基于攻击感知的能量高效源位置隐私保护算法

周倩[1,2]，秦小麟[1,2]，丁有伟[1,2]

（1. 南京航空航天大学计算机科学与技术学院，江苏 南京 211106；
2. 江苏省物联网与控制技术重点实验室，江苏 南京 211106）

摘 要：提出了一种静默池机制方法（SPA, silent-pool approach），当传感器节点感知到附近移动攻击者的存在，通过控制节点的转发状态从而阻止和减少攻击者收到有效数据分组。在此基础上，进一步提出了对当前路由路径没有任何影响的安全机制——池外虚假信息注入（DPIOP, dummy packet injection out pool）法，诱使攻击者远离传输路径。实验结果验证了 SPA 和 DPIOP 的隐私性能，与现有方法相比可减少能耗约为 63%，降低时延约为 35%。

关键词：位置隐私；传感器网络；能量高效；攻击感知；上下文感知

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000-436x.2018001

Preserving source-location privacy efficiently based on attack-perceiving in wireless sensor network

ZHOU Qian[1,2], QIN Xiaolin[1,2], DING Youwei[1,2]

1. College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
2. Jiangsu Key Laboratory of Internet of Things and Control Technology, Nanjing 211106, China

Abstract: Sensors' ability was utilized to perceive the mobile attacker nearby, and SPA (silent-pool approach) was proposed, which was able to hinder or reduce the packets hunted by the attacker by controlling the forwarding state of the nodes. In addition, a novel DPIOP (dummy packet injection out pool) method was proposed to entice the adversary far away from the transmission path without changing the original routing path. Through simulation studies and experiments, the outstanding performance of SPA and DPIOP in privacy preservation were demonstrated, with saving energy by about 63%, and reducing delay by about 35%.

Key words: location privacy, sensor network, energy-efficiency, attack-perceiving, context-aware

1 引言

传感器网络因其节点体积小、组网能力强、部署维护简单等特性，广泛应用在人迹罕至的敏感环境中[1]，如战场或野生动物保护区等。在监测濒临灭绝的野生动物（如大熊猫）的传感器网络中，大熊猫身上携带的传感器可以将其位置信息发送到监控中心，大熊猫的位置称为信息源的位置。如图 1 所示，攻击者在传感器节点 V_1 附近，通过信号探测设备监听数据分组，根据数据分组的时间和发送方向等上下文信息，攻击者向传感器节点 V_2 移动，并逐步接近源节点，即大熊猫的位置。

在实际监控系统中，信息源所感知的对象都是需要重点保护的（如图 1 的大熊猫），因此，信息源的位置在数据传输的过程中不能被泄露，以免造成严重的经济或资源损失。信息源的位置，就是一种

收稿日期：2017-01-08；**修回日期**：2017-12-02

基金项目：国家自然科学基金资助项目（No.61373015, No.61300052, No.41301047, No.61402225）；江苏省自然科学基金资助项目（No.BK20140832）；中国博士后基金资助项目（No.2013M540447）

Foundation Items: The National Natural Science Foundation of China (No.61373015, No.61300052, No.41301047, No.61402225), The Natural Science Foundation of Jiangsu Province (No.BK20140832), The Postdoctoral Foundation of China (No.2013M540447)

隐私信息，只有授权者可以查看。隐私又可分为基于内容和基于上下文的隐私[2,3]，基于内容的隐私是指内容形式上的完整性和机密性，即不能篡改信息的内容。本文讨论的隐私是基于上下文的，即根据情境推断出位置源信息。

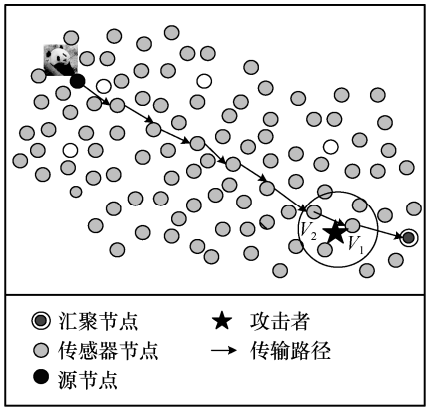


图 1　上下文攻击

现有方法主要通过改变或增加路径长度来保护源位置隐私，如幻影路由、多路径路由、虚假信息源注入等安全路由机制。这些技术主要以牺牲网络性能为代价换取一定的安全，不适用于传感器能耗或响应时间要求较高的应用。如多路径[4]隐私保护方法，其核心思想是先将数据发送到伪源节点，然后从伪源节点以单路径或洪泛的方式发送到汇聚（sink）节点。但伪源节点选取特别复杂，因为攻击者对整个网络是不可见的，节点需要知道整个网络的拓扑情况[5]，导致能耗和时延的增加[6]，并且携带拓扑信息的路由更容易遇到全局攻击者的流量分析攻击[7]。

在实际应用中，传感器网络通常是按需路由，对特定的事件选择对应的路由。例如在一个野生动物保护区部署一个由多事件驱动的网络，用于监控动物的传感器发送数据时通常采用安全路由的方法以保护动物的位置隐私。但当监控地点有紧急情况需要立即上报时，通常使用最短路径或洪泛的方式发送数据，以便最快地响应突发事件。但如果突发事件发生在信息源附近，则很容易泄露信息源的位置（如野生动物的栖息地），因为最短路径和洪泛算法只考虑数据传输效率，未考虑源位置隐私保护[4]。为了应对上述问题，迫切需要一种既不影响原来基于应用的路由，又可以抵御攻击者流量分析[8]的安全机制。

随着硬件的发展和成本的降低，很多应用于边防监控或濒临动物保护的传感器上都加装了移动物体感知和信号检测模块[9]，可以自动识别移动的攻击者[10,11]，然后通过心跳分组广播给邻居节点。Rios 等[12]基于这种攻击者识别技术提出了最小安全区方法和新的最短路径路由算法 CALP。但最小安全区的方法降低了网络的顽健性，造成网络空洞。CALP 虽然基于最短路径，但每次数据分组的投递是通过调用心跳分组来更新路由表信息并选择下一跳节点，从而达到保护隐私的目的。随着心跳分组周期的增加，数据会有很大时延，路由所泄露的拓扑信息更容易被全局监听捕获。用心跳分组传递消息，给网络性能带来了新的挑战[13]，本文的解决方案是在发现攻击者接近路由路径时发送高频心跳分组，并且能高效确保攻击者及时远离真实数据路由路径，从而降低能耗，保护位置隐私。

为了解决上述问题，本文提出的 SPA 安全机制可以准确地隔离攻击者，与 Rios 等[12]提出的最小安全区思路类似，SPA 主要也是利用心跳分组通知攻击者的邻居节点，使真实数据路径偏离攻击者附近。随着 sink 节点到源节点距离的增加，数据源被捕获的几率大大降低。另外，本文提出的 SPA 只有在发现攻击者接近真实路由路径时才会发送高频心跳分组产生静默池，使在传输其他不需要隐私服务的数据时网络依然具有连通性。因此，SPA 方法更能保证网络的顽健性。

针对耐心的攻击者，如果恰好在 sink 节点附近，使用 SPA 会造成数据分组无法到达，可能会造成数据时延长。遇到好奇的攻击者，如果恰好在源节点附近，通过随机行走就可能会发现源节点位置。为此，本文在 SPA 的基础上提出了能量高效的 DPIOP 方法，解决可能出现的这 2 种极端情况。另外，DPIOP 方法对网络当前路由不产生任何影响。

本文的主要贡献如下。

1) 提出 2 种源位置隐私保护算法：SPA 和 DPIOP。SPA 利用心跳分组发送状态信号，改变路由转发状态，在不降低网络顽健性的前提下，准确地隔离攻击者；DPIOP 只需要注入极少的虚假数据分组，就可以诱使攻击者远离真实路径，高效地保护了源位置隐私。

2) SPA 和 DPIOP 可以在攻击者知道路由协议的情况下保护源位置隐私安全。

3) 引入路径偏移量来衡量安全策略对当前路由的影响。DPIOP 策略不会改变原来的路由，使应用场景具有普适性，即便在多事件驱动的应用场景

中也能使路径不发生偏移。

2　相关工作

在传感器网络中对源位置隐私的保护（SLP, source location privacy）[2,14]，一直是一项很重要的研究。攻击者根据攻击能力分为全局攻击者和本地攻击者。全局攻击者[7,15]通过流量分析可以知道网络全局的状况，为了抵御全局攻击者，通常在发送真实信息的间隔注入假消息，带来较大的能量开销。多路径路由[6]增强了负载均衡和服务质量（QoS），也让全局攻击者难以追踪数据分组[5]。本地攻击者[16]只知道网络的局部信息，多个本地攻击者之间可以互相合作以获取更大范围的网络信息[17]。

要抵御攻击者的流量分析就必须隐藏真实数据的传输路径，现有的技术主要有 3 种。首先，Kamat[4]在他的熊猫—猎人模型中第一次提出了幻影算法，幻影算法的主要思想是：第一步，从源点出发，随机游走到一个幻影源；第二步，以最短路径或洪泛的方法到达 sink 节点。然而，实际上随机游走趋向于在数据源附近[4,18]，说明随机游走反而会泄露源位置隐私，后来的一些改进算法如 GROW[19]，旨在减少数据传输时延，提高安全性，但增加了更多能耗。另外，虚假数据机制[3, 20]和伪源节点机制[7, 21]这 2 种方法可以抵御更强的攻击者，但因为注入虚假节点的数量和位置是随机分布的，不可避免地带来不必要的能量开销。

随着硬件技术的发展，攻击者位置是可见的，利用可感知攻击者位置的特性[12]，选择离攻击者相对比较近的邻居节点形成最短路径传给 sink 节点，这给解决此类问题带来了新的启发，移动物体的识别技术[9~11]使在对付攻击者时，增加了策略的确定性。移动物体可能是被授权的，如科学家实地探测数据，只需要简单的身份认证机制[22,23]就可以排除非授权的移动物体侵入。在外部移动物体和传感器节点之间需要会话密钥的建立和更新，而基于椭圆曲线加密（ECC）的方法[24]可以简化流程，与非椭圆曲线加密机制比较只需要更小的公钥。

