计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200400099

WSN 中基于目标决策的源位置隐私保护方案

郭 蕊 芦天亮 杜彦辉
中国人民公安大学信息网络安全学院 北京 100038
(2103008108@qq.com)

摘 要 针对现有基于幻影源的无线传感网(Wireless Sensor Network,WSN)的源位置隐私保护方案,普遍存在无法有效平衡源位置隐私安全性、网络生存周期和传输延迟之间的矛盾关系的问题,提出了一种基于目标决策的幻影源分散路由方案 PSSR(Phantom Source Separate path Routing)。该方案采用分段定象随机游走来确定幻影节点的位置,在保证幻影源距离真实源可视区足够远的同时,实现了幻影源位置的多样性,增大了攻击者定位源位置的难度。除此之外,该方案通过考虑节点的能量消耗、剩余能量及其到基站的距离来选取转发节点,实现了低概率重复分散路由的构建,有效平衡了源位置隐私安全性、网络生存周期和传输延迟之间的矛盾关系。仿真实验结果表明,相比 EPUSBRF 方案、PRLA 方案和 MPRP 方案,PSSR 方案在增强源位置隐私安全性的同时,能够有效延长网络生存周期和降低传输延迟。

关键词:无线传感网;源位置;隐私保护;幻影源;分散路由
中图法分类号 TN929.5;TP212.9

Source-location Privacy Protection Scheme Based on Target Decision in WSN

GUO Rui,LU Tian-liang and DU Yan-hui
College of Police Information Engineering and Network Security,People's Public Security University of China,Beijing 100038,China

Abstract Aiming at the problem that the existing schemes of Wireless Sensor Network(WSN) source-location privacy protection based on phantom source can not effectively balance the contradiction among source location privacy security,network life cycle and transmission delay,a phantom source separate path routing scheme (PSSR) based on target decision is proposed. In PSSR scheme,the phantom node location is determined by random walk of segmented fixed image,which ensures that the phantom source is far enough from the real source visible area,and at the same time realizes the diversity of phantom source location,which increases the difficulty of attacker locating the source location. In addition,by considering the energy consumption of the node,the remaining energy and the distance from the node to the base station,the forwarding node is selected to realize the construction of low probability repeated and decentralized routing,effectively balancing the contradiction among the source location privacy security,network life cycle and transmission delay. Compared with EPUSBRF,PRLA and MPRP,PSSR can not only enhance the source location privacy security,but also effectively prolong the network lifetime and reduce the transmission delay.

Keywords Wireless sensor network,Source-location,Privacy protection,Phantom source,Separate path routing

1 引言

无线传感网主要由大量资源受限的传感器节点组成,通过无线多跳的通信方式来实现监测数据的获取和收集,被广泛应用于国防监测、灾害预警、医疗救援和工业制造等诸多领域。然而,无线通信的开放性在方便人们掌握所需信息的同时,降低了攻击者定位源位置的难度,进而引发了严重的位置隐私泄露问题[1],给监测目标带来了巨大的安全隐患。

由于以目标监测为主要任务的无线传感网覆盖面积广且配置了基本安全防护措施,为了不被察觉,攻击者主要采取借助流量分析执行反向追踪的方式来定位源节点。因此,为了有效增强源位置的安全性,国内外研究人员主要围绕幻影源的选取展开了大量研究,试图通过幻影源来隐藏真实源位置,以达到延长位置隐私保护周期的目的。考虑到现有基于幻影源的源位置隐私保护方案无法有效平衡源位置隐私安全性、网络生存周期和传输延迟之间的矛盾关系[2-17],本文提出了一种基于目标决策的 WSN 源位置隐私保护方案 PSSR,该方案将幻影源与低概率重复分散路由相结合,在增强源位置隐私安全性的同时,有效延长了网络生存周期和缩短了传输延迟。

2 相关工作

基于幻影源的 WSN 源位置隐私保护方案本质上是通过

到稿日期:2020-04-22 返修日期:2020-07-07 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家重点研发计划(20190178);中国人民公安大学 2019 年基本科研业务费重大项目(2019JKF108)
This work was supported by the National Key R & D Program of China(20190178) and Fundamental Research Funds for the Central Universities of PPSUC(2019JKF108).
通信作者:芦天亮(lutianliang@ppsuc.edu.cn)

幻影源来隐藏真实源位置，以达到干扰攻击者追踪视线的目的，因此幻影源的选取对源位置隐私的安全性至关重要。近年来，国内外研究人员主要围绕幻影源的选取展开了大量研究，试图通过改进随机游走方式来确保幻影源的有效性，增大攻击者定位源位置的难度。

基于幻影源的源位置隐私保护方案最早由 Qzturk 等[2]提出，他们通过构建熊猫—猎人模型来阐述开放的无线通信方式存在的泄露源位置隐私的风险，并提出了一种基于洪泛的幻影路由解决方案 PRS(Phantom Routing Scheme)，然而纯随机游走无法确保幻影源足够远离真实源，且洪泛路由容易造成大量的能量消耗。因此，Kamat 等[3]提出了基于定向随机游走的单径幻影路由协议 PSPR(Phantom Single-Path Routing)，该协议通过限制节点选取，确保数据包一直朝着远离或靠近基站的方向转发，但也因此缩小了幻影源的范围。针对幻影源分布过于集中的问题，Chen 等[4]提出了基于源节点有限洪泛的源位置隐私保护协议 PUSBRF(Source Location Privacy Preservation Protocol in Wireless Sensor Network Using Source-Based Restricted Flooding)，该协议借助源节点的有限洪泛和有向路由，有效增强了源位置隐私的安全性，但也造成了较高的网络能耗和传输延迟。除此之外，Yao 等[5]和 Li 等[6]分别通过引入定向增强随机游走策略和随机转发节点机制来实现对 PRS(Phantom Routing Scheme)方案的改进，但仍不能有效平衡能量消耗和位置隐私保护之间的矛盾关系。

