



## 无线传感器网络隐私保护方法<sup>\*</sup>

钱 萍<sup>1,2</sup>, 吴 蒙<sup>3</sup>

(1. 江苏科技大学计算机科学与工程学院 镇江 212003; 2. 南京邮电大学计算机学院 南京 210003;

3. 南京邮电大学通信与信息工程学院 南京 210003)

**摘 要:** 如何保护隐私信息在无线传感器网络的应用过程中不被泄露, 同时能得到较为准确的结果, 是无线传感器网络面临的重大挑战。近年来国内外学者对无线传感器网络的隐私保护技术进行了很多研究, 本文从位置隐私保护和数据隐私保护两方面, 总结了现有的隐私保护方法, 分析了其基本原理和特点。针对现有方法的不足, 本文提出了一种能同时保护位置隐私和数据隐私的隐私保护方法, 该方法基于多节点幻影路由技术和椭圆曲线同态加密技术。与现有技术相比, 该方法具有更好的隐私保护性和更低的能量消耗性。

**关键词:** 无线传感器网络; 隐私保护; 幻影路由; 椭圆曲线同态加密

**doi:** 10.3969/j.issn.1000-0801.2013.01.004

## A Privacy Preserving Method in WSN

Qian Ping<sup>1,2</sup>, Wu Meng<sup>3</sup>

(1. College of Computer Science & Technology, Jiangsu University of Science & Technology, Zhenjiang 212003, China;

2. College of Computer Science, Nanjing University of Posts & Telecommunications, Nanjing 210003, China;

3. College of Telecommunications and Information Engineering,  
Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

**Abstract:** A great challenge to wireless sensor network (WSN) is how to protect privacy from disclosing during application in WSN as well as obtain accurate results. In recent years, researchers at home and abroad have done much work on privacy preserving in WSN. This paper surveyed the general privacy preserving methods from two aspects of location privacy and data privacy in WSN and analyzed their theories and characteristics. A new method based on multi-notes phantom routing protocols and ECC homomorphic encryption was proposed, which could protect location privacy and data privacy at the same time. Compared to current methods, better privacy will be protected and less energy will be consumed.

**Key words:** wireless sensor network, privacy preservation, phantom routing, ECC homomorphic encryption

### 1 引言

近年来, 无线传感器网络 (wireless sensor network, WSN) 的应用日渐广泛, 其安全问题已经越来越多地受到国内外研究者的关注。一方面, 由于传感器节点一般都放

置在无人看管的地点, 因此传感节点面临着容易被攻击者物理俘获、破解和篡改等多方面的安全威胁, 会导致用户及被监测对象的身份、行踪和私密数据等隐私信息暴露; 另一方面, 因为传感器节点的电源能量、通信能力、计算和存储能力等都受到限制, 因此在无线传感器网络中不能采

<sup>\*</sup> 国家重点基础研究发展计划 (“973”计划) 基金资助项目 (No.2011CB302903), 江苏省高校自然科学研究重点基金资助项目 (No.10KJA510035), 南京市重大科技计划基金资助项目 (No.201103003), 江苏省研究生创新工程基金资助项目 (No.CXZZ11\_0404)



用复杂的安全机制,从而使无线传感器网络的安全问题更加突出。无线传感器网络的隐私保护技术是无线传感器安全技术的重要研究方向,是无线传感器网络面临的重大挑战。

通常地讲,隐私保护就是使个人或集体等实体的不愿意被外人知道的信息得到应有的保护。从研究内容的主体来分,无线传感器网络中的隐私问题可分为面向位置的隐私安全和面向数据的隐私安全两个方面<sup>[1]</sup>。

### (1) 位置隐私

定位技术是无线传感器网络中的一项关键性基础技术,其提供的位置信息在无线传感器网络中具有重要的意义,在提供监测事件或目标位置信息、路由协议、覆盖质量及其他相关研究中有着关键性的作用。节点的定位信息一旦被非法滥用,将导致严重的安全和隐私问题。因此位置隐私是无线传感器网络隐私的重要组成部分。

### (2) 数据隐私安全

无线传感器网络的中心任务在于对感知数据的采集、处理与管理,数据隐私是无线传感器网络隐私保护机制中的一个重点研究方向,得到了广泛的研究。面向数据的隐私安全主要包括数据聚合隐私和数据查询隐私。

本文将从位置隐私和数据隐私两个方面对现有的无线传感器网络的隐私保护方法进行分析,针对现有技术的不足,提出有效的可实现位置隐私保护和数据隐私保护的双重保护方法,并讨论今后进一步研究的方向。

## 2 位置隐私保护方法

节点位置信息在无线传感器网络中往往起到标识的作用,位置隐私在无线传感器网络中具有特殊而关键的地位。现有的位置隐私保护技术一般采用基于随机路由策略的路由协议方法,即数据分组的每一次传输并不都是从源节点向汇聚节点方向传输,转发节点会以一定的概率将数据分组向远离汇聚节点的方向传输。同时传输路径不是固定不变的,每一个数据分组的传输路径都随机产生。这样的随机路由策略使得攻击者很难获取节点的准确位置信息。

