通信开销。

从图8可以看出，通过综合对比节点距离基站跳数$d$、通信开销(跳数)、源节点位置隐私安全性等指标，在$p$=70%的情况下本文方法表现良好，主要是因为在$p$=90%的情况下，数据沿Hilbert线序的路由路径过大，直接导致路由路径变长，通信开销也随之增大，而在$p$=50%的情况下，数据沿Hilbert线序的路由路径过小，路径长度也随之变小，通信开销较低，但是，该情况下，可探测角所形成的可探测域变小，源节点被暴露的风险也较大。下面就给定$p$=70%的情况下，比较HLPS与其它3种方法在不同可探测角度下的通信开销，实验结果如图9所示。

从图9可以看出，4种方法的通信开销均随着可探测角度$\theta$的增大而增大。具体来看，MoRF和PLAUDIT方法的通信开销随着$\theta$的增大呈线性增长的趋势，而HLPS方法仅呈亚线性增长的趋势。需要指出的是，由于PU SBRF方法采用洪泛协议生成多个幻象源节点，这导致其初始的可探测角度$\theta$较大，相比之下，在路由初期阶段，HLPS方法形成的可探测角度小于PU SBRF的可探测角度。然而在此阶段，PU SBRF方法的通信开销是参数$n$的线性函数($n$表示生成的幻象源节点的数量)，这使得PU SBRF方法的通信开销远高于其它3种方法。

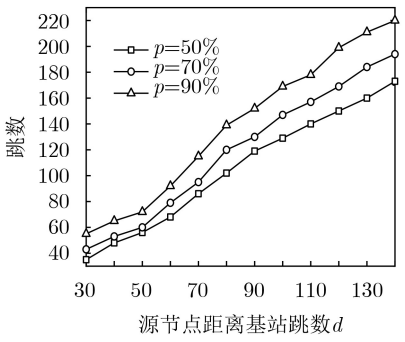



图 8 HLPS方法在源节点/基站不同距离下的通信开销

### 4.2 安全时间对比与分析

本文采用安全时间来衡量各方法的安全性能，安全时间指攻击者从基站追踪到源节点所需经历的跳数之和[2]。与上一小节类似，在给定源节点距离基站跳数$d$=50的情况下，验证HLPS方法在路由所需经过的最大Hilbert填充曲线次数情况下可探测角度的大小，实验结果如图10所示。

从图10可以看出，随着路由最大环数的增加，可探测角度$\theta$逐渐增大，$\theta$愈大则可探测域就越小，提高了源节点的不可追溯性，从而保障源节点位置隐私的安全。在可探测角度$\theta\approx60°$时，HLPS方法取得较为优越的综合性能。可探测角度较小时，攻击者的探测域愈大，源节点被暴露的概率也就愈大；反之，源节点被暴露的概率愈小。但是，由于路由所经过的Hilbert线上路由，过大或过小的可探测角均会给通信开销带来负面影响，因此，在实际

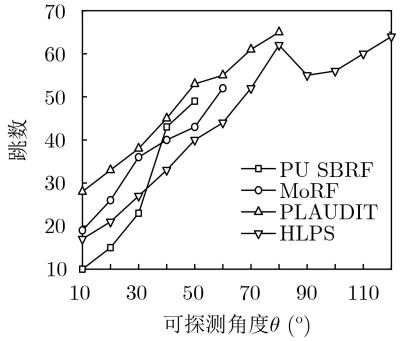



图 9 4种方法通信开销对比

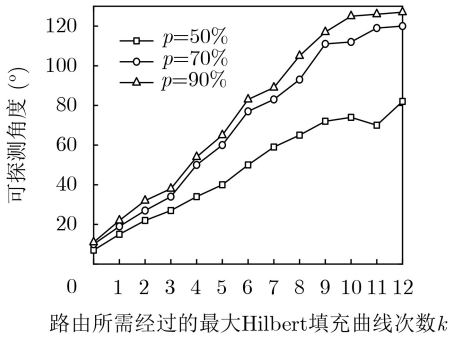



图 10 HLPS方法在路由所需最大Hilbert填充曲线次数下的可探测角

的场景中需要根据隐私保护与通信开销的需求调节参数上环概率以及最大环数。

在理论上，追踪跳数[2]、平均追踪时间(Average Track-back Time, ATT)[10]、流量混淆程度[13]等均可作为衡量安全时间的评价指标。为了统一化，本文以追踪跳数作为评价安全时间的指标。下面将在给定$\theta$=60°时，以源节点到幻象源节点的反向回溯误差跳数为指标评价各方法的安全时间，实验结果如图11所示。

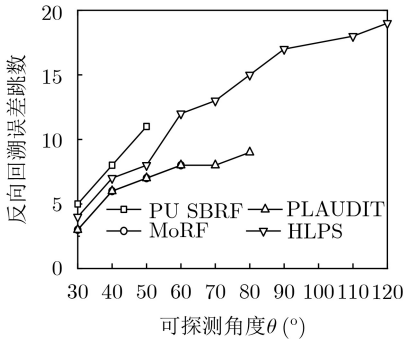



图 11 不同可探测角度情况下4种方法的安全时间对比

图11可以看出，在初始路由阶段，PU SBRF方法采用了洪泛协议，不同于MoRF和PLAUDIT采用流量平衡的方式隐藏源节点的位置信息，其每一跳都被路由到背离真实源节点的方向，因此，PU SBRF的安全时间在初始路由阶段有显著的优势。

## 5　结束语

无线传感器网络已被广泛地应用于各种复杂、恶劣海洋作业环境中，本文考虑了一种更为现实的攻击模型，即攻击者从基站反向回溯源节点的攻击模型，从如何缩小监听域的范围入手，本文提出了基于Hilbert填充曲线的源节点位置隐私保护方法HLPS，与传统方法相比，本文提出的方法具有更低的通信开销和更高的安全时间。但是HLPS方法中由于Hilbert曲线路由引入了额外的通信开销，如何优化网络流量的路由策略仍需要进一步研究。

## 参 考 文 献

[1] WALID E, THOMAS N, EOIN O, *et al*. Trust security mechanism for maritime wireless sensor networks[J]. *Concurrency and Computation*: *Practice and Experience*, 2017, 29(23): e3945. doi: 10.1002/cpe.3945.