考虑到可能存在较强视觉能力的攻击者，Wang 等[7]首次提出了可视区的概念，并将幻影源路由阶段经过可视区的路径定义为失效路径。为了降低失效路径产生的可能性，Wang 等[7]研究了一种基于位置角的 PRLA(Phantom Routing with Locational Angle)协议，该协议根据节点的位置角选择转发节点，增大了某条路径或某些节点被重复选择的可能，从而降低了攻击者反向追踪到源位置的难度。Chen 等[4]在 PUSBRF 协议的基础上，通过对可视区内节点进行标记来避免失效路径的产生。Long 等[8]和 Kumar 等[9]分别通过创建与攻击者具有完全同质分支的结构树和设定幻影节点、源节点和基站之间的角度范围，来拉大幻影节点与源节点之间的间距，从而降低失效路径产生的可能性，但该方法仍然存在能量不均衡消耗的问题。Xu 等[10]通过非线性划分来限制随机游走方位，虽然该方法较好地避开了可视区，但无法有效延长网络的生存周期。

为了平衡能量消耗和位置隐私保护之间的关系，Liu 等[11]基于最小能耗提出了一种可控能耗的源位置隐私保护协议 LPBMR(Source-Location Privacy Protection Based on the Minimum Cost Routing)，该协议虽然有效提高了网络性能，但也限制了节点的选取范围。Yao[12]提出了一种基于定向贪婪游走的源位置隐私保护策略 DGWK(Directed Greedy Walk)，该策略有效降低了网络能耗和传输延迟，但由于数据包的传输具有方向指示性，因此大大降低了攻击者定位源位置的难度。Zhou 等[13]通过定向随机方式选取幻影节点来确保幻影源距离真实源足够远，且幻影节点基于最小能耗转发数据包有效降低了能量损耗，但该方案无法避免失效路径的存在。除此之外，部分研究还基于伪正态分布[14]、随机角度和圆周路由[15]、能耗控制[16]以及逃脱角和能量因子[17]等因素来优化幻影源位置的多样性，从而实现源位置安全周期的有效延长，但这些方法也都不同程度地造成了能量的过度损耗。

针对现有基于幻影源的 WSN 源位置隐私保护方案普遍存在无法有效消除源位置隐私安全性、网络生存周期和传输延迟之间的矛盾的问题，本文提出了一种基于目标决策的幻影源分散路由方案 PSSR。性能分析结果表明，该方案在增强源位置隐私安全性的同时，能有效延长网络生存周期和降低传输延迟。

3　问题描述

3.1　系统模型

本文的系统模型与熊猫—猎人模型[2]相似，主要由网络模型和攻击者模型组成。假设传感器节点均匀部署在网络中并用于监测目标行为，一旦发现目标，距离其最近的传感器节点成为源节点并周期性地发送包含监测目标活动内容和自身位置坐标的加密数据包到基站。攻击者在节点处实施窃听，试图通过反向追踪的方式来发现监测目标。

3.1.1　网络模型

无线传感网主要由大量均匀部署且不再移动的传感器节点和一个基站组成。所有传感器节点的性能和预期寿命相同并拥有唯一 ID，且能够通过 RSSI 测距方法获取节点间距。基站具有较强的存储性能、计算性能以及充足的能量供应，且具备安全防护措施以避免攻击者获取除前向节点之外的信息。为了避免流量相似性分析，网络将传输具有固定大小的加密数据包。当传感器节点接收到需要转发的数据包时，依据路由策略选择转发节点进行传输，并造成一定程度的能量消耗。依据能量消耗模型[13]，在信噪比合理的情况下，节点发送和接收阶段的能量消耗分别如式(1)、式(2)所示：

$$\boldsymbol{E}_{TS}(\boldsymbol{k},\boldsymbol{d})=\begin{cases}E_{\text{elec}}\times\boldsymbol{k}+\varepsilon_{fs}\times\boldsymbol{k}\times\boldsymbol{d}^2, & \boldsymbol{d}<d_0\\ E_{\text{elec}}\times\boldsymbol{k}+\varepsilon_{amp}\times\boldsymbol{k}\times\boldsymbol{d}^4, & \boldsymbol{d}\geqslant d_0\end{cases} \tag{1}$$

$$\boldsymbol{E}_{RS}(\boldsymbol{k})=E_{\text{elec}}\times\boldsymbol{k} \tag{2}$$

