无线传感器网络中优化源节点位置隐私强度策略

蒋占军，周涛*，杨永红
兰州交通大学电子与信息工程学院，甘肃 兰州 730070

摘要 针对幻影节点与源节点之间跳数较少、分布区域集中以及传输路径不够多样化等问题，提出一种优化源节点位置隐私强度的保护策略。该策略可以增强幻影节点选取的多样性，有效避开攻击者的可视区。设置选取幻影节点的条件，将幻影节点待选区域利用源节点生成的动态随机数以及存储位置信息分层，确保幻影节点与源节点之间具有足够的安全距离。设置距离 Sink 节点最小跳数且距离相等的等邻居节点组成的集合作为一个虚拟圆环，当数据包到达虚拟圆环时随机选择传递方向，利用动态生成的跳数值逐跳传递，可以有效增强传输路径的多样性，延长攻击者的平均追踪时间。仿真结果表明，与传统策略相比，所提策略可以使源节点位置隐私的安全性更高。

关键词 图像处理；源节点；Sink 节点；攻击者；网络能耗
中图分类号 TP391 **文献标志码** A **doi**：10.3788/LOP57.241017

Privacy Intensity Policy for Optimizing Source Node Location in Wireless Sensor Networks

Jiang Zhanjun, Zhou Tao*, Yang Yonghong
School of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou, Gansu 730070, China

Abstract In this study, a protection strategy is proposed to optimize the privacy strength of the source node location for mitigating problems such as fewer hops between the phantom node and the source node, concentrated distribution areas, and insufficient diversification of the transmission paths. Using the proposed strategy, the diversity of phantom node selection can be enhanced and the visual area of an attacker can be effectively avoided. First, set the conditions for selecting phantom nodes, and the dynamic random number generated by the source nodes, and the storage location information layering in the area to select phantom nodes ensures that there is sufficient safe distance between phantom nodes and source nodes. Then, set the set of neighbor nodes with the least number of hops from the sink node and equal distances as a virtual ring. When the data packet arrives at the virtual ring, the transmission direction is randomly selected, and the dynamically generated hop value is used to transmit hop by hop, which can effectively enhance transmission the diversity of paths extends the average tracking time of the attacker. Simulation results show that compared with the traditional strategy, the proposed strategy can enhance the privacy strength of the source node location.

Key words image processing; source node; Sink node; attacker; network energy consumption
OCIS codes 100.4999; 060.4250; 230.6080; 230.7020; 280.4788

1 引 言

无线传感器网络(WSN)是由大量的微型传感器节点组成，因其具有部署便捷和成本较低的优点，能够在复杂的环境条件下采集或收集环境信息，广泛应用于军事侦查、医疗护理和地震救灾等诸多领域。但在 WSN 中，节点存储空间和计算能力等有限，同时节点大多部署在错综复杂的环境中，导致其

收稿日期：2020-04-14；**修回日期**：2020-05-22；**录用日期**：2020-06-24
基金项目：甘肃省高校科研项目(2017C-09)、兰州交通大学“百名青年优秀人才培养计划”基金(150220232)
* **E-mail**：59444069@qq.com

容易受到各种威胁的攻击。攻击者采用逆向回溯追踪的方式来获取源节点的位置信息进而破坏源节点，这给 WSN 的大规模应用带来了巨大挑战。

针对局部的被动攻击者，Ozturk 等[1]提出了幻影路由协议(PRS)，数据包先从源节点出发通过随机多跳后抵达幻影节点，从而伪装成源节点，接着采用洪泛的方式将数据包传递给 Sink 节点，但该协议存在选取的幻影节点不能远离源节点且因洪泛而造成较大能耗等问题。Kamat 等[2]在数据包的头部加入了指示性信息，用来指示源节点发送到幻影节点的下一跳方向，该策略中的节点每次都要对接收到的头部信息进行读取和解析，这会额外耗费大量能量。Li 等[3-5]将真实路径上的节点按照距离 Sink 节点的远近，分为近邻居节点集与远邻居节点集，当源节点刚开始传输时，随机地从近邻居节点集中选择一个节点作为幻影节点，然而此时选取的幻影节点比较单一，若节点存储的能量一旦耗尽，则会造成该路径失效。为了避免选取失效路径上的节点，Lopez 等[6-7]引入了偏夹角的概念并提出了基于角度的随机路由策略(PRLA)，该策略能够减少随机步的跳数，增强源节点位置隐私保护强度。陈娟等[8]引入了源节点可视区的概念，并提出了基于源节点有限洪泛的源位置隐私保护协议(PUSBRF)和增强性源位置隐私保护协议(EPUSBRF)，该协议能够抵御具有更强能力的攻击者。皮顿等[9]提出了位置隐私保护协议 DBT(Dynamic Bidirectional Tree)和 ZBT(Zigzag Bidirectional Tree)，这两种协议对于保护源节点位置隐私起到很好的保护作用，但路径中产生的虚假分支较多且网络能耗较大。孔祥雪等[10-12]提出了 PRVR(Protocol based on Random Virtual Rind)，利用设置的随机虚拟圆环增加了源节点到 Sink 节点路由路径的随机性和多样性，这可以有效避免失效路径的产生，增加源节点位置隐私保护强度。