为了进一步降低数据传输的开销，根据 IEEE 802.15.4 MAC 层的特性，Shao 等[25]利用心跳分组的有效负载携带一些数据，在应用层再通过编程来提取处理这些信息。MAC 层除了维持可靠的通信链路之外，还可以利用心跳分组来广播信息，不同 MAC 协议对网络性能的影响也是不同的，而本文提出的 MAC 是基于存在心跳分组（beacon-enabled）的，根据文献[26]可知，心跳分组间隔时间过短会引起过多的同步开销，而时间过长会因为时间漂移导致更长的守护时间。心跳分组间隔可以根据网络的流量进行自适应调整，如 T-MAC 和 S-MAC[27]可以依据网络中的通信量来调整占空比（duty ratio），增加吞吐量，当然也可以根据应用通过上层软件改变心跳分组的发送频率。用心跳分组传输数据的好处是：节省能量和隐藏路径。

3　问题描述

3.1　网络模型

一个同构的传感器网络中包含 N 个传感器节点 $\{v_i|1\leqslant i\leqslant N\}$，每个传感器节点的计算、存储和能耗资源相同，并且每个节点 v_i 均知道自身的位置(x_i,y_i)和 sink 节点的位置(x_s,y_s)。

假设传感器网络部署在无障碍平面空间中，传感器节点之间的距离为欧式距离，若节点 v_1 和节点 v_2 的位置分别为(x_1,y_1)和(x_2,y_2)，则两点之间距离为

$$d(v_1,v_2)=\sqrt{(x_1-x_2)^2+(y_1-y_2)^2} \tag{1}$$

在稀疏的网络里，由于邻居节点数量稀少，攻击者容易定位到数据分组的直接发送者和接收者，因此，本文假设网络是稠密连通的。

在外部的攻击者看来，每个数据分组的大小和格式相同，节点 ID 信息都是加密的，安全加密机制可以保证攻击者无法解密数据分组的具体内容，也无法分辨出真消息和假消息。

假设传感器的识别模块可以判断出攻击者的位置 $H(x_h,y_h)$。在节点中引入授权机制，以便在攻击者识别过程中排除干扰，非授权的移动物体（带有广播信号）被视为攻击者。

3.2　攻击模型

在传感器网络中，由于每个传感器节点的通信范围有限，数据传输采用逐跳传输的方式。攻击者根据数据分组发送的时间相关性和不同通信节点的流量模式，从而追踪到基站或数据源。本文考虑 2 种攻击者[28]：1) 耐心的攻击者，当捕获到新的数据时，向数据分组的发送方向移动，否则一直处于原地等待状态；2) 好奇的攻击者，若在一个节点等待时间未收到任何数据分组，则随机行走。这 2 种攻击者比较典型，也更具代表性。在实际应用中，这 2 种

攻击者的攻击能力并无明确的强弱之分，尽管好奇的攻击者在收不到任何数据时策略会更灵活，但耐心的攻击者的攻击能力也可能会大于好奇的攻击者，如基于最短路径的路由，耐心的攻击者可以捕获更多的数据分组[4]。

假设这里的攻击者有如下特性：1) 本地的，即攻击者的监视范围是它邻近的传感器节点；2) 被动的，其攻击方式为监听且无法控制或破坏传感器节点，不会对网络产生任何的功能性影响；3) 移动的，从 sink 节点出发寻找源节点的位置。

攻击者的攻击轨迹如算法 1 所示。每发动一次攻击，攻击者都从 sink 节点出发（第 1)~3)行），在没有捕获到源节点之前，每捕获到一个新的数据分组（第 4)和 5)行），便根据收到数据分组的发送角度和信号强度，判断出数据分组直接发送者所在位置的方向，从而向直接发送者移动（第 6)~9)行）。若攻击者在一定时间 T 内未监听到数据分组（第 10)行），则采用随机游走的方式寻找正发送数据的节点，并继续监听（第 11)~13)行），直到找到源节点或没有找到但时间耗尽算法结束。若 T 的时间比较短，则为好奇的攻击者；若 T 无限大，则为耐心的攻击者。

攻击者以恒定的速度 V_A 移动，其中，$V_A \ll V_m$，V_m 为相邻节点间数据分组的发送速度。攻击者的监听范围不大于节点的通信范围，即 $D \leqslant R$，其中，D 和 R 分别为攻击者的监听半径和传感器节点的通信半径。

算法 1 攻击者攻击轨迹

1) *hunter* = sink;//攻击者从 sink 出发
2) *pre_hunter* = sink;
3) *next_hunter* = sink;
4) while (*next_hunter*≠ *source* & *time* < *Time*)
5) *msg* = *ListenMessage*();
6) if (*TimedListen*()<*T*&*IsNewMessage* (*msg*))
7) *next_hunter* = *alculateImmediateSender* (*msg*);
//判断出发送节点位置
8) *pre_hunter* = *hunter*;
9) *hunter* = *next_hunter*;
10) else if (*TimedListen*() ≥ *T*)
11) *next_hunter* = *ran_hunter* ;
12) *hunter* = *next_hunter*;
13) *ran_hunter* = *GetRandomHunter*(*hunter*);
//攻击者随机游走后的位置
14) end if
15) end while

3.3 能量模型

研究表明 2 个节点在 100 m 的距离内传输 1 kbit 的数据相当于执行 300 万次的一般程序指令[29]，因此，传感器的能量消耗主要是通信引起的。传感器发送数据分组所消耗的能量与传感器的电子元器件功率成正比，同时，传输的距离越长，消耗的能量也越大，即

$$E_t(v_i, v_j) = E_{\text{elec}} + \xi_{\text{amp}} d^n \tag{2}$$

$$E_r(v_j) = E_{\text{elec}} \tag{3}$$

其中，$E_t(v_i,v_j)$为在时间 t 内从 v_i 发送 1bit 到 v_j 需要的能量，$E_r(v_j)$为 v_j 接收 1bit 的能量，d 为 v_i 到 v_j 的距离，n 为路径损耗指数，E_{elec} 为通信电子消耗的能量，ξ_{amp} 为功率放大器消耗的能量。因此，网络中的总能耗为

$$E_{\text{network}} = \sum_{k=0}^{p-\lambda} s\left(E_t\left(v_i, v_j\right) + E_r\left(v_j\right)\right)k \tag{4}$$

其中，p 和 λ 分别为网络中经过时间 T，所有参与数据传输的节点数量以及形成的数据传输路径条数，因此，网络中分别有 p–λ 个发送节点和接收节点。经过时间 T，网络中共有 p 个节点形成 λ 条路径，发送 s bit 的数据会在网络中产生的总能量如式(5)所示。

$$E_{\text{network}} = s(2E_{\text{elec}} + \xi d^n)(p - \lambda) \tag{5}$$

由此可见，在网络发送的数据量相同，并且路由算法是固定的情况下，路径越短，能量消耗越少。

4 基于攻击感知的源位置隐私保护方法

4.1 攻击感知技术

攻击者不会对网络结构和功能产生任何影响，所以传统的入侵检测（IDS）系统无法检测出攻击者。但攻击者还是有其自身特点的，首先它是一个移动对象，并且它是携带有电磁广播信号的，本文部署的传感器节点可以监测和追踪非授权的或异常的移动物体。

本文使用的传感器节点包括移动物体检测（M-DS, motion detection sensor）模块和控制模块 2 个功能模块，如图 2 所示。

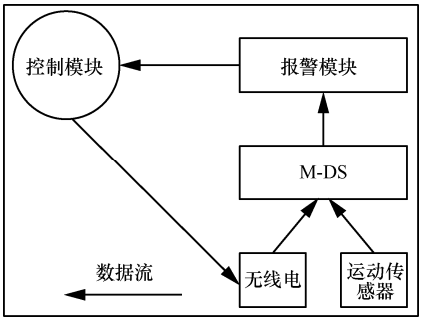


图 2　传感器功能模块

M-DS 模块用于判断附近是否存在攻击者，并能根据现有技术判断出攻击者的位置，如果存在攻击者，则向控制模块发出 readysilent 警报。控制模块通过发射高频 beacon 信号，凡是收到该心跳分组信号的，警告信号 readysilent_beacon 置为 1。另外，正在发送数据分组的节点，同时发送确认信号 confirmsilent_beacon，和自身的经过加密的 ID_1，收到确认信号的当前节点将其标记为 1，ID_2 通过算法计算获得，当节点收到的虚假信号 fake_beacon 心跳分组中 ID_2 和自身 ID 一样的心跳分组信号，则发送虚假数据分组。这里设定 3 个参数，如表 1 所示。

4.2　心跳分组

上文提到用心跳分组传递网络信息可以节约传输数据的能耗，因为和网络层的数据分组不同，心跳分组是属于 MAC 层的。MAC 层对网络层是透明的，一般负责监测和处理冲突以及分配信道与通信资源。

每个传感器节点都会周期性地广播心跳分组，从而告知邻居节点自己的存在。由式(2)和式(3)可知，网络能耗取决于数据分组的大小。心跳分组的大小由其 MAC 标准决定，图 3 为 IEEE 802.15.4 的心跳分组帧格式，除去 MAC 负载，分组大小只有 10 B 左右，而一个 LEACH 协议的网络数据分组大小为 500 B，约为心跳分组的 50 倍，所以本文中心跳分组的能耗基本可以忽略不计。

然而，过于频繁的心跳分组广播也会给网络带来一些负担，已知心跳分组的广播周期为 T_{beacon}，网络发送分组周期为 T_{message}，要保障本文机制的应用，