其中，E_{elec}表示节点发送/接收每比特消息的能量消耗，$\boldsymbol{k}$ 表示消息大小，单位是比特。ε_{fs}和ε_{amp}分别为在自由空间和多路径衰减传输模式下，功率放大造成的单位能量消耗。传输模式由节点间距 $\boldsymbol{d}$ 与距离阈值d_0的大小关系决定，d_0值的求解如式(3)所示：

$$d_0=\sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{amp}}} \tag{3}$$

3.1.2　攻击者模型

与普遍存在的攻击者模型相似，攻击者配备优质的目标追踪设备，拥有强大的计算能力、存储能力以及充足的能量供应。假定攻击者最初位于基站窃听消息，当窃听到消息时，其能够迅速识别并移动到前向节点。但攻击者只能采取被动流量监测，且当其在某一节点位置上实施窃听时，无法窃听到其他节点接收到的消息，同时攻击者具有强大的耐心，即使长时间没有窃听到消息，也仍停留在原地继续窃听，直至发现源节点。考虑到攻击者可能具有较强的视觉能力，因此一旦攻击者追踪到可视区内的节点，就视为源位置暴露。

3.2　目标函数

根据系统模型可知，保护源位置隐私安全的关键在于增

加攻击者定位源位置的难度，同时为了更好地适用于无线传感网，保护方案应尽可能地降低能量消耗和传输延迟。因此，WSN 源位置隐私保护问题实质上是一个多目标优化问题，即寻求源位置安全性、网络生存周期和传输延迟之间的平衡最优解。考虑到任意一个节点能量耗尽或可视区内节点暴露都将导致问题求解变得无意义，因此源位置隐私保护问题的目标函数和约束条件分别如式(4)、式(5)所示：

$$F(t,x_1,x_2,\cdots,x_n)=(\max SP,\max LT,\min DT) \tag{4}$$

$$\text{s.t.}\begin{cases}\forall i,j\in\{1,2,\cdots,n\},e_{x_i}>\min[E_{TS}(\boldsymbol{k},\boldsymbol{d}_{ij})+E_{RS}(\boldsymbol{k})]\\ L_{atta}(t)\notin U_{sour}(x_s,r)\end{cases} \tag{5}$$

其中，$L_{atta}(t)$表示第 t 个数据包传输完成后攻击者的位置坐标，$U_{sour}(x_s,r)$表示以源节点x_s为圆心、r 为半径的可视区内部节点的位置坐标集合。SP 表示源位置的安全周期，即源位置暴露前发送的数据包数目[1]，LT 和 DT 分别表示网络生存周期和传输延迟。考虑到均衡化的网络低能耗能够有效延长网络生存周期，因此可以通过式(6)对网络生存周期进行衡量，其中，TE 和 RE 分别表示网络总能耗和节点剩余能量均方差，求解过程如式(7)、式(8)所示：

$$\max LT=\min(TE,RE) \tag{6}$$

$$TE=\sum_{t=1}^{SP}\{\sum_{x_i=R_t[m]\wedge x_j=R_t[m+1]}^{m+1=len(R_t)}[E_{TS}(k,d_{ij})+E_{RS}(k)]\} \tag{7}$$

$$RE=\sqrt{\sum_{i=1}^{n}\frac{[e_{x_i}-(\frac{OTE-TE}{n})]^2}{n}} \tag{8}$$

其中，R_t 和 $len(R_t)$分别表示传输第 t 个数据包途径的节点序列和节点数，OTE 表示网络初始总能量，e_{x_i} 表示节点 i 的剩余能量。传输延迟 DT 则通过数据包传输所需的平均时间来进行衡量。

除此之外，通过式(5)定义的约束条件来确保网络生存周期 LT 和源位置安全周期 SP 具有意义，规定在任意一个节点的剩余能量值不小于该节点完成数据包传输所需能量消耗的最小值且在攻击者未追踪到可视区内部节点的情况下，求解源位置隐私保护问题，从而确保问题求解的有效性。

4 基于目标决策的 WSN 源位置隐私保护方案 PSSR

基于上述系统模型和目标函数，PSSR 方案旨在通过网络初始化、定象随机游走和最优路径路由这 3 个阶段来实现对源位置隐私的保护，该方案使用的主要符号及其含义如表 1 所列。

表 1 PSSR 方案使用的主要符号及其含义

Table 1 Main symbols and their meanings used in PSSR scheme

符号	含义
B	基站
i,j	传感器节点
l_{ij}	节点间的直线距离
S	源节点
α_i	节点 i 的变向角
e_i	节点 i 的剩余能量
r	可视区半径
θ	可视区偏转角
β_i	节点 i 的旋转角
C,D	数据包已途径的转发节点
R	传感器节点的通信半径

4.1 网络初始化

网络初始化作为 PSSR 方案的准备阶段，为决策路由的实现提供了信息支撑。该阶段主要由 3 个步骤组成：首先，所有传感器节点和基站通过定位算法[18]计算自身位置坐标；然后，基站在整个网络中广播包含自身 ID 和位置坐标的数据包，以供节点记录相关信息；最后，所有传感器节点在其通信范围内广播包含自身 ID、位置坐标和剩余能量的数据包，接收到此类数据包的节点记录发送节点的相关信息，同时根据式(9)计算自身及其邻居节点到达基站的直线距离l_{iB}，建立包含邻居节点和基站相关信息的完备列表。

$$l_{iB}=\sqrt{(x_i-x_B)^2+(y_i-y_B)^2} \tag{9}$$

4.2 定象随机游走

在定象随机游走阶段，采用十字象限法将幻影源选择过程与低概率重复分散路由相结合，在构建低能耗、低时延和均衡化分散路由的同时，确保幻影源的有效性，增大攻击者定位源位置的难度。

