doi:10.3969/j.issn.1000-436x.2014.11.018

# 安全的 WSN 数据融合隐私保护方案设计

赵小敏，梁学利，蒋双双，陈庆章
(浙江工业大学 计算机科学与技术学院，浙江 杭州 310023)

**摘 要**：针对无线传感器网络数据融合过程中的数据隐私和完整性保护问题，提出一种安全的数据融合隐私保护方案(SPPDA)，把节点的私密因子与原始数据构成复数，采用同态加密方法对复数进行加密，实现在密文不解密的情况下进行数据融合，同时采用基于复数的完整性验证方法，确保数据的可靠性。理论分析和仿真结果表明，SPPDA 方案的计算代价和通信开销较少，数据融合的精确度高。
**关键词**：无线传感器网络；数据隐私；数据融合；完整性
**中图分类号**：TP393 **文献标识码**：A **文章编号**：1000-436X(2014)11-0154-08

# Design of secure privacy-preserving data aggregation scheme for wireless sensor network

ZHAO Xiao-min, LIANG Xue-li, JIANG Shuang-shuang, CHEN Qing-zhang
(College of Computer Science & Technology, Zhejiang University of Technology, Hangzhou 310023, China)

**Abstract:** A secure privacy-preserving data aggregation (SPPDA) scheme was proposed to preserve data privacy and integrity during data aggregation in wireless sensor network. Firstly, a complex number is composed from the private factor of the nodes and the original data; then the complex number is encrypted with homomorphic encryption method,which can realize the data aggregation in the case of not decrypt ciphertext. Also,the reliability of date is ensued by using integrity verification method based on complex.Theoretical analysis and simulation results show that computational cost and communication overhead of the SPPDA are less, and accuracy of data aggregation results is high.
**Key words:** wireless sensor network; data privacy; data aggregation; integrity

## 1 引言

无线传感器网络（WSN, wireless sensor network）是由大量部署在监测区域内具有感知能力、计算能力、数据处理能力及无线通信能力的低功耗微型传感器节点形成的网络，其目的是实时采集、处理和传输监测区域内感测对象的信息并报告给用户[1]，在动植物监测、医疗卫生、智能交通、智能家居、国防军事等领域具有广阔的应用前景[2]。随着 WSN 的广泛应用，数据隐私保护问题也日益突出[3]。在实际应用过程中存在着严重的隐私数据泄露或被篡改的风险，攻击者可以通过窃听、加入伪造或非授权的传感器节点等方式获取敏感信息。比如，在野生动物监测应用中，野生动物的位置信息可能被用于非法捕猎[4,5]；在医疗应用领域，患者的体征敏感数据可能被泄露用于非法行医[6]；在车载传感网络应用中，车辆位置和运动轨迹等敏感信息可能被泄露用于非法跟踪[7]；在智能家居领域，水电煤等远程抄表数据可能被泄露用于分析该户居民的作息规律和收入水平；在军事应用领域，重要数据、基站或事件源位置等敏感信息泄露可能造成严重后果[8]。

**收稿日期**：2014-10-05；**修回日期**：2014-11-05
**基金项目**：国家自然科学基金资助项目(61379023)；浙江工业大学自然科学基金资助项目(2012XZ010)；浙江省公益性技术应用研究计划基金资助项目(2014C33073)
**Foundation Items:** The National Natural Science Foundation of China (61379023); The Natural Science Foundation of Zhejiang University of Technology(2012XZ010); Science and Technology Research Project of Zhejiang Province(2014C33073)

因此，在 WSN 的实际应用中急需解决数据隐私保护问题[9~11]。

WSN 中的传感器节点一般用多跳的方式将采集到的信息传送给 sink 节点（汇聚节点），若每个节点都将自己采集到的原始数据单独地传输给 sink 节点，势必会使网络中存在大量的冗余信息，从而浪费大量的能量资源和通信带宽。解决这个问题的方法之一是数据融合。数据融合是将采集到的多份原始数据信息进行去除冗余处理，整合出符合用户需求数据的过程，以达到减少网络中的数据通信量和提高信息收集效率的目的。

针对 WSN 数据融合过程中的隐私保护问题，本文提出了一种安全的数据融合隐私保护方案(SPPDA, secure privacy-preserving data aggregation)。节点的私密因子与原始数据构成复数，采用同态加密方法对复数进行加密，在不解密的情况下对密文进行融合，降低了计算开销，减少了时延。同时采用基于复数的完整性验证方法，确保数据的可靠性。

## 2　相关工作

在典型的 WSN 应用中，传感器节点通常是资源受限和能量有限的。为了节省资源和能量，避免网络中出现大规模的通信数据，应将数据进行融合去除冗余信息，从而减少带宽和节约能量。在很多实际的应用中，数据融合过程需解决隐私保护问题。文献[12]提出了 CPDA(cluster-based private data aggregation)协议和 SMART(slice-mix-aggRegaTe)协议，对网络传输中的传感器节点数据提供了隐私保护。但是这 2 个协议都存在计算开销和通信开销过大的问题，且没有提供对数据的完整性保护。针对 CPDA 协议不能提供数据完整性的问题，文献[13]提出了 iCPDA(cluster-based protocol to enforce integrity and preserve privacy in data aggregation)协议。文献[14]提出了 KIPDA (*k*-indistinguishable privacy-preserving data aggregation)协议，通过在一组伪装数据中隐藏原始的感测数据，使感测数据是 *K* 不可分的，从而达到隐私保护的目的。文献[15]对 SMART 协议进行了改进，采用逐跳的数据融合方式和节点到节点的加解密模式，降低了计算复杂度和数据传输量。