根据保护范围的不同,位置隐私保护可分为本地位置保护和全局位置保护,下面将从这两个方面展开讨论。

### 2.1 本地位置隐私保护

针对无线传感器网络的位置隐私保护,研究较早的是 Ozturk Celal 等提出的幻影路由协议<sup>[2,3]</sup>。

幻影路由协议中包含了一个“熊猫—猎人”模型,作为恶意攻击方的“猎人”希望通过对 WSN 中无线传播信号的

监测而逐跳追踪获取“熊猫”出现的位置。协议由两阶段构成:第一阶段是直接随机漫步,将报文随机漫步到网络中的一个伪源节点;第二阶段将报文从伪源节点以洪泛路由<sup>[2]</sup>或单路径路由<sup>[3]</sup>的方式路由到 sink 节点(基站节点)。利用伪源节点保护真实源节点的位置隐私。

在第一阶段的过程中,为了达到更好的位置隐私保护效果,应该使伪源节点尽可能地远离真实源节点,要采用定向随机步的方式路由到 sink 节点。所谓定向随机步是指源节点事先知道邻居节点的相对位置,按基于扇形划分<sup>[2]</sup>或基于跳数划分<sup>[3]</sup>的方法把邻居节点分成两类,路由开始时由源节点随机选择一类,沿着这类节点路由到伪源节点。

幻影路由协议基于随机路由策略保护节点的位置信息,但由于参考文献[2]中采用了洪泛技术,使得攻击者能很快地收集位置资源的信息。针对这一不足,国内有研究者提出了幻影路由的改进方法,姚剑波等提出了定向随机幻影路由<sup>[4]</sup>,与洪泛幻影路由不同的是,第二阶段中报文采用定向随机步的方式路由到基站,从而具有更大的安全期和更低的损耗;陈娟等提出了基于源节点有限洪泛的源位置隐私保护协议——PUSBRF 协议<sup>[5]</sup>,该协议能够产生远离真实源节点且地理位置多样性的幻象源节点,与参考文献[3]中的单路径幻影路由相比,产生的随机有向路径数至少增加了 33.33%。

无线传感器网络中的主要资源消耗在通信模块,而路由协议保护方法需要发送大量额外的通信量以实现隐私保护,特别是对于洪泛幻影路由协议来说,洪泛路由的通信开销大,能量消耗多;并且,由于每一个消息都要先路由到幻影节点,这就增加了总的通信时延。

### 2.2 全局位置隐私保护

Li Yun 和 Jian Ren 等提出了可以保护本地和全局源位置隐私的方案<sup>[6]</sup>。该方案由两种方法组成:路由到随机选择中间节点(RRIN)方法和网络混合环(NMR)方法,通过构建一个网络混合环,实现全局位置隐私保护。

RRIN 方法保护本地源位置隐私,与幻影路由协议类似,采用两步路由策略把信息从实际源节点路由到网络混合环上的一个节点,通过一个或多个随机选择的中间节点使攻击者不能通过逐跳路由分析追踪到源节点;NMR 方法中,让数据沿着网络混合环上的节点路由到目的节点区域,从而保护了全局位置隐私。

为了保护 sink 节点的全局位置隐私,参考文献[7]中提出了对抗全局攻击的位置隐私保护方法——DCARPS 匿名路由协议,该协议中提出了一个新的网络拓扑发现方

法,该方法中由 sink 节点负责所有的路由计算,允许 sink 节点获得全局拓扑而不泄露自己的位置信息。

### 3 数据隐私保护方法

现有的数据隐私保护技术中,针对隐私保护数据挖掘的研究比较多<sup>[9]</sup>,主要包括数据扰乱技术、加密技术、随机化技术和安全多方计算技术等,但是有些技术并不适用于无线传感器网络。数据聚合是无线传感器网络中的重要技术,包括和、平均、最大值和最小值等多种聚合计算。本文将主要讨论数据聚合过程中的隐私保护问题。

#### 3.1 基于同态加密技术的 WSN 数据隐私保护方法

基于同态加密技术可以实现无线传感器网络中端到端的数据聚合隐私保护。

同态加密(homomorphic encryption, HE)最初由 Rivest 等人于 1978 年提出<sup>[9]</sup>,是一种允许直接对密文进行操作的加密变换技术,可以实现乘法同态计算。后来由 Domingo 等做了进一步的改进,设计的 Domingo-Ferrer 算法可以实现加法和乘法同态计算。利用同态加密算法的同态性保证了用户可以对敏感数据进行操作但又不泄露数据信息。

在 WSN 的数据聚合过程中,利用同态加密技术可以实现数据的端到端加密,即中间节点可以在不需要解密数据的前提下直接对已加密数据进行聚合,避免了中间节点在解密数据时的隐私泄露,从而保证了数据的隐私性。参考文献[10]中提出了基于 Domingo-Ferrer 算法同态算法的数据聚合隐私保护方法 CDA,该方法的基本原理如图1所示。

