文章编号: 1001-0920(2017)02-0255-07 DOI: 10.13195/j.kzyjc.2016.0059

基于椭圆模型的无线传感器网络源位置隐私保护算法

白乐强[1a†], 李 玲[1a], 钱施光[1b], 张士宏[2]

(1. 沈阳建筑大学 a. 信息与控制工程学院，b. 科技处，沈阳 110168；2. 奥维通信公司，沈阳 110179)

摘 要: 针对现有源位置隐私保护算法安全周期较低的问题,提出基于椭圆模型的无线传感器网络源位置隐私保护算法. 该算法借助源节点和基站节点的坐标构建椭圆,随机分散地选择椭圆上的节点作为预期幻影源节点,为幻影源节点提供选择方向,分散相邻数据包的传输路径. 理论分析表明,所提出算法能增加数据包在传输过程中远离源节点和基站节点的概率. 仿真结果表明,与现有源位置隐私保护算法相比,所提出算法能提高安全周期,有效保护源位置隐私.

关键词: 无线传感器网络；源位置隐私；预期幻影源节点；幻影源节点

中图分类号: TP393 **文献标志码:** A

Source-location privacy protection algorithm in WSNs based on ellipse model

BAI Le-qiang[1a†], *LI Ling*[1a], *QIAN Shi-guang*[1b], *ZHANG Shi-hong*[2]

(1a. Information & Control Engineering Faculty，1b. Department of Science and Technology，Shenyang Jianzhu University，Shenyang 110168，China；2. Allwin Telecommunication Company，Shenyang 110179，China)

Abstract: To restore the lower safety periods of the existing source location privacy protection algorithms, a source-location privacy protection algorithm in wireless sensor networks(WSNs) based on the ellipse model is proposed. Both the coordinates of the source node and the sink node are used to establish the ellipse model. In order to disperse transmission paths of adjacent packets, the algorithm selects a node randomly on the ellipse as the expected phantom source node, which provides the direction for selecting the phantom source node. Theoretical analysis shows that the probability of the packet away from the source node and the sink node is increased during transmission process by using the proposed algorithm. The experimental results show that the algorithm can enhance the safety period and protect source-location privacy effectively in comparison with the existing source-location privacy protection algorithms.

Keywords: wireless sensor networks；source-location privacy；expected phantom source node；phantom source node

0 引 言

无线传感器网络(WSNs)已广泛地应用于各个领域,如军事侦查、灾害预警、目标追踪和环境监测等[1]. WSNs是分布式的网络,每个节点具有价格低、布置方便、计算能力有限等特点. WSNs依赖于无线通信技术,相比于有线通信,由于无线通信缺少物理边界的保护,更容易受到各种攻击的威胁[2]. 现有的WSNs隐私问题主要分为数据内容隐私和数据位置隐私两种[3]. 内容隐私保护技术主要是保护信息的内容,攻击者通过监听并控制传感器节点,窃取或篡改信息内容,针对这种攻击者,主要采用匿名和加密等隐私保护技术. 位置隐私保护技术主要是保护源节点或基站节点[4]的物理位置隐私,攻击者监听并分析通信模式,通过回溯获取数据源节点或基站节点的位置,针对这种攻击者,主要采用随机路径选择、多路径路由等隐私保护技术.

根据监听范围,攻击者分为全局和局部攻击者两类[5]: 全局攻击者拥有完整的网络拓扑知识,统计网络流量,完成流量分析[6]; 局部攻击者监听范围有限,监听半径为传感器节点的通信半径,监听到数据包后,移动到上一跳节点. 攻击者的移动速度远小于数据包的传输速度,一个数据包传输期间,攻击者只能

收稿日期: 2016-01-13；**修回日期:** 2016-03-30.

基金项目: 国家自然科学基金项目(60973022/F020202).

作者简介: 白乐强(1962−), 男, 教授, 从事无线传感器网络技术、物联网技术开发与应用等研究；李玲(1991−), 女, 硕士生, 从事无线传感器网络技术的研究.

†通讯作者. E-mail：baileqiang@sjzu.edu.cn

回溯一跳[7]. 根据攻击模式,攻击者分为积极和消极攻击者. 积极攻击者俘获控制节点;消极攻击者逐跳回溯[8],不影响节点的正常通信.