针对 CPDA 协议中计算开销大的问题，文献[16]提出了一种对 CPDA 算法改进的方案，以减小 CPDA 协议中的计算开销和通信开销。文献[17]指出了 CPDA 协议存在的安全脆弱性，提出了由恶意的簇头节点或簇成员节点发起的攻击，给出了应对这 2 种攻击的解决方法。Bista 等分析了 iPDA[18]和 iCPDA 2 个协议的缺点，提出了 DCIDA（data confidentiality and integrity for data aggregation）协议[19]，实现了数据的私密性和完整性保护，提供了逐跳的完整性验证。Chen 等[20]提出了 RCDA(recoverable concealed data aggregation)协议，通过给每一个传感器节点分配密钥和对其感知数据进行签名，来解决 CPDA 协议中基站不能恢复所有传感器节点感测数据的问题。文献[21]提出了节能的 PEPPDA 算法，该算法运用同态加密算法，减少系统时延，并保证系统的数据新鲜性(data freshness)，即系统的数据均是最新的数据，能够检验出旧数据，以应对重放攻击。文献[22]提出了可恢复的 EERCD 方案，可以实现多种融合函数的查询，但由于可恢复数据，通信量较大。

Ozdemir 等[23]提出了 IPHCDA(integrity protecting hierarchical concealed data aggregation)协议，采用椭圆曲线同态加密算法对数据加密，同时对融合数据求 MAC 值来认证完整性。IPHCDA 协议可以收集多个监测区域的融合数据，且可以在基站将它们分离出来。由于使用椭圆曲线加密算法，IPHCDA 协议计算复杂度大，且加密时采用指数运算，导致密文数据变大，增加了通信开销。另外，IPHCDA 仅对融合结果进行完整性验证，却无法保证数据融合阶段的完整性。本文提出的 SPPDA 方案，将感测的原始数据与私密因子构成复数，其中原始数据为实部，私密因子为虚部，对实部和虚部分别采用加法同态加密算法进行加密，加密过程简单，且密文不大。相较于 IPHCDA，通信量更低，计算更简单。利用复数的可加性，对数据进行融合，实部的融合结果即是所求的内容，而虚部的融合结果用以完整性验证，保证了数据从融合到传输直至 sink 节点阶段的完整性，融合结果比 IPHCDA 更可靠。

## 3　方案设计

### 3.1　网络模型

在 SPPDA 方案中，数据通过一棵以 sink 节点为根的融合树进行数据融合，其中 sink 节点的计算

能力、存储能力、能量等资源充足。假设 WSN 由 3 种节点组成：sink 节点（基站或者查询节点）、融合节点和叶子节点。sink 节点主要负责接收用户的查询命令，接收融合结果并认证结果的完整性，决定是否接受该融合结果。融合节点负责收集叶子节点的数据，与自身的数据融合后沿着融合树上传结果。叶子节点监测周围环境，并将感测的数据上传给融合节点。

定义融合函数为 $y(t)=f(d_1(t),d_2(t),\cdots,d_N(t))$，其中，$d_j(t)(j=1,2,\cdots,N)$ 为节点 $j$ 在 $t$ 时刻收集的数据。典型的融合函数有 sum、average、max 等。为讨论方便，本文仅采用 sum 函数，记为 $f(t)=\sum_{j=1}^{N}d_j(t)$。

当数据从传感器节点传输到 sink 节点时，如无安全与隐私保护机制，数据可能泄露给恶意节点或者非信任的邻居节点。为避免非信任节点加入错误的数据到网络中，通过同态加密和完整性验证，保证数据的私密性和可靠性。

在窃听攻击中，攻击者试图窃听通信信道获取私密信息。窃听分为 2 种：内部窃听和外部窃听。内部窃听者一般是信任的节点或者被俘获的节点，它们可以截获发到其他节点的私密数据。本文通过同态加密数据阻止内部和外部窃听。针对恶意节点注入错误数据而影响融合结果的情况，通过验证融合结果的完整性来保证数据的可靠性。

### 3.2 方案描述

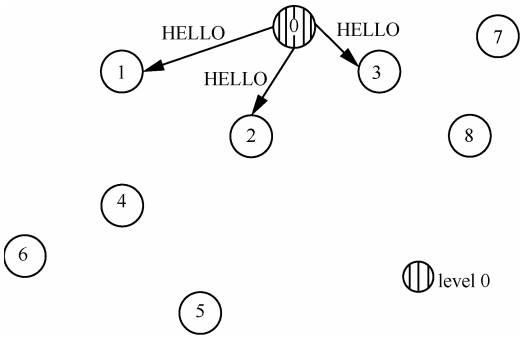
SPPDA 方案包括密钥分发、融合树构建、数据融合和完整性验证等 4 个阶段，本节将对这 4 个阶段进行描述。

