doi:10.11959/j.issn.1000-436x.2016069

传感网中能量均衡高效的源位置隐私保护协议

牛晓光[1,2]，魏川博[1,2]，姚亚兰[1,2]
（1. 武汉大学计算机学院，湖北 武汉 430072；
2. 武汉大学空天信息安全与可信计算教育部重点实验室，湖北 武汉 430072）

摘 要：针对无线传感网中现有信源匿名协议大都存在无法同时兼顾源位置匿名性、延迟和生存周期的问题，对数据混淆、虚假信息注入等方法在隐私性、网络性能等方面进行了分析，在此基础上首次提出了基于匿名量化动态混淆环的源位置隐私保护协议 ADRing：以能量均衡消耗确保的动态混淆环以及相应基于区位象限的匿名度量化评估机制来高效地保护信源节点位置隐私。仿真实验结果表明，ADRing 相比于现有协议能明显改善网络能耗和延迟均衡性，延长网络寿命，能满足网络节点对于数据分组匿名性和延迟的不同需求。

关键词：源位置隐私；匿名量化动态混淆环；全网侦听攻击；匿名度；无线传感网
中图分类号：TP393 **文献标识码：**A

Energy-consumption-balanced efficient source-location privacy preserving protocol in WSN

NIU Xiao-guang[1,2], WEI Chuan-bo[1,2], YAO Ya-lan[1,2]
(1. School of Computer, Wuhan University, Wuhan 430072, China;
2. Key Laboratory of Aerospace Information Security and T usted Computing MOE, Wuhan University, Wuhan 430072, China)

Abstract: Considering the conflicts among anonymity, network load and transmission latency for most of the existing event source-location privacy (SLP) in wireless sensor network (WSN). Firstly, the effect of the data mixing and fake packet injection on the privacy and network performance was analyzed. Then, the anonymity-quantified dynamic mix-ring-based source-location anonymity protocol(ADRing)was proposed, ADRing which was designed to achieve source anonymity and balance between network traffic and real event report latency through the dynamic mix-ring based packet confusion and the corresponding sector-based anonymity assess and the radius of non-uniform clusters. The simulation results demonstrate that ADRing is very efficient in balancing energy consumption and transmission latency, and can significantly prolong survival period of the network and ensure security as well as latency to satisfy the packets' requirements.

Key words: source-location privacy, anonymity-quantified dynamic mix-ring, global attacker, anonymity degree, wireless sensor network

1 引言

无线传感网由于其无线通信方式及自身资源受限等原因容易遭受各种安全威胁，其中，信源位置隐私问题已成为制约其实际部署应用的主要障碍[1]。无线传感网络具有不可控的环境因素、传感器节点的资源限制、拓扑结构的限制等特性。同时，在实际应用中，无线传感网往往处于无人维护、条件恶劣的环境中，这将导致其面临着许多潜在的恶意攻击和破坏。在事件监测的传感网应用中，事件的源位

收稿日期：2015-05-31；**修回日期：**2015-07-28
基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（No.2011CB707106）；国家高技术研究发展计划（“863”计划）基金资助项目（No.2013AA122301）；国家自然科学基金资助项目（No.41127901-06）；长江学者和创新团队发展计划基金资助项目（No.IRT1278）
Foundation Items: The National Basic Research Program of China (973 Program) (No. 2011CB707106), The National High Technology Research and Development Program of China (863 Program) (No. 2013AA122301), The National Natural Science Foundation of China (No. 41127901-06), The Program for Changjiang Scholars and Innovative Research Team in University (No. IRT1278)

置具有相当高的敏感性，是一项非常重要的信息，必须得到保障。由于无线传感网自身独有的特点，传统的匿名性技术不适用于无线传感网络中。攻击者有能力对传感网中的无线通信进行监听，在不破坏节点、不破解数据分组内容、不扰乱网络正常工作的情况下通过流量分析、逐跳回溯等方式定位到源节点。因此，在无线传感网中提供数据源位置隐私保护成了一项具有挑战性的工作。

由于无线传感网具有资源受限的特点，对于其安全协议的设计需要对安全性与资源利用率进行折中考虑，需要以尽可能低的代价获取尽可能高的性能。

针对无线传感网的功能特点以及其面临的源位置隐私威胁，本文提出了基于匿名量化动态混淆环的源位置隐私保护协议 ADRing：首先，为了抵抗能力更强的全局攻击者发起的流量分析攻击，网络中所有节点均按相同策略向网络中注入数据分组；其次，在网络中建立混淆环，在防止攻击者通过逆向回溯定位到数据分组源节点的前提下大幅削减基站附近流量；为了量化数据分组混淆后对源位置隐私保护的效果，本文设计了匿名度量化机制，主要贡献如下。

1) 根据传感网在能耗、延迟等方面的非均衡分布特性，提出了基于匿名量化动态混淆环的源匿名协议。设置混淆环对数据流量逐跳转发过滤掉虚假流量，同时保证了真实数据分组的匿名性；提出了匿名度评估机制，对混淆过程进行量化评估。

2) 通过混淆环位置的动态调整来改变网络能耗的分布状况，建立不同混淆环下的能耗模型，通过求解模型得到最优混淆环调整策略，以此达到长效能耗高效，尽可能延长网络寿命。

2 相关工作

已有的无线传感网中源位置隐私保护工作根据作用环节及保护手段的不同，主要分为 2 类[2]：数据分组转发环节的基于传输扰动(transmission perturbation)的源位置隐私保护协议和数据分组产生环节的基于信源泛化(source generalization)的源位置隐私保护协议。

