基于可逆数字水印认证的无线传感网数据融合协议

蒋文贤[1]，张振兴[1]，吴晶晶[2,3]

（1. 华侨大学计算机科学与技术学院，福建 厦门 361021；
2. 泉州师范学院数学与计算机科学学院，福建 泉州 362000；
3. 福建省大数据管理新技术与知识工程重点实验室，福建 泉州 362000）

摘 要：针对无线传感网隐私保护协议的高能耗与传感网络资源受限的对立问题，基于可逆数字水印与同态加密技术，提出一种同时保证数据完整性与机密性的可恢复数据融合协议。一方面采用可逆数字水印技术中的差异扩展方法对传感器采集数据进行嵌入，在融合数据被破坏时可以通过可逆水印恢复原始数据，保证融合数据的完整性校验；另一方面采用基于椭圆曲线的同态加密对数据进行加密融合，防止在数据传输过程中传感器数据被感知。安全推理表明，所提协议可以很好地抵御簇头节点妥协和篡改攻击。性能分析表明，该协议比其他算法在计算与通信开销、传输时延方面具有显著优势。实验对比结果表明，该协议有更低的资源开销，可以提升网络性能。

关键词：可逆数字水印；同态加密；完整性校验；数据恢复

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000-436x.2018046

Reversible digital watermarking-based protocol for data integrity in wireless sensor network

JIANG Wenxian[1], ZHANG Zhenxing[1], WU Jingjing[2,3]

1. College of Computer Science & Technology, Huaqiao University, Xiamen 361021, China
2. College of Mathematics & Computer Science, Quanzhou Normal University, Quanzhou 362000, China
3. Fujian Provincial Key Laboratory of Data Intersive Computing, Quanzhou 362000, China

Abstract: For the contradiction between high energy consumption of WSN privacy protection algorithm and constrained resources of sensor network, a recoverable data fusion protocol that ensures data integrity and confidentiality based on reversible digital watermarking and homomorphic encryption technology was proposed. On the one hand, the data from the sensor was embedded by the difference expansion method by using the reversible digital watermarking technique, and original data could be recovered by using a reversible watermark to ensure the integrity check of the fusion data when the fusion data were destroyed. On the other hand, elliptic curve homomorphic encryption encrypted data to prevent sensor data from being perceived during data transmission. Security results show that the proposed protocol performs well against cluster head node compromise as well as tampering from an attack. Performance analysis shows that the protocol has significant advantages over other algorithms in terms of computation, communication overhead and propagation delay. The experimental results show that the protocol has a low resource overhead and improves network performance.

Key words: reversible digital watermarking, homomorphic encryption, integrity authentication, data recovery

收稿日期：2017-05-12；**修回日期**：2018-02-05

通信作者：蒋文贤，jwx@hqu.edu.cn

基金项目：福建省自然科学基金资助项目（No.2017J01776）；福建省泉州市科技计划基金资助项目（No.2017Z006）

Foundation Items: The Natural Science Foundation of Fujian Province (No.2017J01776), The Science and Technology Plan Key Project of Quanzhou City of Fujian Province (No.2017Z006)

1　引言

无线传感器网络（WSN, wireless sensor network）是一种以数据为中心的网络，基于传感器网络的任何应用系统都离不开感知数据的管理和处理技术。同时由于感知数据流巨大，每个传感器仅具有有限的计算资源，难以处理巨大的实时数据流[1]，所以需要 WSN 中的数据进行融合处理，节约传感器节点资源，进而提高收集信息的效率，延长网络寿命和节点的生命周期。军事或医学等领域的传输数据都比较敏感，数据的丢失将造成个人与团体的重大损失，需要应对各种的攻击手段如共谋攻击、洪泛攻击、分布式拒绝服务（DDoS, distributed denial of service）攻击等。目前隐私保护主要分为机密性与完整性 2 个方面，机密性方面主要通过加密的方式，而完整性方面一般使用摘要认证码来实现。但由于隐私保护协议的高能量消耗与 WSN 资源受限的对立矛盾，已成为亟待解决的问题[2]，分析如下。

1) 传统的逐跳加密融合机制会将明文数据暴露给聚集节点，如果聚集节点被俘获控制将带来敏感信息泄露的风险。基于此，椭圆曲线密码[3]（ECEG, elliptic curve eigamal）、可恢复原始数据的融合协议[4]（RCDA, recoverable concealed data aggregation）等基于同态加密的隐私方案被提出，这些协议实现端到端的安全检查，保证数据在传输过程中不被感知。但是由于使用的校验方法比较复杂或缺少校验方案，导致资源开销比较大或不安全的后果。