1) 密钥分发阶段

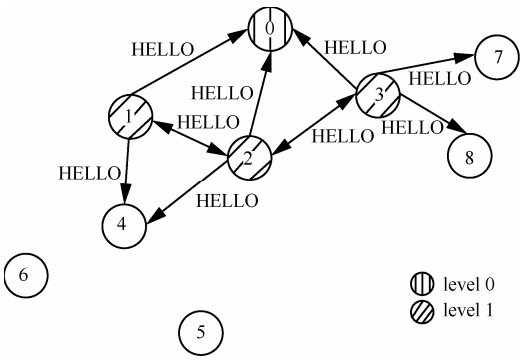
节点被部署至监测区域前，首先从 sink 节点那里获得密钥（$k_j$，$M$，$s_j$）。为了保证数据的私密性，$k_j$ 和 $s_j$ 由 RC4 算法生成。在节点数为 $N$ 的网络中，$M$ 可取为 $2^{\lceil \mathrm{lb}(\mathrm{MAX}(m_j)N)\rceil}$，其中，MAX($m_j$)表示原始数据可能的最大值。节点采集到原始数据 $m_j$ 后与 $s_j$ 组成复数 $R_j=m_j+s_ji$。节点 $j$ 利用 $k_j$ 和 $M$ 对复数 $R_j$ 进行加密得到 $c_j=Enc(R_j, k_j, M)$。根据复数的可加性，数据融合时，实部与实部融合，虚部与虚部融合。当融合结果到达 sink 节点时，sink 节点对结果先解密，然后通过虚部进行完整性验证，实部即是最终的融合结果。

2) 融合树构建阶段

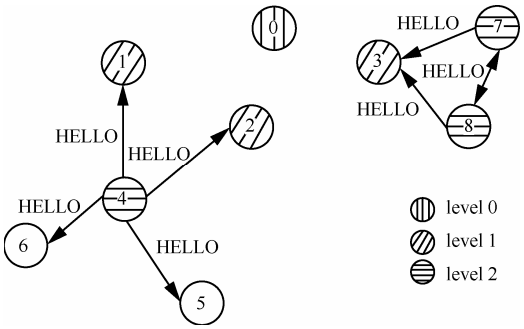
构建融合树分 3 步完成，图 1 中的(a)~(d)描述了节点数 $N=8$ 时，融合树的构建过程。



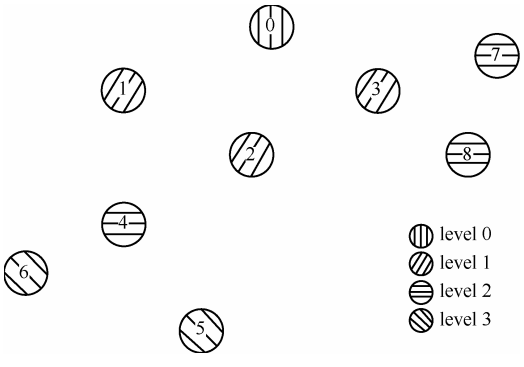

(a) level 0 广播 HELLO 数据分组




(b) level 1 广播 HELLO 数据分组




(c) level 2 广播 HELLO 数据分组




(d) 融合树构建结果

图 1 融合树构建过程

**Step1**　sink 节点将自己的 level 标记为 0，记为 Lv，然后在网内广播一个包含自身 level 等级 Lv 的 HELLO 数据分组。

**Step2**　节点首次收到 HELLO 数据分组，则记录下 HELLO 数据分组的源地址，将其作为自己的父节点，并读取其中的 Lv，加 1 后作为自己的 level 值 Lv，然后广播一个含有自身 Lv 的 HELLO 数据分组。如果节点已经接收过 HELLO 数据分组，则忽略该数据分组。

**Step3**　节点重复 Step2，直至设定的时间片（建树时间片）耗尽为止。

3) 数据融合阶段

数据融合阶段开始时，各节点首先对原始数据进行加密。加密过程如下

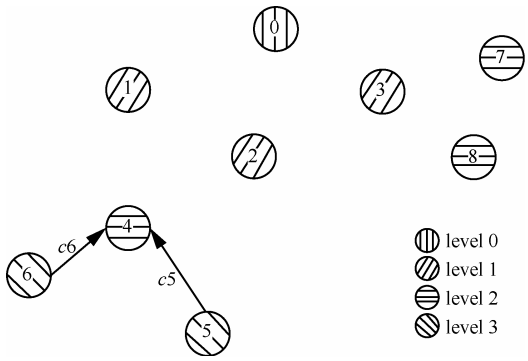
$$\begin{aligned} c_j &= Enc(R_j, k_j, M) \\ &= Enc(m_j + s_j i, k_j, M) \\ &= Enc(m_j, k_j, M) + Enc(s_j i, k_j, M) \\ &= (m_j + k_j (\bmod M)) + (s_j + k_j (\bmod M))i \end{aligned}$$