[2] 陈娟, 方滨兴, 殷丽华, 等. 传感器网络中基于源节点有限洪泛的源位置隐私保护协议[J]. 计算机学报, 2010, 33(9): 1736–1747. doi: 10.3724/SP.J.1016.2010.01736.
CHEN Juan, FANG Binxing, YIN Lihua, *et al*. A source-location privacy preservation protocol in wireless sensor networks using source-based restricted flooding[J]. *Chinese Journal of Computers*, 2010, 33(9): 1736–1747. doi: 10.3724/SP.J.1016.2010.01736.

[3] BAROUTIS N and YOUNIS M. Using fake sinks and deceptive relays to boost base-station anonymity in wireless sensor network[C]. The 40th IEEE Conference on Local Computer Networks, Clearwater Beach, USA, 2015: 109–116. doi: 10.1109/LCN.2015.7366289.

[4] DI PIETRO R and VIEJO A. Location privacy and resilience in wireless sensor networks querying[J]. *Computer Communications*, 2011, 34(3): 515–523. doi: 10.1016/j.comcom.2010.05.014.

[5] AL-MISTARIHI M F, TANASH I M, YASEEN F S, *et al*. Protecting source location privacy in a clustered wireless sensor networks against local eavesdroppers[J]. *Mobile Networks and Applications*, 2020, 25(1): 42–54. doi: 10.1007/s11036-018-1189-6.

[6] NGAI E C H and RODHE I. On providing location privacy for mobile sinks in wireless sensor networks[J]. *Wireless Networks*, 2013, 19(1): 115–130. doi: 10.1007/s11276-012-0454-z.

[7] WANG Jian, WANG Fengyu, CAO Zhenzhong, *et al*. Sink location privacy protection under direction attack in wireless sensor networks[J]. *Wireless Networks*, 2017, 23(2): 579–591. doi: 10.1007/s11276-015-1179-6.

[8] 彭志宇, 李善平. 移动环境下LBS位置隐私保护[J]. 电子与信息学报, 2011, 33(5): 1211–1216. doi: 10.3724/SP.J.1146.2010.01050.
PENG Zhiyu and LI Shanping. Protecting location privacy in location-based services in mobile environments[J]. *Journal of Electronics & Information Technology*, 2011, 33(5): 1211–1216. doi: 10.3724/SP.J.1146.2010.01050.

[9] LONG Jun, LIU Anfeng, DONG Mianxiong, *et al*. An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing[J]. *Journal of Parallel and Distributed Computing*, 2015, 81–82: 47–65. doi: 10.1016/j.jpdc.2015.04.003.

[10] LIU Anfeng, LIU Xiao, TANG Zhipeng, *et al*. Preserving smart sink-location privacy with delay guaranteed routing scheme for WSNs[J]. *ACM Transactions on Embedded Computing Systems*, 2017, 16(3): 68. doi: 10.1145/2990500.

[11] BAROUTIS N and YOUNIS M. Load-conscious maximization of base-station location privacy in wireless sensor networks[J]. *Computer Networks*, 2017, 124: 126–139. doi: 10.1016/j.comnet.2017.06.021.

[12] LIN Xiaodong, LU Rongxing, LIANG Xiaohui, *et al*. STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in

VANETs[C]. 2011 IEEE INFOCOM, Shanghai, China, 2011: 2147–2155. doi: 10.1109/INFCOM.2011.5935026.

[13] FAN Yanfei, JIANG Yixin, ZHU Haojin, *et al*. An efficient privacy-preserving scheme against traffic analysis attacks in network coding[C]. The 28th IEEE International Conference on Computer Communications, Rio de Janeiro, Brazil, 2009: 2213–2221. doi: 10.1109/INFCOM.2009.5062146.

[14] HU Ling, KU W S, BAKIRAS S, *et al*. Spatial query integrity with voronoi neighbors[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2013, 25(4): 863–876. doi: 10.1109/tkde.2011.267.

[15] KALNIS P, GHINITA G, MOURATIDIS K, *et al*. Preventing location-based identity inference in anonymous spatial queries[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2007, 19(12): 1719–1733. doi: 10.1109/TKDE.2007.190662.

[16] WANG Weiping, CHEN Liang, and WANG Jianxin. A source-location privacy protocol in WSN based on locational angle[C]. 2008 IEEE International Conference on Communications, Beijing, China, 2008: 1630–1634. doi: 10.1109/ICC.2008.315.

李攀攀：男，1983年生，讲师，研究方向为隐私保护、网络空间安全等.

谢正霞：女，1982年生，工程师，研究方向为传感器网络，隐私保护等.

周志刚：男，1986年生，博士，讲师，研究方向为隐私保护、网络空间安全等.

乐光学：男，1963年生，博士，教授，研究方向为多云融合与协同服务、无线Mesh网络与移动云计算、网络空间安全等.

郑仕链：男，1984年生，博士，高级工程师，研究方向为认知无线电、深度学习、通信信号处理等.

杨小牛：男，1961年生，研究员，研究方向为软件无线电、深度学习、通信信号处理等.