针对 WSN 源节点位置隐私保护策略的研究，国内外学者已经提出了很多的优秀方案。然而，因 WSN 的特性以及需求不同，导致其对源节点的保护强度也不同，如何以较低的能耗防止攻击者捕获源节点是目前的研究热点之一。本文基于路径伪装的思想，在保证源节点位置隐私安全的情况下，提出 RVRS(Random Virtual Ring Strategy)策略，该策略能够有效增加幻影节点的随机分布性和数据包传递路径的多样性以及随机性，从而有效提高源节点位置隐私保护强度。

2 RVRS 策略

RVRS 策略的运行步骤主要分为定向随机步和虚拟圆环两步。

2.1 定向随机步

策略模型如图 1 所示。

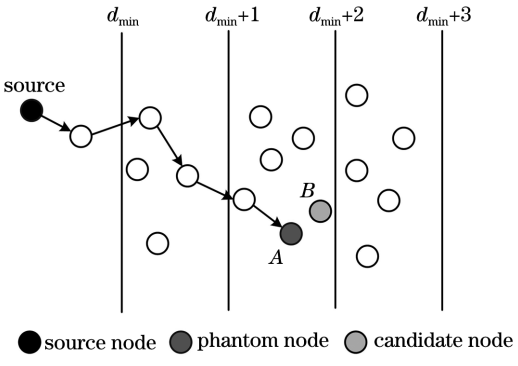

图 1 定向随机步的策略模型

Fig. 1 Strategy model for directional random step

具体步骤如下[13]。

1) 第一次定向随机过程。假设源节点与待选取的幻影节点 A 之间的最近物理距离为 d_{min}，根据 d_{min} 来确定 A 节点的分布区域，即$[d_{min}, d_{min}+1]$、$[d_{min}+1, d_{min}+2]$和$[d_{min}+2, d_{min}+3]$，在这三个区域中随机选择一个区域作为本轮幻影节点所在的区域。

2) 第二次定向随机过程。假设源节点的位置为(x_s, y_s)，源节点在发送数据包之前生成随机数 $i\in[1,3]$。根据

$$d_i = d_{min}\times(|x|+1) \tag{1}$$

来计算幻影节点与源节点之间的实际距离。假设 A 节点在$[d_{min}+1, d_{min}+2]$区域内。

3) 选择满足条件的幻影节点。由(1)式得到 d_i 后，根据

$$d_i = \sqrt{(x_d^2 - x_s^2)+(y_d^2 - y_s^2)} > 3 \tag{2}$$

来选择满足条件的 A 节点位置(x_d, y_d)，并将其作为待选的幻影节点。源节点将数据包转发给 A 节点，若 A 节点位置处没有节点，则随机选择距离 A 节点最近的 B 节点作为候选节点。该策略的主要优势：通过对幻影节点进行区域划分和定向随机选取，能够确保选取的幻影节点具有随机性和多样性。根据幻影节点与源节点之间的位置信息，能够缩短数据包传递路径的长度，减少数据包的虚假分支以及缩短数据包的收集时延。当攻击者逆向追踪幻影节点的位置时，很难再监听到连续的数据包信号，这增强源节点的安全性。

2.2 虚拟圆环

2.2.1 参数定义

1) 节点到 Sink 节点的最小跳数。对于任意一个节点 U,假设其邻居节点为 V,则 U 与 Sink 节点间的最小跳数为 $h_{U,\mathrm{Sink}}$,V 与 Sink 节点的最小跳数为 $h_{V,\mathrm{Sink}}$。