其中，$c_j$ 表示加密后的数据，$m_j$ 为节点的原始数据，$k_j$、$s_j$ 和 $M$ 是从 *sink* 节点获得的密钥。

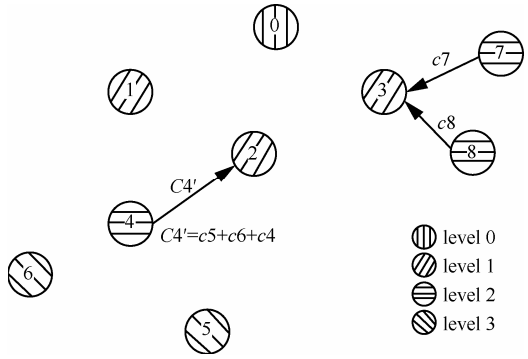
节点加密后，根据节点在融合树中的等级 level，分层次地进行数据融合。首先从等级高的节点开始融合，即 Lv 大的节点，子节点在本等级的融合阶段将自己的加密数据发送到父节点进行融合，父节点收到融合数据后，融合自己的加密数据后发送给它的父节点。设数据融合的节点数为 $N$，融合表达式如下

$$\sum_{j=1}^{N} c_j = \sum_{j=1}^{N} (m_j + k_j (\bmod M)) + \sum_{j=1}^{N} (s_j + k_j (\bmod M))i$$

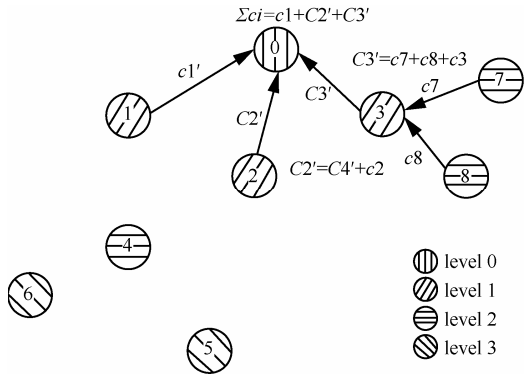
数据融合的过程如图 2 所示。假设 4 号节点的父节点为 2 号节点，融合从 level 值高的层开始，逐步向低层融合，直到融合数据到达 *sink* 节点。图 2(a)中节点 5 和 6 为 level3 的节点，首先使用自己的密钥将传感数据加密后上传至父节点，父节点将收到的数据和自身的加密数据进行求和融合，该层的时间片耗完后，开始下一层的融合，即 level2。图 2 (b)中 level2 层的节点将自身的数据（如果是叶子节点，则是自身的加密数据；如果是非叶子节点，则是其子节点的加密数据与其自身加密数据融合后的数据）发送至其父节点。图 2(c)是 level1 层节点的数据融合，融合结果到达 sink 节点，数据融合结束。




(a) level 3 节点数据融合




(b) level 2 节点数据融合




(c) level 1 节点数据融合

图 2　节点数据融合过程

4) 完整性验证阶段

完整性验证阶段主要是 sink 节点对融合的结果进行解密并验证其完整性的过程。sink 节点接收到的数据由传感数据密文融合值和用于完整性认证的私密因子密文融合值组成，解密时先将这 2 个数值分离，然后分别解密。设 $K=\sum k_j$，$S=\sum s_j$，则

$$\begin{aligned} sum &= Dec(\sum_{j=1}^{N} (m_j + k_j (\bmod M)), K, M) \\ &= \sum_{j=1}^{N} (m_j + k_j (\bmod M)) - K (\bmod M) \end{aligned}$$

$$S' = Dec(\sum_{j=1}^{N}(s_j + k_j(\bmod M))\ ,K,M)$$

$$= \sum_{j=1}^{N}(s_j + k_j(\bmod M))\ -K(\bmod M)$$

sink 节点首先计算 $S$ 的值，如果$|S-S'|\leqslant\delta$，$\delta$ 是sink节点根据实际情况和完整性等级要求而设定的阈值，则表示该融合结果可以接受，即原始数据的融合结果为 *sum*；否则，说明融合结果不可靠，在融合过程中被篡改或者传输时发生错误，应当舍弃该融合结果。

## 4 性能分析

从隐私保护性、通信量、计算开销、精确度、完整性和与已有加密算法的比较等 6 个方面评估SPPDA 方案的性能，并与经典的 IPHCDA 和 iPDA 算法进行了比较分析。采用基于 TinyOS 的 TOSSIM 仿真软件，设置背景噪声为−105 dBm，高斯白噪声为 4 dB。

