计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200100056

基于改进蚁群算法的 WSN 源位置隐私保护

郭 蕊 芦天亮 杜彦辉 周 杨 潘孝勤 刘晓晨
中国人民公安大学警务信息工程与网络安全学院 北京 100038
(2103008108@qq.com)

摘 要 面向目标监测任务的无线传感网(Wireless Sensor Network,WSN)通常部署在无人监管和关键敏感的环境中,无线通信的开放性严重威胁了监测目标的安全性,因此需要对源节点位置隐私进行有效保护。针对现有 WSN 源位置隐私保护方案普遍存在的高延迟和高能耗问题,提出了一种基于改进蚁群算法的源位置隐私保护方案 EESLP-ACA(Energy Efficient Source Location Privacy based on Ant Colony Algorithm)。传感器节点接收到数据包时,将根据信息素浓度和改进的路径启发素含量选择转发节点,以最小化和均衡化网络能耗;同时通过引入参照距离并改进信息素更新机制,增大未选中节点成为转发节点的可能性,构建低概率重复动态路由,减少攻击者能够接收到的数据包数目,增加反向追踪的难度。性能分析表明,所提方案不但能有效提高蚁群算法(Ant Colony Algorithm,ACA)的性能,使其更好地应用于 WSN 源位置隐私保护领域;而且相较于 CDR 和 ELSP 方案,在延长网络生存周期和缩短传输延迟的同时,能有效提升源位置隐私的安全性。

关键词:无线传感网;源位置;隐私保护;蚁群算法;动态路由
中图法分类号 TN929.5;TP212.9

WSN Source-location Privacy Protection Based on Improved Ant Colony Algorithm

GUO Rui,LU Tian-liang,DU Yan-hui,ZHOU Yang,PAN Xiao-qin and LIU Xiao-chen
College of Police Information Engineering and Network Security,People's Public Security University of China,Beijing 100038,China

Abstract Wireless Sensor Network (WSN) oriented to target monitoring tasks is usually deployed in unsupervised,critical and sensitive environments. The openness of Wireless communication seriously threatens the security of monitoring targets,so it is necessary to effectively protect the location privacy of source nodes. Considering the low computational complexity of ant colony algorithm and its unique advantages in path planning,a source location privacy protection scheme based on improved ant colony algorithm EESLP-ACA (Energy Efficient Source Location Privacy based on Ant Colony Algorithm) is proposed. When the sensor node receives the packet,it will select the forwarding node according to the pheromone concentration and the improved path heuristic content to minimize and balance the network energy consumption. At the same time,by introducing the reference distance and improving the pheromone update mechanism,the possibility of the unselected node becoming the forwarding node is increased,and the repeated dynamic route with low probability is constructed to reduce the number of packets an attacker can receive and increase the difficulty of reverse tracking. The performance analysis shows that it not only effectively improves the performance of ant colony algorithm and makes it better applied in the field of WSN source location privacy protection,but also effectively enhances the security of source location privacy while prolonging the network life cycle and shortening the transmission delay compared with CDR and ELSP schemes.

Keywords Wireless sensor network,Source-location,Privacy protection,Ant colony algorithm, Dynamic route

1 引言

无线传感网主要由资源受限的传感器节点组成,以无线通信的方式通过节点间自组织相互协作形成多跳无线传感网络,实现感知信息的传输与汇聚。随着无线通信和低功耗嵌入式技术的飞速发展,无线传感网被广泛应用于军事监控、安防监测、智能家居以及智慧医疗等领域,其在方便人们获取所需信息的同时,也产生了新的安全威胁[1]。其中,隐私内容的泄露和关键位置的暴露,使得人们对无线传感网发展的必要性和可靠性产生了质疑。现有的加密、认证等技术尽管可以保证内容安全,但无法阻止攻击者通过流量分析识别关键位置,无法满足以目标监测为主要任务的应用对通信安全的需求。

到稿日期:2020-01-07 返修日期:2020-04-13 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)

面向目标监测任务的无线传感网覆盖面积广泛，攻击者很难掌握全局视图，且篡改数据包或毁坏传感器节点易触发安全报警设施，因此本文主要针对通过流量分析执行逐跳跟踪来识别源位置隐私的局部攻击者。为了更好地保护监测目标，国内外研究人员展开了大量研究，主要通过幻影源[2-12]、随机游走[2-12]、动态路由[13-14]、多路径传输[15]、环路机制[16-18]以及虚假数据包[17-18]等方式保护源位置隐私。这些方法本质上都是通过创建冗余干扰攻击者视线，从而提升源位置隐私的安全性，因此普遍存在高延迟和高能耗问题，无法有效地适用于无线传感网。

考虑到蚁群算法计算复杂度低且在路径规划方面具有独特优势，本文提出了一种基于改进蚁群算法的 WSN 源位置隐私保护方案 EESLP-ACA。该方案应用改进的蚁群算法构建低概率重复动态路由，增加了局部攻击者逆向追踪的难度，在延长网络生存周期和缩短传输延迟的同时，提升了源位置隐私的安全性。