近几年,WSNs的源位置隐私保护问题得到了广泛关注. 当WSNs的监测对象为珍稀野生动物或重要资产时[9],保护监测对象的隐私成为一个重要问题. Ozturk等[10]最早考虑WSNs中源节点的位置隐私问题,提出了熊猫-猎人位置隐私保护模型和基于洪泛的幻影路由算法. 幻影路由算法分为两个阶段,第1阶段源节点通过随机步把数据包发送到幻影源节点,第2阶段幻影源节点把数据包发送到基站节点. Kamat等[11]提出了基于单径路由的幻影路由算法,将基于洪泛的幻影路由算法的第2阶段改为单径路由,克服了洪泛过程通信开销较大这一缺点. 陈娟等[12]提出了基于源节点有限洪泛的源位置隐私保护算法(PUSBRF),通过数据源节点有限洪泛,保证随机步阶段每一跳都沿着远离数据源节点的方向进行. 李云等[13]提出了利用网络混合环的隐私保护算法,有效保护源节点的位置隐私. 陈娟等[14]从攻击和防御两个方面研究了基站节点位置隐私问题. Jhumka等[15]提出了基于假源的隐私保护算法. 牛晓光等[16]提出了基于优化非均匀统计特性的源匿名协议.

为了有效保护源位置隐私,本文提出基于椭圆模型的WSNs源位置隐私保护算法(ABOEM). 借助邻居节点的信息,随机选择预期幻影源节点,为幻影源节点的选择提供依据. 基于熊猫-猎人位置隐私保护模型进行验证,结果表明,所提出算法能够有效保护源位置隐私.

1 网络模型

1.1 系统模型

本文的系统模型类似于熊猫-猎人位置隐私保护模型[10-11]. 系统模型化为一个六元组(N, B, P, H, M, A),其中:

1) N代表WSNs中的普通传感器节点集合,节点是静止的[13].

2) B代表网络内唯一的基站节点,即sink. 基站节点是所有数据包的目的节点,每个数据包的内容被加密,攻击者不能直接从监听到的数据包中读取出源节点的位置信息,基站节点的位置信息对所有节点公开.

3) P代表WSNs监测的重要资产,即熊猫. 为了研究熊猫的生活习性,科学家在熊猫栖息地内部署大量传感器节点,一旦熊猫在任意时刻出现在网络的任意位置,感知到熊猫且距离熊猫最近的传感器节点成为数据源节点S,S将感知到的熊猫生活习性信息周期性地发送到基站节点B.

4) H代表攻击者,即非法猎人,采用攻击方式M确定源节点的位置,从而定位熊猫并进行盗猎. 假设攻击者具有如下特征:

特征I消极攻击,初始位于基站节点附近,监听基站节点与邻居节点的通信;

特征II局部攻击,监听范围有限,监听半径为传感器节点的通信半径[17];

特征III借助GPS接收器、天线、频谱分析仪等设备,分析出信号到达的角度和强度,逐跳回溯追踪. 当监听到一个数据包时,判断出数据包的上一跳节点,移动到上一跳节点,继续监听.

5) M代表攻击者H采用的攻击方式:逐跳回溯追踪. 对于跳数为n的固定路径,攻击者H监听到n个数据包时,能定位源节点[13].

6) A代表网络所采用的隐私保护算法,抵御攻击者H的M攻击.

1.2 基于源节点和基站节点坐标的椭圆模型

如图1所示,XOY为网络初始化时节点定位的参考坐标系,$B(0,0)$代表基站节点,位于XOY坐标系的原点,$S(x_S, y_S)$代表随机选择的源节点. $UO'V$为建立椭圆模型的参考坐标系,a、b和c为椭圆方程参数,θ为U轴的正向与X轴的正向之间的夹角,Q为网络中任意一点.

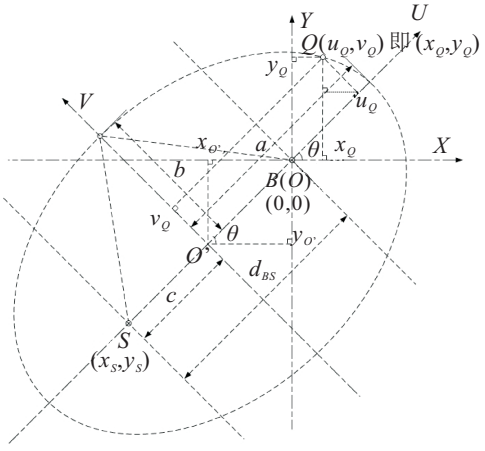

图1 椭圆模型示意图

由图1可知

$$d_{BS} = \sqrt{x_S^2 + y_S^2}. \tag{1}$$

其中:d_{BS}为B到S的距离,x_S和y_S分别为S的X轴和Y轴坐标.