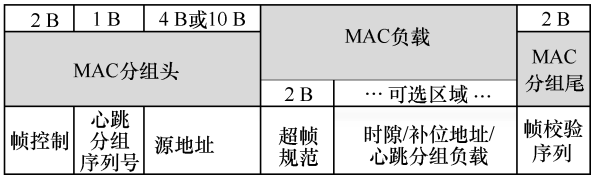


图 3　IEEE 802.15.4 心跳分组帧格式

为了阻止或减少攻击者收到新的数据分组，可能需 3 个心跳分组的广播时间才能完成整个机制，即 $3T_{\text{beacon}} \leqslant T_{\text{message}}$。根据 IEEE 802.15.4 中定义，心跳分组的发送分组周期 T_b 为 15.36 ms ~786.432 s。采用扩频技术数据的传输速率为 250 kbit/s。如果每一步投递都需要心跳分组来更新路由，这样网络最大时延 $T \approx T_b h$，h 为传输路径跳数。一些基于心跳分组的路由技术为了降低时延只能加快心跳分组发送频率和缩短传输路径，本文的策略不需要等待心跳分组来更新路由，节点的邻居节点一旦配置之后不会发生变化，数据的传输速率不受心跳分组速率影响。

4.3　静默池机制

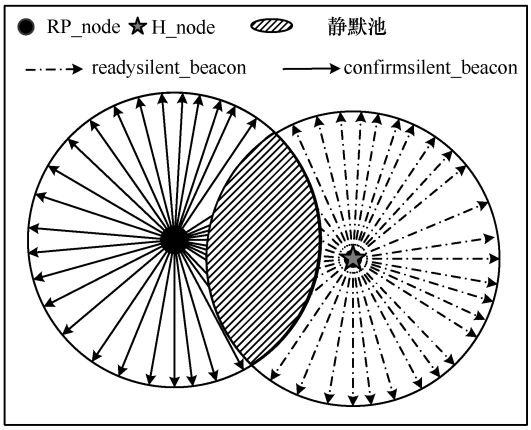
首先引入静默池（silent-pool）机制。如果一个节点接收到任何数据后即丢弃，则称这个节点是沉默的。传感器节点感知到附近的攻击者后，发送信号使一定距离内的所有节点不再转发消息保持沉默状态，攻击者便不能再接收到周边的任何信号，能够覆盖攻击者监听区域的最短距离为最小安全距离。沉默的状态可利用软件便可实现，安全距离之内的所有节点可以通过心跳分组来通知，一般情况传感器节点是发送正常心跳来证明自己的存在。

如果节点 H_node 为第一个检测到攻击者的传感器节点，它可以通过感知模块确定攻击者的位置，并发出一个警告信号 readysilent_beacon，则 H_node 通信半径范围内所有传感器都可以接收到警告信号。同时，网络中正在发送真实数据分组的节点 RP_node 会发送 confirmsilent_beacon。在本研究中，传感器的通信半径和攻击者的侦听半径都相等。当攻击者在真实数据传输路径附近时，若节点同

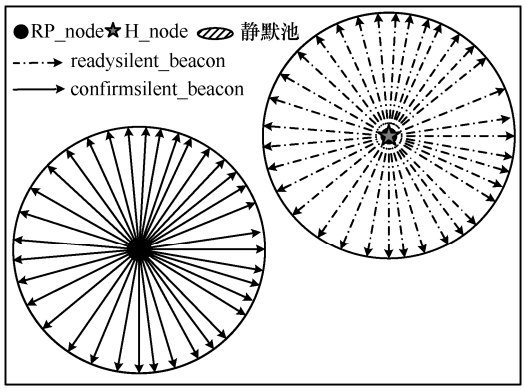
表 1　　**心跳分组设计**

心跳分组段标识	段内数据集	情况 1	情况 2
readysilent_beacon	{0},{1}	检测到附近有攻击者，置 1	没有检测到攻击者，置 0
confirmsilent_beacon	{0},{1}	当前节点为转发真实数据的节点，置 1	当前节点没有在转发真实数据，置 0
fake_beacon	$\{ID_1,ID_2\}$	ID_1 为静默池中节点标识	ID_2 为虚假节点标识

时收到 readysilent_beacon 和 confirmsilent_beacon 这 2 个心跳分组的信号，如图 4(a)阴影区域所示，则将自身调至沉默状态。当攻击者远离真正发送分组的节点时，如图 4(b)所示，此时网络是安全的，攻击者窃听不到任何真实数据。然而，当攻击者捕获到真实数据分组和分组的发送节点 RP_node，就可以一步步发现源节点。RP_node 和攻击者相交范围形成静默池，池内的节点都只能收到分组但不能转发，这个节点的状态就是静默的，如图 4(a)所示，就可以保证 RP_node 节点和源节点的安全，并且不依赖网络当前的路由。



(a) 攻击者靠近真实数据分组



(b) 攻击者远离真实数据分组

图 4 静默池的形成

定义 1 所有接收到警告信号 readysilent_beacon 的节点集合为 R，所有接收到确认信号 confirmsilent_beacon 的节点集合为 C，静默池的集合为

$$SET\_Silent\_pool = \{n_s \mid n_s \in R \cap C\} \tag{6}$$

每个节点知道自身和 sink 节点的位置，并且每个节点都可以通过心跳分组发送信号。警告信号 readysilent_beacon 由离攻击者最近的节点发送。确认信号 confirmsilent_beacon 由正在发送真实数据分组的节点发送。*SET_Silent_pool* 为那些既收到警告信号又收到确认信号的点，也就是如图 4(a)所示的阴影部分。当然，*SET_Silent_pool* 有可能为空，如图 4(b)所示，即发送分组节点的下一跳节点，攻击者是侦听不到的，因为本地攻击者只能收到其监听范围内的信号。

根据攻击模型，攻击者在捕获不到数据后就会在网络中随机游走，在静默池机制中，每次当攻击者靠近真实数据传输路径时，都会引起数据传输偏移原路径，大大降低了攻击者捕获的真实数据分组数量，但网络路径的增加导致了更高的能耗。

采用静默池机制可以阻止或减少攻击者收到新的数据分组，然而当攻击者一直在 sink 节点附近时，会产生 2 个弊端：1) 造成数据分组无法到达，导致非常低的投递率；2) 当源节点和 sink 节点很近时，攻击者会收不到任何数据，处于随机游走状态，随着游走步数的增加，游走的范围也会相应增加，如果源节点和 sink 节点之间距离较近，那么攻击者在有限的时间内就可以通过随机游走找到源节点。

完全隔离攻击者的优点在于攻击者无法收到任何上下文的信息，这时敌人处于随机游走的状态，当前节点的位置 $CN_0(x_0,y_0)$已知，则 h 步之后的敌人的位置 $DN_{h_{\text{walk}}}$ 如下所示。

$$DN_{h_{\text{walk}}} = CN_0 + CN_1 + CN_2 + \cdots + CN_{h_{\text{walk}}} \tag{7}$$

设 $X=CN_i-CN_{i-1}(i>0)$，X 为独立分布随机变量，分别是(1,0),(−1,0),(0,1),(0,−1)。$k\cdot h_{\text{walk}}$ 为 h_{walk} 步后到 CN_0 的距离，其中，$0<k<1$，攻击者离初始位置距离为 $k\cdot h_{\text{walk}}$ 的渐近概率如式(8)所示。

$$P = \frac{1}{\pi h}\int_0^{k\cdot h_{\text{walk}}}\int_0^{2\pi} \mathrm{e}^{-\frac{r^2}{h_{\text{walk}}}} r\mathrm{d}\theta\mathrm{d}r = 1-\mathrm{e}^{-\frac{d^2}{h_{\text{walk}}}} \tag{8}$$

随着游走步数 h_{walk} 持续增加，游走之后还在原地附近的概率趋于 1，从直观上看，攻击者只能在原地打转，从而保证了源节点的位置隐私。如果源节点至 sink 距离较小，源节点的位置是可以落在 sink 附近较小范围内，只要增加 h_{walk}，攻击者便可在一定时间找到源节点。而当源节点位置和攻击者之间距离越远，随机游走状态的攻击者找到 sink 节点的概率越小。因此，需要保证攻击者远离源节

点，即尽量使攻击者追溯数据分组的移动方向都是远离源节点的。

当攻击者在原路由附近时，越大的最短安全距离导致越大的路线偏移，网络消耗的能量更多，也会导致网络的不稳定。虽然 SPA 在保护隐私方面具有很好的优越性，但当面临耐心的攻击者时，SPA 会产生很大的路由偏移量，造成数据分组投递时延。为了让隐私保护机制更广泛应用，因此，在设计隐私保护策略时既要使攻击者远离源节点，又要能够最大限度地保障现有路由，保证数据分组实时到达。

4.4　静默池机制的优化

维持现有路由路径，可以保证网络中的数据分组的转发次数，避免安全策略对网络能耗和时延产生较大影响。下面首先定义了路由偏移量，越小的路由偏移量对保证网络的服务质量越高。

定义 2　基于应用的原路由平均路径长度（即跳数）为 μ，隐私保护安全机制后的路由第 i 次路径的长度为 x_i，用 S^2 来定义路由偏移量。

$$S^2=\frac{\sum_{i=1}^{n}(x_i-\mu)^2}{n} \tag{9}$$

当使用安全策略后的路由路径长度与原路由长度相同时，S^2=0 为最小值，即路由偏移量最小。当使用安全策略后的路由路径长度与原路由长度相差越大，S^2 值越大。为了解决静默池技术产生路由偏移量较大的问题，本文在不影响原路由路径的情况下，引入 DPIOP（dummy packet injection out pool）机制。当节点在同时收到 readysilent_beacon 和 confirmsilent_beacon 这 2 个心跳分组后，发送含有自身节点 ID 的 fake_beacon 信号，收到 fake_beacon 信号的 H_node 根据算法 2 选择一个离 ID 节点最远的邻居节点发送虚假数据分组，这里的假消息在攻击者看来和真实数据分组是一样的。于是通过在静默池外选择节点 FP_node 发射虚假消息，攻击者就会追逐假消息，从而达到保护隐私的目的。