2) 距离 Sink 节点的跳数集合。以 Sink 节点为中心,将距离最小且跳数相同的节点组成一个集合,记为等跳邻居节点集合 S_1;将集合 S_1 中满足最小跳数 h 且都为 n_1($3<n_1<n$) 组成的集合,记为集合 S_2,其中 n_1 和 n 均是大于 3 的整数;将既满足 S_1 又满足 S_2 所组成的集合,记为一个虚拟圆环 R_1 上节点集合,表达式为

$$S_2=\{U\,|\,h=n_1,U\in S_1\}。\tag{3}$$

定义 Sink 节点距离虚拟圆环的最小跳数为 $N_{\min}$,Sink 节点距离虚拟圆环最小跳数的集合为 N_u,此时称为第 $\overline{U}$ 个虚拟圆环。

3) 虚拟圆环上的节点数目。将既满足集合 S_1 又满足虚拟圆环 $\overline{U}$ 的区域称为同一个虚拟圆环,虚拟圆环上节点的数目为 N_1,表达式为

$$N_1=\left\{\sum U\,|\,U\in S_1,U\in\overline{U}\right\}。\tag{4}$$

2.2.2 虚拟圆环策略

为了进一步增加幻影节点到 Sink 节点路由路径的随机性和多样性、增加源节点位置隐私的安全性以及避免失效路径的产生,引入虚拟圆环路由策略。假设源节点与 Sink 节点的跳数为 N,当网络初始化时,设由距离 Sink 节点为 R_1($R_1\geqslant3$)的等邻居节点组成一个虚拟环。RVRS 策略路由模型如图 2 所示。

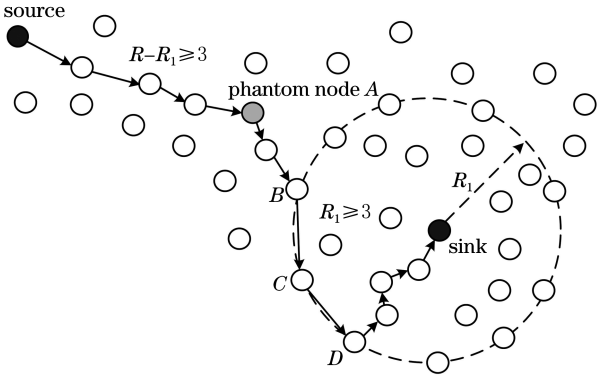

图 2 RVRS 路由模型示意图

Fig. 2 Schematic of RVRS routing model

虚拟圆环路由策略如下。

1) 当网络初始化时,网络中的节点彼此交流数据,每个节点都可以获得自身位置信息、与邻居节点之间的位置关系信息以及与 Sink 节点之间的位置关系信息等,建立了近邻居节点集(NHNT)、远邻居节点集(FHNT)和等邻居节点集(SHNT)。数据包从源节点出发后,从 NHNT 中随机选择一个节点,并向其发送数据包,同时更新源节点的等邻居节点 V 到 Sink 节点的最小跳数 $\hat{h}_{V,\mathrm{Sink}}=h_{V,\mathrm{Sink}}+1$,继续向其他邻居节点传输并重复该过程。经过若干跳后,当定向随机步结束时,此时选择 A 节点作为幻影节点,A 节点通过多跳传递后到达虚拟圆环上任一节点,此刻到达 B 节点,随机选择顺时针或者逆时针中的某一方向作为传递方向。

2) 数据包到达 B 节点后,生成一个均匀分布于[1,$M_s/2$]范围内的随机整数 M,并将其作为环路由上的跳数,其中 M_s 为区域内节点数量。假设数据包到达虚拟圆环上 B 节点后选择逆时针方向进行传递,每到达下一个转发节点后 M 减 1,重复该过程 M 次后直到 $M=0$,最后到达 D 节点,传输路径为 B-C-L-···-D。

3) 数据包到达 D 节点后,再以最短路径的方式将数据包传递给 Sink 节点。

由上述分析可知,源节点的安全时间由攻击者逆向追踪的跳数所决定,因此若要增加源节点的安全性,就需要增加攻击者所追踪数据包的跳数。当 R_1 值过小时,虚拟环路由策略并不能有效延长攻击者的追踪时间。特别是当攻击者距离 Sink 节点较近时,攻击者到达幻影节点之后,便通过视觉查看其到源节点的位置信息。实验研究表明,只有当 $R_1\geqslant3$ 时,才能有效增加攻击者反向追踪的路由长度,故选择 $R_1\leqslant H_{s,b}-3$,其中 $H_{s,b}$ 为源节点到 Sink 节点的最小跳数。当 R_1 值过大时,过长的虚拟环路有可能带来高时延和高能耗,因此为了解决数据包收集时延与源节点安全之间的矛盾,故限制 $M\leqslant M_s/2$。