以B和S组成线段的中点为新建坐标系的原点O',以B和S所在直线为U轴,以B和S组成的线段

的中垂线为V轴,建立坐标系$UO'V$. 以B和S为顶点,以d_{BS}为边长做等边三角形. 以B和S为焦点,经过等边三角形的第3个顶点做椭圆.

在坐标系$UO'V$下,设椭圆方程为

$$\frac{u^2}{a^2}+\frac{v^2}{b^2}=1, \tag{2}$$

其中u和v分别为椭圆上点的U轴和V轴坐标.

由图1可知

$$c=\frac{d_{BS}}{2}. \tag{3}$$

经过等边三角形的第3个顶点向U轴做垂线,有

$$b=d_{BS}\times\sin 60^\circ. \tag{4}$$

椭圆方程参数之间的关系式

$$c^2=a^2-b^2. \tag{5}$$

联立方程(3)、(4)和(5),可得

$$b=\frac{\sqrt{3}\times d_{BS}}{2}, \tag{6}$$

$$a=d_{BS}. \tag{7}$$

将方程(6)和(7)代入椭圆方程(2),解得椭圆方程

$$\frac{u^2}{d_{BS}^2}+\frac{4v^2}{3d_{BS}^2}=1. \tag{8}$$

在坐标系$UO'V$下,任意一点$Q(u_Q,v_Q)$变换到坐标系XOY下对应点$Q(x_Q,y_Q)$(如图1所示),有

$$x_{o'}=\frac{x_s}{2},\ y_{o'}=\frac{y_s}{2}, \tag{9}$$

其中$x_{O'}$和$y_{O'}$分别为新建坐标系$UO'V$的原点O'的X轴和Y轴坐标. 求得夹角θ为

$$\theta=\arctan\left(\frac{y_{o'}}{x_{o'}}\right). \tag{10}$$

如图1所示,可得

$$\begin{cases} x_Q=u_Q\times\cos(\theta)-v_Q\times\sin(\theta)+x_{O'},\\ y_Q=v_Q\times\sin(\theta)-v_Q\times\cos(\theta)+y_{O'}. \end{cases} \tag{11}$$

其中:x_Q和y_Q分别为任意一点Q的X轴和Y轴坐标,u_Q和v_Q分别为任意一点Q的U轴和V轴坐标.

联立方程(9)、(10)和(11),求出坐标系$UO'V$下节点$Q(u_Q,v_Q)$到坐标系XOY下对应点$Q(x_Q,y_Q)$的变换公式

$$\begin{cases} x_Q=u_Q\times\cos\left(\arctan\left(\dfrac{y_{O'}}{x_{O'}}\right)\right)-\\ \qquad v_Q\times\sin\left(\arctan\left(\dfrac{y_{O'}}{x_{O'}}\right)\right)+\dfrac{x_S}{2},\\ y_Q=v_Q\times\sin\left(\arctan\left(\dfrac{y_{O'}}{x_{O'}}\right)\right)-\\ \qquad v_Q\times\cos\left(\arctan\left(\dfrac{y_{O'}}{x_{O'}}\right)\right)+\dfrac{y_S}{2}. \end{cases} \tag{12}$$

2　ABOEM算法设计

2.1　基本ABOEM算法描述

ABOEM算法分为3个阶段:网络初始化阶段、选择幻影源节点阶段和幻影源节点沿最短路径把数据包发送到基站节点阶段. 使用的主要符号如表1所示.

表1　ABOEM算法使用的主要符号

符号	含　义
h_{Q_B}	节点Q到基站节点B的最小跳数
ESP	椭圆上预期幻影源节点,为选择幻影源节点提供方向
SP	真实源节点S借助ESP,实际选择的幻影源节点
h_{least}	源节点S发送数据包到ESP需要经过的理论最小跳数,其值为S到ESP的距离与节点通信半径的比值向上取整得到的值
$[u_p,u_g]$	ESP的横坐标u_{ESP}的选择区间
k	大于1的正整数,决定安全区半径,$k=2,3,\cdots,\infty$
R_{safe}	安全区半径,$R_{\text{safe}}=d_{BS}/k$

基站节点B进行网络初始化,每个节点得到相关信息. S计算出符合椭圆条件的ESP,为实际选择SP提供方向,发送数据包到SP,SP沿最短路径将数据包发送到B.