2) WSN 中主要使用消息认证码（MAC, message authenticaion code）进行完整性校验，即在数据流中附加认证信息，但 MAC 如安全散列算法 SHA-1（SHA-1, secure hash algorithm-1）需要 160 bit 长度，消息摘要（MD5, message digest 5）算法需要 128 bit，这些计算 MAC 的同时也带来了高额的数据传输与计算能耗的增加。文献[5]通过引入 MAC 技术，提出一种能量有效的、抗数据丢失的隐私保护聚合方案，有效抵御多种外部攻击。文献[6]提出一种低能耗的非对称簇内隐私保护数据融合方法，进一步降低网络节点的计算量和通信量。文献[7]基于隐私同态和聚合 MAC 技术提出一种同时保障数据隐私性与完整性的可恢复数据聚合方案。由于需要附加认证消息，所以仍存在验证完整性开销等较大的问题。

近年来，数字水印技术具有安全性、隐蔽性、顽健性等特点，将信息嵌入原始数据流中可节省完整性验证部分的资源开销，因此，基于数字水印的 WSN 认证方法得到较多的研究。文献[8]提出了一种链式水印方法对数据流分组，通过嵌入水印构建前后相连的散列链来实现完整性认证。文献[9]提出了一种节点数据采样间隔的数字水印算法，可以阻止克隆攻击。文献[10]提出了一种基于零水印的方法，每个传感器节点对应一个独特的水印并嵌入数据中，通过基站来验证数据的完整性。基于传统数字水印的方法，虽然不增加额外的传输数据量，但在数据流上嵌入水印需要修改原始数据，这对于某些敏感的 WSN 应用是不允许的，而可逆数字水印[11]可以避免在产生额外数据的同时对数据进行完全恢复，满足某些特殊应用对原始数据的需求文献[12]设计了一种支持数据信任的可逆水印技术方案，解决物理信息和社会计算中海量数据的版权保护和完整性问题。文献[13]利用了 WSN 数据流相邻数据之间的相关性，通过拓展当前数据与前导数据预测值之间的误差嵌入水印，使汇聚节点在提取水印之后能恢复原始数据。

本文方案将可逆数字水印技术引入无线传感网数据的完整性验证中，提出了一种融合椭圆曲线加密的同态加密算法与可逆数字水印技术的新方法——基于可逆数字水印认证的无线传感网安全数据融合协议（RDWPDI, reversible digital watermarking based protocol for data integrity in wireless sensor network）。通过计算量分析和实验数据对比，在通信开销、传输时延等方面具有显著优势，能够抵抗大多数攻击且其计算开销比同类协议更低，对于资源受限的 WSN 的整体性能提高有很大帮助。

2　关键技术

2.1　可逆数字水印

可逆数字水印是用可逆的方法将数据嵌入一个数字图像中，算法的操作流程与普通数字水印相同，如图 1 所示。普通水印会对载体中存在的敏感信息造成损害，因此，在接收端，原始数据的完全恢复几乎是不可能的，而可逆数字水印则可以避免这些问题。

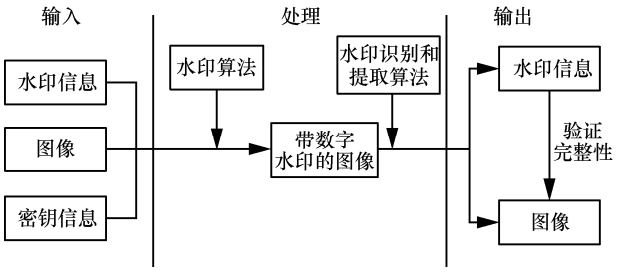

图 1　数字水印示意

本文方案使用可逆数字水印的原始数据可恢复性作为数据恢复方法。具体方法描述如下。

假设有灰度值对 (n_1,n_2)，$0 \leqslant n_1,n_2 \leqslant 255$。$n_1$、$n_2$ 的整数平均值 l 和差值 h 分别为

$$l = \left\lfloor \frac{n_1+n_2}{2} \right\rfloor$$

$$h = n_1 - n_2 \tag{1}$$

使用差异扩展法将水印 W_ϕ 嵌入差值 h 的最低有效位，扩展之后的差值 h' 为

$$h' = 2h + W_\phi \tag{2}$$

对式(1)进行哈尔小波变换可得

$$n_1 = l + \left\lfloor \frac{h+1}{2} \right\rfloor$$

$$n_2 = l - \left\lfloor \frac{h}{2} \right\rfloor \tag{3}$$

将式(2)代入式(3)，可得到嵌入数字水印的数据 n_1'、n_2'。由于嵌入水印的数据也是灰度值数据，所以也要满足 $0 \leqslant n_1',n_2' \leqslant 255$，对可以满足条件的点进行判断。

在对端接收到嵌入水印的数据后，通过相反的操作计算式计算 n_1'、n_2' 的均值 l' 和差值 h'，并求出嵌入的水印数据 $w_\phi = h' \bmod 2$，计算出原来的差值 $h = \left\lfloor \frac{h'}{2} \right\rfloor$，把 l'、h 代入式(3)后可以恢复出原始数据。