定义 3　设所有收到警告分组信号（readysilent_beacon=1）但没有收到确认分组信号（confirmsilent_beacon=0）的节点为 $v_i(0<i<N)$，并且，v_i 到 sink 的距离大于攻击者到节点的距离，即 $d(v_i,v_s)>d(\text{H\_node}, v_s)$。此时的节点集合为 SET_Far，如图 5 灰色区域，FP_node∈SET_Far。

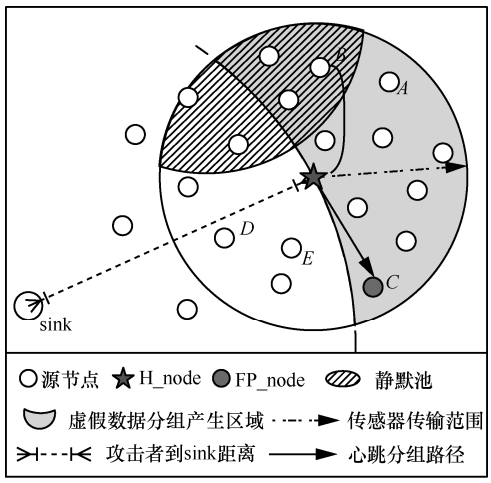


图 5　虚假数据分组的产生

首先发现攻击者的传感器节点，即最接近攻击者的传感器节点，所以它的位置近似于攻击者的位置。如图 5 有 3 个部分，第 1 个条纹阴影是静默池，第 2 个部分为 H_node 周边小于其到 sink 距离的所有邻居，第 3 个阴影部分是虚假数据分组所在范围。虚假节点选择这个部分的原因在于：1) 攻击者已知 sink 节点的位置，为了找到源节点，其攻击路径逐渐远离 sink 节点寻找源节点，如果攻击者捕获的数据总是在 sink 周围，那么它会判断那是虚假路径；2) 真实数据的路径是有可能穿越静默池的，而选取静默池之外的传感器作为虚假节点，可以不影响真实数据的原始路径，并且依照既定策略可以诱使攻击者远离真实路径，从而保障网络的隐私安全。具体虚假节点的选择如算法 2 所示，首先在 H_node 的邻居节点中选择虚假节点 FP_node（第 1)行和 2)行），其到 sink 的距离必须大于攻击者到节点的距离，并有 FP_node∈SET_Far（第 3)行），在满足上述条件的点中选择离当前发送数据节点距离最远的点为虚假节点（第 4)行和 5)行）。

算法 2　Find_Fake_Node

输入　H_node

输出　FP_node

1) 找出 H_node 的邻居 Nei_node(H_node);

2) 从 H_node 的邻居节点 Nei_node (fake_beacon) 选择一个虚假节点 n_i;

3) If($d(n_i,\text{sink})>d(\text{H\_node},\text{sink})$ & $n_i\in\text{SET\_Far}$)

4) FP_node=max($d(n_i, node_{\text{ID(fake\_beacon)}})$) ;
//选择离当前发送数据节点距离最远的点

5) return FP_node;

6) else go to 2);

给定 H_node 的邻居节点分别为{*A*、*B*、*C*、*D*、*E*}，如表 2 所示，若节点 *B* 收到了 readysilent_beacon 和 confirmsilent_beacon，即 $B \in SET\_Silent\_pool$ 的点，所以在其 fake_beacon 的负载里加上自己的 *ID* 并以心跳分组广播。

表 2 邻居节点的选择

邻居节点	距离	readysilent_beacon	confirmsilent_beacon	fake_beacon
$A(x_A,y_A)$	$d(A,\text{sink})$	1	0	0
$B(x_B,y_B)$	$d(B,\text{sink})$	1	1	ID_B
$C(x_C,y_C)$	$d(C,\text{sink})$	1	0	ID_C
$D(x_D,y_D)$	$d(D,\text{sink})$	1	0	0
$E(x_E,y_E)$	$d(E,\text{sink})$	1	0	0

H_node 收到节点 *B* 的心跳分组后计算出最远的节点为 FP_node。如果每次选择的节点总在 sink 附近，作为有感知能力的攻击者，可能判断此为虚假数据分组。节点 *D* 和 *E* 不在选择范围，因为节点 *D* 和 *E* 到 sink 的距离小于 H_node 到 sink 的距离。根据定义 3，相对节点 *A*，会选择离 *B* 更远的节点 *C* 作为 FP_node。于是 H_node 会把节点 *C* 的 ID 信息放在 fake_beacon 负载中广播出去，这些心跳分组的发送频率高于数据分组发送的 3 倍以上，节点 *C* 收到包含自身 ID 的心跳分组后即发送虚假数据分组，诱使攻击者远离发送真实数据分组的节点 *B*，向节点 *C* 方向移动。

虚假数据分组的生存周期为 *TTL*，生存周期越长，产生的虚假路径就越长，消耗的能量就越大。这里设 *TTL*=0，只需要一跳的生存周期就达到保护隐私的目的。

4.5 隐私分析

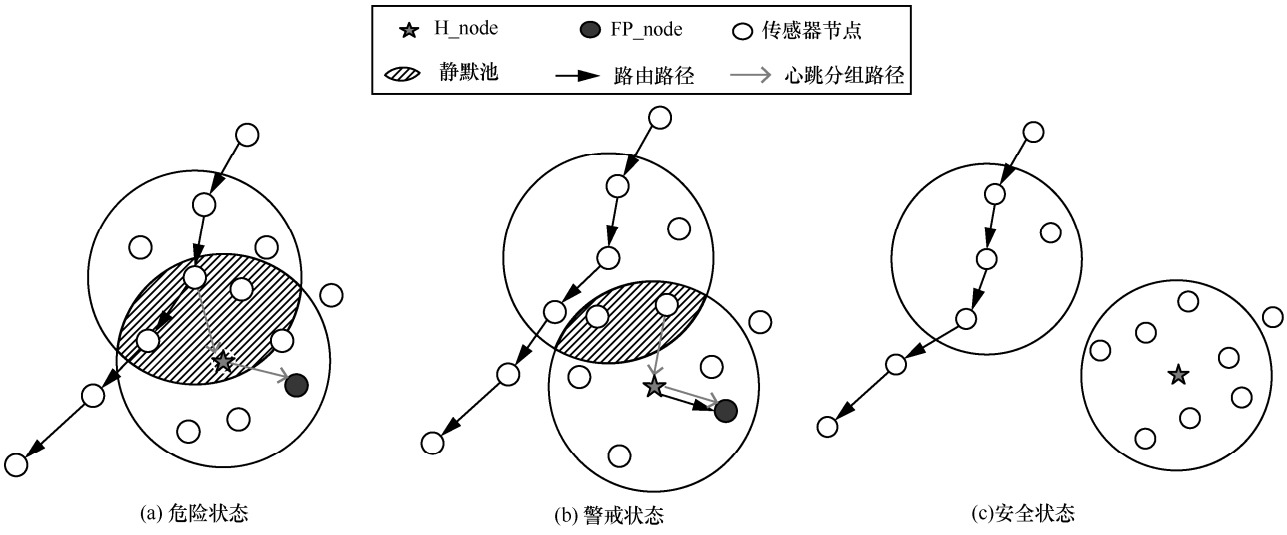
如图 6 所示，DPIOP 机制不会影响网络中的当前路由，根据攻击者距离正发送数据节点的远近，网络有如下 3 个状态：1) 危险状态，攻击者接近正发送真实数据的节点，节点随时被捕获；2) 警戒状态，攻击者虽然不能立即捕获真实节点，但一旦往真实路径方向随机游走，就会变成危险状态；3) 而如果攻击者往相反方向，则达到第 3 种状态——安全状态，如图 6(c)所示。

攻击者被 H_node 发现，并且 H_node 的邻近节点接收到 confirmsilent_beacon，如图 6(a)所示，静默池中的节点向 H_node 发送携带其 ID 的 fake_beacon，在同一个时间戳内的 fake_beacon 选择第一个接收心跳分组内含 ID 的节点，且保证 $\{n_{\text{ID}} | n_{\text{ID}} \in SET\_Silent\_pool\}$，其他则丢弃，H_node 在其邻居节点中选取一个虚假节点发送虚假数据分组，直到攻击者偏离原路线（即 $SET\_Silent\_pool=\Phi$）。

定义 4 为了衡量网络的安全性能，对于单个攻击者，在确定的当前路由和攻击模型下会使用安全周期或捕获率[4]来衡量隐私安全。

1) 安全周期。攻击者从 sink 节点出发，到捕获到源节点或离开网络监视区过程中，源节点发送的监测数据分组数量。

2) 捕获率（*L*）。在规定时间范围内，攻击者捕



(a) 危险状态 (b) 警戒状态 (c)安全状态

图 6 状态模型

获源节点的概率。

在源节点被捕获之前发送的数据分组越多，安全周期越长，安全性越高；在规定时间内和固定的源节点到 sink 的距离（*s*-*d*），捕获的源节点次数越多，捕获率越大，安全性就越差。

网络中的攻击如图 6 所示，共 3 种状态，假如源节点到 sink 一共有 h 步，产生静默池并且真实数据分组落在静默池中时为危险状态，概率为 P_{A}，如图 6(a)所示。在图 6(b)中，网络处于警戒状态的概率为 P_{C}，攻击者会追随虚假数据分组而去，并且也收不到真实数据分组，所以真实数据分组捕获率为 0。若网络处于安全状态的概率为 P_{S}，如图 6(c)所示，对一个好奇的攻击者，它处于随机游走状态，所以捕获源节点的概率为 $\frac{1}{N}$（网络中有 N 个传感器节点），攻击者在危险状态选择真实数据的概率为 P_h，被源节点被捕获的概率为

$$L = P_h^{P_{\mathrm{A}} \cdot h} P_{\mathrm{A}} + \frac{P_{\mathrm{S}}}{N} \tag{10}$$