4.2.1 十字象限法形成分散路由

十字象限法定义已接收数据包但未进行转发的传感器节点为中间节点，并将发送数据包至中间节点的传感器节点定义为前向节点，其工作原理如图 1 所示。通过将前向节点指向中间节点方向的直线视为 y 轴，同时将过中间节点垂直于 y 轴的直线视为 x 轴，把中间节点的通信范围划分为 4 个区域，且按照先经过近基区域后再经过远基区域的顺序将近源近基区域、远源近基区域、远源远基区域和近源远基区域确定为第一象限至第四象限。随着数据包的传输，前向节点和中间节点基本呈现出无规律动态性，导致定象传输不具备确切方位指示性，这不仅扩大了幻影源的选取范围，而且增大了攻击者定位源位置的难度。

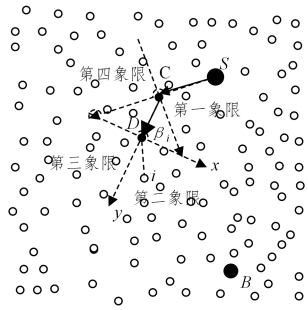


图 1 十字象限法的工作原理

Fig. 1 Working mechanism of cross quadrant method

考虑到第一、第四象限基于 x 轴与源节点同侧易形成失效路径，且第三、第四象限基于 y 轴远离基站易造成较高的网络能耗和传输延迟，因此该方案提出了定象函数 $FX(i)$作为选择转发节点的依据，如式(10)所示：

$$FX(i)=\frac{1}{(-\cos\beta_i)\times l_{iB}} \tag{10}$$

其中，β_i表示前向节点 C 旋转至中间节点 D 与备选节点 i 共线位置时所需途径的角度，即$\angle CDi$，其计算式如式(11)所示：

$$\cos\beta_i=\frac{l_{iD}^2+l_{CD}^2-l_{iC}^2}{2\times l_{iD}\times l_{CD}} \tag{11}$$

虽然定象函数 $FX(i)$有效增大了第二象限节点成为转发节点的可能性，但仍无法实现均衡化分散路由，因此引入均衡

评估函数 $Fit(i)$，如式(12)所示：

$$Fit(i)=\frac{e_i}{E_{TS}(k,l_{Di})+E_{RS}(k)} \tag{12}$$

剩余能量的引入不仅降低了节点被重复选择的可能性，而且其与节点能耗相结合更能促进均衡化低能耗路由的实现。

综上所述，中间节点 D 应结合式(10)和式(12)选取转发节点 i，如式(13)所示，且适应度函数 $F(i)$ 值越大，节点 i 成为转发节点的可能性就越大。考虑到源节点作为中间节点时，备选节点 i 不存在旋转角 β_i，因此源节点应依据式(14)选取转发节点，角度的非限制性使数据包转发路径更具多样化。

$$\begin{aligned}F(i)&=FX(i)\times Fit(i)\\&=\frac{e_i}{(-\cos\beta_i)\times l_{iB}\times[E_{TS}(k,l_{Di})+E_{RS}(k)]}\end{aligned} \tag{13}$$

其中，E_{TS} 对应式(1)，表示传输阶段的能量消耗。

$$F_S(i)=\frac{e_i}{l_{iB}\times[E_{TS}(k,l_{Si})+E_{RS}(k)]} \tag{14}$$

除此之外，为了确保节点选取的有效性，每个节点在接收和发送数据包后应分别根据式(15)和式(16)对前向节点和下一跳节点的剩余能量进行更新(以中间节点 D 为例)。

$$e_c^{t+1}=e_c^t-[E_{TS}(k,l_{CD})+E_{RS}(k)] \tag{15}$$

$$e_i^{t+1}=e_i^t-[E_{TS}(k,R)+E_{RS}(k)] \tag{16}$$

4.2.2　规避可视区选择幻影源

为了避免失效路径的产生，PSSR 方案提出了变向角的概念，其原理如图 2 所示。该方案将邻居节点 i，j 偏离源节点 S 和基站 B 之间连线的角度视为变向角，变向角 α_i 的求解如式(17)所示：

$$\cos\alpha_i=\frac{l_{iB}^2+l_{BS}^2-l_{iS}^2}{2\times l_{iB}\times l_{BS}} \tag{17}$$

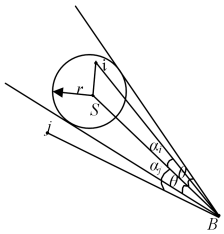


图 2　变向角 α_i 和 α_j

Fig. 2　Angle of change α_i and α_j

为有效增强真实源位置的安全性，PSSR 方案规定只有与源节点的间距大于可视区半径且变向角大于可视区偏转角的节点才能成为幻影节点，同时要求最初满足幻影源条件的中间节点通过执行 h 跳分散路由来确定幻影源的位置。为了确保幻影源的有效性，该方案通过调整适应度函数 $F(i)$ 来形成基于幻影源目标的 h 跳分散路由，如式(18)所示：

$$\begin{aligned}F(i)&=FX(i)\times Fit(i)\times CS\times JS\\&=\frac{e_i\times CS\times JS}{(-\cos\beta_i)\times l_{iB}\times[E_{TS}(k,l_{Di})+E_{RS}(k)]}\end{aligned} \tag{18}$$