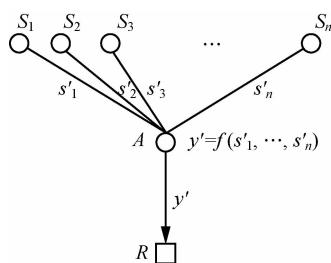


图1 基于同态加密的 CDA 方法

具体实现过程如下。

(1)  $n$  个节点( $S_1$  到  $S_n$ )分别将各自的数据  $s_1$  到  $s_n$  加密后得到  $s'_1$  到  $s'_n$ ,再将加密后的数据发送到中间节点  $A$ :

$$s'_i = E_{(r,g')}(s_i), i=1, \dots, n \quad (1)$$

(2) 节点  $A$  对收到的已加密数据进行聚合后得到  $y'$ ,将  $y'$  发送到目标节点  $R$ :

$$y' = f(s_1, \dots, s_n) \quad (2)$$

(3) 节点  $R$  将收到的  $y'$  解密后得到  $y$ :

$$y = D_{(r,g')}(y') \quad (3)$$

其中,  $(r, g')$  是节点  $S_1, \dots, S_n$  和节点  $R$  共享的密钥,该密钥利用 Domingo-Ferrer 算法得到。可以证明,当选取合适的聚合函数  $f$ (如求平均值计算)时,可以得到:

$$y = f(s_1, \dots, s_n) \quad (4)$$

同态加密方法的优点在于可以实现端到端加密,每一个中间节点不需要解密数据就可以实现聚合,有效地保护了各个节点的隐私数据;不足之处在于同态加密方法一般基于公钥密码体制,计算复杂度高,资源消耗较多。

#### 3.2 基于分簇技术的 WSN 数据隐私保护方法

参考文献[11]中提出了两种用于数据聚合隐私保护的方法——基于分簇的隐私数据保护(CPDA)和基于分片的聚合隐私保护(SMART),这两种方法都是实现数据的“和”聚合计算的。

CPDA 方法的实现包括 3 个步骤。

##### (1) 构建簇

传感器节点利用分布式协议随机地分成多个簇。

##### (2) 簇内数据聚合

每个簇内的节点共享一个非零的数作为种子,簇头节点利用多项式的加法性质,通过节点之间交换数据,实现簇内节点的数据聚合,在实现簇内聚合和时,必须保证每一个节点都不能获得其他节点的隐私数据。

##### (3) 簇间数据聚合

每个簇头节点将聚合后的数据利用路由树协议路由到目的节点。

CPDA 方法中为了保证簇内聚合时每个节点不能获得其他节点的隐私数据,引入的额外计算量大,增加了计算消耗;优点是额外的通信消耗相对较少。从隐私保护性来看,单个簇包含的节点越多,隐私性越好,但计算量越大。

#### 3.3 基于分片技术的 WSN 数据隐私保护方法

参考文献[11]中提出了 SMART 方法,通过把原始数据分片后,再加密路由到目的节点,包括以下 3 个步骤。

##### (1) 分片

每一个源节点首先随机地选择  $h$  跳内的  $J$  个节点形成一个节点集  $S$ ,然后将自己的隐私数据分成  $J$  个小的数据,将分片数据加密后分别发送给节点集  $S$  中的节点。

##### (2) 混合

当某个节点收到加密后的分片数据后,利用共享密钥解密数据,将该节点收到的所有来自不同源节点的数据



据相加。

### (3) 聚合

所有节点将相加后的数据利用路由树协议路由到目的节点。

可以看出,该方法中聚合的中间节点只能获得分片数据,而不能获得原始全部数据,从而保护了数据隐私。

SMART 中需要将分片发送到不同的邻居节点,从而引入了额外的通信量;优点是引入的额外计算量小。总的来说,由于随机化技术在原始数据中引入了噪声,会影响数据聚合结果的准确性。从隐私保护性来看,分片的数据越多,隐私性越好,但通信量越大。

## 4 位置隐私、数据隐私双重保护技术研究

从前面的分析可以看出,无线传感器网络中存在许多能量和资源都受限的传感器节点,而现有的隐私保护技术资源消耗较多,因此需要研究有效的隐私保护方法以实现隐私性和资源消耗性之间的平衡;另一方面,现有的技术只能实现位置隐私或数据隐私的单一保护,缺乏实现双重隐私保护的方法。本文研究如何改进现有技术,提高其算法性能,并提出一种新的可以同时保护位置隐私和数据隐私的方法。

### 4.1 多节点幻影路由技术

如前所述,幻影路由技术中通过幻影伪节点保护真实节点的位置隐私,是一种有效的位置隐私保护方法。本文对幻影路由协议进行改进,设计基于多个随机幻影伪节点的路由方法。

在幻影路由协议中,数据首先采用定向随机步的方法从源节点路由到一个幻影伪节点,再路由到 sink 节点。单幻影伪节点方法主要适用于小型的传感器网络,本文研究基于多幻影伪节点的路由方法,即数据从源节点同时路由到多个同一方向的不同幻影伪节点,再分别从每个幻影伪节点路由到 sink 节点,适用于大型传感器网络。