Ozturk 等[3]提出了基于随机漫步思想的“幽灵路由”源位置隐私保护协议，该协议分为 2 个阶段：数据分组首先进行随机漫步 h 跳后到达一个伪信源节点；随后开始进入第二阶段，数据分组将从伪信源节点通过洪泛或者最短路径策略逐跳转发最终到达基站。文献[4]研究了随机漫步策略对幽灵路由机制的影响，发现其在统计意义上不具有完备的隐私保护作用，提出了 2 种改进的定向随机漫步技术：基于扇区的定向漫步和基于跳步数的定向漫步技术。文献[5]提出的基于源节点有限洪泛的方案和可视区的概念，不仅能有效地保证前 h 跳的每一跳均朝着远离真实源节点的方向进行，同时保证了伪源节点具有更高的地理位置多样性。基于随机漫步思想的信源位置隐私保护研究工作还有文献[6, 7]等，这类方法大都存在分组传输延迟大、路由维护开销较高、传输可靠性较低的问题。针对以上问题，文献[8,9]提出了基于混淆环思想的源位置隐私保护方法：选取网络中部分节点构成混淆环，信源节点首先把数据分组发送到混淆环上任意节点，数据分组随后在环上循环转发以便与来自其他信源节点的数据分组和环内已有的虚假数据分组进行混淆，当混淆到一定程度后由环内节点直接发送至基站。Rios 等[10]利用节点对其邻近区域内移动敌手位置的感知能力，动态选择一条能有效避开敌手侦听的到达基站的近似最短路径，从而实现信源位置隐私保护的目的。该方法能够取得接近传统最短路径路由算法的传输延迟和能量消耗，但它关于节点具备感知邻近区域内敌手位置信息能力的假设限制了其适用性和实用性。总体而言，基于数据传输扰动的信源位置隐私保护技术基本上集中在抵御非入侵恶意敌手在局部侦听逐跳回溯模型下的位置隐私攻击上，但是由多个敌手联合发起的具备全网侦听能力的流量分析攻击则能够容易定位到发起通信信源节点的位置。

针对基于数据传输扰动的源位置隐私保护机制无法抵御全网侦听流量分析攻击的问题，文献[11]首次提出了基于周期采集的源位置隐私保护方案。在周期性采集方案中，全网内所有节点无论是否监测到事件发生均以恒定速率发送数据分组。这种方式的好处是源位置隐私能获得最大程度上的保护，但引入过多虚假数据分组在逐跳转发过程中节点上的排队等待会导致延迟和能耗增大的问题。为了更好地平衡隐私和性能，文献[12, 13]提出了统计强源匿名性的概念，力图根据监测数据分组的延迟需求和已发送数据分组的统计特征调整监测数据发送时机和虚假数据分组的注入时机，使网络中所有节点的数据发送特性在统计意义上相同，即使具备

全网侦听能力的敌手也无法识别出信源节点的位置。但是，基于统计特征的方案需要所有节点都参与虚假数据分组的注入，不仅会引入大量的能量开销，也会增加数据分组冲突的概率，降低传输效率。文献[14, 15]对全网所有节点参与虚假数据分组注入方案做了改进，通过基站与网络节点协同工作的方式选出一定数量的具备地理多样性特征节点作为虚假信源节点，只有被选定的虚假信源节点和实际信源节点能够向网络注入数据。文献[16~20]针对虚假数据分组注入方案中网络流量和能量开销过大的问题，提出通过在网络中选取部分代理节点负责汇集邻近区域内的数据分组并对虚假数据分组进行过滤和消减。总体而言，基于信源泛化的源位置隐私保护技术能够有效抵御所有类别的源位置隐私攻击，但额外注入的虚假数据分组会引起网络负载增大、网络生存周期与事件报告延迟之间矛盾加剧、传输可靠性降低等问题，虽然能够降低匿名度为代价减少虚假数据量，但仍然无法适应大规模的网络应用。

3　系统模型和设计目标

3.1　网络模型

事件监测无线传感网中的节点以基站为圆心均匀分布，如图 1 所示。设网络的半径为 N_s 跳，节点之间的通信半径为 R，节点的密度为 $?$，那么网络中的节点数为 $N_{All}=p?(N_sR)^2$。

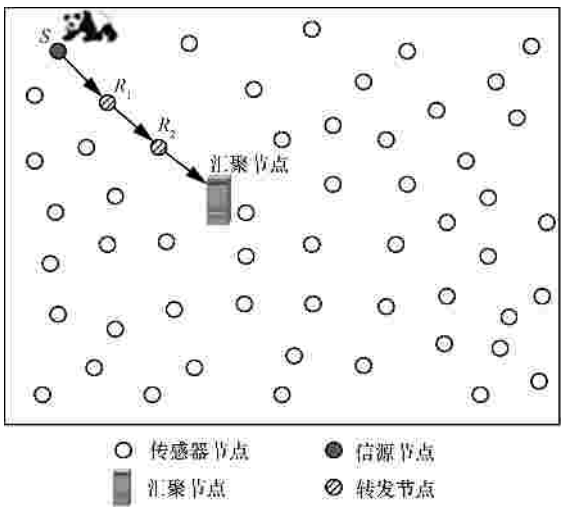

图 1　事件监测无线传感网示意

节点能与同跳邻居节点和相邻跳的邻居节点直接通信，其他节点不能直接通信。

基站是唯一的消息传送到的目的节点。

每一个消息都包含唯一的与信息产生位置相关的编号，每个消息的内容都用节点和基站之间的公开秘钥进行加密。

假设传感器节点知道彼此之间的相对位置，每个传感器节点都知道邻节点的信息。

3.2　攻击者攻击模型

获取事件源位置对于攻击者来说意义重大，因此攻击者会尽可能地配备先进的设备，有很强的运算能力和破空能力，假设攻击者具有如下特点。

攻击者有充足的能源、充分的计算能力以及足够的内存来存储数据。当监控到数据通信时，攻击者可以通过分析接收到信息的强度和方向来确定发送信息的上一个直接节点。此处本文假设只要攻击者在事件附近就能捕获事件。

攻击者具备很强攻击能力：在监测区域中部署多个监听点，配备性能强大的监听设备，对整个网络具有全局视图，能够获得全网的数据流量信息。

攻击者只发起外部（被动）攻击。由于攻击者发起主动攻击很容易被监测到，同时假设攻击者无法破译密钥，所以攻击者仅仅采用被动侦听方式侦听全网数据流量，采用流量分析等手段进行攻击。

3.3　设计目标

现有源位置隐私保护机制存在隐私和性能无法兼顾的问题，这会导致网络服务质量及资源消耗不均衡程度加剧、隐私性减弱、网络生存时间缩短等后果。本文设计了一套机制，能够在确保源位置隐私安全的前提下，优化能耗的均衡性，平衡了报告延迟，延长了网络的生存周期。