其中，CS 表示长度约束，如式(19)所示：

$$CS=l_{is}-l_{DS} \tag{19}$$

CS 的引入进一步确保了数据包朝着远离源节点的方向进行转发。JS 表示角度约束，其计算式如式(20)所示：

$$JS=e^{\cos\alpha_D-\cos\alpha_i} \tag{20}$$

JS 的引入增大了变向角大于中间节点变向角的节点成为转发节点的可能性，进一步拉大了幻影节点与可视区的间距。

综上所述，定象随机游走阶段通过分段分散路由实现了基于目标决策的幻影源选择，如式(21)所示：

$$F(i)=\begin{cases}\dfrac{e_i}{(-\cos\beta_i)\times l_{iB}\times[E_{TS}(k,l_{Di})+E_{RS}(k)]}, & \cos\theta-\cos\alpha_D\geqslant 0\ \text{或}\ l_{DS}-r\leqslant 0\\ \dfrac{e_i\times CS\times JS}{(-\cos\beta_i)\times l_{iB}\times[E_{TS}(k,l_{Di})+E_{RS}(k)]}, & \cos\theta-\cos\alpha_D<0\ \text{且}\ l_{DS}-r>0\end{cases} \tag{21}$$

首先，通过十字象限法构建低能耗、低时延的均衡化分散路由，确保数据包一直朝着远离源位置的方向转发；然后，当中间节点满足幻影源约束条件时，执行基于幻影源目标的 h 跳分散路由来确定幻影节点的位置；最后，在保证幻影源距离可视区足够远的同时，实现了幻影源位置的多样性。

4.3　最优路径路由

幻影节点采用不同于最短路径的最优路径路由策略将数据包转发到基站，该路由策略要求转发节点的选取不仅要实现低能耗和低延迟，还要增大攻击者反向追踪到可视区内节点的难度。因此，该方案综合考虑了攻击者模型、可视区半径和网络能耗等因素，结合式(12)提出了最优决策函数 $Y(i)$，如式(22)所示：

$$\begin{aligned}Y(i)&=Fit(i)\times\frac{CX}{l_{iB}}\\&=\frac{e_i\times(l_{iS}-r)}{[E_{TS}(k,l_{Di})+E_{RS}(k)]\times l_{iB}}\end{aligned} \tag{22}$$

其中，CX 表示长度限制，不同于长度约束 CS，CX 旨在避免失效路径的产生。

除此之外，为了避免基站周围节点能耗过高，最优路径要求中间节点一旦确定基站位于其通信范围内，就直接转发数据包到基站。

4.4　安全性分析

幻影节点到源节点的平均距离 $\bar{d}_p$ 和幻影节点的数目 n_p 是衡量幻影源路由策略安全性的重要参数。本文将从这两个方面对 PSSR 方案进行安全性能评估，并将其与 EPUSBRF 方案[4]、PRLA 方案[7]和 MPRP 方案[10]进行比较。

4.4.1　幻影节点到源节点的平均距离 $\bar{d}_p$

由文献[7]可知，当攻击者追踪到距离源位置一定范围内的节点时，可通过目测来识别源节点。因此，幻影节点与源节点之间的距离在很大程度上影响着源位置的安全性。

考虑到可能存在具有较强视觉能力的攻击者，PSSR 方案通过分段定象随机游走来确保幻影节点的有效性，借助十字象限法确保中间节点一直朝着远离源节点的方向选择转发节点。当中间节点满足幻影源约束条件时，执行附有长度约束和角度约束的 h 跳分散路由，保证该方案产生的幻影节点到源节点的距离处于 $[r+h\times R, r+(h+1)\times R]$ 范围内。EPUSBRF 方案基于源节点的有限洪泛和 h 跳有向路由，使产生的幻影节点分布在以 S 为圆心、跳数 h 为半径的圆周上，

即$d_p(EPUSBRF)\approx h\times R$。PRLA 协议基于位置角选择转发节点，其产生的幻影节点分布在以 S 为圆心、跳数 h 为半径、弧度为 $4\arccos(1-\frac{1}{h})$的圆弧上，因此幻影节点到源节点的距离$d_p(PRLA)\approx h\times R$。MPRP 方案通过源节点随机游走 h 跳来实现幻影源位置的多样性，再依据邻居节点距离源节点的跳数来划定幻影源的选取范围，使幻影节点到真实源位置的距离处于$[h\times R,(h+1)\times R]$范围内。考虑到可视区半径 r 必然大于节点的通信半径 R，因此$d_p(PSSR)>(h+1)\times R$，即这 4 种方案产生的幻影节点到源节点的平均距离$\bar{d}_p$应满足如下关系，即：

$$\bar{d}_p(PSSR)>\bar{d}_p(MPRP)>d_p(EPUSBRF)=\bar{d}(_pPRLA) \tag{23}$$

相比 EPUSBRF 方案、PRLA 方案和 MPRP 方案，PSSR 方案产生的幻影节点距离源节点更远，因此攻击者定位源位置的难度更大。

4.4.2 幻影节点的数量n_p

幻影节点的数量n_p也是影响源位置隐私安全性的重要因素之一[11]，方案产生的幻影源数量越多，真实源到幻影源的传输路径就越多样化，攻击者也就越难定位到源节点。

为了平衡源位置隐私安全性、网络生存周期和传输延迟之间的关系，PSSR 方案要求中间节点综合考虑节点剩余能量、节点能耗、节点到基站的距离以及可视区等因素执行分散路由策略，使产生的幻影节点均匀分布在以 S 为圆心、内环半径为$(r+h\times R)$、外环半径为$[r+(h+1)\times R]$的圆环 EG 和圆环 FH 上，如图 3 所示。幻影节点数量n_p的计算式如式(24)所示：

$$\begin{aligned}n_p(PSSR)&=2\pi[r+(h+1)R]-2\gamma(d_{EB}+d_{GB})+2\pi(r+hR)-2\gamma(d_{KB}+d_{MB})=2\pi[2r+(2h+1)R]-8\gamma\sqrt{l_{BS}{}^2-r^2}\end{aligned} \tag{24}$$