2.3 RVRS 策略路由协议设计

RVRS 策略是建立在已知网络中各节点位置以及其与邻居节点位置关系的基础上,RVRS 策略路由协议的实现过程,如图 3 所示。实现过程分为网络初始化、定向随机步、有限洪泛路由、虚拟圆环路由、危险警告和路由路径的改变 6 个阶段,每个过程介绍如下。

1) 网络初始化。网络节点部署完成后,由 Sink 节点在全网范围内洪泛一个包含自身位置信息的数据包,此时 Sink 节点的初始跳数值为 0,节点 U 收

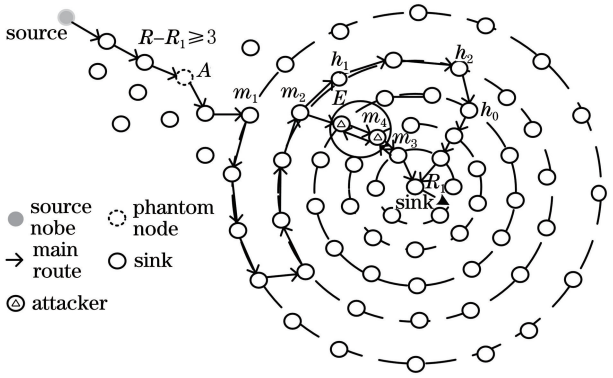

图 3 RVRS 策略路由协议的实现过程

Fig. 3 Implementation process of RVRS policy routing protocol

到洪泛消息后，对 $\hat{h}_{U,\mathrm{Sink}}=h_{U,\mathrm{Sink}}+1$ 进行更新，将 $\hat{h}_{U,\mathrm{Sink}}=1$ 存入本地内存。接着将更新后的自身位置信息加入数据包中，继续向节点 V 广播，重复此过程直到泛洪结束。最后，将节点内存中保存的最小值作为节点 U 到 Sink 节点的跳数值。对于虚拟圆环，初始化的主要目的是记录距离 Sink 节点相同且最短跳数的等邻居节点，以及统计每个节点 U 自身所在虚拟环的节点总数 N_{u}，并将这些信息存入本地内存。初始化结束后，整个网络被划分为距离 Sink 节点不同半径的虚拟环。

2）定向随机步。使用数据包 $T=\{h_{\mathrm{hop\_r}},n_{\mathrm{next\_id}}\}$ 将采集到的数据周期性地发送出去，其中 $h_{\mathrm{hop\_r}}$ 为数据包转发跳数的计数变量，$n_{\mathrm{next\_id}}$ 为下一跳节点的 ID(Identity Document)号。网络初始化后，数据包为 $T=\{0,n_{\mathrm{next\_id}}\}$，数据包每被转发一次则 $h_{\mathrm{hop\_r}}$ 加 1，直到数据包达到 $T=\{h_{\mathrm{w}},n_{\mathrm{next\_id}}\}$ 则停止转发，其中 h_{w} 为有限洪泛跳数，此时数据包经过 h_{w} 跳定向随机步后到达选择的幻影节点 A。以幻影节点 A 为中心，记幻影节点 A 周围的邻居节点为 V。当 $h_{V,A}>h_{A,\mathrm{Sink}}$ 时，则将该节点 V 划入 FHNT 中，其中 $h_{V,A}$ 为 V 与 A 节点间的最小跳数，$h_{A,\mathrm{Sink}}$ 为 A 与 Sink 节点间的最小跳数。然后，幻影节点 A 再向下一跳节点转发数据包，为了避免失效路径的产生，则随机地在幻影节点 A 周围的等梯度 FHNT 中选择一个节点并将其作为下一跳节点。

3）有限洪泛路由。数据包到达幻影节点 A 后生成广播消息 $O=\{h_{\mathrm{hop\_r}},c_{\mathrm{current\_id}},f_{\mathrm{flag}},(x_{\mathrm{s}},y_{\mathrm{s}})\}$，其中 $c_{\mathrm{current\_id}}$ 为当前发送消息的节点号，f_{flag} 为失效路径的标志符，然后幻影节点 A 将消息 O 在网络中进行广播，O 每到达一个转发节点后更新 $\hat{h}_{\mathrm{hop\_r}}=h_{\mathrm{hop\_r}}+1$，重复此过程直到数据包到达虚拟圆环上的 m_1 节点，不再广播消息。传递过程中，若下一跳节点在失效区域内，则设置 $f_{\mathrm{flag}}=1$，否则 $f_{\mathrm{flag}}=0$。幻影节点 A 与虚拟圆环之间的节点经过有限洪泛之后，能够获得自身及其邻居节点距离源节点的最小跳数值，同时可以判断邻居节点中那些会引发失效的路径[14]。