### 4.1 隐私保护性

在 SPPDA 方案中，传感器节点将采集到的数据与自身的私有数据通过求和与取模运算进行隐藏，并与从 sink 节点获得的私密因子形成一个复数形式的自定义数据。$k_j$ 和 $s_j$ 由 RC4 算法生成，RC4 的安全性保证了 $k_j$ 和 $s_j$ 的安全性，即使传感器节点被攻击者窃听或破解，由于无法通过查询服务器获知传感器节点自身的隐私数据（$k_j$，$M$，$s_j$），也就无法恢复出传感器节点真实的私有数据。在这种情况下，SPPDA 方案中任意一个节点的隐私数据被破解的概率几乎为 0。因此，在 sink 节点不被窃听或捕获的情况下，SPPDA 方案可以满足隐私保护的要求。

### 4.2 通信量

设在 50×50 的区域中随机播撒 20、40、60、80 和 100 个节点，对 SPPDA、IPHCDA 和 iPDA 算法仿真测试发送的数据以评估通信量，仿真结果如图 3 所示。由图 3 可以看出， SPPDA 方案相较于 IPHCDA 算法，通信量平均减少了近 2/3，而 SPPDA 的通信量是 iPDA（$l$=2）的 20%～25%。

SPPDA 方案和 IPHCDA 算法的通信量相差巨大的原因是 2 个算法的加密过程引起的。在 SPPDA 中，$c_j = Enc(m_j, k_j, M) = m_j + k_j(\bmod M)$ 由于只是加了一个密钥 $k_j$，然后对 $M$ 取模，所以密文不会太大。而 IPHCDA 算法加密过程采用如下公式

$$c = P_Z^m + h^r \tag{1}$$

式(1)对 $P_Z$ 求 $m$ 次幂，使密文数值较大，导致无法一次发送，需分多次发送，从而大大增加了通信量。比如在 TinyOS 协议中，MAC 层最大有效负载是 39 byte，一次可传输 30 byte 的数据。对于椭圆曲线算法来说，密文大小普遍超过 30 byte，所以节点在传输密文时往往分多次传送。

iPDA 算法通过分片和重组保护数据的隐私，建立不相交的融合树保护数据完整性。该算法构建了 2 棵融合树，分别称为红融合树和蓝融合树。分片 $l$=2 时，由于要分别向红融合树和蓝融合树发送数据，所以一个节点的数据相当于被分成了 4 片，从而使通信量大大增加了。

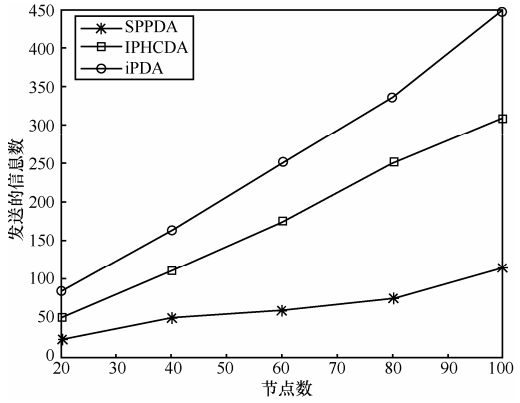



图 3 通信开销

### 4.3 计算开销

iPDA 与 IPHCDA 都是采用端到端的加密算法，节点需要完成加密和数据融合等计算。在融合阶段都是对密文进行求和操作，所以这 2 种方案在融合阶段计算复杂度相当。而在数据加密阶段，SPPDA 方案只有一个求和操作和一个取模操作，计算开销比较小，而 IPHCDA 算法有求幂运算，运算较为复杂。因此，SPPDA 方案的计算开销比 IPHCDA 和 iPDA 算法少。

下面对 IPHCDA、iPDA 和 SPPDA 的计算开销做进一步分析。这里分 2 种情况来分析计算开销：1)普通节点（即叶子节点）的计算开销；2) 融合节点的计算开销。设 $\alpha$、$\beta$、$\gamma$ 和 $\delta$ 分别表示加减运算、乘除运算、指数运算和其他运算的计算开销。假定有 A、B、C 3 个节点，其中，A 是融合节点，B 和 C 是普通节点。节点的计算开销定义为加减运算、乘除运算、指数运算和其他运算的开销之和，表示为

$$C_{\text{ovh}} = \alpha + \beta + \gamma + \delta \tag{2}$$

1) IPHCDA 的计算开销

IPHCDA 算法中的普通节点执行以下操作：生成随机数 $r_j$，计算 $P^{mj}$ 和 $h^{rj}$ 的值。设 $\delta$ 表示生成随机数 $r_j$ 的计算开销，则普通节点的计算开销可以表示为

$$C1_{\text{IPHCDA}} = 2\gamma + \delta \tag{3}$$

对于簇头节点，其加密计算开销与普通节点相同；融合 B、C 节点数据与自身数据的操作需要 4 次乘法运算，包括 2 次 $P^{mj}$ 融合乘法运算和 2 次 $h^{rj}$ 融合乘法运算。设 $\delta_1$ 表示生成随机数 $r_j$ 的计算开销，$\delta_2$ 表示计算融合结果 MAC 值的开销，所以融合节点（这里指簇头）的计算开销表示为