其中，γ为θ的弧度制。

EPUSBRF 方案基于 h 跳有限洪泛使幻影节点分布在以 S 为圆心、$(h\times R)$为半径的圆周上，因此该方案产生的幻影节点数量$n_p(EPUSBRF)=2\pi hR$；同理，PRLA 方案产生的幻影节点数量$n_p(PRLA)=4\arccos\frac{h-1}{h}$；MPRP 方案是在由随机游走 h 跳所到节点及其大于 h 跳的邻居节点组成的 P 集合中，依据 θ 角判断和确定幻影节点的选取范围，因此该方案产生的幻影节点数量$n_p(MPRP)=3\pi hR-4\gamma l_{BS}$。

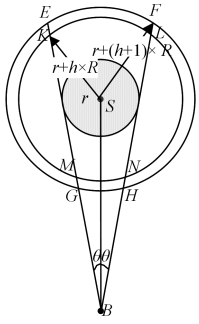


图 3 幻影节点的分布范围

Fig. 3 Distribution range of phantom nodes

表 2 列出了在 R 定值为 1 和 r 定值为 3 的条件下，4 种方案的幻影节点数量。相比 EPUSBRF 方案、PRLA 方案和 MPRP 方案，PSSR 方案在同等条件下产生的幻影节点数量最多，且产生的幻影节点能够较好地避开可视区，较大程度地保护了源位置的安全。

表 2 4 种方案产生的幻影节点数量比较

Table 2 Comparison of the number of phantom nodes generated by 4 schemes

h	l_{BS}	$n_p(PRLA)$	$n_p(EPUSBRF)$	$n_p(MPRP)$	$n_p(PSSR)$
5	30	12.87	31.42	35.12	82.93
15	30	22.03	94.25	129.37	208.59
30	30	31.07	188.49	270.74	397.08
15	10	22.03	94.25	129.37	209.58
15	60	22.03	94.25	129.37	208.50

5 实验与分析

本文采用基于离散事件的 OMNet++平台进行仿真实验，仿真参数如表 3 所列。将 20000 个传感器节点随机且均匀地部署在 1500m×1500m 的网络中，设置基站位置坐标为(750,750)，源节点随机产生并依据路由策略转发数据包到基站。仿真实验将分别控制源节点到基站的距离和路由跳数这两个变量，从源位置的安全周期、网络生存周期和传输延迟这 3 个方面对 PSSR 方案进行评估，并将其与 EPUSBRF 方案、PRLA 方案和 MPRP 方案进行比较。

表 3 仿真实验的参数值

Table 3 Parameters of simulation experiment

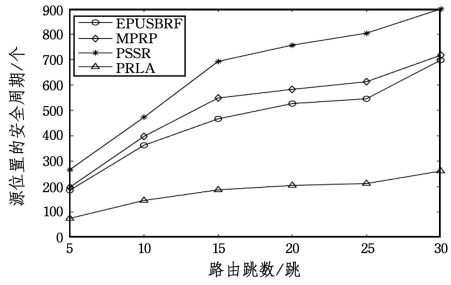
参数	值	参数	值
E_{elec}	50nJ/bit	R	10m
ε_{fs}	100pJ/(bit·m²)	r	30m
ε_{amp}	0.013nJ/(bit·m⁴)	k	512B

5.1 源位置的安全周期

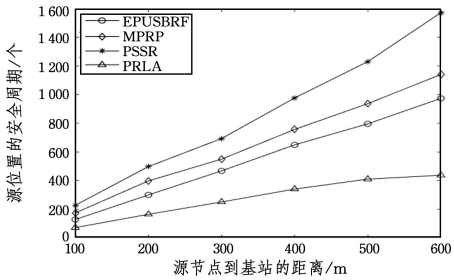
图 4(a)给出了路由跳数与源位置安全周期之间的关系。由图 4(a)可知，当源节点与基站间距一定时，随着路由跳数的增大，源位置的安全周期也随之延长，这主要是因为路由跳数的增加导致幻影节点到源节点的平均距离以及幻影节点的数量均随之增加，这在一定程度上增加了攻击者定位源位置所需途径的节点数目，从而有效延长了源位置的安全周期。而当路由跳数一定时，源位置的安全周期同样也会随着源节点到基站的距离的增加而延长，如图 4(b)所示，这是由攻击者模型决定的。考虑到攻击者最初位于基站处窃听消息，改变源节点到基站的距离必然会影响攻击者定位源节点所需经历的跳数，因此源节点与基站的间距越大，攻击者定位源位置所需捕获的数据包就越多，源位置的安全周期也就越长。