2.2　椭圆曲线同态加密技术

同态加密允许在加密中直接计算数据（加法和/或乘法）。它可以提供端到端隐私，不需要中间节点执行加解密操作。假设 Q 和 R 是 2 个环，+和× 分别代表环中的加法和乘法，⊕、⊗ 代表某种操作，K 是密钥空间，则有加密运算 $E{:}K\times Q\rightarrow R$ 和解密运算 $D{:}K\times R\rightarrow Q$。若 $n_1,n_2 \in Q$ 且 $k \in K$，则加法同态运算和乘法同态运算分别为

$$Ek(n_1+n_2) = Ek(n_1) \oplus Ek(n_2) \tag{4}$$

$$Ek(n_1 \times n_2) = Ek(n_1) \otimes Ek(n_2) \tag{5}$$

椭圆曲线密码属于公钥密码体制，它的安全性建立在椭圆曲线离散对数问题的困难性之上。椭圆曲线上的点全体构成一个加法群，点与点之间可以进行加法运算，具有加法同态的性质。

假设有 2 个数据 n_1、n_2，将其映射到椭圆曲线之后进行加和，与直接将数据进行相加的值映射到椭圆曲线上是相等的。

$$map(n_1) + map(n_2) = map(n_1+n_2) \tag{6}$$

3　协议描述

3.1　网络模型及协议介绍

本文提出的 RDWPDI 协议首先将网络进行分簇，每个簇由一个簇头与多个成员节点组成，生成簇的方式采用低功耗自适应集簇分层型（LEACH, low energy adaptive clustering hierarchy）协议的分簇方法。簇内采用汇聚树协议[14]（CTP, collection tree protocol）进行数据传输，簇间采用树型结构，以基站为根，簇头为叶子节点进行数据的汇总。协议主要包括 5 个部分：1) 系统参数初始化后采集数据；2) 在感知节点生成水印信息并将水印信息嵌入分片后的数据中；3) 将采集数据与最小值差值编码，编码后数据加密；4) 在汇节点进行数据融合与带水印信息的重组；5) 最终在基站处恢复原始数据并进行完整性校验。RDWPDI 协议具体流程如图 2 所示。

3.2　系统初始化设置

在簇内使用汇聚树协议建立路由。簇头作为汇聚节点直接连接基站，基站通过簇头向整个网络可靠的广播融合请求信息，该信息包含当次查询数据的最大值与最小值对 $(N_{\max},N_{\min})$ 与一个随机数 X。

构建有限域 F_p 上的椭圆曲线 E，基站随机选择 $k \in Z_P^*$ 作为私钥。生成椭圆曲线参数四元组 K，如式(7)所示，并生成公私钥对 (k,Y)，$Y = kG$。基站将椭圆曲线参数与生成的公钥发给每一个传感器，在所有感知节点上预置与基站同样的随机函数 *Rand*()，可以把当次的随机数 X 作为随机数种子抵制重放攻击。

$$K = (E,G,p,\xi) \tag{7}$$

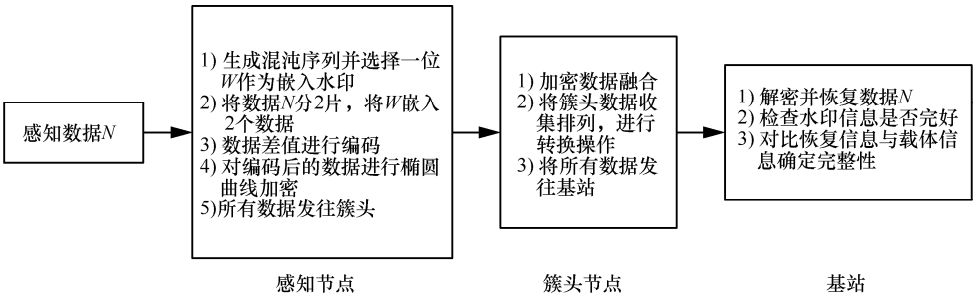

图 2　RDWPDI 协议流程

其中， p 是一个大素数且 E 的阶数 ξ 有大素数因子，$|p|=\xi$。$E(F_p)$ 表示曲线 E 上所有点的集合，G 是 $E(F_p)$ 的一个生成元。

3.3　生成数字水印及嵌入载体

具体的嵌入水印算法如算法 1 所示。

算法 1　生成数字水印及嵌入载体算法描述

1) L = AVG($N_{\min}$, $N_{\max}$) && 将后 5 位取反

2) $L = L < 15 \ ? \ L$ PLUS 16 : L

3) 初始值 x_0 取随机数 $X\{0,1\}$

4) $r = 4$

5) for i = 0 to L do

6)　　x_0=MULTIPLICATE(r, x_0, (1−x_0))

7) end for

8) 采用基于数据分片的差异扩展水印

9) do

10)　　n_1 = DATASLICE(N, chaos)

11)　　n_2 = DEFFERENCE(Nchaos, n_1)

12)　　l = AVG(n_1, n_2)

13)　　h = SUM(SQUARE (DIFFERENCE (n_1, n_2)), watermark)

14) while h 在(0, DOUBLE l)范围内&& h 不大于 DOUBLE (255 − l)

15)　　n_1 = SUM(l, HALF(h + 1))

16)　　n_2 = DEFFERENCE(1, HALF(h))