4）虚拟圆环路由。幻影节点 A 将数据包以多跳转发的方式传输到第 $\bar{U}$ 个虚拟圆环上的 m_1 节点，然后随机地选择一方向作为传递方向，此时选择逆时针方向作为传递方向。网络区域为 $L\times L$ 大小的方形，在该区域中均匀部署 M_{x} 个节点，则这一区域节点密度为

$$\rho=\frac{M_{\mathrm{x}}}{L\times L}。\tag{5}$$

虚拟圆环上的节点数目为

$$N_{\mathrm{x}}=\pi R_1^2\rho-\pi(R_1-1)^2\rho=$$
$$\pi(2R_1-1)\rho=\pi\frac{M_{\mathrm{x}}}{L\times L}(2R_1-1)。\tag{6}$$

数据包到达第 $\bar{U}$ 个虚拟环上的 m_1 节点后，从 $[1,N_{\mathrm{x}}]$ 中随机选择一个整数 n_{x}，并将其作为在圆环上传递的跳数，每传递一次则跳数减 1。数据包到达 m_1 节点后，再传递到第 J 个圆环上的 m_2 节点，重复此过程直到第 K 个虚拟圆环上的 m_4 节点且 $n_{\mathrm{x}}=0$，再通过最短路径的方式将数据包传递给 Sink 节点[15]。

5）危险警告。为了进一步减少数据包的传递时延以及节省能量，引入触发式隐私保护机制。在该机制中，若虚拟环中的某节点检测到攻击者，将该攻击者的信息以单播形式发送给主路径上的远跳节点，收到警告消息的远跳节点继续转发该消息。为了避免数据包经过攻击者所在的区域，当数据包传输到距离 Sink 节点 $3R$ 跳时，将改变传输路径。假设攻击者在距离 Sink 节点 q 跳的 m_3 节点处监听，当攻击者监听到数据包 T 时，攻击者回溯到感测范围内距离 Sink 节点($q+1$)跳的 m_4 节点。若 m_4 节点检测到攻击者，向主路径上距离其 $3R$ 跳的 m_2 节点发送危险警告的消息[16-17]。

6）路由路径的改变，主要目的是规避攻击者。网络中的攻击者行动灵敏，能够朝任意方向移动，因此为了减少攻击者捕获的数据包数量，则数据包的传递方向应尽量避开攻击者的移动轨迹。m_2 节点收到危险警告的消息后，会迅速调整移动轨迹。m_2 节点从其同跳邻居节点中随机选择一个 h_1 节点作为下一跳的转发节点，数据包经过若干转发节点传

递之后，直到距离 Sink 节点 $3R$ 跳的 h_0 节点后再通过最短路径的方式转发至 Sink 节点。

3 分析与讨论

3.1 系统模型

3.1.1 网络模型

实验采用经典的熊猫-猎人模型，该模型中大量的传感器节点随意散播在网络的监控区域内以监测熊猫行踪。熊猫在监控区域内随意移动，活动过程中，当距离其最近的节点一旦检测到熊猫时，就会变成一个源节点，从而开始周期性地采集有关熊猫的各类信息，再通过多跳传输的方式发送给 Sink 节点，直到熊猫不在该源节点的感测范围内就不再发送监测数据。对传感器网络模型进行如下假设。

1）传感器节点均匀散播在 $L\times L$ 大小的方形区域内。Sink 节点洪泛之后，网络中的每个节点都获得自身和邻居节点之间的相对位置关系。

2）任意节点间均是通过单跳的方式进行传递，而各节点的通信半径 R 相等以及发射功率相同。

3）整个网络中源节点的位置随机，但仅有一个位于中心位置处的 Sink 节点。

3.1.2 攻击者模型

局部攻击者重点关注的是网络中数据包的来源、发送和接收等状态，可以在有限范围内监听数据包传输信号，因此其只能了解局部范围内的通信情况，具体特征如下。

1）局部攻击者配备无线天线以及频谱分析仪等设备。根据三角定位法，计算局部范围内的数据包接收方向，从而推断数据包的来源方向，然后通过不断地逆向追踪来找到源节点的位置。