在路由到伪节点时,采用基于东西方向分类的定向随机步方法<sup>[2]</sup>,即源节点根据事先知道的邻居节点位置信息,把邻居节点分成东西方向两类,如图 2 所示。图 2 中的中心黑色实心节点是源节点,节点 1~8 是其邻居节点,按照东西方向分类后,节点 1~4 是属于东方向节点类,节点 5~8 属于西方向节点类。节点在路由时沿着同一类方向的节点选择路径,以保证伪源节点尽可能的远离真实源节点。经典幻影路由协议中定向随机步的分类方向信息存储在消

息的头部,一旦消息被截获,容易暴露真实源节点的位置,本方法中不在信息中保存分类方向信息,而是由接收节点根据已接收数据的方向来判断出分类方向信息,如图 3 所示,若节点从图 3(a)中所示的几个方向的节点接收到数据,则可判断分类方向是东分类方向,反之分类方向是西分类方向,如图 3(b)所示。

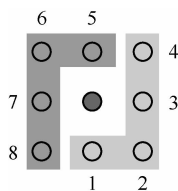


图 2 基于东西方向的随机步分类

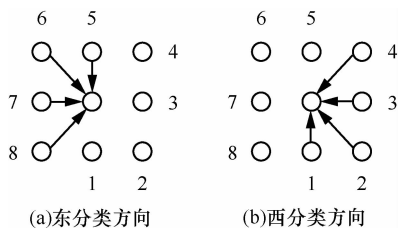


图 3 根据节点接收数据的方向判断分类方向

图 4 是基于多个伪节点的定向随机步路由的示意,图中黑色实心节点为真实源节点,数据发送前由源节点随机确定伪节点的个数以及到达每个伪节点的跳数,并随机选择定向路由方向。数据从源节点出发后,根据选定的路由方向和跳数分别定向路由到不同的伪节点。数据到达伪节点后再以洪泛路由或单路径路由的方式到达 sink 节点。

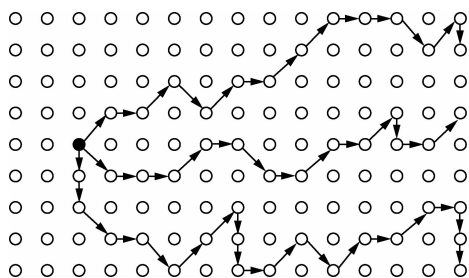


图 4 基于多节点的定向随机步路由

可以看出,多个幻影伪源节点将会增加攻击者追踪到真实源节点的难度,从而比现有的方法能更有效地保护源节点的位置隐私。图 4 中只是一个简单的示意,图中节点个数较少,当该方法用于中大规模的传感器网络时,伪节点的位置分布会更加分散,将起到更好的保护作用。

### 4.2 基于椭圆曲线算法的同态加密隐私保护方法

利用同态加密技术的同态性质可以实现无线传感器

网络中端到端的数据加密隐私保护,但基于 RSA 或 ElGamal 公钥密码体制的同态加密技术计算复杂度较高,不符合无线传感器网络资源受限的特点。1985 年 Koblitz 和 Miller 分别独立地提出了椭圆曲线加密体制(ECC)<sup>[12,13]</sup>, ECC 的安全性建立在椭圆曲线离散对数问题之上,与 RSA 和 ElGamal 相比,在相同的安全要求下,ECC 需要的公钥位数较小,计算速度快。本文研究基于 ECC 的同态加密隐私保护技术。

#### 4.2.1 椭圆曲线加密机制

常用的椭圆曲线方程为:

$$E: y^2 = x^3 + ax + b \quad (5)$$

其中,  $a, b \in F_q, q$  为一个足够大的素数,且  $4a^3 + 27b^2 \neq 0$ 。 $F_q$  上的椭圆曲线  $E$  被定义为由参数  $a$  和  $b$  决定的点  $q = (x, y)$  的集合,此外,  $E$  还包括一个无穷远点  $0$ 。

椭圆曲线的加法准则为: 设  $P(x_1, y_1), Q(x_2, y_2)$  是  $E$  上的两点,过  $P, Q$  的直线  $L$  交  $E$  于  $R(x_3, y_3)$  点,  $R$  点关于  $x$  轴的对称点即为  $P+Q$ , 即  $P+Q = (x_3, -y_3)$ 。在椭圆曲线  $E$  上,对于等式  $Q=kP$  ( $k$  为正整数),由加法准则可以证明由  $k$  和  $P$  计算  $Q$  比较容易,而由  $Q$  和  $P$  计算  $k$  则比较困难。这就是椭圆曲线上离散对数问题,离散对数问题是比整数因子分解问题更难的数学难题。

下面以传感器节点  $S$  向传感器节点  $R$  发送信息  $m$  为例,讨论两种基于椭圆曲线实现加解密的方法。

##### (1) 方法一

①指定椭圆曲线  $E$  上的一点  $G$  作为基点;

②接收传感器节点  $R$  选取一个随机数  $k$  ( $k < n, n$  为基点  $G$  的阶)作为私钥,计算:

$$K = kG \quad (6)$$

其中,  $K$  作为公钥,并将  $K$  广播出去;