2.2　ABOEM算法流程

2.2.1　网络初始化阶段

为了令每个节点得到以下信息:节点自身的坐标、基站节点B的坐标、节点自身到B的跳数、邻居列表,邻居列表需要包含邻居节点的ID、坐标和到基站节点B的跳数. 网络中的任意节点通过定位算法获得自己的坐标[18],设置到基站节点B的跳数值为$+\infty$. 基站节点B生成Sink_Init信息包[12],在整个网络范围内广播,有

$$\begin{aligned}&\text{Sink\_Init}=\\&\{\text{sink\_broadcast},\text{sender\_ID},\text{sender\_coordinate},\\&\ \text{sink\_hop},\text{sink\_coordinate}\}.\end{aligned}$$

其中:sink_broadcast代表消息类型;sender_ID代表发送节点的ID;sender_coordinate代表发送节点的坐标;sink_hop代表发送节点到基站节点B的跳数,初始值设为0;sink_coordinate代表基站节点的坐标.

设节点Q为网络中收到Sink_Init信息包的节点,处理Sink_Init信息包的步骤如下.

Step 1: 节点Q读取Sink_Init信息包. 若sender_ID在邻居列表中, 则更新邻居列表中该邻居节点到基站节点B的跳数值, 否则在邻居列表中存储sender_ID、 sender_coordinate和sink_hop. 节点Q不是基站节点, 首次收到Sink_Init信息包时存储sink_coordinate.

Step 2: 若sink_hop $<$ $h_{Q\_B}-1$, 则更新$h_{Q_B}=$ sink_hop $+$ 1, 更新Sink_Init信息包中的sender_ID为节点Q的ID、sender_coordinate为节点Q的坐标、sink_hop为h_{Q_B}, 转发Sink_Init信息包, 节点Q的处理过程结束, 否则丢弃Sink_Init信息包, 节点Q的处理过程结束.

2.2.2 选择幻影源节点阶段

ABOEM算法示意如图2所示. 图2中: ESP为预期幻影源节点, SP为幻影源节点, $R_{\rm safe}$为安全区半径, e为切点, f和h为切线与椭圆的交点, n为椭圆与U轴正半轴的交点, $[u_p,u_g]$为$u_{\rm ESP}$的选择区间.

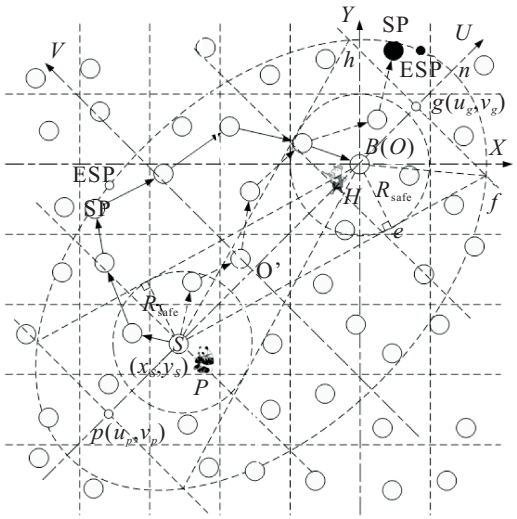

图 2 ABOEM算法示意图

源节点S初始化步骤如下.

Step 1: 源节点S按照式(8)在坐标系$UO'V$下建立椭圆方程.

Step 2: 源节点S计算ESP$(x_{\rm ESP},y_{\rm ESP})$和$h_{\rm least}$.

Step 2.1: 如图2所示, 为了选出有效的预期幻影源节点ESP$(u_{\rm ESP},v_{\rm ESP})$, 分别以$B$和$S$为圆心, 以$R_{\rm safe}$为半径建立圆形安全区, 将预期幻影源节点ESP的横坐标$u_{\rm ESP}$的选择区间调整为$[u_p,u_g]$;

Step 2.2: 将区间$[u_p,u_g]$划分成多个子区间, 为了分散相邻数据包的传输路径, 排除上一次选择的子区间, 在其余子区间中随机选择一个, 选择该子区间内的随机值作为$u_{\rm ESP}$, 代入椭圆方程(8), 求出对应的预期幻影源节点ESP的纵坐标$v_{\rm ESP}$, $v_{\rm ESP}$的值随机取正负, 利用式(12)求出对应坐标系XOY下的ESP$(x_{\rm ESP},y_{\rm ESP})$;

Step 2.3: 源节点S计算$h_{\rm least}=\lceil$源节点S到ESP的距离/通信半径$\rceil$.

Step 3: 源节点S设置数据包的跳数计数为0.