$$C2_{\text{IPHCDA}} = 4\beta + 2\gamma + \delta_1 + \delta_2 \tag{4}$$

所以，IPHCDA 总的计算开销为融合节点 A 和 2 个普通节点 B 和 C 的计算开销之和

$$C_{\text{IPHCDA}} = 4\beta + 6\gamma + 2\delta + \delta_1 + \delta_2 \tag{5}$$

2) iPDA 的计算开销

设节点 A、B、C 属于红融合树，数据分片 $l$=2，则节点收到分片的平均值为 $n(l-1)/n=l-1$，融合这些分片需要 $l-1$ 次求和操作。对于普通节点，要分片 2 次，分别用以红融合树和蓝融合树，共需 2 次减法运算。如果收到蓝融合树的一个分片，需要进行 1 次加法运算；红融合树融合需要 1 次加法运算。设 $\delta$ 表示加密运算的计算开销，则普通节点的计算开销可表示为

$$C1_{\text{iPDA}} = 4\alpha + \delta \tag{6}$$

融合节点与普通节点相比，多了解密和融合操作。A 有 2 个子节点，需解密 2 次，融合 1 次，融合需要进行 2 次加法运算。设 $\delta_1$、$\delta_2$ 分别表示加密操作和解密操作，则融合节点的计算开销可以表示为

$$C2_{\text{iPDA}} = 6\alpha + \delta_1 + 2\delta_2 \tag{7}$$

所以，从式(6)和式(7)可知，iPDA 总的计算开销为

$$C_{\text{iPDA}} = 14\alpha + 2\delta + \delta_1 + 2\delta_2 \tag{8}$$

3) SPPDA 的计算开销

SPPDA 方案中，叶子节点进行同态加密，融合节点需要进行加密和融合操作。叶子节点加密操作时有一次加法运算和一次取模运算，需对原始数据和 $s_j$ 加密，所以普通节点的计算开销可以表示为

$$C1_{\text{SPPDA}} = 2\alpha + 2\beta \tag{9}$$

融合节点的加密操作计算开销与普通节点相同，融合节点 B 和 C 的数据需要 4 次额外的加法操作（实部和虚部的融合各需 2 次）。所以融合节点的计算开销可以表示为

$$C2_{\text{SPPDA}} = 6\alpha + 2\beta \tag{10}$$

所以，从式(9)和式(10)可知 SPPDA 总的计算开销为

$$C_{\text{SPPDA}} = 10\alpha + 6\beta \tag{11}$$

由于加减、乘除运算的计算开销远小于指数运算，也小于生成随机数、IPHCDA 中的计算 MAC 值以及 iPDA 中的加解密复合运算。因此，从式 (5)、式(8)和式(11)可知，相比 iPDA 和 IPHCDA，SPPDA 方案的计算开销是最小的。

### 4.4　精确度

这里的精确度是指融合结果与实际数值的比值，也是数据融合算法的一个重要指标。理想情况下，精确度为 1。然而，由于通信信道有噪声，数据传输时会发生数据碰撞、丢失、延迟等情况，精确度一般小于 1。图 4 显示了 SPPDA、IPHCDA 和 iPDA 的精确度仿真结果。从图 4 可知，SPPDA 随着融合时间片增大而趋于稳定，从变化趋势上可以看出，SPPDA 的精确度要高于 IPHCDA，主要是因为 IPHCDA 密文较大，可能会分多次发送，容易产生数据碰撞和丢失。iPDA 采用分片的方法保护数据的隐私性，在分片过程中，数据片由于碰撞而发生丢失，故其精确度相比于其他 2 个算法较低。图 4 中精确度的变化有波动，但总体上是随时间片的增大而增大的。出现波动的原因是由无线传感器网络的通信方式引起的，比如遇到碰撞时，节点采取的是二进制退避法，其退避时间本身就有一定的不确定性。

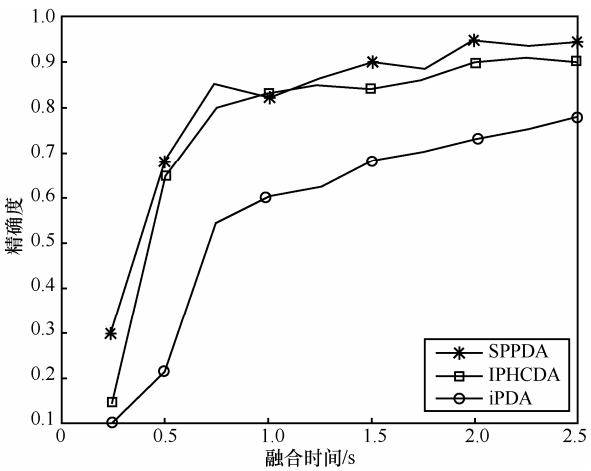



图 4　SPPDA、IPHCDA 和 iPDA 精确度

### 4.5 完整性

IPHCDA 算法采用分簇的网络拓扑结构，簇头接收簇内节点的数据并进行融合，对融合结果计算 MAC 值，簇头的 MAC 值在上传的过程中与其他簇头的 MAC 值进行异或运算，最终到达 sink 节点。sink 节点通过接收到的 MAC 值来验证数据的完整性。然而该算法只能验证融合结果上传至 sink 节点的完整性，无法验证在融合阶段簇内节点数据发送到簇头时的完整性，可能会导致恶意节点在融合节点注入错误数据，sink 节点却无法察觉的情况。对于 iPDA，由于完整性采取 2 个不相交的融合树进行融合，比较其结果，增加了通信量。如果恶意节点能同时向这 2 个融合树注入错误数据，则 sink 节点无法发觉。SPPDA 方案用复数的可加性融合数据，虚部用以验证数据完整性，每个节点都有一个不同的私密因子 $s_j$，加密后上传进行融合。如果恶意节点注入错误数据，sink 节点必然会察觉，所以 SPPDA 方案完整性验证可靠性高。