③传感器节点  $S$  将待传输的明文编码  $m$  到椭圆曲线  $E$  上一点  $M$ , 选取一个随机数  $r$ , 计算:

$$C_1 = rG \quad (7)$$

$$C_2 = rK + M \quad (8)$$

④节点  $S$  发送消息  $(C_1, C_2)$ ;

⑤传感器节点  $R$  接收到消息后利用自己的私钥  $k$  计算:

$$C = kC_1 = k(rG) = rK \quad (9)$$

⑥节点  $R$  进一步计算:

$$C_2 - C = rK + M - rK = M \quad (10)$$

解码  $M$  得到明文消息  $m$ 。

##### (2) 方法二

步骤①、②与方法一相同,下面从步骤③开始讨论。

③传感器节点  $S$  选取一个随机数  $r, m$  为待传输的明文计算:

$$C_1 = rG \quad (11)$$

$$C_2 = rK \quad (12)$$

$$C_3 = mC_2 \quad (13)$$

④节点  $S$  发送消息  $(C_1, C_3)$ ;

⑤传感器节点  $R$  接收到消息后利用自己的私钥  $k$  计算:

$$kC_1 = k(rG) = rK = C_2 \quad (14)$$

⑥节点  $R$  进一步计算:

$$C_3 C_2^{-1} = m \quad (15)$$

从而得到明文消息  $m$ 。

这两种方法可以分别用于加法同态和乘法同态的计算。

#### 4.2.2 基于 ECC 的同态加密数据聚合

下面利用 4.2.1 节中介绍的两种 ECC 加密方法实现同态加密运算,用于无线传感器网络中的数据聚合隐私保护。节点分布如图 1 所示,节点  $S_1$  到  $S_n$  为发送数据的源节点,节点  $A$  为完成聚合功能的中间节点,节点  $R$  为目的节点。

##### (1) 加法聚合

利用 4.2.1 节中介绍的 ECC 加密方法一可以实现同态加法运算,从而完成数据的加法聚合。具体步骤如下。

①首先由目的节点  $R$  确定椭圆曲线  $E$ 、基点  $G$  和以及私钥  $k$ , 计算出公钥  $K$ , 将椭圆曲线参数、 $G$  和  $K$  都广播出去。

②各源节点  $S_i$  将待传输的明文编码  $m_i$  到椭圆曲线  $E$  上一点  $M_i$ , 选取一个随机数  $r_i$ , 根据式(7)和式(8)计算得到  $C_{1i}$  和  $C_{2i}$ , 发送消息  $(C_{1i}, C_{2i})$ 。

③中间节点  $A$  收到各源节点发送的消息  $(C_{1i}, C_{2i})$  后, 做加法运算后得到  $(\sum C_{1i}, \sum C_{2i})$ , 将其发送给目的节点  $R$ 。

④目的节点  $R$  收到  $(\sum C_{1i}, \sum C_{2i})$  后利用私钥  $k$ , 根据式(9)计算  $C = k \sum C_{1i}$ , 容易证明:

$$k \sum C_{1i} = kG \sum r_i = K \sum r_i \quad (16)$$

再根据式(10)计算:

$$\sum C_{2i} - C = K \sum r_i + \sum M_i - K \sum r_i = \sum M_i \quad (17)$$

从而得到各源节点的加法聚合数据  $\sum M_i$ , 当采用线性编码方式对  $m$  到  $M$  进行编码时, 可以将  $\sum M_i$  直接解码为  $\sum m_i$ , 即加法聚合的明文数据。

##### (2) 乘法聚合

利用 4.2.1 节中介绍的 ECC 加密方法二可以实现同



态乘法运算,从而完成数据的乘法聚合。具体步骤如下。

①首先由目的节点  $R$  确定椭圆曲线  $E$ 、基点  $G$  以及私钥  $k$ ,计算出公钥  $K$ ,将椭圆曲线参数、 $G$  和  $K$  都广播出去。

②各源节点  $S_i$ ,确定待发送明文信息  $m_i$ ,并选取一个随机数  $r_i$ ,根据式(11)、式(12)和式(8)分别计算得到  $C_{1i}$ ,  $C_{2i}$ ,  $C_{3i}$ ,发送消息  $(C_{1i}, C_{3i})$ 。

③中间节点  $A$  收到各源节点发送的消息  $(C_{1i}, C_{3i})$  后,做乘法运算后得到  $(C_{11} \times C_{12} \times \cdots \times C_{1n}, C_{31} \times C_{32} \times \cdots \times C_{3n})$ ,将其发送给目的节点  $R$ 。

④目的节点  $R$  收到  $(C_{11} \times C_{12} \times \cdots \times C_{1n}, C_{31} \times C_{32} \times \cdots \times C_{3n})$  后利用私钥  $k$ ,根据式(14)计算  $k_n \times C_{11} \times C_{12} \times \cdots \times C_{1n}$ ,容易证明:

$$\begin{aligned} k^n \times C_{11} \times C_{12} \times \cdots \times C_{1n} &= k^n \times G^n \times r_1 \times r_2 \times \cdots \times r_n \\ &= K^n \times r_1 \times r_2 \times \cdots \times r_n = C_{21} \times C_{22} \times \cdots \times C_{2n} \end{aligned} \quad (18)$$