2）局部攻击者具有一定的存储能力，能够将攻击过程的位置信息保存进路由表中避免重复，这可以提高其逆向追踪的成功率。

3）局部攻击者开始在 Sink 节点附近随机游走，当监听到 Sink 节点与其邻居节点间有数据包传输信号时，先检查该节点是否在保存的路由表中，如果不存在，则迅速移至该节点所在的位置，否则忽略此消息继续等待。

3.1.3 位置隐私评估模型

实验主要从安全周期和数据包收集时延两个方面来评估模型。

1）安全周期为局部攻击者从监听到第一个数据包开始到发现源节点位置的时间，其主要用于评估源节点位置隐私保护强度。由于源节点是按照一定的频率发送数据包，则安全周期与源节点发送数据包的个数成正比。在给定攻击者追踪策略的情况下，源节点在被攻击者发现之前需要发送数据包来衡量安全周期。源节点发送数据包的个数越多，则安全周期越长。

2）数据包收集时延为数据包从源节点传输至 Sink 节点所经历的时间，其主要用于评价策略性能。采用优化策略之后，必然会对网络的通信质量产生一定的影响，如传输时延和数据包传递率等，因此采用数据包收集时延来衡量网络的通信质量。RVRS 策略中的数据包收集时延主要由定向随机步、虚拟环转发跳数和最短路径三个部分组成。假设源节点为 S、幻影节点为 A 和中间节点为 Z，那么策略中从源节点到 Sink 节点的数据包收集时延为 $t_{\mathrm{sum}}=t_{S,Z}+t_{A,Z}+t_{Z,\mathrm{Sink}}$。

3.2 性能仿真比较

实验是在 MATLAB 平台上对 RVRS 策略进行路由仿真。假设将 5000 个传感器节点均匀部署在 100 m×100 m 的区域内，Sink 节点位于整个网络的中心位置。攻击者的初始位置在 Sink 节点附近，源节点的监听半径和通信半径均为 80 m，网络中每个节点的平均邻居节点数为 10。设置局部攻击者的可视区半径 $r_0=4$ m。为了验证所提策略的优越性，与 PRS 策略和 EPUSBRF 策略进行对比。设置 PRS 策略中的随机步长为 20；EPUSBRF 策略是 PRS 策略的改进，网络经过初始化后，有限洪泛跳数 $h_w=15$。

3.2.1 节点平均能量损耗

数据包转发的过程中，网络节点发送和接收的数据包次数正比于源节点到 Sink 节点的跳数，所以使用发送和接收的数据包总次数来衡量网络的能量损耗。但在实际过程中，每个保护策略中，数据包均有可能沿着不同的路径传输至 Sink 节点，因此使用平均跳数来衡量数据包的转发能耗。

图 4 为三种策略下节点的平均能耗。从图 4 可以看到，随着 $H_{s,b}$ 值的不断增大，PRS 策略中网络节点的平均能耗在整体上最小，主要原因是在数据包的传递阶段，其总是沿着最短路径进行传输，所以其位置隐私保护的强度最低；与 EPUSBRF 策略相比，RVRS 策略在提升位置隐私性能的情况下，其网络能耗在整体上下降约为 27.2%，说明 RVRS 策略能够有效节约网络能耗，与 EPUSBRF 策略相比网络能耗增大约为 10.5%。在位置隐私保护强度方面，RVRS 策略并未减弱，主要原因是源节点发送的

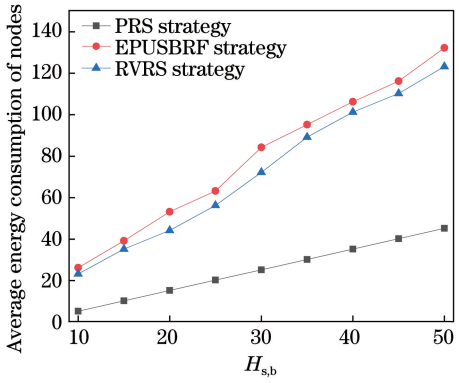

图 4 三种策略下节点的平均能耗对比

Fig. 4 Comparison of average energy consumption of nodes under three strategies

数据包经过定向随机步后到达幻影节点，可以减少节点的能量损耗。除此之外，虚拟环路由上的节点并未改变数据包到 Sink 节点的跳数。

3.2.2 安全周期

RVRS 策略中，源节点经过定向随机步后选定幻影节点，以 Sink 节点为中心，在距离其不同跳数的虚拟环上均匀选取 10 个节点。源节点每次发送 1000 个数据包，当攻击者在 1000 个数据包内未追踪到源节点时，则认为源节点的安全周期为 1000。重复进行此实验 100 次，获取源节点到 Sink 节点的跳数与源节点平均安全周期之间的关系，如图 5 所示。