源节点S发送数据包到幻影源节点SP. 设节点Q为源节点S和收到数据包的节点, Q处理数据包的步骤如下.

Step 1: 节点Q判断自身是否为源节点S, 若是源节点S, 则转至Step 2, 否则节点Q将数据包中的跳数计数加1, 转至Step 2.

Step 2: 节点Q计算自身到ESP的距离, 若距离小于通信半径, 则转至Step 6, 否则转至Step 3.

Step 3: 节点Q计算每个邻居节点到ESP的距离, 若距离的最小值小于自己到ESP的距离, 则转至Step 5, 否则转至Step 4.

Step 4: 节点Q比较数据包中的跳数计数和$h_{\rm least}$, 若跳数计数小于$h_{\rm least}$, 则转至Step 5, 否则转至Step 6.

Step 5: 节点Q将数据包转发给离ESP最近的邻居节点, 节点Q处理过程结束.

Step 6: 节点Q成为SP, 节点Q处理过程结束.

2.2.3 幻影源节点沿最短路径把数据包发送到基站节点阶段

SP发送数据包到基站节点, 设节点Q为幻影源节点SP和收到数据包的节点, 处理数据包步骤如下.

Step 1: 若节点Q为基站节点, 则节点Q处理数据包的过程结束, 否则转至Step 2.

Step 2: 节点Q检查邻居列表, 转发数据包到距离基站节点跳数最小的邻居, 节点Q处理过程结束.

3 算法性能分析和仿真分析

3.1 性能分析

3.1.1 ESP选择范围分析

若在整个椭圆上选择预期幻影源节点ESP, 则选择的ESP可能靠近椭圆与U轴正半轴的交点n, 如图2中的黑色实心ESP和SP, 带箭头的虚线表示S发送数据包到SP的传输路径. 由图2可见, 靠近交点n的ESP增加了数据包在发送到SP的过程中经过基站节点B的概率, 导致攻击者监听到更多数据包, 影响安全周期, 降低源位置的安全性.

在S将数据包发送到SP的过程中, 为了降低经过B的概率, 以B为圆心、以$R_{\rm safe}$为半径设置圆形安全区, 在ESP的选择范围中排除弧fnh, 对应到U轴, ESP的横坐标小于u_g.

性质**1** u_g仅取决于d_{BS}和$R_{\rm safe}$.

证明　如图2所示,过S作安全区的切线,与安全区相切于点e,交椭圆于点f和h,过点f作U轴的垂线,交U轴于点g. 在$\triangle SeB$中,d_{BS}已知,$d_{Be}=R_{\text{safe}}$,由边角关系可知,$\angle BSe=\arcsin(d_{Be}/d_{BS})$,即

$$\angle BSe=\arcsin\left(\frac{R_{\text{safe}}}{d_{BS}}\right), \tag{13}$$

其中R_{safe}为安全区半径.

由边角关系,可得

$$d_{Se}=d_{BS}\times\cos\left(\arcsin\left(\frac{R_{\text{safe}}}{d_{BS}}\right)\right). \tag{14}$$

其中:d_{Se}为S点到e点的距离,d_{Be}为B点到e点的距离.

在$\triangle feB$中,由勾股定理可得

$$d_{Bf}=\sqrt{d_{Be}^2+d_{ef}^2}. \tag{15}$$

其中:d_{Bf}为B点到f点的距离,d_{ef}为e点到f点的距离.

因为椭圆上任意一点到两焦点的距离之和为$2a$,有

$$d_{Sf}+d_{Bf}=2\times a, \tag{16}$$

其中d_{Sf}为S点到f点的距离.

联立方程(7)、(14)、(15)和(16),解得

$$d_{ef}=\frac{(2\times d_{BS}-\sqrt{d_{BS}^2-R_{\text{safe}}^2})^2-R_{\text{safe}}^2}{4\times d_{BS}-2\sqrt{d_{BS}^2-R_{\text{safe}}^2}}, \tag{17}$$

其中d_{ef}为e点到f点的距离.

由$\angle BSe=\angle fSg,\angle SeB=\angle Sgf$可知,$\triangle SeB$相似于$\triangle Sgf$,且有

$$\frac{d_{BS}}{d_{Sf}}=\frac{d_{Se}}{d_{Sg}}. \tag{18}$$

其中:d_{Se}为S点到e点的距离,d_{Sg}为S点到g点的距离.