当各节点的明文信息是一维数据时,可根据式(15)计算:

$$C_{31} \times C_{32} \times \cdots \times C_{3n} \times C_{21}^{-1} \times C_{22}^{-1} \times \cdots \times C_{2n}^{-1} = m_1 \times m_2 \times \cdots \times m_n \quad (19)$$

从而得到各源节点的乘法聚合数据  $m_1 \times m_2 \times \cdots \times m_n$ 。

可以看出,不管是使用加法聚合还是乘法聚合,都可以实现源节点和目的节点之间的端到端加密,中间节点不需要解密数据就可以实现聚合。

### 4.3 路由协议技术和同态加密技术相结合的双重隐私保护方法

在前面研究内容的基础上,研究一种新的可以同时保护位置隐私和数据隐私的方法。具体实现步骤如下。

(1)sink 节点确定椭圆曲线参数、基点  $G$  和公钥  $K$  等,并将其广播给各节点。

(2)源节点随机确定伪节点的个数  $n$ 、到达每个伪节点的跳数  $h_i$  和定向路由方向。

(3)源节点将数据分成  $n$  片,分片时要根据数据聚合的种类进行分片,加法聚合则按  $m=m_1+m_2+m_3+\cdots$  分片,乘法聚合则按  $m=m_1 \times m_2 \times m_3 \times \cdots$  分片。

(4)根据 4.2.2 节中介绍的数据聚合方法,源节点为每个分片数据选择一个随机数  $r_i$ ,利用公钥  $K$  和  $r_i$  对每个分

片数据进行同态加密。

(5)源节点根据选定的路由方向和跳数将加密后的分片数据分别定向路由到不同的伪节点。

(6)将分片数据从多个不同的幻影伪源节点路由到sink 节点,在路由的过程中,中间节点对数据直接进行加法聚合或乘法聚合,不需要解密数据。

(7)sink 节点收到聚合的加密数据后,利用私钥解密并进行分片重组,加法聚合中重组时直接将解密后的数据相加,乘法聚合中重组时直接将解密后的数据相乘。

### 4.4 性能分析

下面从隐私保护性、能量消耗和时延等方面讨论本文方法的性能。

#### 4.4.1 隐私保护性

与现有的幻影路由技术相比,本文的方法使用了多个随机的幻影伪源节点,使攻击者很难追踪到真实源节点的位置,从而能更好地保护源节点的位置隐私。并且消息头部不包含随机步路由的分类方向信息,能更好地抵抗攻击。本文采用的同态加密方法保护了端到端的数据隐私,基于椭圆曲线的公钥体制中私钥由 sink 节点保管,不在网络中传输,保证了密钥的安全性。本文的方法把幻影路由技术和同态加密技术相结合,能同时保护无线传感器网络的位置隐私和数据隐私。

#### 4.4.2 能量消耗

无线传感器网络中的能量消耗主要包括计算能量消耗和通信能量消耗两个方面,下面从这两个方面分别讨论。

##### (1)计算能量消耗

由于同态乘法技术消耗计算资源较多,下面讨论同态加法计算的性能。本文的同态加法计算主要包括以下几个部分,见表 1。

与标量加法相比,标量乘法耗时很多,因此同态加法聚合过程中计算能量消耗最多的是源节点加密明文数据时,消耗最少的是中间节点聚合数据时,下面以最简单的二进制展开法为例讨论单标量乘法的运算量。

以计算  $kG$  为例,设  $k$  的二进制展开式的长度为  $m$ ,则

表 1 同态加法计算包括的内容

|             | 计算公钥            | 加密明文                   | 加法聚合    | 解密密文                   |
|-------------|-----------------|------------------------|---------|------------------------|
| 完成节点        | 目的节点            | 各源节点                   | 中间节点    | 目的节点                   |
| 标量乘法        | 1 次             | 2 次                    |         | 1 次                    |
| 标量加法        |                 | 1 次                    | $n-1$ 次 | 1 次                    |
| 决定运算速度的主要因素 | 私钥 $k$ , 基点 $G$ | 基点 $G$ , 公钥 $K$ , 明文大小 | 源节点数目   | 私钥 $k$ , 基点 $G$ , 密文大小 |

$k$  和  $kG$  可以表示为:

$$k = \sum_{i=m-1}^0 k_i \times 2^i \quad (20)$$

$$kG = \left( \sum_{i=m-1}^0 k_i \times 2^i \right) G = 2[\cdots 2[2(2k_{m-1}G + k_{m-2}G) + k_{m-3}G] \cdots] + \cdots + k_1G + k_0G \quad (21)$$

其中,  $k_i \in \{0,1\}$ ,  $k_{m-1} \neq 0$ 。可见, 采用二进制法计算  $kG$  共需要  $m-1$  次倍的点运算和  $m/2$  次的点加运算, 运算速度与  $k$  的长度和有限域大小有关。