并且有

$$P_{\mathrm{A}} + P_{\mathrm{C}} + P_{\mathrm{S}} = 1 \tag{11}$$

随着 h 的增加，捕获率越来越小，即攻击者远离数据分组传输路径，此时攻击者无法收到数据分组。P_h 越小，在危险状态的概率也越小，捕获到源节点的概率极低。在给定路由和攻击模型的情况下以及 sink 节点与源节点的距离固定时，使用本文提出的安全隐私机制后，与其他安全策略进行比较，在第 5 节中用实验结果说明了运用 DPIOP 具有极高的优越性。

4.6　DPIOP 算法能耗

本文使用心跳分组只是用于传输状态信号，并不传输源节点收集的数据，真实数据依然通过正常路由投递。心跳分组传递的信号状态只有 3 种，如表 1 所示，所以心跳分组的数据负载中只需要 2 bit 大小的数据段。如 4.2 节所述，正常的心跳分组大小不会影响网路能耗。传感器只有在感知到攻击者的情况下才会发送心跳分组，发送并不频繁。而且，心跳分组的发送范围只是在攻击者附近，不会造成全网大规模的影响。所以在本文中使用心跳分组的能耗基本可以不用额外考虑。

在 DPIOP 算法中，每个传感器都会在邻居发现阶段记住自己的一跳邻居，初始情况下攻击者位于 sink 节点，源节点开始发送分组至 sink 节点，每次事件从源节点传输到 sink 节点需要时间为 T，事件长度为 s bit。心跳分组发送的能量可以忽略不计，则网络中的时间和能量代价主要是数据收发引起的，因此，主要分析算法处理过程中网络收发的数据分组数量。

在最佳情况下，攻击者都远离真实数据的传输路径，如图 6(c)所示。此时没有静默池形成，所以也没有 fake_beacon 发出，此时网络只有真实数据在发送分组，所以能量消耗只和网络传输协议有关。最短路径一般是能耗最小的，假设最短路径长度为 h，根据式(5)可以计算每个传输事件到 sink 节点网络消耗的总能量为 $\widehat{E}_{\mathrm{network}} = hE_{sr}$，其中，$E_{sr}$ 为网络单个节点发送单个数据分组的收发能耗。那么安全地发送 η 个事件（数据分组），网络的总能量即为 $\eta\widehat{E}_{\mathrm{network}}$。

在最差情况下，攻击者一直在真实数据的传输路径附近，即每次都捕获到真实数据的节点，直到最终捕获到源节点（算法 1 第 4) ~15）行）。此时，攻击者每次监听的节点附近都会形成静默池并有虚假数据分组产生。假设真实数据路径长度为 h，则在捕获源节点前会产生 h 个虚假数据分组，攻击者也应该每次都捕获到了真实数据分组，所以真实的事件也应该为 λ=h。虚假数据分组的生存周期只有一跳，产生的额外能量为 hE_{sr}，收到虚假数据分组的节点会将其丢弃不再转发，此时网络消耗的总能量为发送 h 个真实数据分组的能量加上额外虚假数据分组的能量，为 $h\widehat{E}_{\mathrm{network}} + hE_{sr}$，即 $\widehat{E}_{\mathrm{network}}(h+1)$。

在危险和警戒状态时，除正常数据分组传输以外，发送虚假数据产生的平均能耗为 $(1-P_{\mathrm{S}})hE_{sr}$，在此状态下没有额外虚假数据分组发送。综合 3 种状态，网络平均总能耗为 $\widehat{E}_{\mathrm{network}}(h+1-P_{\mathrm{S}})$。实际上，当攻击者捕获到虚假数据分组之后便远离传输路径，就不会产生静默池，攻击者不再收到任何信号，于是攻击者开始随机游走。根据式(9)，随着游走步数的增多，攻击者基本还是在原地附近，所以回到传输路径附近的可能性很小，即 P_{A}<P_{C}<P_{A}+P_{C}<P_{S}。通过后面的仿真实验也说明，实际能耗是远小于最坏情况而接近最优能耗的。

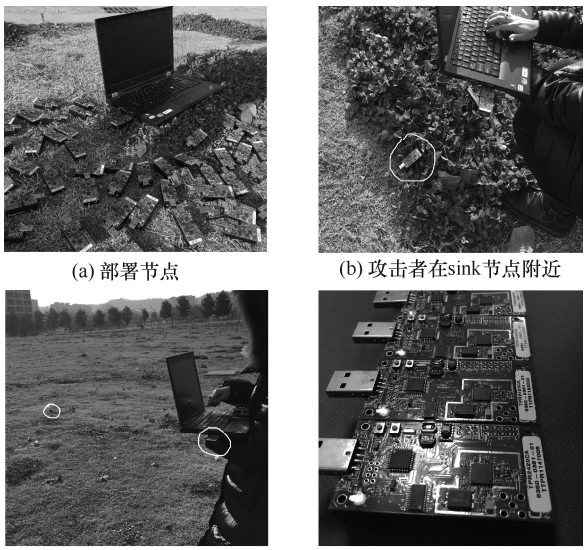
5 性能测试与分析

为了验证本文方法的高效低耗，分别利用小规模真实传感器节点和大规模仿真验证本文算法的性能。从时延、隐私安全、路径偏移量和能耗 4 个方面评价不同隐私保护方法。1) 时延定义为一个真实数据分组从源节点出发，经过一些中继节点，到达 sink 节点所需要的时间。2) 根据本文的安全衡量标准，通过统计源节点在规定时间内被捕获的次数来衡量隐私安全性。被捕获次数越少，安全周期越长，捕获率越小，即安全隐私性越高。3) 使用不同安全策略会使原始的路由路径发生偏移，路径偏移量为使用安全策略后真实数据分组投递路径长度相比平均最短路径长度的期望值的偏离程度。4) 据式(5)计算网络能耗，且能量与发送分组数成正比，在真实实验中，节点能耗难以测量，通过统计节点收发的数据分组数来衡量，路由算法的优劣会影响到网络的能耗。

5.1 真实节点实验

在空旷的操场上，随机放置 8×8 个传感器节点，如图 7(a)所示，节点选用 TelosB，使用 2 节 AA 电池进行供电，CPU 为 8 MHz TI MSP430，内存大小为 10 KB，通信芯片为 CC 2420，频率为 2.4 GHz。MAC 协议为 IEEE 802.15.4，操作系统采用 Tiny OS 2.0。如图 7(b)所示，攻击者手持一个传感器节点从 sink 节点出发，监听网络中的数据，通过 USB 端口读取发送者的序列号，从而向发送该数据的节点方向移动。如图 7(c)所示，攻击者附近的传感器利用心跳分组发送报警信号。源节点和 sink 节点之间的最短距离为 7 跳。实验共进行 10 次，源节点发送数据分组为 50 个，数据分组发完后实验结束。

图 7(d)为所有传感器节点，实验将通过收集每个节点的收发数据分组的个数，验证本文方法的低耗高效，并通过统计攻击者捕获源节点的次数验证方法的安全性。虽然 CALP 在节点每次转发数据时都需要等待心跳分组来更新路由表，引起超长时延，但其本质也是最短路径，与本文应用的原路由相同。另外，幻影路由作为一种安全策略不受攻击者影响，适用于做基准比较。真实实验中将本文的方法和幻影路由（RP）做出比较。



(a) 部署节点 (b) 攻击者在sink节点附近

(c) 攻击者捕获到新节点 (d) 收集实验数据

图 7 源节点隐私保护实验

1) 时延

为了精确测量数据分组投递的时延，分别在源节点和 sink 节点记录数据分组的发送和到达时间。表 3 和表 4 分别显示了在面临耐心和好奇攻击者时，SPA、DPIOP、RP 这 3 种算法在实际网络中投递数据分组所需的时延。

表 3 面临耐心攻击者的时延

算法	数据分组时延/s	与 RP 相比的时延变化率
SPA	1.78	+641.7%
DPIOP	0.17	−29.2%
RP	0.24	0

表 4 面临好奇攻击者的时延

算法	数据分组时延/s	与 RP 相比的时延变化率
SPA	0.19	−26.9%
DPIOP	0.18	−30.7%
RP	0.26	0

由表 3 和表 4 可以看出，DPIOP 在遇到 2 种攻击者时，时延几乎没有变化。由于 DPIOP 仍然以最短路径来投递数据分组，因而比幻影路由（RP）的时延分别减少了 29.2%和 30.7%。SPA 在面临好奇的攻击者时，攻击者会因为收不到数据分组而随机游走远离真实路径，从而减少了路径偏移量，虽然 SPA 比 DPIOP 的时延稍有增加，但比 RP 减少了 26.9%。然而在面临耐心的攻击者时却产生了高于 RP 算法 641.7%的时延，这是因为当 SPA 遇到耐心的攻击者时，

数据分组会一直在静默池边缘周旋而无法投递至 sink 节点。

2) 隐私安全

从安全性的角度，无论是面对耐心的攻击者还是好奇的攻击者，SPA 的捕获率最低，安全性最高，与 RP 相比，隐私安全性分别高出了 100%和 87.5%。因为 SPA 一直接收不到真实的数据分组，耐心的攻击者会一直等待直到时间结束，好奇的攻击者即使随机游走，活动范围也有限，无法找到距离较远的源节点。如果 DPIOP 在真实原路径节点附近，则会同时收到真实的数据分组和虚假数据分组，真实实验最短路径长度为 7 跳，所以当 7 次都恰好一直向真实数据分组的方向移动就捕获到了源节点。如表 5 和表 6 所示，面临耐心的攻击者，DPIOP 的隐私性相比 RP 高出 90%；遇到好奇的攻击者，DPIOP 的隐私性相比 RP 提高了 75%。相比耐心的攻击者，好奇的攻击者因为随机行走而增加了被捕获的概率，降低了隐私安全性。