嵌入的水印数据必须具有充分的随机性。文献[15]中的混沌函数是不可预测的并且对初值敏感，所以使用 *Logistic* 映射作为水印信息。

$$x_{L+1} = rx_L\ (1-x_L)\ ,\ 0<x_L<1,\ L=0,1,2,\cdots \quad (8)$$

其中， r 的取值为[3.569 945 6，4]，这里选择 r 为 4，见算法 1 的步骤 4)。根据文献[15]的实验结果，在 $L \geqslant 15$ 的时候相差极小的数据也会出现明显变化，所以需要保证 L 值大于 15。L 值的获取通过对查询数据的平均值 N_{average} 的后 5 位取反，若小于 15 则将最高位置 1，否则，不变化。x_L 的初始值 x_0 取随机数 X 与 N_{average} 异或的最低有效位 2 位，见算法 1 的步骤 1)和步骤 2)。

$$e_2e_1 = \begin{cases} 00,\ x_0 = y_1 \\ 01,\ x_0 = y_2 \\ 10,\ x_0 = y_3 \\ 11,\ x_0 = y_4 \end{cases} \quad (9)$$

根据节点 ID 号从生成的混沌序列 x_L 中，如算法 1 的步骤 5)~步骤 7)，由低位开始取水印数据 $w_\phi, w_\phi \in x_L, \phi = 0,1,2,\cdots$。在路由算法分簇之后会给每个节点在内部分发一个簇内 ID(ID_{in})，根据 ID_{in} 在簇头对数据进行排列。

基于差异扩展的无线传感网水印方案一般是使用分组方案[16]，本文提出基于数据分片的差异扩展方案。混沌序列 e 有 n 位，将传感器节点的数据 N 与 e 的前 4 位数据进行异或操作，再使用 Rand()函数进行分片操作，最后得到可以进行差异扩展的 2 个数据 n_1、n_2，如算法 1 的步骤 8)~步骤 16)。Rand()函数需要保证 $n_1, n_2 \geqslant 0$。

$$N \oplus e_{n,n-1,n-2,n-3} \oplus W_\phi \oplus ID_{\text{in}} = n_{ab} \mid n_c \quad (10)$$

对 n_{ab}、n_c 使用差异扩展算法[17]。

计算 n_{ab}、n_c 的整数平均值 l 和差值 h，分别为

$$l = \left\lfloor \frac{n_{ab}+n_c}{2} \right\rfloor$$

$$h = n_{ab} - n_c \quad (11)$$

使用差异扩展法将水印 W_ϕ 嵌入差值 h 的 LSB 位，如图 3 所示。假设采集到的温度数据为 N，首先，将其与混沌序列前 4 位进行异或操作，其次，通过分片算法将结果分片，最后，使用最低有效位扩展方法取混沌序列中的一位嵌入最低有效位，将

数据 N 分片为嵌入有水印的 2 个新序列。扩展之后的差值 h' 为

$$h' = 2h + W_\phi \tag{12}$$

对式(11)进行哈尔小波变换可得

$$\begin{aligned} n_{ab} &= l + \left\lfloor \frac{h+1}{2} \right\rfloor \\ n_c &= l - \left\lfloor \frac{h}{2} \right\rfloor \end{aligned} \tag{13}$$

将式(11)代入式(12)，可得到嵌入了数字水印的分片数据 n'_{ab}、n'_c。由于是将传感器的值作为图像的灰度值，所以 $0 \leqslant n_{ab}, n_c \leqslant 255$，结合式(11)，可得

$$\begin{cases} n_{ab} + \dfrac{2h_{\max} + W_\phi}{2} \leqslant 510 \\ n_c + \dfrac{2h_{\max} + W_\phi}{2} \leqslant 255 \end{cases} \tag{14}$$

$$\begin{cases} n_c = 2^{k_c}, k_c < 6 \\ n_{ab} = 2^{k_{ab}}, k_{ab} \leqslant 8 \end{cases} \tag{15}$$

一般的传感器网络主要监测的是温度、湿度等数据，获得的数值不会太大，而在本文方案中可以显示的最大数据范围为[0，8 192]。最后可以使用随机函数 *Slice*()进行分片操作，得到 2 个数据 n_{ab}、n_c，*Slice*()函数须确保 $n_{ab}, n_c \geqslant 0$。

$$Slice(n_{ab}) = n_a + n_b \tag{16}$$

3.4 数据预处理及加密

对传感器节点数据 N 与查询数据最小值 $N_{\min}$ 的差值 d_i 使用数据预处理方法（式(17)）对 m_i 进行编码。

$$m_i = d_i \| 0^\beta, \beta = u(i-1) \tag{17}$$

其中，u 是当次查询数据最大值与最小值的差值，i 为簇内节点编号，$i = 1, 2, \cdots, \eta - 1$。将数据映射成为椭圆曲线上的一点，有

$$map(m_i) = m_i G \to M_i,\ c_i = (R_i G, M_i + R_i Y) \tag{18}$$

传感器随机选择 $R_i \in [0, \xi - 1]$，对 M_i 进行加密，得到点对 c_i。使用 RC4 算法来加密簇头节点与感知节点之间的数据 RC4($n_a \,|\, n_b \,|\, n_c$)。将它与点 c_i 一同发往簇头。