根据 ECC 加密运算式(7)和式(8)可以判断加密运算速度与密钥长度、有限域长度近似线性相关;解密时根据式(9)可以看出运算速度与密钥长度、有限域长度近似线性相关。

与逐跳隐私保护技术相比, ECC 算法中源节点消耗计算资源将多于基于对称密钥的加密技术, 但对于中间节点, ECC 算法中只需要做加法运算, 消耗资源少, 而逐跳技术中需要对数据先解密, 聚合后再加密, 聚合过程中消耗的计算资源远多于 ECC 加法运算, 因此本文的方法大大降低了中间节点的计算能量消耗, 延长了其寿命;与其他同态公钥技术相比, 椭圆曲线密码系统在计算时间和密钥占用的存储空间上具有一定的优越性, 在提供相同的安全级别的情况下, ECC 所要求的密钥长度比其他的公钥系统短得多, 160 bit ECC 与 1 024 bit RSA、DSA 具有相同的安全强度, 210 bit ECC 则与 2 048 bit RSA、DSA 具有相同的安全强度。

## (2)通信能量消耗

无线传感器网络中的通信消耗包括发送、接收数据的消耗以及数据在网络中传播时的消耗。传播消耗主要和传播距离相关, 因此不管采用哪种隐私保护数据聚合方法, 其传播消耗是相近的。发送和接收数据的消耗主要和发送、接收数据的大小呈线性关系, 这类消耗发生在以下几处:

- 源节点发送密文数据;
- 中间节点接收密文数据;
- 中间节点发送聚合数据;
- 目的节点接收聚合数据。

可见这类消耗主要由密文的大小决定。ECC 算法中得到的密文是根据式(7)和式(8)计算得到的  $C_1$  和  $C_2$ ,  $C_1 = rG$ ,  $C_2 = rK + M = rkG + M$ , 其中  $M$  是明文  $m$  编码到椭圆曲线  $E$  上的点, 可以看出密文的大小将大于明文大小, 其大小主要由明文大小和有限域长度决定。表 2~表 4 列出了用椭圆

曲线算法对不同大小的明文进行加密后密文的大小。对于 RC5 算法, 加密后的密文大小与明文大小基本一样。

表 2 有限域长度为 200 bit, 不同密钥长度时, 256 byte 明文的密文大小

| 密钥长度 (bit)  | 128 | 64  | 32  |
|-------------|-----|-----|-----|
| 密文大小 (byte) | 924 | 896 | 920 |

表 3 密钥长度为 64 bit, 不同有限域长度时, 256 byte 明文的密文大小

| 密钥长度 (bit)  | 200 | 150 | 100 |
|-------------|-----|-----|-----|
| 密文大小 (byte) | 896 | 700 | 476 |

表 4 密钥长度为 64 bit, 有限域长度 150 bit 时, 不同大小的明文的密文大小

| 明文大小 (byte) | 1   | 32  | 64  | 128 | 256 | 512   |
|-------------|-----|-----|-----|-----|-----|-------|
| 密文大小 (byte) | 100 | 100 | 200 | 396 | 700 | 1 260 |

综上, 与逐跳加密技术相比, ECC 算法中密文比明文要大, 在源节点发送密文数据、中间节点接收和发送数据, 目的节点接收数据时都将比 RC5 算法消耗更多的通信资源, 但是当明文数据为少量数据时, 增加的密文数据大小并不多, 相应消耗的额外通信资源也较少;与其他公钥体制相比, 对于短消息加密, 椭圆曲线密码系统所要求的带宽要低得多。本文中将数据分片后传输, 因此发送的明文数据量并不大, ECC 加密产生的额外通信量也是有限的。

## 4.4.3 时延少

无线传感器网络中的时延主要包括数据发送时延、每个中间节点的处理时延以及网络中的传播。不管采用哪种隐私保护技术, 数据在网络中的传播时延都是近似的, 因此主要考虑发送时延和处理时延。下面比较本文方法与基于 RC5 的逐跳加密技术的。

仿真实验环境为 Intel Core2 Duo CPU 1.8 GHz, 内存 2 GB 的 PC 机, Windows XP SP2 操作系统。取大小分别为 1 byte、32 byte、64 byte、128 byte、256 byte 和 512 byte 的文本文件作为待加密的明文, 通过改变有限域大小和私钥长度得到的椭圆曲线加密、解密和加法聚合的计算时间见表 5~表 8。

当采用 RC5 加密体制进行逐跳数据聚合时, 对 256 byte

表 5 密钥长度为 64 bit, 有限域长度 150 bit 时, 不同大小的明文的加解密时间

| 明文大小 (byte) | 1  | 32  | 64  | 128 | 256 | 512 |
|-------------|----|-----|-----|-----|-----|-----|
| 加密时间 (ms)   | 94 | 109 | 172 | 252 | 360 | 577 |
| 解密时间 (ms)   | 32 | 47  | 93  | 171 | 234 | 375 |