表 5　面临耐心攻击者的隐私性

算法	捕获源节点的次数	与 RP 相比的隐私提高率
SPA	0	+100%
DPIOP	1	+90%
RP	10	0

表 6　面临好奇攻击者的隐私性

算法	捕获源节点的次数	与 RP 相比的隐私提高率
SPA	1	+87.5%
DPIOP	2	+75%
RP	8	0

3) 路径偏移量

真实节点实验中，最短路由的平均路径 μ=7.8，$\bar{x}$ 为使用安全策略后真实数据分组投递的路径平均跳数，由式(9)计算出路径偏移量，如表 7 和表 8 所示。

表 7　面临耐心攻击者的路径偏移量

算法	$\bar{x}$	路径偏移量	与 RP 相比的偏移量变化率
SPA	53.4	2 061	+3 810.8%
DPIOP	7.7	0.08	−99.8%
RP	14.7	52.7	0

表 8　面临好奇攻击者的路径偏移量

算法	$\bar{x}$	路径偏移量	与 RP 相比的偏移量变化率
SPA	10.4	7.9	−85.6%
DPIOP	7.6	0.06	−99.8%
RP	15.1	54.9	0

DPIOP 有着很小的路径偏移量，真实数据按照最短路径投递，在面临 2 种不同攻击者时，其偏移量均比 RP 低 99.8%。SPA 在面临耐心的攻击者时，由于数据在 sink 附近的重复投递，导致大规模的路径偏移，使其偏移量近高于 RP 路径 38 倍。SPA 在遇到好奇的攻击者这种极端情况消失，比 RP 的路由偏移低 85.6%，达到了很好的投递效果。

4) 能耗

为了验证本文方法的低能耗，实验分别统计了每种方法 10 次之后，所有节点的发送分组数，通过式(12)算出每个数据分组到达 sink 的平均路径长度，因为本文的方法使用了虚假数据分组，所以这里的平均转发节点也包括虚假数据分组的转发。

$$\text{平均转发节点}=\frac{\text{所有节点发送分组的总数}}{\text{实验次数}\times\text{源节点发送分组总数}} \tag{12}$$

实验结果如表 9 和表 10 所示，RP 的投递路径最长，产生的能耗最大。遇到耐心的攻击时，DPIOP 比 PR 减少了 37%的能耗，但 SPA 使数据分组一直在 sink 附近循环投递直到时间结束，路径长度的增加导致了能耗的异常。面临好奇的攻击者时，SPA 产生的数据转发量和 DPIOP 接近，分别节约能耗 31%和 30%。DPIOP 在遇到好奇的攻击者时比耐心的攻击者时产生了稍多能耗，主要因为好奇攻击者在接收不到任何数据时随机游走，使其在真实路径附近的概率增加，多产生了一些虚假数据分组。

表 9　面临耐心攻击者的路由跳数

算法	转发节点	与 RP 相比的能耗变化率
SPA	53.4	+263%
DPIOP	9.3	−37%
RP	14.7	0

表 10　面临好奇攻击者的路由跳数

算法	转发节点	与 RP 相比的能耗变化率
SPA	10.4	−31%
DPIOP	10.6	−30%
RP	15.1	0

5.2 仿真实验

为了验证在本文算法在大规模网络中的性能，实验选用一款基于 OMnet++的仿真器 Castalia，部署 100×100 个传感器于方形的平面网络，节点均匀随机分布，sink 节点随机置于网络的中央。假设网络中只有一个攻击者，且源节点放在离 sink 节点远近不同的位置。MAC 层协议基于 IEEE 802.15.4，心跳分组负载中携带信号信息，节点检测到攻击者的时候即发送心跳分组。虽然本文提出的策略不依赖于任何路由协议，但为了展示 SPA、DPIOP 机制的性能，原应用路由使用最短路径（SP），选取幻影路由（RP）以及同样基于心跳分组机制的 CALP[12]来比较。CALP 方法的敌人发现过程和本文是类似的，主要过程是，每个节点维护一张包含所有邻居节点的路由表，每次发现攻击者以心跳分组来传递信息更新路由表，路由选择每次都选择最靠近最短路径，并以到攻击者距离为惩罚距离的节点作为下一跳节点。这里不仅会比较好奇的攻击者，也会比较耐心的攻击者。

因为调度心跳分组不会发生额外的能量消耗，只是虚假信息的发送会消耗额外能量。虚假数据分组的生存周期 TTL=0，那么虚假数据分组的生存周期只有一跳。仿真进行 50 次，并且每次从源节点共发送 500 个新的数据分组。

1) 时延

时延包括 2 个方面，依赖心跳分组的时延和不依赖心跳分组的路由时延。路由时延与路由算法相关，如跳数和重投次数等。如图 8 所示，随着源节点到 sink 距离的增加，CALP 产生的时延也大幅度增加，远高于其他 4 种方法。CALP 投递时间不仅与路径长度成正比，还受心跳分组更新频率的影响，CALP 每次数据投递前都依赖心跳分组数据来更新路由表，否则无法实现安全保护，这样造成了极大时延。CALP 的路径长度与攻击者的攻击方式有关，对一个守在 sink 附近的耐心攻击者，CALP 虽然基于最短路径，但总是选择偏离攻击者的最远节点，直到攻击者捕获到新的数据分组，而对好奇的攻击者，如果没有捕获到新的数据分组，他就会随机游走，远离了最短路径附近，就不会使路径发生偏移。因此，相比较好奇的攻击者，CALP 在面临耐心的攻击者时会产生多一点时延。

SPA 和 CALP 一样，路径偏移也受到攻击者位置的影响。如图 8(a)所示，对于耐心的攻击者，SPA 机制导致数据分组的投递时延远高于最短路径。这是因为攻击者靠近 sink 节点时，会引起路径偏移，造成了 97%以上的数据分组无法路由至 sink 节点。在仿真实验中，有些数据分组转发了 157 次才到达 sink 节点。如图 8(b)所示，在遇到好奇的攻击者时，SPA 算法的数据分组时延大幅降低，相比幻影路由降低约 28.4%。这是因为好奇的攻击者收不到数据分组随机游走，远离最短路径。因此，实际应用中可以在 sink 节点附近，把最小安全距离调小，等远离 sink 节点时，再相应调回到通信半径。

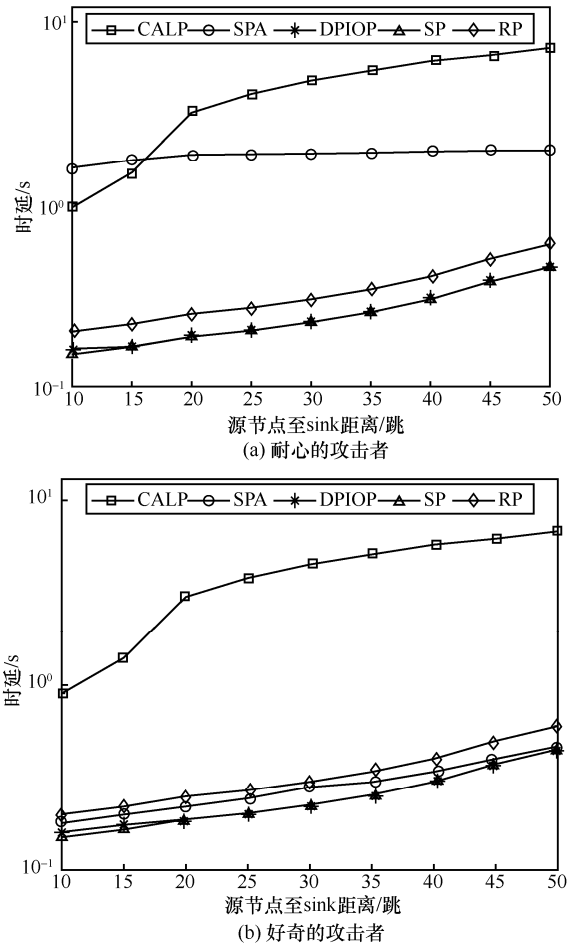


图 8 时延和 *s-d* 距离的关系

SPA、DPIOP 和幻影路由的投递时间只依赖于路径长度（即源节点到 sink 的距离 *s-d*），独立于心跳分组的发送时间，只需要满足 $3T_{\text{beacon}} \leqslant T_{\text{message}}$ 的约束即可。心跳分组的频率虽然会对网络流量造成影响，但实际上，只有在静默池形成时才会加大心跳分组的发送频率，并且不会影响数据正常发送速度，所以增加的网络流量也是极其有限的。DPIOP 算法使用的也是最短路由，所以攻击者一旦远离真实路由，DPIOP 的时延和最短路径路由相同，比幻

影路由的时延减少 35.2%。

幻影路由因为随机游走增加了步数，所以时延要高于最短路径。如图 8 所示，当 *s-d*=10 跳时，SPA、DPIOP 以及幻影路由产生的时延低于真实实验下 7 跳的时延，其原因是在同等实验条件下，真实环境要更复杂，链路干扰、无线带宽等不稳因素导致了实际时延要稍高于仿真环境。

2) 隐私安全

如图 9 所示，随着 *s-d* 的增加，最短路径的安全性并没有增加，并且是最差的，攻击者捕获到一个数据分组之后，就会顺着最短路径找到源节点。从实验结果看出，好奇的攻击者反而比耐心的攻击者捕获到源节点的次数少，因为好奇的攻击者从 sink 出发，没有等到任何数据分组后便随机游走，从而错过一些数据分组，偏移真实路径。因此，耐心的攻击者反而比好奇的攻击者有更高的捕获率。