3.5 数据融合

假设簇头收到 c_1、c_2，根据式(11)，得

$$\begin{aligned} c_1 + c_2 &= (R_1 G, M_1 + R_1 Y) + (R_2 G, M_2 + R_2 Y) \\ &= ((R_1 + R_2)G, (M_1 + M_2) + (R_1 + R_2)Y) \end{aligned} \tag{19}$$

对 $\eta - 1$ 个密文($c_1, c_2, \cdots, c_{\eta-1}$)计算聚合密文 C。将收到的水印载体数据 n'_a、n'_b、n'_c 用 a、b、c 表示。采用矩阵方式按顺序进行排列，可得式(20)，然后对矩阵进行逆置等操作，之后将融合后的加密数据与全部的水印数据发往基站，如图 4 所示。

$$\begin{bmatrix} a_1 & a_2 & \cdots & a_{\eta-1} \\ b_1 & b_2 & \cdots & b_{\eta-1} \\ c_1 & c_2 & \cdots & c_{\eta-1} \end{bmatrix} \tag{20}$$

3.6 解密及水印验证算法

基站对收到的融合数据进行解密，有

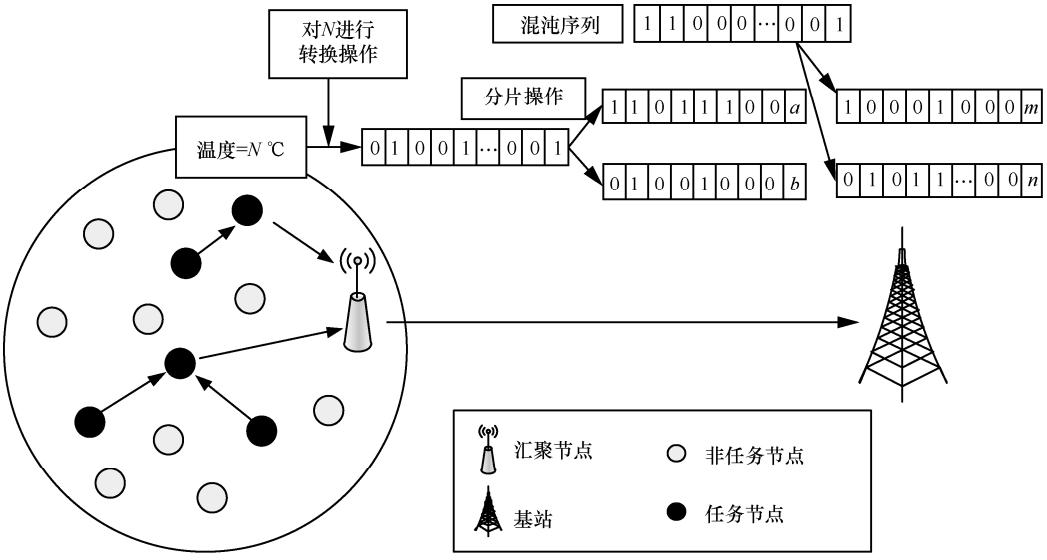

图 3 可逆数字水印方案示意

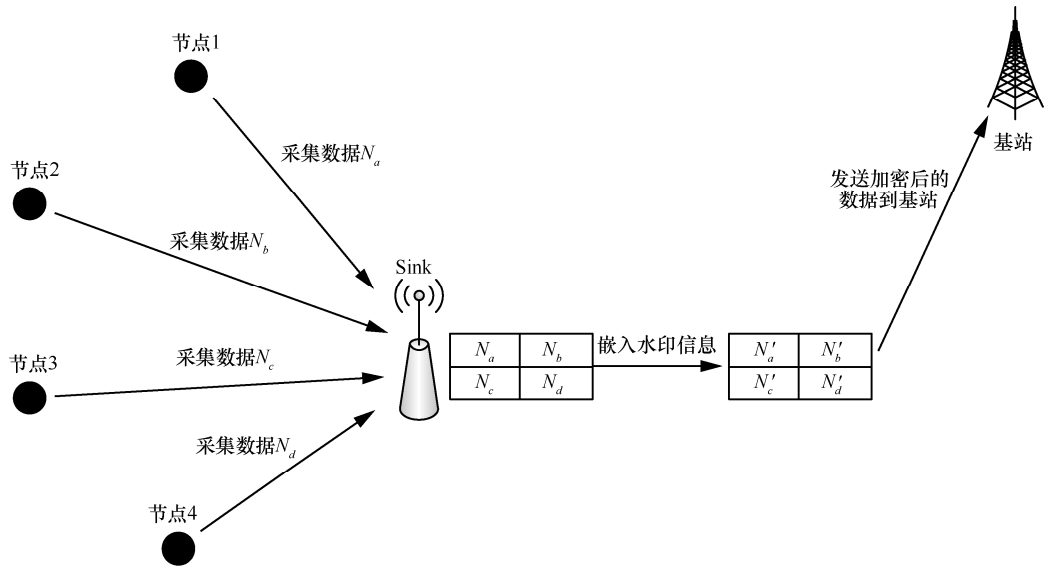

图 4　RDWPDI 中的数字水印方法

$$C=(\sum_{i=1}^{n-1}R_iG,\sum_{i=1}^{n-1}M_i+\sum_{i=1}^{n-1}R_iY) \tag{21}$$

私钥对密文进行解密，得到代表融合数据的点 $\sum_{i=1}^{\eta-1}M_i$，即

$$\begin{aligned}\sum_{i=1}^{\eta-1}M_i&=\sum_{i=1}^{\eta-1}M_i+Y\sum_{i=1}^{\eta-1}R_i-kG\sum_{i=1}^{\eta-1}R_i\\&=\sum_{i=1}^{\eta-1}M_i+Y\sum_{i=1}^{\eta-1}R_i-Y\sum_{i=1}^{\eta-1}R_i\end{aligned} \tag{22}$$

对融合数据的点，使用 Pollard-λ 方法[18]反映射成数据。根据文献[19]可知，当 $0\leqslant m\leqslant T$ 时，解密的时间复杂度为 $O(\sqrt{T})$。

$$rmap(\sum_{i=1}^{\eta-1}M_i)\to\sum_{i=1}^{\eta-1}m_i \tag{23}$$

再使用融合数据恢复计算式，有

$$d_i=\sum_{i=1}^{\eta-1}m_i[(i-1)u,i\times u-1] \tag{24}$$