4　基于匿名量化动态混淆环的源隐私保护协议

本文提出了基于匿名量化动态混淆环的源位置隐私保护协议(ADRing, anonymity-quantified dynamic mix-ring source location anonymity)。网络中的节点以基站为圆心按相同的跳数被分为多个“环”，按策略选择其中一个作为“混淆环”，对全网发来的数据分组进行混淆，其作用是在保证数据分组匿名性的前提下过滤掉大量由各节点注入的虚假数据分组，降低能耗开销，图 2 为该协议的工作流程示意。网络初始化完成开始工作后，网络中所有节点以某种相同策略注入虚假流量——无论节点是否监测到真实事件的发生，节点均按相同的时间间隔分布状况向混淆环发送真实或虚假数据分组，这

一阶段保证了数据分组在初始发起时的源匿名；混淆环不断地收到全网节点发送来的真实或虚假数据分组，混淆环对收到的数据分组进行混淆，最终丢弃虚假数据分组并将真实数据分组发回基站。混淆过程扰乱了数据分组的路径关系，使攻击者无法通过流量分析、回溯等手段定位到数据分组的源节点，能有效保证真实数据分组的源匿名。此过程使用了匿名度评价机制对混淆效果进行评估，对过程进行定量控制；由于混淆环的工作量大、能耗高，为了平衡网络的能耗，延长网络寿命，需要动态地选择不同的“环”作为混淆环。

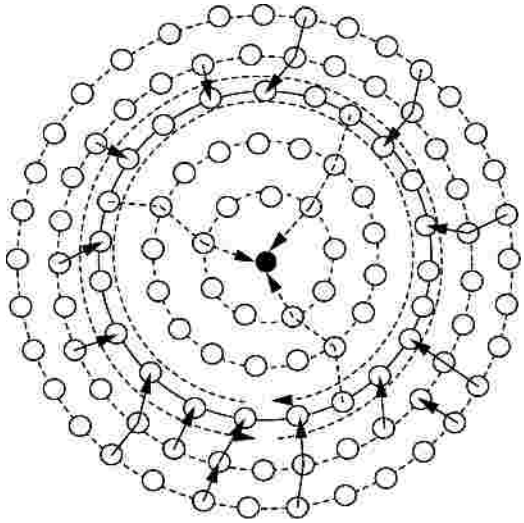

图 2 ADRing 数据流示意

数据分组格式如图 3 所示，字段包括事件信息、真假标志位、匿名度、源象限标识、源象限号等。事件信息只向基站报告，因此首先用基站的公钥加密，再与真假标志位、匿名度等其他字段在节点之间用协商的会话密钥逐跳加密。

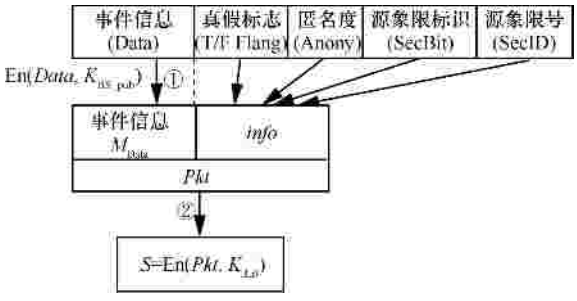

图 3 ADRing 数据分组格式

4.1 网络初始化与混淆环的建立

在网络初始化阶段，基站以广播方式向网络发送 Beacon 分组。Beacon 中包含了控制信息、跳数值 $Hops$ 以及基站公钥信息 $K_{\mathrm{BS\_pub}}$，节点在收到该分组后就能够得到自己所处位置的跳数值，并将 Beacon 分组中的跳数值 h 加 1 后广播出去，最终节点能够获取自己环上相邻节点以及相邻环上的相邻节点信息。节点在得到自己位置信息之后，会与其相邻环上节点以及上下相邻环的相邻节点进行密钥协商，得到对称密钥 K_{S}，用于后面节点之间的数据分组传递。网络拓扑确定后，基站将广播混淆环距离基站跳数 $RingHop$ 及基站公钥 $K_{\mathrm{BS\_pub}}$ 等信息。

4.2 数据发送与捎带机制

为抵御全局攻击，节点即便在没有监测到真实事件也需要模拟真实信源发送虚假数据分组，同一节点发送的数据分组的间隔需要服从相同的统计规律，数据分组的注入就需要采用某种机制，如恒定速率 ConsteRate 或基于指数分布的 FitProbRate 等。这会使攻击者无法区分数据分组真伪，从而无法定位真实信源节点。对于每种注入机制，节点发送数据分组的间隔为均值，设为 μ，那么单位时间内网络内新增的网络流量为 $F_{\mathrm{All}}=\dfrac{N_{\mathrm{All}}}{m}$，这些流量首先会汇聚到混淆环上由混淆环处理。

当节点 A 监测到一个事件数据 $Data$ 时，首先用节点与基站之间的公钥 $K_{\mathrm{BS\_pub}}$ 对事件数据字段进行加密 $M_{\mathrm{Data}}=\mathrm{En}(Data, K_{\mathrm{BS\_pub}})$，然后将数据分组中的数据真假标志字段、匿名度字段等信息字段 $info$ 进行相应的赋值，从而实现整个数据分组的封装 $Pkt=M_{\mathrm{Data}}||info$。在数据分组封装完成之后，利用与下一跳节点 B 之间协商的通信密钥 $K_{A,B}$ 对整个数据分组加密 $S=\mathrm{En}(Pkt, K_{A,B})$，按照预定策略将数据分组发送，数据分组沿着最短路径被转发到混淆环。

由于全网节点产生了大量的虚假数据分组，从源节点到混淆环的中间节点需要转发这些数据分组，因此中间节点可以利用这些数据分组捎带真实的事件信息，不但可以降低真实事件的报告延迟，还可以增加事件源位置的匿名性。中间节点 B 在收到数据分组 S 后，首先需要用 $K_{A,B}$ 对 S 解密，$Pkt=\mathrm{De}(S, K_{A,B})$，根据 Pkt 的信息判断该数据分组是真实或虚假数据分组：如果 Pkt 为真实数据分组，那么用节点 B 与下一跳节点协商的通信密钥 $K_{B,C}$ 对数据分组加密 $S_T=\mathrm{En}(Pkt, K_{B,C})$后转发给节点 C；如果 Pkt 为虚假数据分组，并且此时节点 B 上有真实

的数据分组 Pkt_T 需要等待间隔后发送，那么将虚假的数据分组 Pkt 替换为真实的数据分组 Pkt_T 后，再用 $K_{B,C}$ 对数据分组加密 S_T=En(Pkt_T, $K_{B,C}$)后转发给节点 C；如果此时节点 B 没有真实的数据分组需要发送，那么继续加密原来的数据分组 S_T=En(Pkt, $K_{B,C}$)后发送。