2 相关工作

近年来，国内外研究人员针对 WSN 源位置隐私问题展开了广泛研究。Qzturk 等[2]首次通过构建“熊猫-猎人”攻击者模型阐述了无线通信的开放性允许攻击者执行逐跳追踪，从而威胁源位置隐私的问题，并提出了由定向随机游走和基线洪泛构成的幻影路由协议 PR，在一定程度上保护了源位置隐私。考虑到洪泛路由易造成基站周围节点能量消耗过度以及集合划分单一的问题，Kamat 等[3]提出了单路径幻影路由算法 PSPR，依据节点与基站之间的跳距划分节点集合，沿用随机游走的方式确定幻影源，并通过最短路径将消息传输到基站，但邻居集选择的纯随机性导致部分路径长度的增加不能有效延长安全周期。针对此问题，Wang 等[4]提出了可视区的概念，并研究了一种基于位置角的 PRLA 协议，该协议根据节点的位置角计算转发概率，虽然有效保护了源位置隐私，但也造成了能量消耗的不均衡。考虑到幻影源分布过于集中的缺陷[2-3]，Chen 等[5]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。PUSBRF 通过源节点的有限洪泛和有向路由，使数据包能朝着远离源位置的方向一直转发，实现了幻影源位置的多样性，增加了攻击者识别源位置的难度；EPUSBRF 在不产生额外开销的情况下，采取避开可视区的路由策略，实现了消息从幻影源到基站的转发。随后，大量研究重点围绕幻影源的选取展开，主要基于节点能耗值[6]、有向等高度路由[7]、伪正态分布[8]、区域划分[9]、角度和距离[10]、椭圆模型[11]以及定向随机[12]等方式确定幻影源，但都无法解决幻影源固有的高延迟和高能耗问题。

除此之外，还可以通过动态路由、多路径传输以及环路机制的方法保护源位置隐私。Spachos 等[13]提出了一种基于固定夹角的动态路由方案 ADRS，其通过随机选择实现了传输路径的动态性。为了克服固定夹角造成的路径局限性，Liu 等[14]通过减少剩余时延触发夹角变化，从而构建动态路由 VADRS。但这两种方案都没有考虑节点的能量因素，能量消耗不均衡。Ma 等[15]提出了一种基于多路径的源位置隐私保护协议，通过同时采用远邻、近邻以及等邻 3 种不同的路由方式转发数据包，虽然在一定程度上提升了源位置隐私的安全性，但冗余路径的存在造成了能量的过度损耗。Ren 等[16]提出了一种循环转移路由方案 CDR，以不同的概率在不同的环上建立循环转移路径。Ouyang 等[17]提出了一种基于环路陷阱机制的源位置隐私保护算法 CEM，其通过环路节点概率转发虚假数据包的方式打乱攻击者追踪路径。Zhang 等[18]提出了一种基于假包策略的虚拟圆环路由算法 SVCRM，同时针对节点失效提出了多虚拟圆环策略 MVCRM。实验证明，环路机制结合虚假数据包技术在很大程度上保护了源位置隐私，但也存在高延迟和高能耗问题。ELSP[19]通过将节点分组并要求源数据包在组内和组间随机转发，增加了攻击者反向追踪的难度，但代理节点和关键节点损耗了大量能量。

针对现有 WSN 源位置隐私保护方案普遍存在的高延迟和高能耗问题，本文提出了一种基于改进蚁群算法的源位置隐私保护方案 EESLP-ACA。性能分析表明，该方案在延长网络生存周期和缩短传输延迟的同时，能有效提升源位置隐私的安全性。

3 系统模型

本文的系统模型与“熊猫-猎人”模型[2]相似。假定传感器节点均匀部署在网络中用于监测目标行为，一旦发现监测目标，距离其最近的传感器节点会将监测信息发送到基站，攻击者可以通过反向追踪的方式确定源节点的位置并发现监测目标。系统模型可以分为网络模型、攻击者模型和能量消耗模型。

3.1 网络模型

本文采用的网络模型满足如下要求。

(1)网络主要由大量的传感器节点和一个基站组成。传感器节点在网络中均匀部署且部署后不再移动，每个节点的 ID 编号唯一且至少存在一个有效的邻居节点。

(2)所有传感器节点的性能和预期寿命大致相同，且能够根据 RSSI 测距方法计算节点间距。基站具有强大的计算能力、存储能力和充足的能源供应以及基本的安全防护措施，攻击者无法通过基站获取除前向节点之外的信息。