### 4.6 与已有加密算法的比较

在数据融合隐私保护协议中，比较经典的加密算法是随机密钥分发机制[24]，该机制是逐跳的对称加密机制。密钥分发方案由密钥预分配、发现共享密钥和建立路径密钥 3 个阶段组成。

1) 密钥预分配

首先产生有 $K$ 个密钥的大密钥池以及它们的标识符；其次，每一个传感器节点从 $K$ 个密钥中选择 $k$ 个密钥，并且 $k$ 个密钥形成一个密钥环。

2) 发现共享密钥

通过交换发现消息，每一个传感器节点可以和它的邻居节点共享一个公用密钥。如果一对邻居节点之间共享一个公用密钥，那么在它们之间可能建立起一个安全的链接。

3) 建立路径密钥

在共享密钥发现的最后阶段，没有共享一个公用密钥的 2 个节点间可以通过两跳或者多跳安全链接连接的相邻节点对之间分配一个端到端的路径密钥。在密钥分配后，任何一对节点之间拥有至少一个公用密钥的概率由式(12)给出。

$$p_{\text{connect}} = 1 - \frac{((K-k)!)^2}{(K-2k)!K!} \tag{12}$$

在一个给定的密钥下，任何其他节点可以窃听加密信息的概率用 $p_{\text{overhear}}$ 表示，则 $p_{\text{overhear}} = \frac{k}{K}$。

假设给定密钥池的容量 $K$=10 000，每个节点随机选取密钥的数量 $k$=200，则任意 2 个节点之间共享同一个密钥的概率为 98.3%。换言之，任意 2 个节点之间没有共享密钥的概率为 1.7%。在拥有共享密钥的节点之间，窃听者拥有共享密钥的概率为 0.2%。

本文采用同态加密算法对数据进行加密，在传感器节点部署之前，由中继节点生成密钥发给传感器节点。中继节点生成一个 $n$(1~255) byte 的随机数，通过 RC4 算法得到一个 S 盒，对 S 盒调用字符串散列函数，从而得到 $k_j$ 和 $s_j$。恶意节点得知传感器节点的数据的概率等于 $k_j$ 被破解的概率。恶意节点通过相同的方式生成与 $k_j$ 相等的密钥的概率几乎为 0，如果恶意节点只是简单的生成一个 int 类型的随机数，则该数等于 $k_j$ 的概率为 $1/2^{32}$。

与随机密钥分发机制相比，本文中的同态加密算法的安全性更高，且密钥的分配以及加密操作更加简单，运算速度快。同态加密算法可以在不对密文解密的情况下完成数据的融合，降低了计算开销。

## 5 结束语

本文提出了一种带有完整性验证的同态加密数据融合隐私保护方案 SPPDA，采用端到端的同态加密方式，直接对密文进行数据融合，既保证了数据隐私，又降低了时延。同时，利用复数的可加性实现了数据融合与完整性验证，使融合结果安全可靠。与 IPHCDA 和 iPDA 算法相比，SPPDA 的计算开销更小、通信量更少、精确度更高、完整性可验证。本文的 SPPDA 方案也适用于 count、average 等可通过 sum 间接求出的融合函数，但无法应用到 MAX、MIN 等融合函数。以后的工作将研究适用更多融合函数的隐私保护算法，考虑节点的移动性和网络的多样性，研究移动无线传感器网络的数据隐私保护方法。

## 参考文献：

[1] 李建中,高宏.无线传感器网络的研究进展[J].计算机研究与发展,2008,45(1):1-15.
LI J Z, GAO H. Survey on sensor network research[J]. Journal of Computer Research and Development, 2008, 45(1):1-15.

[2] 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):1501-1514.

[3] MOHAMED M E, MAHMOUD A, SHEN X M. A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks[J]. IEEE Transactions on Parallel and Distributed System, 2012,23(10): 1085-1818.

[4] 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.

[5] LIANG X H, BARUA M, LU R X, *et al*. HealthShare: achieving secure and privacy-preserving health information sharing through health social networks[J].Computer Communications, 2012, 35 (15): 1910-1920.

[6] XIONG H, CHEN Z, LI F G. Efficient and multi-level privacy-preserving communication protocol for VANET[J].Computers and Electrical Engineering,2012, (38):573-581.