表 6 有限域长度为 200 bit,不同密钥长度时,  
256 byte 明文的加解密时间

|           |     |     |     |
|-----------|-----|-----|-----|
| 密钥长度(bit) | 128 | 64  | 32  |
| 加密时间(ms)  | 766 | 453 | 266 |
| 解密时间(ms)  | 484 | 265 | 126 |

表 7 密钥长度为 64 bit,不同有限域长度时,  
256 byte 明文的加解密时间

|            |     |     |     |
|------------|-----|-----|-----|
| 有限域长度(bit) | 200 | 150 | 100 |
| 加密时间(ms)   | 453 | 360 | 297 |
| 解密时间(ms)   | 265 | 234 | 172 |

表 8 明文大小为 256 byte 时,不同密钥长度,  
不同有限域长度的加法时间

|            |       |       |       |       |      |
|------------|-------|-------|-------|-------|------|
| 有限域长度(bit) | 200   | 200   | 200   | 150   | 100  |
| 密钥长度(bit)  | 128   | 64    | 32    | 64    | 64   |
| 加法时间(ms)   | 0.287 | 0.292 | 0.288 | 0.228 | 0.17 |

明文加密和解密的时间分别为 3.8 ms 和 3.57 ms, 加法的时间可忽略。

从以上的数据可以看出,ECC 同态加密和解密的时间与明文大小、密钥长度以及有限域长度有关。在保证安全性的前提下,减少有限域长度和密钥长度,可以有效地减少加解密时间。ECC 加法聚合运算时间比加解密时间要少得多,相差了多个数量级,即中间节点的聚合时间较少。RC5 算法的加解密时间远小于 ECC 同态加解密时间,其加法运算时间更是可以忽略。但是基于 RC5 的逐跳算法中,中间节点需要对每个数据都进行加解密,当需要聚合的节点数较多时,中间节点的处理时延将会大于 ECC 同态加密技术。并且,本文方法中将数据分片后在网络中传输,分片数据的发送时延和处理时延与完整数据相比都比较少。

## 5 结束语

无线传感器网络是一种与应用相关的网络,随着无线传感器网络应用的日益增多,其面临的隐私威胁也更加复杂,因此解决好无线传感器网络的隐私保护问题是其能得到大规模应用的关键。本文从数据隐私保护和位置隐私保护两个方面出发,对现有的无线传感器网络隐私保护方法进行了总结和分析,并在此基础上提出了一种新的无线传感器网络隐私保护方法。该方法包含了基于多节点幻影路由技术的位置隐私保护方法和基于椭圆曲线算法的同态加密技术的数据隐私保护方法,并且将两种方法相结合以实现位置隐私和数据隐私的双重保护。

## 参考文献

- Li N, Zhang N, Das Sajal K, *et al.* Privacy preservation in wireless sensor networks: a state-of-the-art survey. *Ad Hoc Networks*, 2009, 7(8): 1501~1514
- Celal O, Zhang Y Y, Wade T. Source-location privacy in energy-constrained sensor network routing. *Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks*, Washington, DC, USA, 2004:88~93
- Kamat P, Zhang Y, Trappe W, *et al.* Enhancing source-location privacy in sensor network routing. *Proceedings of 25th IEEE International Conference on Distributed Computing Systems*, Columbus, OH,USA, 2005:599~608
- Yao J B, Wen G J. Preserving source-location privacy in energy-constrained wireless sensor networks. *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops*, (ICDCS Workshops), Beijing, China, 2008: 412~416
- 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. *计算机学报*, 2010, 33(9): 1736~1746
- Ren J, Li Y, Li T T. Routing-based source-location privacy in wireless sensor networks. *Proceedings of 2009 IEEE International Conference on Communications*, Dresden, Germany, 2009
- Pietro R D, Alexandre V. Location privacy and resilience in wireless sensor networks querying. *Computer Communications*, 2011, 34(3)
- 钱萍, 吴蒙. 同态加密隐私保护数据挖掘方法综述. *计算机应用研究*, 2011, 28(5): 1614~1617
- Rivest R L, Adleman L, Detrouzos M L. On data banks and privacy homomorphism. *Foundations of Secure Computation*, 1978: 169~179
- Westhoff D, Girao J, Acharya M. Concealed data aggregation for reverse multicast traffic in sensor networks: encryption, key distribution, and routing adaptations. *IEEE Transactions on Mobile Computing*, 2006, 5(10): 1417~1431
- He W, Liu X, Nguyen H, *et al.* PDA: privacy-preserving data aggregation in wireless sensor networks. *Proceedings of 26th IEEE International Conference on Computer Communications (Infocom 2007)*, Anchorage, Alaska, USA, 2007: 2045~2053
- Koblitz N. Elliptic curve cryptosystems. *Mathematics of Computation*, 1987(48): 203~309
- Miller V S. Use of elliptic curves in cryptography. *Proceedings of CRYPTO 1985*, California, USA, 1985: 417~426

[作者简介] 钱萍,女,江苏科技大学讲师,南京邮电大学博士研究生,主要研究方向为网络安全、隐私保护。吴蒙,男,南京邮电大学教授、博士生导师,主要研究方向为无线通信、信息安全。

(收稿日期:2012-09-24)