4.3　混淆与匿名度机制

数据分组在转发到混淆环后，混淆环对数据分组进行混淆，模糊掉数据分组与信源节点之间的相关性。

1) 数据分组运动方向随机确定

数据分组达到混淆环上的首个节点后，该节点首先以相同概率随机选择数据分组初始运动方向——顺时针或逆时针运动。每个节点有 2 个数据分组缓存队列，用于缓存 2 个方向上的数据分组。数据分组的方向确定后，数据分组被放入相应方向的队列中，之后其在混淆环上的转发就沿着该方向进行。因此，混淆环上存在顺时针和逆时针 2 个方向的数据流量。

2) 单点混淆过程

混淆环上节点在收到数据分组后将数据分组以随机次序插入到对应方向的缓存队列中，以此来随机扰乱数据分组进入/离开节点的顺序。由于数据分组中信息字段 $info$ 中的值会改变，而且采用了逐跳加密机制，因此同一个数据分组在进入和离开节点时的密文内容是不相同的，攻击者无法通过密文内容的相关性推测出数据分组的路径，如图 4 所示。

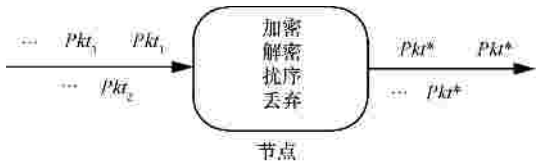

图 4　节点中数据分组扰序混淆示意

混淆环上节点有数据分组驻留队列，流量过高（节点内驻留数据分组过多）会导致数据分组等待延迟的期望增大，流量过低（节点内驻留数据分组过少）会使参与混淆的数据分组数量稀少，需要很多次节点间的转发混淆才能达到数据分组的源匿名。因此，需要控制混淆环上节点的流量处于合理范围。每个节点上有 2 个数据缓存队列以存储不同方向流量，每个队列最大长度为 L，如图 5 所示。

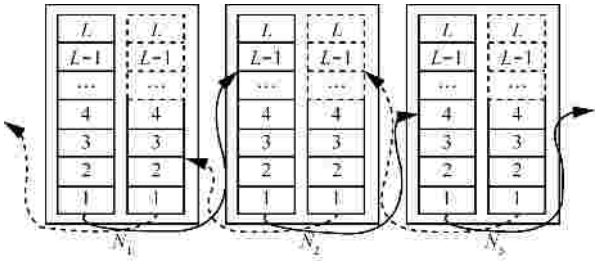

图 5　节点间数据分组转发混淆示意

节点收到来自某个方向的数据分组后，首先将该数据分组随机插入队列中某个次序。如果此时对应的队列长度超过 L，那么从该队列中丢弃掉一个跳数 $hops$ 最小的虚假数据分组，如果队列中全部为真实数据分组，那么将跳数 $hops$ 最大的数据分组发回基站。每隔时间 T 这 2 个队列向 2 个方向转发一次数据分组。

节点内某数据分组第 k 次被转发出去的概率为

$$P_{\text{fwd}}(k)=\left(\frac{L-1}{L}\right)^{k-1}\left(\frac{1}{L}\right) \tag{1}$$

被转发出去等待次数的期望为

$$\mathrm{E}(k)=\sum_{i=1}^{\infty} i\left(\frac{L-1}{L}\right)^{i-1}\left(\frac{1}{L}\right) \tag{2}$$

网络中不同的事件报告对延迟的需求不同，对于高延迟需求的数据分组，在插入队列时放到队列前端，使数据分组能够尽快完成混淆，发回基站。

3) 匿名度机制

匿名度机制用于衡量混淆过程对数据分组的源位置隐私保护程度。如图 6 所示，网络以基站为中心，被划分为 Q 个象限，编号为 0,1,2,…,Q- 1，处于一个象限区域内的所有节点编号一致。

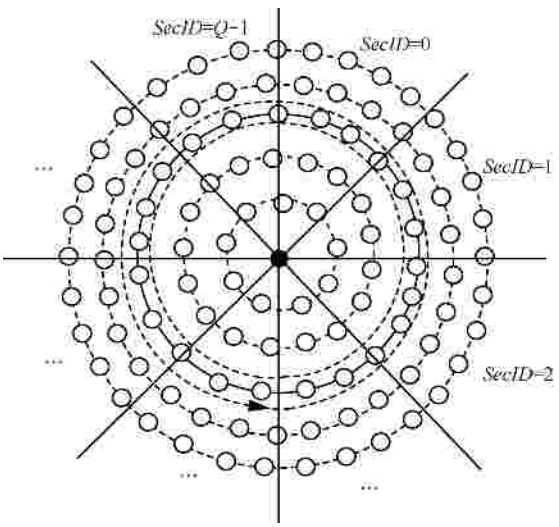

图 6　象限划分示意

协议中用二进制位来标识象限，源节点在生成数据分组时，节点根据自身所在的象限号 $SecID$(0≤$SecID$≤Q- 1)对数据分组的源象限标识 $SecBit$ 初始置位：第 $SecID$ 位置 1，其余置 0，即 $SecBit$=1<<$SecID$，表示该数据分组来自象限 $SecID$。

数据分组在到达混淆环后，源象限标识 $SecBit$ 中数值为 1 的位数表示数据分组的源节点可能所在的象限。在节点上对数据分组进行混淆时，由于数据分组进出节点的顺序完全是随机的，因此混淆后每个数据分组来自的区域均有可能是这些数据分组源象限标识所表示的象限。所以节点的源象限标识变化如下

$$SecBit_i=SecBit_i|(1<<SecID_1)|(1<<SecID_2)|\cdots|(1<<SecID_{N_p})\ (i=1,2,\cdots,N_p)$$

即队列中 N_p 个节点在混淆后所有节点的源象限标识是同向队列中各节点象限号位置 1 后依次按位或操作后的结果。

4.4 混淆环上数据分组的消除

数据分组在混淆环上经过充分混淆后，需要将达到匿名性要求的数据分组从环上消除。

数据分组中匿名度阈值字段 $Anony$ 表示源节点对该数据分组匿名程度的需求，即所需的数据分组经过混淆后所需的源象限数与网络总象限数 Q 的比值不小于 $Anony$。