(3)距离监测目标最近的节点为源节点，源节点周期性地发送监测信息到基站。攻击者尽管可以通过窃听追溯到前向节点，但是无法确定具有固定数据包长度的加密内容。

3.2 攻击者模型

受利益驱使，本文假定攻击者配备目标追踪设备。除此之外，攻击者模型还具有如下特征：

(1)资源充足，即攻击者具备充足的能量供应、强大的计算能力和较大的内存容量；

(2)局部被动攻击，即攻击者只能窃听消息，不能篡改数据包和毁坏节点，同时，攻击者在某一位置上窃听时，无法窃听其他位置接收的消息。

类似于普遍存在的攻击者模型，攻击者初始位于基站窃听消息，当窃听到消息时，攻击者能够识别并移动到发送节点。由于有耐心的攻击者具有更强的追踪能力[3]，因此即使攻击者长时间没有窃听到消息，他仍停留在原地继续侦听，直

至确定了源节点位置。

3.3　能量消耗模型

本文采用与文献[16]相同的能量消耗模型，能量参数及其含义如表 1 所列。

表 1　能量消耗模型的参数及其含义

Table 1　Parameters and its meanings of energy consumption model

参数	含义
E_{TS}	节点发送阶段的能量消耗
E_{RS}	节点接收阶段的能量消耗
E_{elec}	发送/接收每比特消息的节点能量消耗
k	消息的比特数
ε_{fs}，ε_{amp}	功率放大电路损耗的节点单位能量
d	节点之间的距离
d_0	区分不同传输模式的距离阈值

根据能量消耗模型，在信噪比合理的情况下，节点发送阶段的能量消耗如式(1)所示：

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

其中，d_0 的求解如式(2)所示。当节点间距 d 小于 d_0 时，采用自由空间模式；反之，采用多路径衰减模式。

$$d_0=\sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{amp}}} \tag{2}$$

不同于发送阶段的能量消耗，接收阶段的能量消耗仅与通信量有关，如式(3)所示：

$$E_{RS}(k)=E_{elec}\times k \tag{3}$$

4　改进蚁群算法的 WSN 源位置隐私保护方案

4.1　基本的蚁群算法

蚁群算法是模拟自然界中蚂蚁觅食方式的一种智能仿生算法。蚂蚁在觅食过程中，能够根据其他蚂蚁留下的信息素(pheromone)浓度寻找路径方向，并在获取食物后根据食物的数量及质量在原路径上遗留信息素增量，为其他蚂蚁的觅食提供线索。图 1 给出了蚁群算法的基本原理。

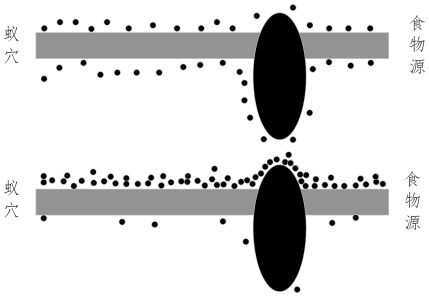


图 1　蚁群算法的基本原理

Fig. 1　Basic principle of ant colony algorithm

在 WSN 中，常用蚂蚁代表消息。设蚂蚁的个数为 m，则蚁群算法的实现过程如下。

(1)假设蚂蚁 k 在 t 时刻处于节点 i 的位置，它选择节点 j 作为转发节点的概率为 $P_{ij}^k(t)$。$P_{ij}^k(t)$ 的求解过程如式(4)所示：

$$P_{ij}^k(t)=\begin{cases}\dfrac{\tau_{ij}^{\alpha}(t)\times\eta_{ij}^{\beta}(t)}{\sum\limits_{s\in allowed_k}\tau_{is}^{\alpha}(t)\times\eta_{is}^{\beta}(t)}, & j\in allowed_k\\ 0, & \text{other}\end{cases} \tag{4}$$

其中，$allowed_k$ 表示可以作为转发节点的集合，由通信范围内未接收过该消息的节点组成；$\tau_{ij}(t)$ 表示 $arc(i,j)$ 上的信息素浓度，$arc(i,j)$ 为节点 i,j 之间的路径；$\eta_{ij}(t)$ 表示启发素含量，通常由路径长度 d_{ij} 决定，如式(5)所示；α 和 β 分别表示信息素和启发素的权重。

$$\eta_{ij}(t)=\frac{1}{d_{ij}} \tag{5}$$

(2)为了提供寻径依据，回退蚂蚁会对信息素浓度进行更新。在 $(t+n)$ 时刻，$arc(i,j)$ 上的信息素更新为：

$$\tau_{ij}(t+n)=(1-\rho)\tau_{ij}(t)+\Delta\tau_{ij}(t) \tag{6}$$

$$\Delta\tau_{ij}(t)=\sum_{k=1}^{m}\Delta\tau_{ij}^k(t) \tag{7}$$

$$\Delta\tau_{ij}^k(t)=\begin{cases}\dfrac{1}{L_k}, & (i,j)\in R_k\\ 0, & \text{else}\end{cases} \tag{8}$$