恢复出每一个融合数据 d_i。

查找基站内的簇内 ID 与节点 ID 的映射表，用式(11)计算嵌有水印的第 i 个传感器的分片数据对 (a_i+b_i,c_i) 的均值 l' 和差值 h'，确定节点 ID 并求出嵌入的水印数据 w_ϕ。$w_\phi=h'\bmod 2$，计算出原来的差值 $h=\left\lfloor\frac{h'}{2}\right\rfloor$。把 l'、h 代入式(13)再进行加和后可以恢复出原始数据。基站计算混沌序列得到嵌入的水印信息 W_ϕ，与所提 w_ϕ 进行对比。

4　安全及计算量分析

4.1　安全分析

命题 1　所提协议可以很好地抵御簇头节点妥协、重放攻击、窃听攻击、篡改攻击和已知明文攻击。

证明　加密算法使用的 ECEG 是基于椭圆曲线上的离散对数问题，$Y=kG$。已知 Y 和 G，无法在多项式时间内求解 k 值。EIGamal 加密机制已被证明是 IND-CPA 安全的，ECEG 拥有同样的性质。很容易证明本文方案对簇头节点妥协有抵御效果，由于使用基于椭圆曲线的同态加密算法，在簇头节点对收到的数据 c_i 并不会进行解密操作，在没有私钥 k 的情况下簇头节点无法得知传感数据。同时在数字水印中采用了混沌序列 e 与传感数据 N 进行异或的方法对原始数据进行变换，再对变换后的数据进行差异扩展，丢失了原来的数据特性，保证了数据的安全，确保在传输过程中与簇头处可以抵御窃听攻击。

假设敌方已知某一数据对应的分片数据 a、b，可以推断出目前使用的混沌序列部分，但是混沌序列的选择是随着收集数据的轮数在变换的，可以保证原始数据的安全性。对于篡改攻击有 2 种情况。

1) 同态加密部分数据被篡改，水印无损 $w_\phi=W_\phi$。可以通过对水印嵌入载体进行逆向操作恢复原始数据。

2) 同态加密部分无损，水印损坏 $w_\phi \neq W_\phi$。水印的值会发生变化，将逆向恢复的数据与解密后的数据进行比较，如果不同则使水印损坏部分的节点单独向基站发送数据。

最后使用时间戳结合每轮查询生成的随机数 X 来防止重放攻击。

4.2 计算量分析

命题 2 提出的协议可以节省感知节点与聚集节点的计算开销。

证明 由于基于数字签名的方案 RCDA[4]和聚合 MAC 的方案 RPIDA[20]与本文方案应用了相同的加密方式，所以主要对比完整性验证算法的开销。为统一计算，基于聚合 MAC 方案在实验中使用散列算法 SHA-1，簇头进行 MAC 聚合操作，在基站对恢复的数据计算 MAC，最后再进行 MAC 值的对比。RCDA 使用的是 Boneh 等提出的融合数字签名方案，与加密方式类似，在传感节点对数据的散列值进行签名后发送到簇头，在簇头进行签名融合后发送到基站。