节点中任何一个数据分组 Pkt 完成混淆过程的条件如式(3)所示。

$$\begin{aligned}&\exists Pkt\in List\\&\exists Pkt^*\in List^*\\&\left(\frac{B(Pkt.SecBit\mid Pkt^*.SecBit)}{Q}\geq Anony\right)\wedge\\&\left(\frac{B(Pkt.SecBit)}{Q}\geq\frac{Anony}{2}\right)\end{aligned}\tag{3}$$

其中，$B(Pkt.SecBit)$表示 $Pkt.SecBit$ 中二进制位为 1 的位数。

式(3)表示 2 个条件：1）该节点上另一方向的队列($List^*$)中存在一个反向数据分组(Pkt^*)，这 2 个数据分组的源象限标识 $SecBit$ 按位或后为 1 的位数不小于 $Q\cdot Anony$；2）该数据分组的源象限标识为 1 的位数不小于 $Q\frac{Anony}{2}$。条件 1）的意义是由于混淆环的流量是双向的，表示数据分组具有 2 个方向的可能性，而且 2 个方向综合的源象限数与总象限数比例达到匿名度阈值；条件 2）是为了保证对称性，自身所在方向提供的源象限数与总象限数的比例达到匿名度阈值的一半。

达到以上条件后，数据分组 Pkt 从环上离开或擦除：如果 Pkt 是真实的数据分组，那么将其直接发回基站；如果是虚假数据分组，那么从队列中直接擦除。

4.5 混淆环的动态调整

由于混淆环需要转发大量的数据分组，因此混淆环的能耗远大于其他环的能耗，为了平衡各环的能耗，延长网络寿命，需要对混淆环的位置进行调整。

在传感网中，节点绝大部分的能量用于通信，因此本文仅把通信的能耗作为衡量的指标。假设每个节点接收一个数据分组消耗的能量为 a，转发一个数据分组消耗的能量为 $ß$。当混淆环为第 Rh 跳时，各环上节点的能耗值为

$$E(Rh,x)=\begin{cases}\dfrac{(a+b)\sum_{i=x+1}^{N_s}F(i)+bF(x)}{N_r(x),x}, & x>Rh\\[2ex]\dfrac{(a+b)\sum_{i=1}^{x-1}F(i)+bF(x)}{N_r(x),x}, & x<Rh\\[2ex]a\dfrac{\sum_{i=Rh+1}^{N_s}F(i)+\sum_{i=1}^{Rh-1}F(i)}{N_r(Rh)}+\dfrac{2(a+b)}{INTVL_{Rh}}, & x=Rh\end{cases}\tag{4}$$

其中，$F(x)$表示第 x 跳上单位时间内初始产生的数据分组数量如式（5），在单位时间内，各环需要接收和发送上游所有环产生数据分组以及发送自身产生的数据分组；混淆环需要接收其他环发来的所有数据分组，以及每隔 $INTVL_{Rh}$ 接收和发送 2 个方向上各一个数据分组。

$$F(x)=\frac{N_r(x)}{m}\tag{5}$$

对 Rh,x 取 1,2,⋯,N_S，得出式(6)所示的能耗比矩阵 $\boldsymbol{M}_{engy}$。

$$\boldsymbol{M}_{engy}=\begin{bmatrix}E_{1,1} & E_{1,2} & E_{1,3} & \cdots & E_{1,N_s}\\ E_{2,1} & \ddots & & & \\ E_{3,1} & & \ddots & & \vdots\\ \vdots & & & \ddots & \\ E_{N_s,1} & & \cdots & & E_{N_s,N_s}\end{bmatrix}\tag{6}$$

第 k 行表示当混淆环为第 k 跳时，各个环上的单节点平均能耗。

设选取第 k 跳作为混淆环的工作时间为 Tr_k，为了延长网络寿命，需要使 $\sum_{i=1}^{N_s} Tr_i$ 最大，那么应该以最优的策略选择不同的环作为混淆环，使能耗得以充分利用，能效达到最高。

设每个节点的总能量为 $E_{\max}$，得到式(7)所示的线性规划函数，目标函数为各环作为混淆环的时间之和最大，即生存时间最长。限制条件表示各环上节点在不同环作为混淆环时的能耗限制。通过求解式(7)得到 $Tr_i\,(1\le i\le N_s)$ 的取值，即各环作为混淆环的时间比。

$$\max \quad z=Tr_1+Tr_2+\cdots+Tr_{N_s}$$
$$\text{s.t.}=\begin{cases} E_{1,1}Tr_1+E_{2,1}Tr_2+\cdots+E_{N_s,1}Tr_{N_s}\le E_{\max} \\ E_{1,2}Tr_1+E_{2,2}Tr_2+\cdots+E_{N_s,2}Tr_{N_s}\le E_{\max} \\ \vdots \\ E_{1,N_s}Tr_1+E_{2,N_s}Tr_2+\cdots+E_{N_s,N_s}Tr_{N_s}\le E_{\max} \end{cases} \tag{7}$$

其中，$Tr_i\ge 0(i=1,2,\cdots,N_s)$。

4.6　参数分析

网络中节点总数为

$$N_{\text{All}}=\pi(N_sR)^2q \tag{8}$$

第 x 跳的节点数为

$$N_r(x)=\pi(xR)^2q-\pi((x-1)R)^2q=(2x-1)\pi qR^2 \tag{9}$$

那么单位时间内混淆环上各节点收到的数据分组数量为

$$PN(Rh)=(N_{\text{All}}-N_r(Rh))\frac{1}{m}\frac{1}{N_r(Rh)} \tag{10}$$

Rh 为混淆环跳数，为了保证混淆环上每个节点每转发一次都能有一个新的数据分组参与混淆，那么混淆环发送分组的间隔必须满足条件

$$INTVL_{Rh}\ge\frac{1}{PN(Rh)} \tag{11}$$

根据式(8)~式(10)，得

$$INTVL_{Rh}\ge\frac{2m(Rh-1)}{N_s^2-2Rh+1} \tag{12}$$

不同环上的节点数不相同，为保持选择不同环作为混淆环时数据分组运动时间的统一，本文用角速度作为混淆环发送分组间隔的度量。设节点发送分组角速度为 $?$（单位时间/周），则各环上的发送分组间隔为

$$INTVL_{Rh}=\frac{w}{N_r(Rh)} \tag{13}$$

当 $Rh=N_s$ 时，即使用最外环作为混淆环时间隔 $INTVL_{Rh}$ 最小，再根据式(12)可以得

$$\frac{w}{(2N_s-1)\pi qR^2}\ge\frac{2m(N_s-1)}{N_s^2-2N_s+1} \tag{14}$$

通过式(14)可以得到网络中各参数的关系。

5　仿真实验和分析

5.1　性能仿真与分析

在仿真实验中，设置节点之间的通信半径为 30 m，节点平均分布且密度为每 330 m^2 一个节点，网络规模为 10 跳，根据式(8)计算出各跳的节点数，结果如表 1 所示，网络中共有 861 个节点，网络划分为 16 个象限，在仿真实验中仅考虑数据分组在队列中的等待延迟，不考虑其他延迟，假设网络中没有数据分组冲突。比较网络在不同的注入速率、转发混淆间隔、队列长度下的能耗、延迟等指标。