其中，ρ 表示信息素的挥发系数，且 $\rho\in(0,1]$。信息素浓度的增加表现为 $arc(i,j)$ 上的信息素增量累积和 $\Delta\tau_{ij}$。$\Delta\tau_{ij}^k(t)$ 表示蚂蚁 k 在 $arc(i,j)$ 上遗留的信息素增量，其大小取决于路径的总长度 L_k。

4.2　EESLP-ACA 算法

根据系统模型，保护源位置隐私的关键在于阻碍攻击者反向追踪。同时，为了更好地适用于无线传感网，解决方案应尽可能满足低能耗和低延迟要求。因此，WSN 源位置隐私保护问题实质上是一个多目标路径寻优问题，目标函数和约束条件分别如式(9)和式(10)所示。

$$Z=\begin{cases}\max S(t,x_1,x_2,\cdots,x_n)\\ \max LT(t,x_1,x_2,\cdots,x_n)\\ \min DT(t,x_1,x_2,\cdots,x_n)\end{cases} \tag{9}$$

$$\begin{cases}\exists\, i\in\{1,2,\cdots,n\},\sigma(i)\neq\varnothing\\ L_{atta}(t)\neq L_{sour}(t)\end{cases} \tag{10}$$

其中，S 表示匿名熵，即攻击者需要明确源位置所需的信息量，匿名熵越大，源位置的安全性越高；LT 和 DT 分别表示网络生存周期和传输延迟。本文所提算法旨在满足任意节点至少存在一个可用邻居节点且攻击者未发现源位置的条件下，寻求目标函数的非劣解。

EESLP-ACA 算法对蚁群算法的状态转移概率函数 $P_{ij}^k(t)$ 进行相关改进，以构建低能耗、低延迟和低概率重复动态路由，在延长网络生存周期和缩短传输延迟的同时，减少攻击者接收到的数据包数量，从而增加其反向追踪的难度，以更好地保护源位置隐私。

4.2.1　引入参照距离

蚁群算法根据状态转移概率函数 $P_{ij}^k(t)$ 确定转发节点。由于仅靠信息素浓度和路径长度容易导致路径局部寻优问题和区域短暂环路现象，不仅消耗了大量能量，还严重威胁了源位置隐私的安全性，因此本文在算法中引入参照距离的概念。参照距离的原理如图 2 所示。

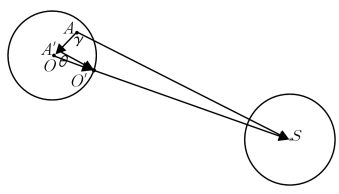


图 2　参照距离的原理

Fig. 2　Principle of reference distance

图 2 中，点 O 和点 A 为传感器节点，点 S 为基站。以点 O 为圆心、R 为半径的圆 O 表示节点 O 的通信范围；同理，圆 S 为基站的通信范围。线段 OS 交圆 O 于点 O'，d_{OS} 表示节点 O 与基站 S 之间的距离；同理，d_{AS} 和 d_{OA} 分别为节点 A 与基站 S 和节点 O 之间的距离，$\angle AOS=\theta$ 且 $\angle OAS=\gamma$。角 θ 和角 γ 的求解如式(11)、式(12)所示：

$$\cos\theta=\frac{d_{OS}^2+d_{OA}^2-d_{AS}^2}{2\times d_{OS}\times d_{OA}} \tag{11}$$

$$\cos\gamma=\frac{d_{AS}^2+d_{OA}^2-d_{OS}^2}{2\times d_{AS}\times d_{OA}} \tag{12}$$

过点 O' 作线段 $O'A'$ 交线段 OA 于点 A'，满足 $O'A'\parallel SA$，点 A' 即为点 A 相对于点 O 的参照点，$d_{O'A'}$ 表示参照距离。在 $\triangle OA'O'$ 中，根据正弦定理(如式(13)所示)求解 $d_{O'A'}$，结果如式(14)所示：

$$\frac{d_{O'A'}}{\sin\theta}=\frac{d_{O'O}}{\sin\gamma}=\frac{R}{\sin\gamma} \tag{13}$$

$$d_{O'A'}=\frac{R\times\sin\theta}{\sin\gamma} \tag{14}$$

根据式(14)，$d_{O'A'}$ 考虑了转发节点的角度因素。在其他条件一定时，节点 A 偏离最短路径方向的角度越大，其相对于节点 O 的参照距离就越大。参照距离的引入，弥补了寻径方式的不足。

4.2.2 改进路径启发函数

由于目标监测任务大多部署在无人看管的环境中，加上传感器低功耗受限的特性，WSN 在路由决策时必须充分考虑节点的能量因素。为了延长网络的生存周期，综合考虑节点间距离、剩余能量和能量消耗 3 个因素，改进路径启发函数 $\eta_{ij}(t)$，如式(15)所示：

$$\eta_{ij}(t)=\frac{E_{\mathrm{cur}}(i)}{E_{\mathrm{TS}}(k,d_{ij})}\times\frac{E_{\mathrm{cur}}(j)}{E_{\mathrm{RS}}(k)} \tag{15}$$