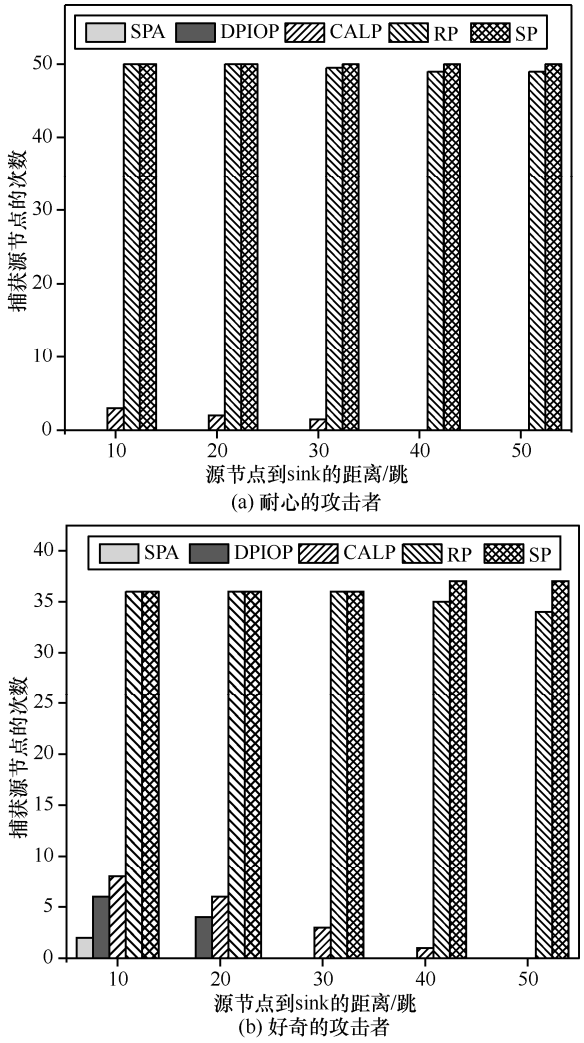


图 9　捕获节点数量和 *s-d* 距离的关系

CALP 的本质是贪婪最短路径，但每次都是选择离攻击者最远的，而且 CALP 的策略和攻击者的攻击半径设定相关。在仿真中，当攻击半径等于通信半径时，攻击者在 sink 附近是可以收到一些真实数据分组的，所以耐心的攻击者也可以捕获到一些数据源。好奇的攻击者收不到信息的时候则随机游走，*s-d* 较小时会捕获一些源节点。幻影路由在仿真中遇到耐心的攻击者时，并没有比最短路径表现更好，只是随着 *s-d* 的增加，随机游走的步数增加，好奇的攻击者会因暂时没有收到数据分组而偏移路线，丢失了捕获源节点的部分机会。

如图 9(a)所示，在 SPA 安全策略下，耐心的攻击者由于一直收不到数据分组而停留在原地，而无法继续追踪数据源，隐私安全性近乎 100%。当源节点离 sink 较近时，好奇攻击者因基本收不到数据分组处于随机游走状态，根据式(9)所示的随机游走概率分布，当源节点特别近时就会被捕获。如图 9(b)所示，当 *s-d*=10 跳且 SPA 遇到好奇攻击者时，SPA 比幻影路由（RP）的隐私性提高约 89.6%，高于实际实验中的 87.5%，这是因为实际实验中距离 *s-d* 更短，且攻击者在真实环境中随机游走的速度和范围都比仿真环境小。

在 DPIOP 安全策略下，由图 9(a)显示，从 *s-d*=10 跳到更远的距离，耐心的攻击者几乎捕捉不到源节点。遇到好奇的攻击者，图 9(b)显示当源节点至 sink 节点 20 跳在以内，DPIOP 捕获率虽低于 CALP 但也还能捕捉到源节点，因为 DPIOP 攻击者可以收到真实数据分组，相比较 SPA 的完全随机游走，DPIOP 追踪到源节点的概率要比 SPA 大。在真实实验中 *s-d*=7 跳时，遇到好奇攻击者，DPIOP 比幻影路由（RP）的隐私性高约为 75%，而在仿真实验中当距离 *s-d*=10 跳，SPA 遇到好奇攻击者比 RP 的隐私性高约为 94.9%，说明在仿真实验中有更高的捕获率，这是因为攻击者在真实实验中探测到的数据分组方向和距离会因环境因素而有误差。

随着路由路径 *s-d* 的继续增加，SPA 和 DPIOP 不管是针对耐心的攻击者还是好奇的攻击者，在保护源节点位置隐私上都有极好的安全性。

3) 路径偏移量

这里比较 4 种安全机制，本文选取最短路径 SP 作为原始的路由策略。根据式(9)，通过比较本文方法和 CALP、幻影路由（RP）的路由偏移量，可以看出不同路由对路径的影响，如图 10 所示。

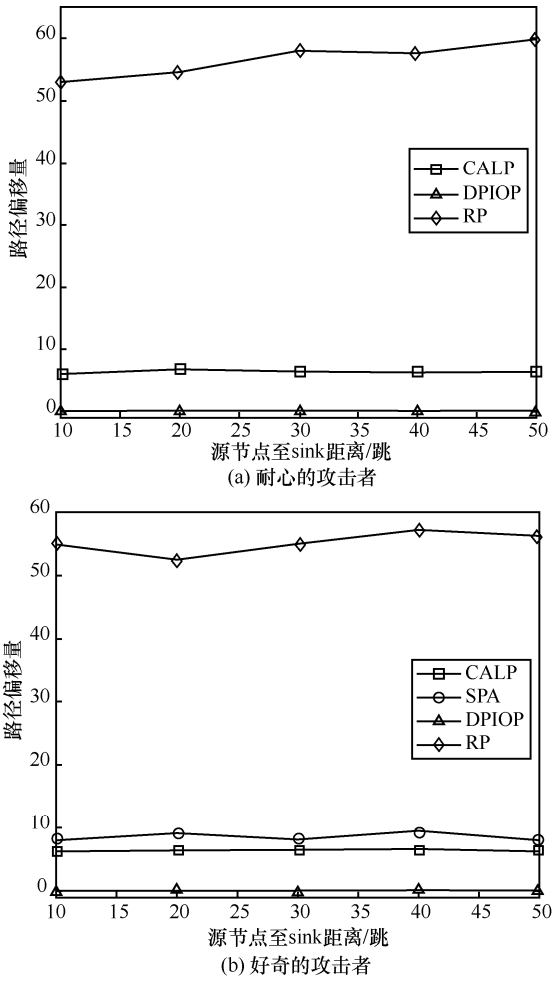


图 10　捕获路径偏移量和 *s*-*d* 距离的关系

从图 10 实验结果可以看出，只有 DPIOP 对原路由影响较小。其仿真结果与实际试验结果相似，与幻影路由相比偏移量减少约为 99%。幻影路由和最短路径的不同在于多了 h_{walk}=7 的随机游走，游走的方向是随机的，远离 sink 方向的游走会造成更大的路径偏移。

CALP 本质也是最短路径，当源节点离 sink 较远时，最短路由也会在选取路径时稍有偏移，这是由路由算法和网络拓扑决定的。CALP 在攻击者靠近真实路径时，每次选取离攻击者最远并且离 sink 最近的节点进行中继，真实路径在最短路径附近变化。

对于耐心的攻击者，在图 10(a)中没有显示 SPA，由于攻击者守在 sink 附近并一直收不到消息，而数据分组一直就在 sink 附近转发到达不了 sink 节点，所以造成路由偏移非常大，SPA 的偏移量和攻击者的攻击能力有关，越大的安全距离使偏移量越大。好奇的攻击者收不到数据分组后就进入随机游走状态，远离最短路径附近后就不再会对原始路径造成偏移。SPA 遇到好奇的攻击者的仿真实验结果如图 10(b)所示，与幻影路由相比偏移量减少约 85.8%，与真实实验的结果相符。

4) 能耗

根据式(5)来计算能耗，本次仿真实验中使用如下参数，如表 11 所示。

表 11　　参数设置

参数	数值
E_{elec}	60 nJ·bit
ξ_{amp}	10 pJ·bit^{-1}·m^{-2}
n	2

因为 CALP 的本质也是最短路径 SP，所以下面只需要比较本文方法与 SP 和 RP 之间的关系。图 11(a)中 SPA 产生的能量异常高于其他方法而无法显示在正常能量区间，因为面对在 sink 附近耐心的攻击者，数据分组一直围绕着静默池循环投递而无法到达 sink，从而消耗了更多的能量。所以遇到耐心的攻击者时，DPIOP 机制更高效、低耗。DPIOP 机制不会改变原路由的最短路径，只有虚假数据分组产生了额外的消耗能量，而只有存在静默池的时候才会产生虚假数据分组。实际上，耐心的攻击者被虚假数据分组诱使远离开原始路径后，静默池消失，攻击者便收不到任何真假数据分组。如图 11(a)所示，当网络保持稳定的安全状态（如图 6(c)所示）时，DPIOP 按最短路径投递真实数据分组。相比幻影路由 RP，DPIOP 遇到耐心的攻击者可节省能耗约为 62.6%，幻影路由的随机游走方向一旦是远离 sink 节点的方向，会产生更多能耗。在同等实验参数下，仿真实验比实际实验会产生较少能耗，这是因为实际环境有更多损耗能量的物理因素。

如图 11(b)所示，当遇到在 sink 附近好奇的攻击者时，SPA 会使攻击者无法收到任何数据分组而随机游走，偏离原路由路径后，数据分组按最短路径投递，比幻影路由降低能耗约为 55.2%。DPIOP 机制下好奇的攻击者在真实路径附近会一直同时收到 2 个数据分组，当他追踪假的数据分组时，一旦远离原始路径后，静默池也随之消失，攻击者便收不到任何真假数据分组，从而进入随机游走的状态，DPIOP 相比幻影路由能耗最多减少 54.7%。

在图 11(b)中，当路径 *s*-*d*<30 跳时，面对好奇的攻击者时，SPA 和 DPIOP 产生的能耗相差不大，这与真实实验结果相符，因为源节点到 sink 路径距