联立方程(7)、(15)和(18),解得

$$d_{Sg}=\Big(\frac{(2\times d_{BS}-\sqrt{d_{BS}^2-R_{\text{safe}}^2})^2-R_{\text{safe}}^2}{4\times d_{BS}-2\times\sqrt{d_{BS}^2-R_{\text{safe}}^2}}+\sqrt{d_{BS}^2-R_{\text{safe}}^2}\Big)\times\frac{\sqrt{d_{BS}^2-R_{\text{safe}}^2}}{d_{BS}}. \tag{19}$$

点g的横坐标为$d_{Sg}-c$,有

$$u_g=\Big(\frac{(2\times d_{BS}-\sqrt{d_{BS}^2-R_{\text{safe}}^2})^2-R_{\text{safe}}^2}{4\times d_{BS}-2\times\sqrt{d_{BS}^2-R_{\text{safe}}^2}}+\sqrt{d_{BS}^2-R_{\text{safe}}^2}\Big)\times\frac{\sqrt{d_{BS}^2-R_{\text{safe}}^2}}{d_{BS}}-\frac{d_{BS}}{2}, \tag{20}$$

其中u_g为g点的U轴坐标.

综上,u_g的值仅取决于d_{BS}和R_{safe}. □

类似地,在SP将数据包发到基站节点的过程中,数据包可能经过S.同理,如图2所示,在S周围建立安全区,u_p的值仅取决于d_{BS}和R_{safe}.

3.1.2　通信开销分析

在节点均匀分布的大规模WSNs中,用节点之间的最小跳数表示路径长度[12].

性质**2**　算法通信开销约为h_{S_B}的2倍.

证明　本文算法没有引入假包和洪泛,通信开销即为传输时延$h_{S_SP}+h_{SP_B}$. 假设幻影源节点SP都靠近椭圆,因为椭圆上任意一点到两焦点的距离之和为$2a$,所以通信开销即传输时延为$2a=2d_{B_S}\approx 2h_{S_B}$. □

3.2　仿真分析

采用Matlab仿真平台对单径幻影路由算法、PUSBRF算法和ABOEM算法进行仿真实验. 分析安全周期、通信开销(传输时延)两个性能指标. 安全周期指源节点被攻击者发现前发送数据包的个数;通信开销(传输时延)指一个数据包由源节点发送到基站节点需要经过的跳数. 为方便对比分析,采用与文献[11-12]相似的实验环境:6 000m×6 000 m的网络,均匀划分成100×100个网格,10 000个普通传感器节点均匀随机地分布于各个网格中. 为了保证均匀且随机,每个节点的初始位置为网格中心,加上随机扰动,保证每个网格中有且仅有一个节点,且每个节点的位置不同. 节点的通信半径为100m. 每个节点平均有8.72个邻居节点. 实验时,基站节点位置固定,位于网络的中心[19]. 随机选取源节点,ABOEM参数$k=2,3,4,5,6,7,8,9,+\infty$. 预期幻影源节点ESP的横坐标$u_{\text{ESP}}$选择区间$[u_p,u_g]$划分子区间的具体方法如表2所示.

表 2　划分子区间方法

符号	子区间
Interval-1	(u_p,u_g)
Interval-2	$(u_p,0)$、$(0,u_g)$
Interval-3	$(u_p,0)$、$(0,d_{BS}/2)$和$(d_{BS}/2,u_g)$
Interval-4	$(u_p,-d_{BS}/2)$、$(-d_{BS}/2,d_{BS}/2)$和$(d_{BS}/2,u_g)$
Interval-5	$(u_p,-d_{BS}/2)$、$(-d_{BS}/2,0)$和$(0,u_g)$
Interval-6	$(u_p,-d_{BS}/3)$、$(-d_{BS}/3,d_{BS}/3)$和$(d_{BS}/3,u_g)$
Interval-7	$(u_p,-d_{BS}/2)$、$(-d_{BS}/2,0)$、$(0,d_{BS}/2)$和$(d_{BS}/2,u_g)$

3.2.1 安全周期

ABOEM算法参数k取值为6、7或8时,安全周期较大. 当参数$k = 6$时,不同的划分子区间方法对安全周期的影响如图3所示. 总体上,划分子区间为Interval-4、Interval-5和Interval-6时,算法的安全周期较高.