表 1　各环上节点数

跳数	节点数
1	9
2	26
3	43
4	60
5	78
6	95
7	112
8	129
9	146
10	163

首先设混淆环转发角速度为 $?$=16 秒/周，选择第 4 跳作为混淆环(Rh=4)，根据式(13)，每个节点的转发间隔为

$$INTVL_4=\frac{w}{N_r(4)}=\frac{16}{60}=0.267$$

设 μ=1 s，根据式(10)，$PN(4)$=13.35，$1>\frac{1}{13.35}$，满足式(11)的条件，网络能够正常工作。真实数据分组占全部流量的 5%。首先比较不同数据分组匿名度阈值和不同队列长度下真实数据分组混淆所经过的象限数，结果如图 7 所示。在匿名度需求相同时，队列长度越小，象限数的期望越大，这是由

于队列长度小，每个节点能够提供混淆的数据分组数量少，需要经历更多的节点对数据分组混淆才能达到数据分组所需的匿名度阈值，因此需要的象限数就越多。同理，在相同队列长度下，匿名度阈值越高，所需要的象限数也越多。反之当匿名度阈值越低，同时队列长度越大时，队列中有大量数据分组，源象限标识的位数越多，使大量真实数据分组不需要运动就可以达到阈值，如图 7(a) 中 *Length*=16 的曲线所示。

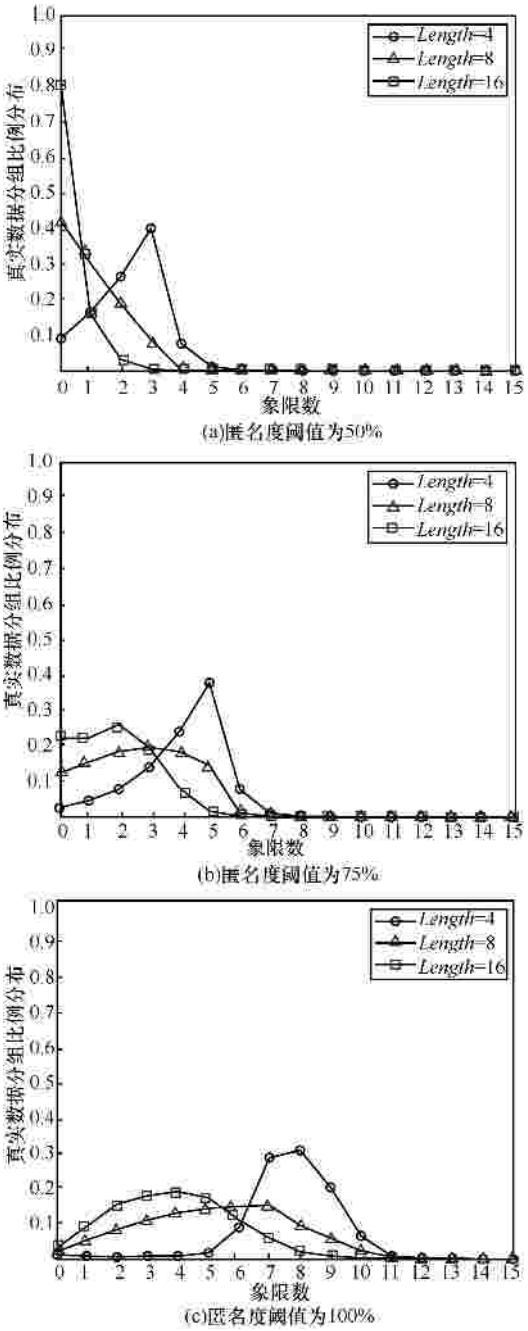

图 7 不同匿名度阈值下不同队列长度真实数据分组混淆所需象限数分布

接下来，考察真实数据分组进入和离开混淆环的象限之间的对应关系，本文把所有的真实数据分组都从 8 号象限注入混淆环，统计得到数据分组离开混淆环的象限号分布，得到的结果如图 8 所示。