其中，$E_{\mathrm{cur}}(i)$ 和 $E_{\mathrm{cur}}(j)$ 分别表示节点 i 和 j 的剩余能量，E_{TS} 和 E_{RS} 分别表示发送阶段和接收阶段的能量消耗。

将改进的路径启发函数代入状态转移概率函数 $P_{ij}^k(t)$ 中，如式(16)所示：

$$P_{ij}^k(t)=\begin{cases}\dfrac{\tau_{ij}^{\alpha}(t)\times\left[\dfrac{E_{\mathrm{cur}}(i)}{E_{\mathrm{TS}}(k,d_{ij})}\times\dfrac{E_{\mathrm{cur}}(j)}{E_{\mathrm{RS}}(k)}\right]^{\beta}}{\sum\limits_{s\in allowed_k}\tau_{is}^{\alpha}(t)\times\left[\dfrac{E_{\mathrm{cur}}(i)}{E_{\mathrm{TS}}(k,d_{ij})}\times\dfrac{E_{\mathrm{cur}}(j)}{E_{\mathrm{RS}}(k)}\right]^{\beta}}, & j\in allowed_k\\ 0, & \text{other}\end{cases} \tag{16}$$

可以看出，通过在路径启发函数中加入节点的能量因素，增大具有较多剩余能量和较少能量消耗的节点成为转发节点的可能性，既实现了网络能耗的最小化和均衡化，又增大了低概率重复动态路由实现的可能性。

考虑到节点剩余能量实时获取与能量消耗以及源位置安全性之间的矛盾关系，引入局部能量评估过程。要求在节点 i 转发消息到节点 j 后，对节点 j 的剩余能量进行评估更新(如式(17)所示)，以进一步保证网络能耗均衡化的实现。

$$E_{\mathrm{cur}}(j)=E_{\mathrm{cur}}(j)-E_{\mathrm{TS}}(k,R)-E_{\mathrm{RS}}(k) \tag{17}$$

4.2.3 改进信息素更新机制

在无线通信中，通常用信息素来寻找源节点与基站之间的最短路径，以最小化网络能耗，但路径的收敛性无法有效保护源位置隐私。为了延长源位置隐私的安全周期，借助参照距离，采取局部更新的方式差异化路径信息素的挥发，增大未选中节点成为转发节点的可能性，推动低概率重复动态路由的实现。基于上述目的，在节点 i 发送消息到节点 j 后，采用局部更新替代已选路径的挥发过程，同时为了避免信息素零值化，采用分段函数对信息素更新过程进行表示，如式(18)所示：

$$\tau'_{ij}(t)=\begin{cases}\left(1-\dfrac{d_{i'j'}}{2R}\right)\tau_{ij}(t), & d_{i'j'}\in[0,2R)\\ \left(1-\dfrac{2R}{2R+1}\right)\tau_{ij}(t), & d_{i'j'}=2R\end{cases},\ j\in choose_i \tag{18}$$

其中，$d_{i'j'}$ 表示节点 j 相对于节点 i 的参照距离，$(\tau_i)'_{\min}$ 表示一个更新周期(记为 $update$)内 $\dfrac{d_{i'j'}}{2R}$ 的最小值。

考虑到回退蚂蚁会削弱未选中节点成为转发节点的可能性，采用周期内全局最优更新策略，要求蚂蚁 k 记录途径节点序列 $L_t^k[n]$ 和总长度 $L_k(t)$，同时要求基站在每个周期开始时初始化 $L_{\min}$ 和 $L[n]$，通过对比周期内接收到的 $L_k(t)$ 对其进行更新。若 $L_k(t)<L_{\min}$，则 $L_{\min}=L_k(t)$ 且 $L[n]=L_t^k[n]$。当时间 t' 为 $update$ 的整数倍时，执行未选路径信息素挥发和全局最优更新过程，如式(19)、式(20)所示。

$$\tau_{ij}(t')=\begin{cases}\tau'_{ij}(t)+\Delta\tau_{ij}(t), & j\in choose_i\\ [1-(\tau_i')_{\min}]\tau_{ij}(t)+\Delta\tau_{ij}(t), & \text{others}\end{cases} \tag{19}$$

$$\Delta\tau_{ij}(t)=\begin{cases}\dfrac{d_s}{L_{\min}}, & i_{id}\in L[n]\text{且}j_{id}\in L[n]\\ 0, & \text{otherwise}\end{cases} \tag{20}$$

其中，d_s 表示源节点到基站的最短距离。

根据式(18)－式(20)对式(16)中的信息素浓度 $\tau_{ij}^{\alpha}(t)$ 进行更新，采用局部更新和全局最优更新相结合的方式，在减少节点能耗的同时，保证了低概率重复动态路由的实现。