离较短时，SPA 产生的路径偏移路径长度和 DPIOP 产生的假数据分组发送的次数相差不多，所以产生的能耗也很接近。当 *s-d* 增加时，虽然 DPIOP 使攻击者捕获源节点的概率变小了，但捕获真实数据分组的数量也随之增加，而此时 SPA 随机游走造成的路径偏移并没有实质性变化，因此 DPIOP 产生的能耗就会稍高于 SPA。

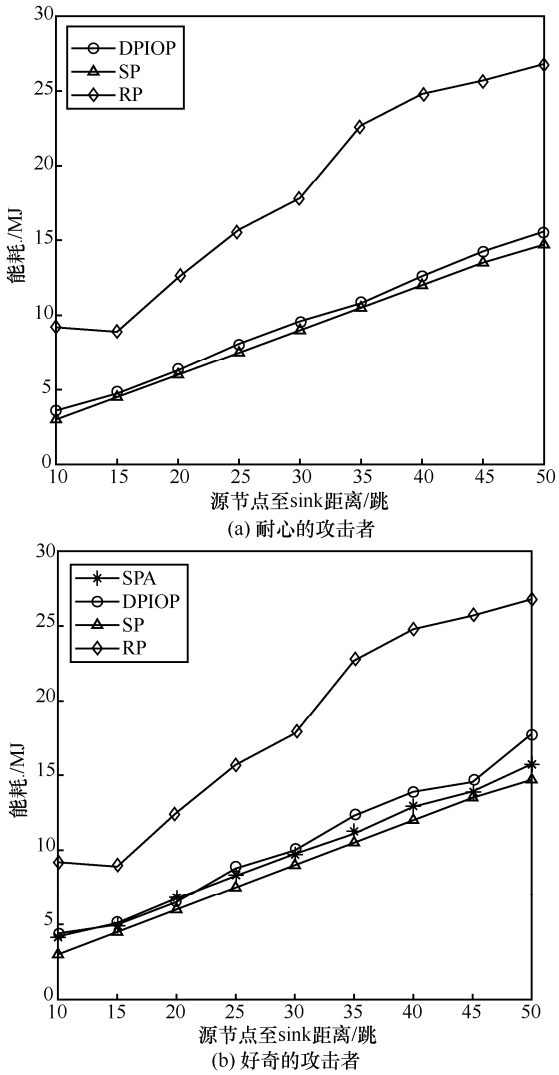


图 11　网络能量消耗和 *s-d* 距离的关系

6　结束语

本文提出了 2 种不依赖原路由的新方法 SPA 和 DPIOP 来解决源位置隐私的问题。SPA 通过让攻击者周围的节点只接收不发送从而阻止或降低攻击者收到新数据分组的可能性。实验结果证明了 SPA 具有极高的安全性，虽然面临耐心的攻击者，SPA 有可能会造成数据时延，然而在面对安全要求极高且可以牺牲一点时延的网络应用，如时延容忍网络（DTN, delay/disruption -tolerant network），SPA 是一个更好的选择。能量高效的 DPIOP 机制在路径较短的情况下安全性能稍差于 SPA，但只需要注入极少的虚假信息，就能达到保护源节点位置信息的目的，并且对当前的路由没有任何影响。实际应用中，可以灵活应用，如在 sink 附近使用 DPIOP，在源节点附近使用 SPA 机制。随着攻击者能力的增加，比如更大的窃听范围和更快的移动速度，网络的安全性能会有所下降。未来我们会继续研究网络面临更强大攻击者时的隐私保护安全策略。

参考文献：

[1] 牛晓光, 魏川博, 姚亚兰. 传感网中能量均衡高效的源位置隐私保护协议[J]. 通信学报, 2016, 37(4): 23-33.
NIU X G, WEI C B, YAO Y L. Energy-consumption-balanced efficient source-location privacy preserving protocol in WSN[J]. Journal on Communication, 2016, 37(4): 23-33.

[2] LIGHTFOOT L, LI Y, REN J. STaR: design and quantitative measurement of source-location privacy for wireless sensor networks[J]. Secur Commun Netw, 2016, 9(3): 220-228.

[3] 周倩, 秦小麟, 丁有伟. 无线传感器网络中基于哈希函数的上下文隐私保护[J]. 南京理工大学学报, 2017, 41(6): 753-759.
ZHOU Q, QIN X L, DING Y W. Hash-based contextual privacy preservation in wireless sensor networks[J]. Journal of Nanjing University of Science and Technology, 2017, 41(6): 753-759.

[4] 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: 599-608.

[5] ZHANG Y, WANG G, HU Q, et al. Design and performance study of a topology-hiding multipath routing protocol for mobile ad hoc networks[C]// IEEE INFOCOM. 2012: 10-18.

[6] RAHAT A A M, EVERSON R M, FIELDSEND J E. Evolutionary multi-path routing for network lifetime and robustness in wireless sensor networks[J]. Ad Hoc Netw, 2016(52):130-145.

[7] MEHTA K, LIU D, WRIGHT M. Protecting location privacy in sensor networks against a global eavesdropper[J]. IEEE Trans Mob Comput, 2012, 11(2): 320-336.

[8] YANG Y, SHAO M, ZHU S, et al. Towards statistically strong source anonymity for sensor networks[J]. ACM Trans Sen Netw, 2013, 9(2): 1-23.

[9] LOURENÇO P, BATISTA P, OLIVEIRA P, et al. Simultaneous localization and mapping in sensor networks: a GES sensor-based filter with moving object tracking[C]//European Control Conference (ECC). 2015: 2354-2359.

[10] NANDHINI S A, RADHA S. Compressed sensing based object detection and tracking system using measurement selection process for wireless visual sensor networks[C]//International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). 2016: 1117-1122.

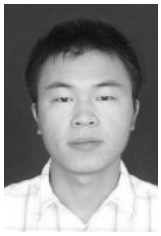
[11] APICHARTTRISORN D, APICHARTTRISORN K, KASETKASEM T. A moving object tracking algorithm using support vector machines in binary sensor networks[C]//13th International Symposium on Commu-

nications and Information Technologies (ISCIT). 2013: 529-534.
[12] RIOS R, LOPEZ J. Exploiting context-awareness to enhance source-location privacy in wireless sensor networks[J]. Oxford University Press, 2011, 54(10): 1603-1615 .
[13] BURATTI C. Performance analysis of IEEE 802.15.4 beacon-enabled mode[J]. IEEE Transactions on Vehicular Technology, 2010, 59(4): 2031-2045.
[14] BRADBURY M, LEEKE M, JHUMKA A. A dynamic fake source algorithm for source location privacy in wireless sensor networks[C]//IEEE Trustcom/BigDataSE/ISPA. 2015: 531-538.
[15] OUYANG Y, LE Z, LIU D, et al. Source location privacy against laptop-class attacks in sensor networks[C]//The 4th International Conference on Security and Privacy in Communication Networks. 2008: 5-10.
[16] RAJ M, LI N, LIU D, et al. Using data mules to preserve source location privacy in wireless sensor networks[J]. Pervasive & Mobile Computing, 2014(11): 244-260.
[17] JHUMKA A, LEEKE M, SHRESTHA S. On the use of fake sources for source location privacy: trade-offs between energy and privacy[J]. Computer Journal, 2011, 54(6): 860-874.
[18] SHI R, GOSWAMI M, GAO J, et al. Is random walk truly memoryless traffic analysis and source location privacy under random walks[C]//IEEE INFOCOM. 2013: 3021-3029.
[19] XI Y, SCHWIEBERT L, SHI W. Preserving source location privacy in monitoring-based wireless sensor networks[C]//20th IEEE International Parallel Distributed Processing Symposium. 2006.
[20] ALOMAIR B, CLARK A, CUELLAR J, et al. Toward a statistical framework for source anonymity in sensor networks[J]. IEEE Transactions on Mobile Computing, 2013, 12(2): 248-260.
[21] 吴博, 胡小龙. WSN 中基于假路径的源位置保护策略[J]. 计算机工程与应用, 2008, 44(16): 114-117.
WU B, HU X L. Strategy of protecting source-location privacy in WSN based on fake paths[J]. Computer Engineering and Applications, 2008, 44(16): 114-117.
[22] AMIN R, BISWAS G P. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks[J]. Ad Hoc Networks, 2016, 36(1): 58-80.
[23] SRINIVAS J, MUKHOPADHYAY S, MISHRA D. Secure and efficient user authentication scheme for multi-gateway wireless sensor networks[J]. Ad Hoc Networks, 2017, 54: 147-169.
[24] REDDY A G, DAS A K, YOON E J, et al. A secure anonymous authentication protocol for mobile services on elliptic curve cryptography[J]. IEEE Access, 2016(4): 4394-4407.
[25] SHAO M, HU W, ZHU S, et al. Cross-layer enhanced source location privacy in sensor networks[C]//6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. 2009: 1-9.
[26] XING Y, CHEN Y, YI W, et al. Optimal beacon interval for TDMA-based MAC in wireless sensor networks[C]//11th International Conference on Innovations in Information Technology (IIT). 2015: 156-161.
[27] HUANG P, LIU C J, XIAO L. TAS-MAC: a traffic-adaptive synchronous MAC protocol for wireless sensor networks[J]. ACM Transaction Sensor Network, 2016, 12(1): 1-30.
[28] ZHOU L, WAN C, HUANG J, et al. The location privacy of wireless sensor networks: attacks and countermeasures[C]//Ninth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA). 2014: 64-71.
[29] POTTIE G J, KAISER W J. Wireless integrated network sensors[J]. Communication ACM, 2000, 43(5): 51-58.

[作者简介]

周倩（1983-），女，江苏兴化人，南京航空航天大学博士生，主要研究方向为数据信息安全、传感器网络、数据隐私保护等。

秦小麟（1953-），男，江苏苏州人，南京航空航天大学教授，主要研究方向为分布式数据管理、物联网、数据安全与隐私保护、大数据管理与分析等。



丁有伟（1987-），男，江苏宿迁人，南京航空航天大学博士生，主要研究方向为云计算、能量高效数据管理和数据挖掘等。