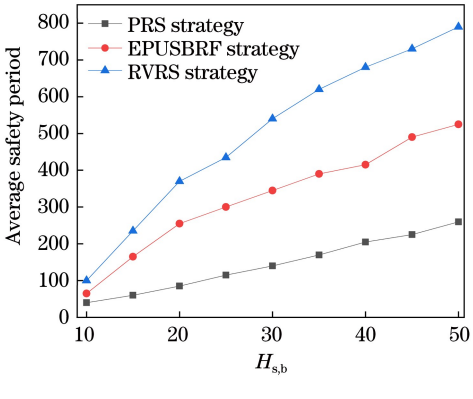

图 5 节点跳数与平均安全周期的关系

Fig. 5 Relationship between node hops and average safety period

从图 5 可以看到，随着 $H_{s,b}$ 值的增加，源节点的平均安全周期不断增加；与其他两种策略相比，RVRS 策略的平均安全周期增速明显较高；与 PRS 策略相比，RVRS 策略的平均安全周期增加近 2 倍，原因在于 RVRS 策略经过第一阶段后，待选取的幻影节点的区域更加多样化，幻影节点与源节点之间的安全距离足够大，则减少定向路由传输的盲目性；与 EPUSBRF 策略相比，RVRS 策略的平均安全周期增加近 50%，原因在于 RVRS 策略除了在第一阶段产生位置分布更加多样化的幻影节点之外，第二阶段中引入的虚拟圆环可以增加幻影节点到 Sink 节点路由路径的多样性。在全网范围内，当攻击者从 Sink 节点反向逐跳进行追踪时，容易陷入环形陷阱，此时只能重新开始追踪，但这会增加攻击者的追踪时间，所以提高源节点的隐私安全性。

3.2.3 数据包收集时延

若数据包收集时延越小，也就是数据包所经历的跳数越少，那么消息传递的越及时，但这会带来一定的安全隐患。仿真模拟过程中，对距离 Sink 节点不同跳数的源节点分别发送 1000 个数据包，然后统计不同跳数的源节点到 Sink 节点的平均路径长度即数据包收集时延，结果如图 6 所示。

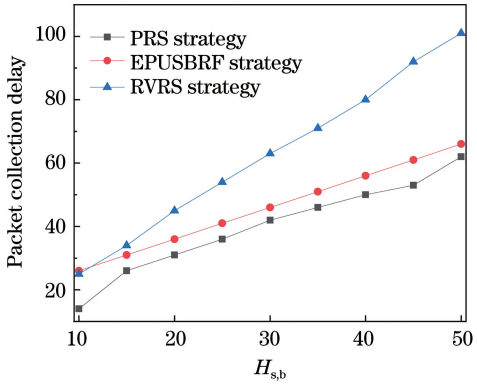

图 6 节点跳数与数据包收集时延的关系

Fig. 6 Relationship between node hops and packet collection delay

从图 6 可以看到，随着 $H_{s,b}$ 值的不断增加，数据包的收集时延会相应增加，也就是说，数据包需要经过更多跳数才能到达 Sink 节点；当 $H_{s,b}$ 值小于 13 时，EPUSBRF 策略中数据包经过的跳数最多，而 PRS 策略中数据包经过的跳数最少，主要原因是 PRS 策略中数据包采用最短路由的方式进行传输，而 EPUSBRF 策略产生较为集中的幻影节点，减少数据包传递的盲目性，使得 EPUSBRF 策略中数据包的收集时延在整体上略大；与 EPUSBRF 策略相比，RVRS 策略中数据包的收集时延最大，原因在于其使用虚拟圆环的策略，传输过程中增加虚拟环节点会增加数据包的收集时延。随着 $H_{s,b}$ 值的不断增加，虚拟环路由的路径长度明显变长，原有数据的转发长度也相应变长。结合图 4 的仿真结果可以分析得到，虽然在 RVRS 策略中，随着 $H_{s,b}$ 值的增