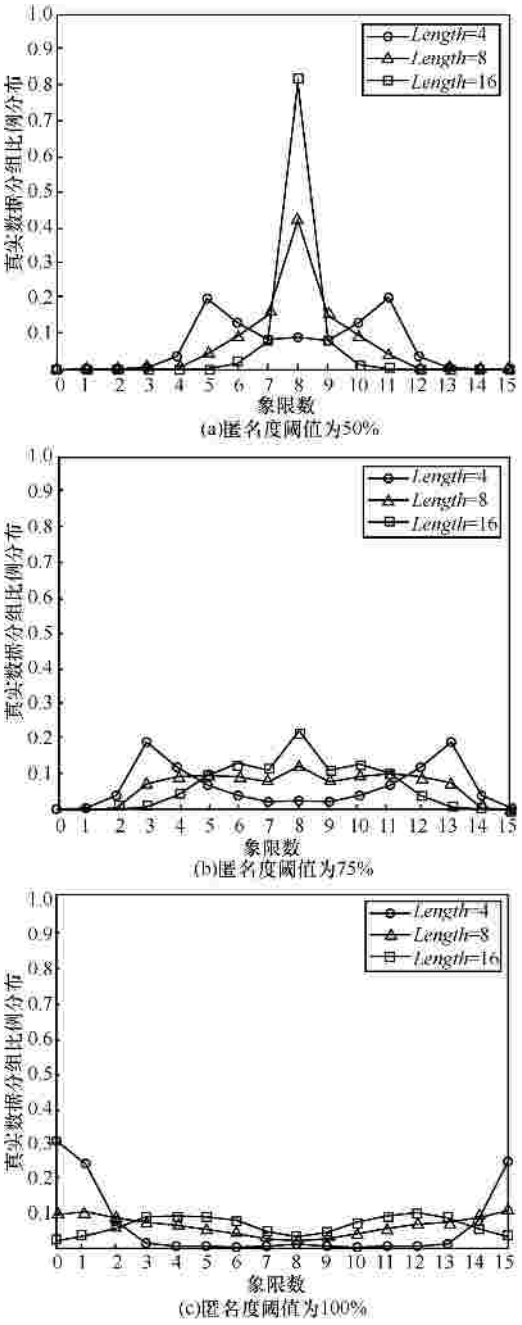

图 8 源象限为 8 的真实数据分组离开混淆环时象限编号分布

当队列长度为 8 时，在不同的匿名度阈值下相比长度为 16 和 4 的曲线波动最小，真实数据分组进入和离开混淆环象限之间的关系最弱，攻击者通过对应关系得到数据分组源象限的可能性也就最低。当队列为 8 时，匿名度阈值为 50%时，比例大

于 0 的区间是[5,11]，共计 7 个，$\frac{7}{16}$~50%；匿名度阈值为 75%时，共计 11 个，$\frac{11}{16}$~75%；匿名度阈值为 100%时，所有区间均有可能，能够较好地反映出匿名度阈值和运动象限之间的关系。因此在之后的仿真实验中，设置队列长度为 8。

在延迟方面，当队列长度为 8 时，不同匿名度需求数据分组混淆延迟分布如图 9 所示，匿名度阈值越高，混淆所需时间期望越大，期望分别为 $E_t(50\%)=5.1$，$E_t(75\%)=13.6$，$E_t(100\%)=27.9$，混淆延迟的累积分布如图 10 所示。约 90%的匿名阈值为 50%的数据分组在 10 s 内完成混淆，约 90%的匿名阈值为 75%的数据分组在 25 s 内完成混淆，对于 100%阈值的数据分组，90%的可能性在 45 s 内完成混淆。

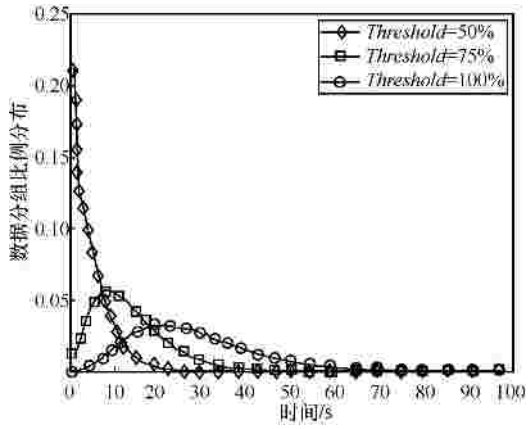

图 9　不同匿名度需求数据分组混淆延迟分布

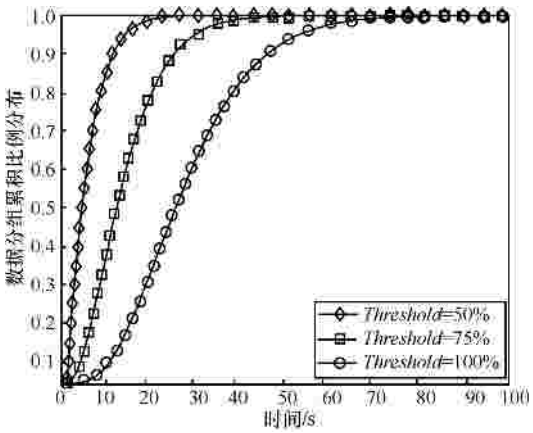

图 10　不同匿名度需求数据分组混淆延迟累积分布

在能耗方面，与普通注入机制 Inject 作对照，比较在相同注入间隔均值 μ=1 下的能耗情况选择不同环作为混淆环时的能耗分布及 Inject 的能耗分布，结果如图 11 所示。每个环作为混淆环时，该环上的能耗出现很高峰值，这是因为混淆环承担了大量密集的数据分组转发，为了优化能耗效率，使能耗充分使用，通过解式(7)计算出表 2 所示的时间比，得到优化后的能耗分布，如图 12 所示，网络在生命周期内有尽可能多的环能耗得以均衡消耗，与普通注入机制的生命周期比是 18:1。随着网络规模的增大，Inject 漏斗效应急剧加重，而 ADRing 能优化能耗，因此在网络规模越大时，同等最大能量情况下，2 种机制相比 ADRing 的生存周期比更大，如图 13 所示。