相比 EPUSBRF 方案、PRLA 方案和 MPRP 方案，PSSR 方案的源位置安全周期始终是最长的。这一方面是因为 PSSR 方案产生的幻影节点数量(见表 2)及其到源节点的平均距离均大于其他 3 种方案的，这导致攻击者定位源位置的难度增大；另一方面是因为该方案选取转发节点时考虑了节点的剩余能量因素，实现了低概率重复分散路由的构建。通过降低某些路径或某个节点被重复选择的可能性，PSSR 方

案减少了攻击者能够捕获的数据包数量，从而增大了其反向追踪的难度。



(a)源节点到基站的距离l_{BS}定值为 300 m



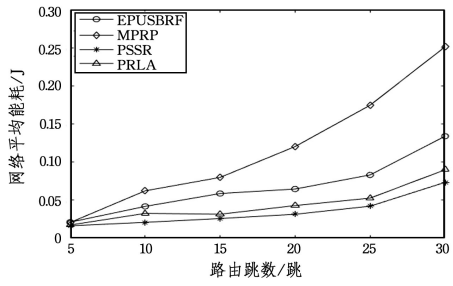
(b)路由跳数 h 定值为 15

图 4　源位置的安全周期

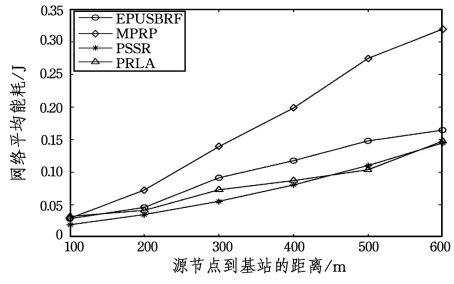
Fig. 4　Safety cycle of source location

5.2　网络生存周期

因为 4 个方案实现的源位置安全周期不一致，所以源节点发送的数据包数量成为了影响网络总能耗的重要因素。为了确保影响因素单一化，采用网络平均能耗替代网络总能耗来对方案进行能耗分析，如图 5 所示。



(a)源节点到基站的距离l_{BS}定值为 300 m



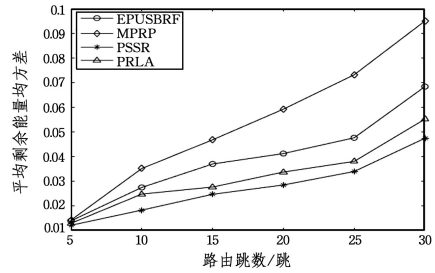
(b)路由跳数 h 定值为 15

图 5　网络平均能耗

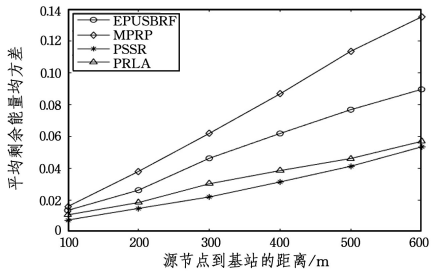
Fig. 5　Average network energy consumption

由图 5 可知，网络平均能耗与路由跳数和源节点到基站的距离均成正比。这是由网络模型决定的，源节点依据路由策略发送数据包到基站，增加了路由跳数或源节点到基站的距离，进而必然导致路径长度增加，从而增大能量消耗。除此之外，相比 EPUSBRF 方案、PRLA 方案和 MPRP 方案，PSSR 方案的网络平均能耗始终是最小的。这是因为该方案选取转发节点时考虑了备选节点的能量消耗及其到基站的距离，而 EPUSBRF 方案、PRLA 方案和 MPRP 方案考虑的因素过于单一，EPUSBRF 和 MPRP 方案仅根据备选节点到源节点的最短距离选取转发节点，PRLA 方案也仅将位置角作为选择依据，虽然上述方式在一定程度上均增加了源位置隐私的安全性，但也造成了过多的能量消耗。

由图 6 可知，与网络平均能耗变化趋势相同，节点剩余能量均方差与路由跳数和源节点到基站的距离均成正比。这是由基于幻影源的路由策略决定的，该策略通常由随机游走和最短路径两个阶段组成。路由跳数的增加扩大了随机游走阶段可供使用的节点范围，同理源节点与基站间距的增大也增加了最短路径阶段可供使用的节点数目，可供使用的节点越多，能量消耗越分散，从而越难以趋于平衡。除此之外，PSSR 方案通过考虑节点的剩余能量因素，增大了较大剩余能量节点成为转发节点的可能性，从而使其网络能耗相比 EPUSBRF 方案、PRLA 方案和 MPRP 方案更趋于均衡化。



(a)源节点到基站的距离l_{BS}定值为 300 m



(b)路由跳数 h 定值为 15

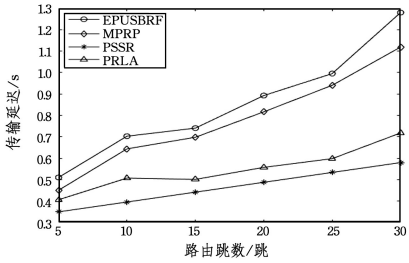
图 6　节点剩余能量的均方差

Fig. 6　Residual energy variance of nodes

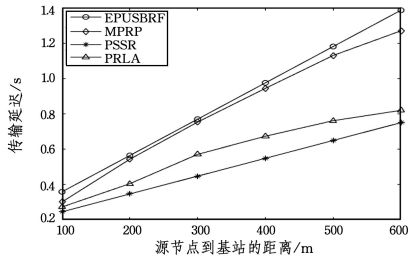
综上所述，相比 EPUSBRF 方案、PRLA 方案和 MPRP 方案，PSSR 方案的能耗量较低且能耗分布较均衡，能够实现网络生存周期的有效延长。