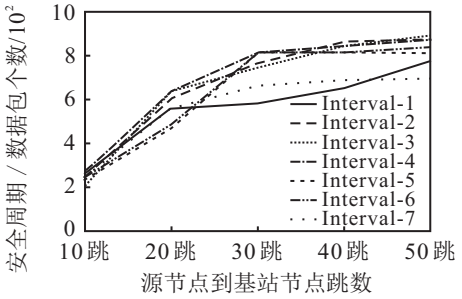

图 3 划分子区间方法对安全周期的影响

当h_{S_B}不同,ABOEM算法划分子区间为Interval-4时,与单径幻影路由算法和PUSBRF的安全周期对比如图4所示,其中h_S表示随机步跳数. 随着h_{S_B}的增加,3个算法的安全周期都在提高. 这是因为随着h_{S_B}的增加,攻击者需要回溯更多的跳数,即需要监听到更多的数据包才能发现源节点. 当ABOEM算法的k取值为6、 7或8时,安全周期最高. 这是因为ABOEM算法在选择幻影源节点时以椭圆上的节点坐标为参考方向,利用随机选择过程分散相邻数据包的传输路径,导致攻击者不能连续监听到数据包,推迟攻击者的逐跳回溯,提高安全周期.

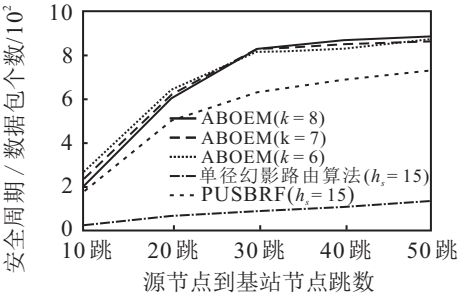

图 4 安全周期变化情况(Interval-4)

3.2.2 通信开销

ABOEM算法、单径幻影路由算法和PUSBRF算法的通信开销变化情况如图5所示. 随着h_{S_B}的增加,3个算法的通信开销都在增加. 整体上,单径幻影路由算法的通信开销最小,这是因为单径幻影路由算法在选择幻影源节点阶段完全随机选择下一跳节点;PUSBRF算法在随机步阶段每一跳都在远离真实源节点,相比于单径幻影路由算法增加了通信开销;当源节点到基站节点的跳数在17跳以内时,ABOEM算法的通信开销最小,随着h_{S_B}的增加,ABOEM算法通信开销增加的趋势更明显,当源节点到基站节点的跳数超过23跳后,ABOEM算法通信开销最大. 由性质2可知,ABOEM算法的通信开销与h_{S_B}成线性关系,所以增加趋势更明显.

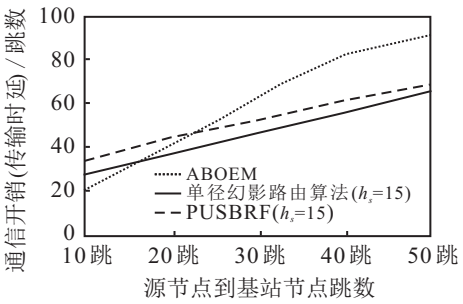

图 5 通信开销(传输时延)变化情况

结合图4安全周期和图5通信开销(传输时延)可知,随着h_{S_B}的增加,安全周期在提高,但通信开销和传输时延也随之增加. ABOEM算法增加了通信开销和传输时延,但取得了较高的安全周期. PUSBRF算法存在源节点有限洪泛阶段. 针对熊猫-猎人博弈模型,熊猫在短期内位置是不变的[10],即源节点是短期不变的,因此本文忽略了PUSBRF算法源节点有限洪泛阶段的通信开销. 但当WSNs应用于实际情况,尤其是用于监测快速移动的目标时,源节点洪泛阶段的通信开销不能忽略. 本文提出的ABOEM算法不依赖洪泛技术,在这种情况下可以明显降低通信开销,具有更广泛的适用性. ABOEM算法设置为Interval-4、Interval-5或Interval-6,k取值为6、7或8时,能够取得较高的安全周期.

4 结 论

本文提出了基于椭圆模型的WSNs源位置隐私保护算法ABOEM. 通过调整算法参数分散传输路径,设置安全区调整预期幻影源节点的选择区间,有效抵御了局部攻击者的逐跳回溯攻击. 理论分析表明,算法通过源节点到基站节点的距离和安全区半径确定预期幻影源节点的选择区间,有效降低了数据包传输过程中经过源节点和基站节点的概率. 基于熊猫-猎人位置隐私保护模型,验证了算法参数对安全周期的影响. 实验结果表明,当ABOEM算法参数设置为Interval-4、Interval-5或Interval-6,k取值为6、7或8时,能取得较高的安全周期,有效误导攻击者偏离真实路径,提高源位置的安全性.