4.3 算法流程

根据上述内容，图 3 给出 EESLP-ACA 算法的流程。本文假设攻击者在初始化后实施窃听。

网络初始化和参数初始化为后续动态路由的实现提供了基础。网络初始化主要由两个阶段组成。第一阶段：基站洪泛阶段。首先，基站发送洪泛消息到全网络，节点根据接收信号的强度估算自身和基站之间的距离并存储最短路径的节点序列；然后，所有节点将包含自身 ID 编号和距离信息的数据包通过最短路径发送给基站。第二阶段：节点广播阶段。所有节点在通信范围内广播包含 ID 编号、剩余能量以及最短距离信息的数据包，接收节点记录相关信息并根据接收信号的强度估算与发送节点之间的距离。而参数初始化包括：初始化基站存储的最优路径 $L_{\min}=\infty$ 和途径的节点序列 $L[n]=$ null，以及设定攻击者初始位置位于基站，并要求蚂蚁 k 与数据包的序列号相同。

初始化完成后，启动时间触发函数，实现当计时器 t 为 $update$ 的整数倍时，触发未选路径信息素挥发、基站生成回退蚂蚁执行信息素全局最优更新以及初始化 $L_{\min}$ 和 $L[n]$ 事件

的发生，配合改进的路径启发函数和信息素更新机制实现低概率重复动态路由。同时，要求每当基站接收到消息时，依据消息途径的节点序列、攻击者模型的要求以及攻击者当时所处位置，执行攻击者的位置移动。若攻击者到达源节点，则结束程序，反之继续。

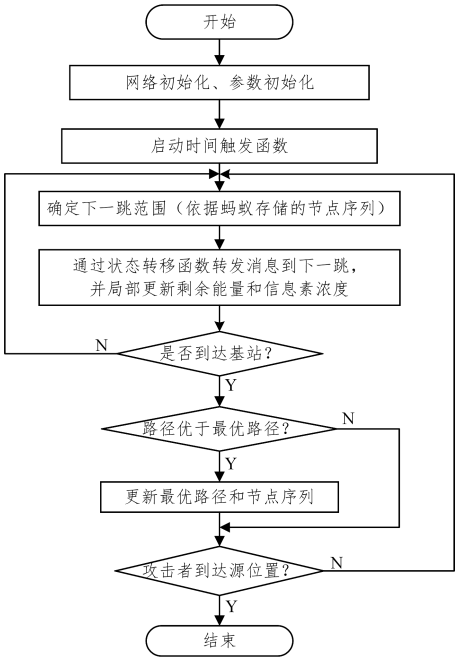


图 3　EESLP-ACA 算法流程

Fig. 3　EESLP-ACA algorithm flow

5　实验与分析

本文采用基于离散事件的 OMNet＋＋仿真平台进行模拟实验，仿真参数及其取值如表 2 所列。传感器节点随机部署在 100 m×100 m 的区域中，且一经部署后不再移动。基站位于无线传感网的中心，接收源节点周期性发送的数据包。由于节点的通信范围小于能量消耗模型中的距离阈值，因此采用自由空间传输模式。仿真实验主要从网络生存周期、源位置隐私的安全性和传输延迟 3 个方面对 EESLP-ACA 的性能进行评估，并与 ACA，CDR 和 ELSP 方案进行性能比较。

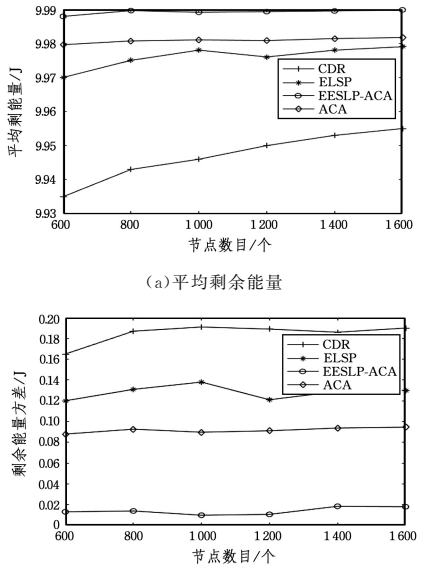
表 2　仿真实验参数值

Table 2　Parameter value of simulation experiment

参数	值	参数	值
E_{elec}	50 nJ/bit	R	10 m
ε_{amp}	0.013 nJ/(bit·m^4)	E_{cur}	50 J
ε_{fs}	100 nJ/(bit·m^2)	α	1
k	512 B	β	5
τ_{ij}	1	*update*	200 s

5.1　网络生存周期

考虑到能量消耗总量和能量消耗均衡化对网络生存周期的影响，仿真实验设定源节点发送 5 000 个数据包，重复实验 20 次，统计不同节点数目下 4 种方案的网络平均剩余能量和网络剩余能量方差，如图 4 所示。可以看出，相对于 CDR 和 ELSP 方案，EESLP-ACA 方案能够有效延长网络生存周期。这是因为 EESLP-ACA 方案不需要在构建和维护网络拓扑结构方面损耗较多能量；且路径启发函数由于考虑了节点能量因素，会优先选择剩余能量较多且耗能较少的节点作为转发节点，克服了 ACA 漫无目的地选择转发节点而造成能量消耗不均衡的弊端，也就有效延长了网络的生存周期。