5.3　传输延迟

由图 7 可知，随着路由跳数或源节点与基站间距的增加，传输延迟也随之增加。这是因为源节点依据幻影源路由策略发送数据包到基站，路由跳数或源节点与基站间距的增加必然导致路径长度的增加，从而增大传输延迟。除此之外，相比 EPUSBRF 方案、PRLA 方案和 MPRP 方案，PSSR 方案在绝大部分情况下的传输延迟更短。这是由该方案的路由策略决定的，该方案通过考虑备选节点到基站的距离，增大近基区域节点成为转发节点的可能性，从而使路径长度的增加更具方向性，有效降低了传输延迟。



(a)源节点到基站的距离l_{BS}定值为 300 m



(b)路由跳数 h 定值为 15

图 7 平均传输延迟

Fig. 7 Average transmission delay

结束语 针对现有基于幻影源的 WSN 源位置隐私保护方案普遍存在无法有效平衡源位置隐私安全性、网络生存周期和传输延迟之间的矛盾的问题，本文提出了一种基于目标决策的幻影源分散路由方案 PSSR。该方案通过将幻影源选择与低概率重复分散路由相结合，在改善网络性能的同时，进一步增大了攻击者定位源位置的难度。仿真实验结果表明，相比 EPUSBRF 方案、PRLA 方案和 MPRP 方案，PSSR 方案在增强源位置隐私安全性的同时，能够有效延长网络生存周期和降低传输延迟。

参 考 文 献

[1] PENG H, CHEN H, ZHANG X Y, et al. Location privacy preservation in wireless sensor networks[J]. Journal of Software, 2015, 26(3): 617-639.

[2] OZTURK C, ZHANG Y, TRAPPE W. Source-location privacy in energy constrained sensor network routing[C]// Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. ACM, 2004: 88-93.

[3] KAMAT P, ZHANG Y, TRAPPE W, et al. Enhancing source location privacy in sensor network routing[C]// 25th IEEE International Conference on Distributed Computing Systems (ICDCS 2005). IEEE, 2005: 599-608.

[4] CHEN J, FANG B X, YIN L H, 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.

[5] YAO J, WEN G. Preserving source-location privacy in energy-constrained wireless sensor networks[C]// Proceedings of the 28th International Conference on Distributed Computing Systems Workshops. 2008: 412-416.

[6] LI Y, LIGHTFOOT L, REN J. Routing-based source-location privacy protection in wireless sensor networks[C]// 2009 IEEE International Conference on Electro/Information Technology. Windsor, Ontario, Canada: IEEE, 2009: 29-34.

[7] WANG W P, CHEN L, WANG J X. A source-location privacy protocol in WSN based on locational angle[C]// Proceedings of IEEE International Conference on Communications. 2008: 1630-1634.

[8] LONG J, DONG M, OTA K, et al. Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks[J]. IEEE Access, 2014, 2(10): 633-651.

[9] KUMAR P, SINGH J P, VISHNOI P, et al. Source location privacy using multiple-phantom nodes in WSN[C]// Proceedings of the Tencon. 2015: 1-6.

[10] XU Y, CHA Q M, KE M Y, et al. Phantom routing design for source location protection[J]. Computer Engineering and Applications, 2018, 54(19): 88-93.

[11] LIU X J, LI J, LI B. Source-Location Privacy Protocol Based on the Minimum Cost Routing[J]. Chinese Journal of Sensors and Actuators, 2014, 27(3): 394-400.

[12] YAO J. Source- location privacy based on directed greedy walk in wireless sensor networks[C]// Proceedings of International Conference on Wireless Communications Networking and Mobile Computing. 2010: 1-4.

[13] ZHOU C, HU X H. Phantom routing privacy protocol based on directed random in WSN[J]. Application Research of Computers, 2018, 35(10): 3109-3112.

[14] HUANG J, SUN M S, ZHU S T, et al. A source-location privacy protection strategy via pseudo normal distribution-based phantom routing in WSNs[C]// Proceedings of the 30th Annual ACM Symposium on Applied Computing. 2015: 688-694.

[15] JIA Z P, WEI X J, PENG W P. Privacy Protection strategy about source location in WSNs based on random angle and circumferential routing[J]. Application Research of Computers, 2016, 33(3): 886-890.

[16] LIGHTFOOT L, LI Y, REN J. Preserving Source-Location Privacy in Wireless Sensor Network Using STaR Routing[C]// Global Telecommunications Conference (GLOBECOM 2010). 2010 IEEE. IEEE, 2011. Miami, FL, 2010: 1-5.

[17] MANJULA R, RAJA DATTA. A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in WSNs[J]. Pervasive and Mobile Computing, 2018, 44: 58-73.

[18] LIU G F, XIAO Y. RSSI positioning method based on improved flower pollination algorithm[J]. Transducer and Microsystem Technologies, 2019, 38(11): 42-45.

GUO Rui, born in 1996, master. Her main research interests include IoT security and information security.

LU Tian-liang, born in 1985, Ph.D, associate professor, is a member of China Computer Federation. His main research interests include cyber security and artificial intelligence.