假设一个簇内有 m 个簇成员。数字签名方案在传感节点进行了一次点乘操作（M），一次散列操作（H），在簇头进行了 $m-1$ 次的点加操作（A）。聚合 MAC 方案进行了一次的散列操作与 $m-1$ 次异或操作（XOR）。而本文方案只使用了多次的异或操作，如表 1 所示。根据文献[20]中实验，SHA-1 计算消耗的能量是 5.9，为点乘一次的消耗，而异或所消耗的能量基本可以忽略。所以在计算开销上可证得 RCDA>> 聚合 MAC 方案 RPIDA>本文方案。

表 1 3 种协议的计算开销比较

协议	感知节点	簇头
RCDA	1 M+1 H	(m−1)A
RPIDA	1 H	(m−1)XOR
RDWPDI	<<(m−1)XOR+RC4	RC4

5 协议性能评估与分析

5.1 仿真参数设置

使用 TOSSIM 仿真环境对提出协议的资源消耗和完整性验证效果进行评估，仿真参数如表 2 所示。

在实验中，100 个传感器节点随机播撒在 100 m×100 m 的预定区域内。通过调整无线传感器网络的簇密度来对比评估的算法性能。

表 2 仿真参数设置

仿真参数选项	参数设定值
簇内路由协议	汇聚树协议
基站设置位置	(50,50)
噪声水平	−105.0 dBm
节点间最小距离	≥1 m
高斯白噪声	4.0 dB
拓扑类型	随机

本文方案主要选择 RCDA 和 RPIDA 这 2 种融合方案进行对比，RCDA 及 RPIDA 同样使用了基于椭圆曲线的同态加密方法，在机密融合方面是一样的方式。主要不同点在于 3 种方案选择的完整性验证方案不同，其中，RCDA 使用了复杂的数字签名方案，而 RDWPDI 及 RPIDA 使用了低能耗的数字水印方案。与 RPIDA 不同的是，本文方案是在分簇后直接进行了水印融合，而 RPIDA 方案是在分组聚集的条件下实现的，比本文方案更复杂。表 3 是本文方案与另外 3 种数据融合方案使用技术的对比。

表 3 方案使用技术对比

方案	数字水印	数据融合	同态加密	椭圆曲线加密	数字签名
RDWPDI	√	√	√	√	—
RCDA	—	√	√	√	√
RPIDA	√	√	√	√	—
ECEG	—	√	√	√	—

下面，从通信开销、时延比较与水印识别率 3 个方面进行实验，分析对比方案的性能。

5.2 通信开销

对于通信开销，文献[20]的研究结果中 Micaz 节点每发送 1 bit 数据消耗 0.6 nJ 能量，每接收 1 bit 数据消耗 0.67 nJ 能量。

借助点压缩技术，椭圆曲线 E 的一个点 (x, y) 可表示为 161 bit。本文方案中各感知节点发送的消息主要包括一个密文和 2 个分片值 n_1、n_2，2 个分片数据占 16 bit。其他节点自身 ID（如节点簇内 ID）和时间戳与其他协议保持一致，占 96 bit，最后还需考虑数据分组的头部长度 88 bit。因此，每个感知节点发送的消息大小 522 bit，发送需 313.2 nJ 能量。在相同安全等级要求下，RCDA 方案中产生的签名表示为 154 bit，数据分组长度 660 bit，发送需 396 nJ 能量。MAC 聚合值使用的 SHA-1 算法，需要 160 bit，分组总长度 666 bit，发送需 399.6 nJ，

如图 5 所示。与 RCDA 与 RPIDA 相比，本文方案有更低的感知节点能耗，ECEG 由于只有加密方案，没有完整性验证方案，感知节点的通信能耗只需要 303.6 nJ，节点通信开销对比如图 5 所示。

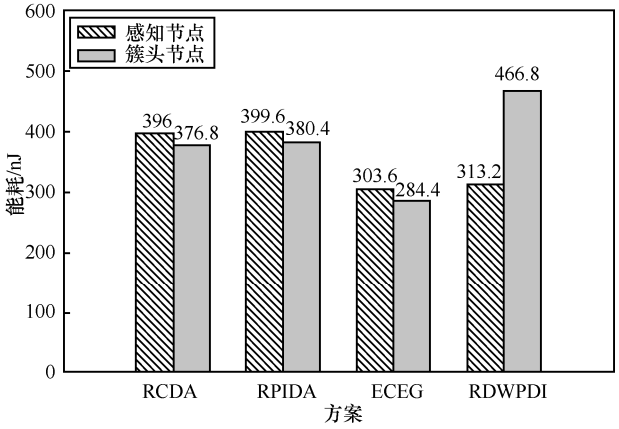

图 5　节点通信开销对比

在 m 个成员的簇中，其他 3 种方案在融合过后数据分组长度基本不变。本文方案会对簇内成员的分片数据进行组合形成一张图像，长度同时会增加 $16(m-1)$ bit，所以在簇头节点的能量开销更多。设定 100 个节点的传感网络中有 5 个簇，取理想平均每个簇 19 个成员，融合过后需要 778 bit 要进行传输。