[7] 范永健,陈红.两层传感器网络中可验证隐私保护 top-*k* 查询协议[J].计算机学报,2012,35(3):423-433.
FAN Y J, CHEN H. Verifiable privacy-preserving top-*k* query protocol in two-tiered sensor networks[J].Chinese Journal of Computers, 2012, 35(3): 423-433.

[8] 范永健,陈红,张晓莹.无线传感器网络数据隐私保护技术[J]. 计算机学报, 2012,35(6):1131-1146.
FAN Y J, CHEN H, ZHANG X Y. Data privacy preservation in wireless sensor networks[J]. Chinese Journal of Computers,2012,35(6): 1131-1146.

[9] CHOW C Y, MOHAMED F, *et al*. A privacy-preserving location monitoring system for wireless sensor networks[J].IEEE Transaction on Mobile Computing,2011,10(1): 94-107.

[10] PIETRO R D, VIEIO A. Location privacy and resilience in wireless sensor networks querying[J]. Computer Communications, 2011,(34): 515-523.

[11] BERGAMINI L, BECCHETTI L, VITALETTI A. Privacy-preserving environment monitoring in networks of mobile devices[A]. Proceedings of the IFIP TC 6th International Conference on Networking[C]. Valencia, Spain, 2011,179-191.

[12] HE W B, LIU X, NGUYEN H, *et al*. PDA: Privacy-preserving data aggregation in wireless sensor networks[A]. Proceeding of the 26th IEEE International Conference on Computer Communications (INFOCOM)[C].Anchorage,USA,2007.2045-2053.

[13] HE W B, LIU X, NGUYEN H V, *et al*. A cluster-based protocol to enforce integrity and preserve privacy in data aggregation[A]. Proceedings of 29th IEEE International Conference on Distributed Computing Systems Workshops[C]. Montreal, Canada ,2009.14-19.

[14] GROAT M M, HE W B, FORREST S. KIPDA: k-indistinguishable privacy-preserving data aggregation in wireless sensor networks[A].Proceeding of the 30th IEEE International Conference on Computer Communications (INFOCOM)[C]. Shanghai, China, 2011. 2024-2032.

[15] 杨庚, 王安琪, 陈正宇等. 一种低耗能的数据融合隐私保护算法[J].计算机学报, 2011, 34(5): 792-800.
YNAG G, WANG A Q, CHEN Z Y, *et al*. An energy-saving privacy-preserving data aggregation algorithm[J]. Chinese Journal of Computers, 2011, 34(5): 792-800.

[16] YAO I B, WEN G I. Protecting classification privacy data aggregation in wireless sensor networks[A]. The 4th International Conference on Wireless Communications, Networking and Mobile Computing[C]. Dalian, China ,2008.1-5.

[17] ZENG W, LIN Y, WANG L. Privacy-preserving data aggregation scheme based on the *p*-function set in wireless sensor networks[J]. Ad Hoc & Sensor Wireless Networks,2014, 21(1-2): 21-58.

[18] HE W B, NGUYEN H, LIU X *et al*. iPDA: an integrity-protecting private data aggregation scheme for wireless sensor networks[A]. Proceeding of the Military Communications Conference (MILCOM)[C]. San Diego, USA, 2008.1-7.

[19] BISTA R, KIM Y K, SONG M S, *et al*. Improving data confidentiality and integrity for data aggregation in wireless sensor networks[J]. IEICE Transactions on Informationand Systems, 2012, 95(1): 67-77.

[20] CHEN S M, LIN Y H, LIN Y C, *et al*. RCDA: recoverable concealed data aggregation for data integrity in wireless sensor networks[J]. IEEE Transaction son Parallel and Distributed Systems,2012, 23(4): 727-734.

[21] IOSE I, PRINCY M, IOSE I. PEPPDA: power efficient privacy preserving data aggregation for wireless sensor networks[A]. Proceedings of IEEE International Conference on Emerging Trends in Emerging Trends in Computing, Communication and Nanotechonlogy[C]. 2013. 330-336.

[22] IOSE I, KUMAR S M, IOSE I. Energy efficient recoverable concealed data aggregation in wireless sensor networks[A]. Proceedings of IEEE International Conference on Emerging Trends in Emerging Trends in Computing, Communication and Nanotechonlogy[C]. 2013. 322-329.

[23] OZDEMIR S, XIAO Y. Integrity protecting hierarchical concealed data aggregation for wireless sensor networks[J].Computer Networks, 2011, 55(8):1735-1746.

[24] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[A]. Proceedings of 9th ACM Conference on Computer and Communications Security[C]. Washington, USA, 2002.41-47.

**作者简介：**

**赵小敏**（1976-），男，浙江文成人，博士，浙江工业大学副教授，主要研究方向为无线传感器网络、信息安全。

**梁学利**（1990-），男，河南郸城人，浙江工业大学硕士生，主要研究方向为无线传感器网络、数据隐私保护。

**蒋双双**（1991-），女，浙江平阳人，浙江工业大学硕士生，主要研究方向为无线传感器网络。

**陈庆章**（1955-），男，河南济源人，浙江工业大学教授，主要研究方向为无线传感器网络、计算机支持的协同工作。