加，数据包的收集时延相比其他两个策略较长，但是其安全周期较长，对源节点位置隐私保护强度更高。

4 结 论

针对无线传感器网络的源节点位置隐私安全问题，提出一种基于虚拟圆环策略的 RVRS 策略，该策略主要分为定向随机步和虚拟圆环两个部分。定向随机步通过三次定向随机的方式，确保待选取的幻影节点与源节点保持足够的安全距离且选取区域多样化；虚拟圆环可以确保数据包从幻影节点向 Sink 节点的传递过程中路径的多样化。局部攻击者采用逆向回溯攻击的方式容易陷入环形陷阱中，这会延长攻击者的平均追踪时间。仿真结果表明，当攻击者采用回溯攻击的方式时，所提策略虽然引入少量的通信开销，但能够有效提高网络的安全周期。未来可以考虑改变系统模型，进一步验证所提策略的优越性。

参 考 文 献

[1] Ozturk C, Zhang Y 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-SASN′04, October 25, 2004. Washington DC, USA. New York: ACM, 2004: 88-93.

[2] 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′05), June 6-10, 2005, Columbus, OH, USA. New York: IEEE, 2005: 599-608.

[3] Li X F, Mao Y C, Liang Y. A survey on topology control in wireless sensor networks [C] // 2008 10th International Conference on Control, Automation, Robotics and Vision, December 17-20, 2008, Hanoi, Vietnam. New York: IEEE, 2008: 251-255.

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

[5] 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, June 7-9, 2009, Windsor, ON, Canada. New York: IEEE, 2009: 29-34.

[6] Lopez J, Rios R, Cuellar J. Preserving receiver-location privacy in wireless sensor networks [M] // Huang X, Zhou J. Information security practice and experience. Lecture notes in computer science. Cham: Springer, 2014: 15-27.

[7] Liang Y F, Xu J N, Wu M, et al. Research progress on optical fiber time-frequency synchronization technology [J]. Laser & Optoelectronics Progress, 2020, 57(5): 050004.
梁益丰, 许江宁, 吴苗, 等. 光纤时频同步技术的研究进展 [J]. 激光与光电子学进展, 2020, 57(5): 050004.

[8] 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.
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.

[9] Pi D, Shan Z H, Wu X K. Nanostructured antireflection micro-optics in the optical fiber communication band [J]. Acta Optica Sinica, 2020, 40(6): 0622002 .
皮顿, 单子豪, 吴兴坤. 光纤通信波段微光学件的抗反射纳米结构 [J]. 光学学报, 2020, 40(6): 0622002.

[10] Kong X X, Yuan S Q, Chen M. Routing protocol of source-location privacy protection based on virtual ring [J]. Transducer and Microsystem Technologies, 2018, 37(1): 66-69.
孔祥雪, 袁少卿, 陈梦. 基于虚拟环的源位置隐私保护路由协议 [J]. 传感器与微系统, 2018, 37(1): 66-69.

[11] Chun C L. Research on source location privacy protection in wireless sensor networks [D]. Tianjin: Tianjin University, 2016.
褚春亮. 无线传感器网络源节点位置隐私保护方案研究 [D]. 天津: 天津大学, 2016.

[12] Yuan S Q. Research on source location privacy protection in wireless sensor networks [D]. Tianjin: Tianjin University, 2017.
袁少卿. 无线传感器网络源节点位置隐私保护策略研究 [D]. 天津: 天津大学, 2017.

[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.
周创, 胡晓辉. WSN 中基于定向随机的幻影路由隐

私保护协议[J]. 计算机应用研究, 2018, 35(10): 3109-3112.

[14] Ni G Y. Research of node privacy protection in IoT perception layer[D]. Nanjing: Southeast University, 2016.
倪广源. 物联网感知层节点隐私保护技术的研究[D]. 南京: 东南大学, 2016.

[15] Zhang J N, Chu C L. A scheme to protect the source location privacy in wireless sensor networks [J]. Chinese Journal of Sensors and Actuators, 2016, 29(9): 1405-1409.
张江南, 褚春亮. 无线传感器网络中源节点位置隐私保护方案研究[J]. 传感技术学报, 2016, 29(9): 1405-1409.

[16] Zhang L. Research of location privacy protection in IoT perception layer[D]. Nanjing: Southeast University, 2015.
张丽. 物联网感知层节点位置隐私保护技术的研究[D]. 南京: 东南大学, 2015.

[17] Zhan J C, Wang Q H, Ouyang X Q. Source-location privacy protection routing protocol in wireless sensor networks by avoiding attackers[J]. Computer Engineering and Applications, 2019, 55(12): 103-109.
詹佳程, 王秋华, 欧阳潇琴. WSNs 中规避攻击者的源位置隐私保护路由协议[J]. 计算机工程与应用, 2019, 55(12): 103-109.