(a)平均剩余能量

(b)剩余能量方差

图 4　5 000 个数据包传输完成后的网络平均剩余能量和剩余能量方差

Fig. 4　Average residual energy and residual energy variance after 5 000 packets transmission

5.2　源位置隐私的安全性

考虑到节点猜测概率的差异性，采用匿名熵 S 来评估源位置隐私的安全性，如式(21)所示。

$$S=-\sum_{i=1}^{N_T}P_i\log_2 P_i \tag{21}$$

其中，P_i 表示节点 i 为源节点的猜测概率且 $\sum_{i=1}^{N_T}P_i=1$，N_T 表示攻击者无法确定的节点数，可以用节点总数 N 与被捕获节点数 N_C 的差值表示，如式(22)所示。

$$N_T=N-N_C \tag{22}$$

假设需要保护的源节点数为 N_P，且每个未确定节点的猜测概率相同，即每个节点为受保护节点的概率为 $\frac{N_P}{N_T}$，则匿名熵可以表示为：

$$S=-\sum_{i=1}^{N_T}\frac{N_P}{N_T}\log_2\frac{N_P}{N_T}=N_P\log_2\frac{N_T}{N_P} \tag{23}$$

结合式(22)和式(23)，可以得出被捕获节点数与匿名熵之间的关系：

$$N_C=N-N_P\times 2^{\frac{S}{N_P}} \tag{24}$$

图 5 描述了受保护节点数不同的情形下，被捕获节点数与匿名熵之间的关系。当受保护节点数一定时，被捕获节点数越多，匿名熵越小，源位置的安全性越低。当被捕获节点数一定时，受保护的节点数越多，匿名熵越高。这主要是因为受保护节点数的增多，增加了攻击者识别其所需源节点的不确定性。

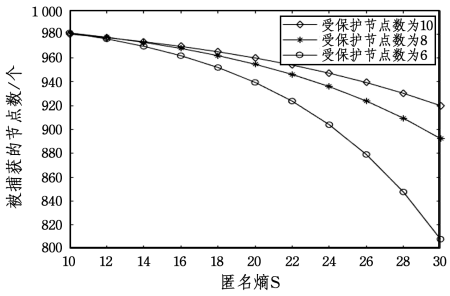


图 5 节点总数为 1 000 时，被捕获节点数与匿名熵之间的关系

Fig. 5 Relationship between number of captured nodes and anonymous entropy when total number of nodes is 1 000

考虑到被捕获节点数与匿名熵之间的关系以及攻击者捕获相应节点数时的网络总能耗，在设定受保护节点数为 8 的条件下，实验通过统计捕获节点数以及相应的网络总能耗，结合式(23)，得到匿名熵与网络总能耗之间的关系，如图 6 所示。可以看出，在网络总能耗一定时，EESLP-ACA 方案的源位置隐私安全性更高。ACA 方案固有的路径收敛性严重降低了攻击者反向追踪的难度，当匿名熵 S 处于(47.5,48]范围的某一值时，路径收敛致使攻击者发现源位置，因此 ACA 方案无法有效保护监测目标。而 EESLP-ACA 方案在选取转发节点时考虑了环路以及已选节点对源位置隐私的威胁，通过增大未选中节点成为转发节点的可能性，实现了低概率重复路由，减少了攻击者接收到的数据包数量，从而提高了源位置隐私的安全性。同时，结合图 4 和图 6 可以看出，当匿名熵一定时，EESLP-ACA 方案的网络总能耗最高，而在传输等量数据包时，EESLP-ACA 方案能实现最小化的能量消耗。可以推断出，EESLP-ACA 方案相比于 CDR 和 ELSP 方案，在匿名熵一定时，基站能够接收更多的数据包，也就有效延长了源位置的平均安全周期。

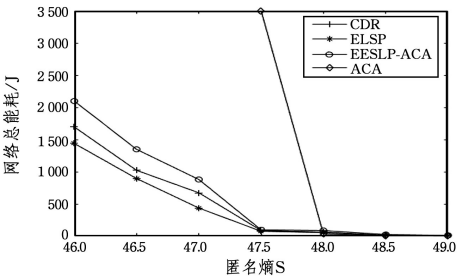


图 6 匿名熵与网络总能耗之间的关系

Fig. 6 Relationship between anonymous entropy and total energy consumption of network