参考文献(References)

[1] 罗小元, 王慧彬, 王金然, 等. 基于最优刚性图的链路质量与能量的拓扑控制算法[J]. 控制与决策, 2015, 30(11): 2055-2060.
(Luo X Y, Wang H B, Wang J R, et al. Link quality and

energy topology control algorithm based on optimally rigid graph[J]. Control and Decision, 2015, 30(11): 2055-2060.)

[2] 彭辉, 陈红, 张晓莹, 等. 无线传感器网络位置隐私保护技术[J]. 软件学报, 2015, 26(3): 617-639.
(Peng H, Chen H, Zhang X Y, et al. Location privacy preservation in wireless sensor networks[J]. J of Software, 2015, 26(3): 617-639.)

[3] 范永健, 陈红, 张晓莹. 无线传感器网络数据隐私保护技术[J]. 计算机学报, 2012, 35(6): 1131-1146.
(Fan Y J, Chen H, Zhang X Y. Data privacy preservation in wireless in sensor networks[J]. Chinese J of Computer, 2012, 35(6): 1131-1146.)

[4] Yao L, Kang L, Shang P F, et al. Protecting the sink location privacy in wireless sensor networks[J]. Personal and Ubiquitous Computing, 2013, 17(5): 883-893.

[5] Rios R, Lopez J. Analysis of location privacy solutions in wireless sensor networks[J]. IET Communications, 2011, 5(17): 2518-2532.

[6] Rios R, Cuellar J, Lopez J. Probabilistic receiver-location privacy protection in wireless sensor networks[J]. Information Sciences, 2015, 321(10): 205-223.

[7] Chen H L, Lou W. On protecting end-to-end location privacy against local eavesdropper in Wireless Sensor Networks[J]. Pervasive and Mobile Computing, 2015, 16(PA): 36-50.

[8] Tan W, Xu K, Wang D. An anti-tracking source-location privacy protection protocol in WSNs based on path extension[J]. IEEE Int of Things J, 2014, 1(5): 461-471.

[9] Tang D, Li T T, Ren J, et al. Cost-aware secure routing(CASER) protocol design for wireless sensor networks[J]. IEEE Trans on Parallel and Distributed Systems, 2015, 26(4): 960-973.

[10] Ozturk C, Zhang Y Y, Trappe W. Source-Location privacy in energy-constrained sensor network routing[C]. Proc of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks. Washington DC: ACM Press, 2004: 88-93.

[11] Kamat P, Zhang Y Y, Trappe W, et al. Enhancing source-location privacy in sensor network routing[C]. Proc of the 25th Int Conf on Distributed Computing Systems. Ohio: IEEE Press, 2005: 599-608.

[12] 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.
(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 J of Computer, 2010, 33(9): 1736-1747.)

[13] Li Y, Ren J, Wu J. Quantitative measurement and design of source-location privacy schemes for wireless sensor networks[J]. IEEE Trans on Parallel and Distributed Systems, 2012, 23(7): 1302-1311.

[14] Chen J, Zhang H L, Du X J, et al. Designing robust routing protocols to protect base stations in wireless sensor networks[J]. Wireless Communications and Mobile Computing, 2014, 14(17): 1613-1626.

[15] Jhumka A, Bradbury M, Leeke M. Fake source-based source location privacy in wireless sensor networks[J]. Concurrency and Computation, 2015, 27(12): 2999-3020.

[16] 牛晓光, 魏川博, 姚亚兰, 等. ONSA: 传感网中基于优化非均匀统计特性的源匿名协议[J]. 通信学报, 2015, 36(6): 70-81.
(Niu X G, Wei C B, Yao Y L, et al. ONSA: Optimal non-uniformly statistic-source anonymity protocol in WSN[J]. J on Communications, 2015, 36(6): 70-81.)

[17] Ren J, Zhang Y X, Liu K. Multiple k-hop clusters based routing scheme to preserve source-location privacy in WSNs[J]. J of Central South University, 2014, 21(8): 3155-3168.

[18] 冯秀芳, 吕淑芳. 基于RSSI,和分步粒子群算法的无线传感器网络定位算法[J]. 控制与决策, 2014, 29(11): 1966-1972.
(Feng X F, Lü S F. Wireless sensor networks locating algorithm based on RSSI and split-step particle swarm optimization algorithm[J]. Control and Decision, 2014, 29(11): 1966-1972.)

[19] Yao L, Kang L, Deng F Y, et al. Protecting source-location privacy based on multirings in wireless sensor networks[J]. Concurrency and Computation: Practice and Experience, 2013, 27(15): 3863-3876.

（责任编辑：郑晓蕾）