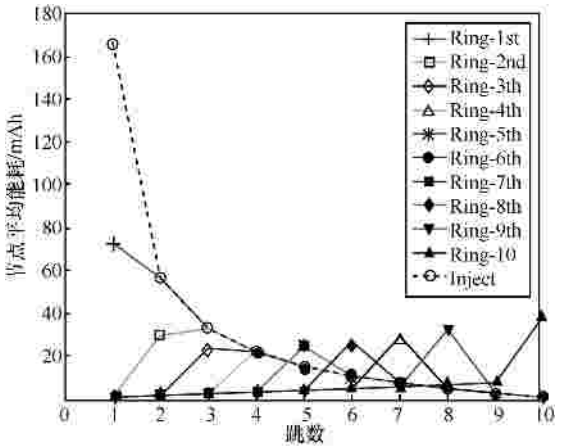

图 11　不同混淆环时各环上节点的平均能耗

表 2　　各环作为混淆环的最优时间比

跳数	时间比
1	14
2	0
3	319
4	0
5	76
6	84
7	101
8	128
9	170
10	234

5.2　安全性分析

在数据分组产生阶段，真实数据分组和虚假数据分组的产生与发送均服从相同的分布，从而使真假数据分组具有了不可区分性，无法定位事件源。

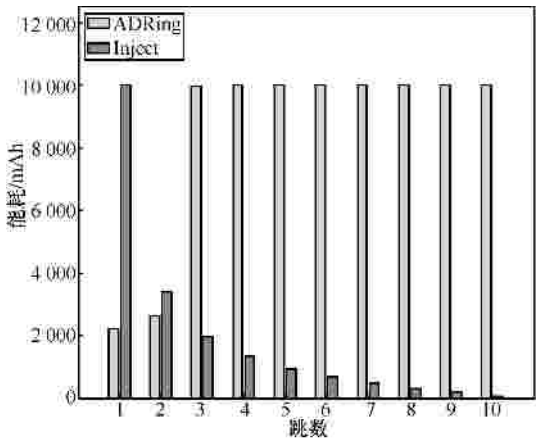

图 12 网络寿命周期内各环的能耗分布

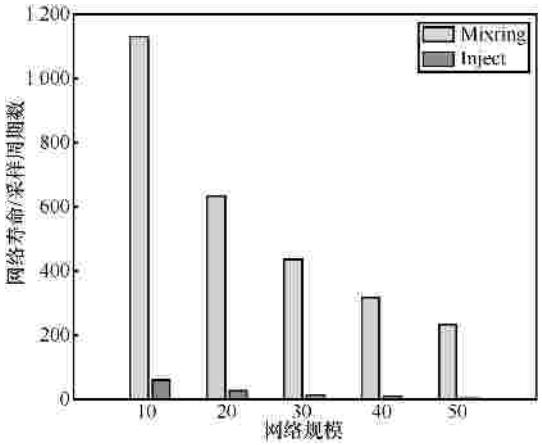

图 13 不同网络规模下节点网络的生存时间

其次，在混淆环阶段，数据分组的源象限标识位表示数据分组与来自哪些象限的数据分组进行了混淆，在达到 100%匿名阈值后，来自所有象限的数据分组与该数据分组进行了混淆，所有节点的行为均相同，使真实数据分组具有了不可追溯性，无法通过流量分析等手段回溯到源节点。

因此，数据分组从源节点产生到基站接收整个过程均能保证源节点的匿名性。

6 结束语

现有的无线传感网源匿名协议大都无法同时兼顾源位置匿名性、延迟和生存周期。针对这一问题，本文提出了面向局部/全局侦听流量分析源匿名攻击的能量均衡高效的基于匿名量化动态混淆环的源位置隐私保护协议 ADRing：首先，在数据产生环节，采用虚假流量注入手段抵抗全局侦听流量分析攻击；其次，在数据传输环节，通过混淆环对数据分组进行混淆，消除了数据分组和源节点之间的相关性，在保证源匿名的前提下，分离了真实数据分组同时削减掉了其余的虚假流量；最后通过动态调整混淆环以均衡网络能耗分布，最大限度延长了网络生存周期。仿真实验结果和理论分析表明：ADRing 一方面能有效抵御具备全网侦听能力的源位置隐私攻击，另一方面能均衡并优化网络能耗与延迟，延长网络生存周期。

参考文献：

[1] WINKLER T, RINNER R. Security and privacy protection i visual sensor networks: a survey[J]. ACM Computing Surveys (CSUR), 2014, 47(1): 1501-1514.

[2] CONTI M, WILLEMSEN J, CRISPO B. Providing source location privacy in wireless sensor networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2013, 15(3): 1238-1280.

[3] OZTURK C, ZHANG Y, TRAPPE W. Source-location privacy in energy-constrained sensor network routing[C]//ACM SASN. Washington, DC, USA, c2004: 88-93.

[4] KAMAT P, ZHANG Y, TRAPPE W, et al. Enhancing source-Location privacy in sensor network routing[C]//IEEE ICDCS. Columbus, OH, USA, c2005: 599-608.

[5] 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 Journal of Computers, 2010, 33(9): 1736-1747.

[6] RAJ M, LI N, LIU D, et al. Using data mules to preserve source location privacy in wireless sensor networks[J]. Journal of Elsevier Distributed Computing and Networking, 2012, 11(2): 309-324.

[7] LI Y, REN J. Source-location privacy through dynamic routing in wireless sensor networks[C]//IEEE INFOCOM. San Diego, California, USA, c2010: 1-9.

[8] YAO L, KANG L, DENG F, et al. Protecting source–location privacy based on multirings in wireless sensor networks[J]. Concurrency Computat Pract Exper, 2013. DOI: 10.1002/cpe.3075.

[9] REN J, TANG D. Combining source-location privacy and routing efficiency in wireless sensor networks[C]//IEEE GLOBECOM. c2011: 1-5.

[10] RIOS R, LOPEZ J. Exploiting context-awareness to enhance source-location privacy in wireless sensor networks[J]. Computer Journal, 2011, 54(10): 1603-1615.

[11] MEHTA K, LIU D, WRIGHT M, Location privacy in sensor networks against a global eavesdropper[C]//IEEE ICNP. Beijing, China, c2007: 314-323.

[12] SHAO M, YANG Y, ZHU S, et al. Towards statistically strong source

anonymity for sensor networks[C]//IEEE INFOCOM. Phoenix, AZ, USA, c2008: 51-55.

[13] ALOMAIR B, CLARK A, CUELLAR J, et al. Towards a statistical framework for source anonymity in sensor networks[J]. IEEE Trans on Mobile Computing , 2013,12 (2): 248-260

[14] CUELLAR J, POOVENDRAN R. Toward a statistical framework for source anonymity in sensor networks[J]. IEEE Trans on Mobile Computing, 2013, 12(2): 248-260.

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

[16] YANG Y, SHAO M, ZHU S, et al. Towards event source unobservability with minimum network traffic in sensor networks[C]// ACM WiSec. Alexandria, Virginia, USA, c2008: 77-88.

[17] MAHMOUD M M, SHEN X S. Secure and efficient source location privacy preserving scheme for wireless sensor networks[C]//IEEE ICC. Ottawa, CANADA, c2012: 1-5.

[18] LIGHTFOOT L, LI Y, REN J. Preserving source-location privacy in wireless sensor network using STaR routing[C]//IEEE Globecom. Miami, Florida, USA, c2010: 1-5.

[19] MAHMOUD M M, SHEN X S. A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks[J]. IEEE Trans on Parallel and Distrib Systems, 2012, 23(10): 1805-1818.

[20] 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.

作者简介：

牛晓光（1979-），男，河北保定人，武汉大学副教授、硕士生导师，主要研究方向为移动计算、无线传感网和信息安全。

魏川博（1990-），男，贵州贵阳人，武汉大学硕士生，主要研究方向为无线传感网和网络安全。

姚亚兰（1995-），女，湖北天门人，主要研究方向为移动计算和隐私保护。