5.3 传输延迟

传输延迟通常根据数据包的传输时间来确定。不同匿名熵下，4 种方案的平均传输延迟大小如图 7 所示。结合图 6，进一步证实了 ACA 方案在匿名熵 S 处于[47.5,48]范围的某一值时路径收敛，攻击者也就无法捕获更多节点，因此 ACA 方案在匿名熵 S 处于[46,47.5)时的传输延迟即为数据包在收敛路径上的传输时间，不等于一定匿名熵下的传输延迟。因此，在有效的数据范围内，EESLP-ACA 方案具有较低的传输延迟。因为 CDR 方案每次发送消息都需要经过所有簇头节点且必须在每个环中传输一圈，所以其传输延迟较高；而 ELSP 的纯随机传输增加了传输延迟。本方案通过引入参照距离，使偏向最短路径角度越小的节点成为转发节点的概率越大，弥补了 ACA 漫无目的地选择转发节点造成传输延迟增加的缺陷，有效缩短了传输延迟。

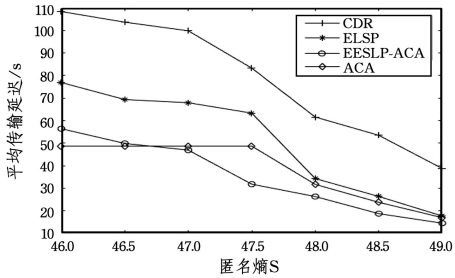


图 7 4 种方案的平均延迟时间

Fig. 7 Average delay time of four schemes

结束语 针对现有 WSN 源位置隐私保护方案普遍存在的高延迟和高能耗问题，本文提出了一种基于改进蚁群算法的源位置隐私保护方案 EESLP-ACA。该方案应用改进的蚁群算法构建低概率重复动态路由，在节点接收到数据包时，将根据信息素浓度、剩余能量和能量损耗选择转发节点，并通过引入参照距离和改进信息素更新机制，增大未选中节点成为转发节点的可能性，减少局部攻击者接收到的数据包数量，从而增加反向追踪的难度。仿真实验表明，该方案能够有效提高蚁群算法的性能，使其更好地应用于 WSN 源位置隐私保护领域；同时，相较于 CDR 和 ELSP 方案，所提方案在延长网络生存周期和缩短传输延迟的同时，提升了源位置隐私的安全性。但该方案还存在一些问题，例如局部能量评估存在一定的局限性，不能较为准确地估算节点的剩余能量，后续可对节点剩余能量的全面、准确评估展开研究。

参 考 文 献

[1] LI N, ZHANG N, DAS S K, et al. Privacy preservation in wireless sensor networks: A state-of-the-art survey[J]. Ad Hoc Networks, 2009, 7(8): 1501-1514.

[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, 2005 (ICDCS 2005). IEEE, 2005: 599-608.

[4] WANG W P, CHEN L, WANG J X. A Source-Location Privacy Protocol in WSN Based on Locational Angle[C]// IEEE International Conference on Communications, 2008(ICC'08). 2008.

[5] 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.

[6] 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.

[7] ZHOU L L,SHI R H,ZHONG H,et al. Source-location Privacy Preservation Based on Constant Altitude Routing in Wireless Sensor Networks[J]. Computer Engineering,2014,40(6):89-94.

[8] SUN M S,LIU Y B,HUANG J. Source-location privacy protection strategy through pseudo normal distribution-based phantom routing in WSN[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2016, 28(1):113-119.

[9] WANG W X,LI P Z. A privacy protection method of source location in wireless sensor networks[J]. Journal of Chongqing University,2018,41(3):100-108.

[10] 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.

[11] BAI L Q,LI L,QIAN S G,et al. Source-location privacy protection algorithm in WSNs based on ellipse model[J]. Control and Decision,2017,32(2):255-261.

[12] 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.

[13] SPACHOS P,TOUMPAKARIS D,HATZINAKOS D. Angle-Based Dynamic Routing Scheme for Source Location Privacy in Wireless Sensor Networks[C]// Vehicular Technology Conference. IEEE,2014:1-5.

[14] LIU Y,XU Y J,SONG L. Variable-angle based dynamic routing scheme for source-location privacy protection in wireless sensor networks[J]. Application Research of Computers,2018,35(1): 257-260,265.

[15] MA W,SONG L. Source location privacy preservation routing protocol based on multi-path[J]. Computer Engineering and Applications,2018,54(16):81-85,106.

[16] REN J,ZHANG Y X,LIU K. An Energy-Efficient Cyclic Diversionary Routing Strategy against Global Eavesdroppers in Wireless Sensor Networks[J]. International Journal of Distributed Sensor Networks,2013,2013:1-15.

[17] OUYANG Y,LE X Y,CHEN G L,et al. Entrapping adversaries for source protection in sensor networks[C]// International Symposium on World of Wireless,Mobile and Multimedia Networks,2006(WoWMoM 2006). 2006.

[18] 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.

[19] RUAN Z,LIANG W,SUN D,et al. An efficient and lightweight source privacy protecting scheme for sensor networks using group knowledge[J]. International Journal of Distributed Sensor Networks,2013,2013:1-14.

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.