通过实验进行 100 次的分簇融合操作，计算出平均每个簇内进行融合可以节约的能量值，如图 6 所示。

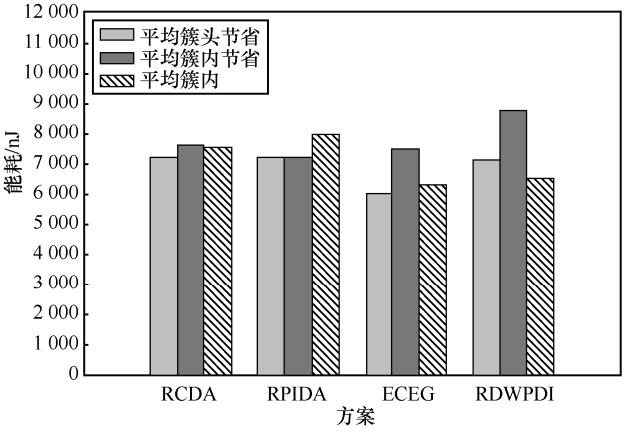

图 6　平均簇内通信开销对比

使用计算式 $\dfrac{\text{节约能量}}{\text{正常损耗能量}}$ 来代表节约的能量比。在簇头处，本文方案跟另外 3 种方案的能量节省相差不多，但在传感节点处该方案可以节省大量的通信能量，如图 7 所示。所以在簇内整体能量节省上，本文方案要优于 RCDA 与 RPIDA。对于融合方案，簇内的成员越多，簇头的通信开销就越小，但成员太多，为了等待全部成员进行融合的时延也会增大。

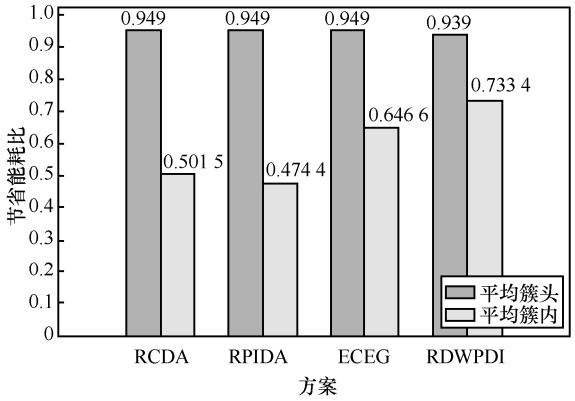

图 7　平均簇内通信开销节省比率对比

5.3　时延比较

对于融合方案，时延是方案必须考虑的一个因素，时延包括传输时延与融合时延。设定不同的簇头会影响簇内成员的数量和数据拥塞的情况，需要减少传输的能量消耗就需要减少簇头的数量，而簇头数量少也会导致融合的时延增加。通过表 4 可以看出，当需要融合的数据多时，由于数据碰撞、等待数据到达时间增多，本文方案的时延远高于非融合的方案。

表 4　　**时延开销对比**

簇头数量	非融合时延/ms	RDWPDI/ms
1	3 458.27	10 290.5
5	2 984.94	8 831.77
10	1 733.44	4 161.58
20	1 561.38	3 601.15
30	1 321.38	2 818.3
50	915.95	1 761.39
70	708.64	1 084.6
80	538.23	862.77
90	409.72	655.82

在簇内需要融合数据的成员减少时，本文方案的时延基本与非融合方案持平。根据图 8 中的时延折线，可以取簇头数在 10 附近，这样既可以保证簇内成员数量来减少传输能耗，也可以最大限度减少融合时延。

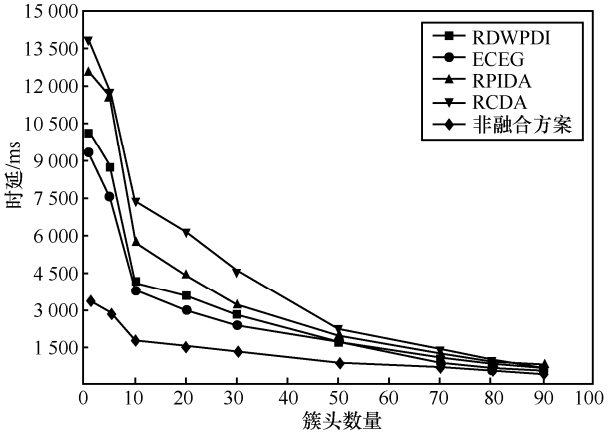

图 8　5 种方案的时延对比

5.4　水印识别率

接下来，从水印本身的认证识别来对提出的水印方案进行评估。

水印识别是指在网络中传输数据被接收后，数据存在更改或不完整情况下，能识别出正确水印的能力。影响识别率的参数很多，分组丢失和数据被篡改后的水印识别率是影响水印验证的 2 个重要因素。在理想情况下该方案的水印识别率是 100%的，但是由于在实际节点部署环境中存在分组丢失与数据篡改，导致水印的识别率下降。理论上设置相对多的簇头数会降低数据分组的丢失率，低的分组丢失率会使水印的识别率提高，所以簇头数量的设置同样会影响水印的识别率。低的篡改率同样会提高水印的正确识别率。

在实验中对比了簇头数为 3、5、7、11 的水印识别率。图 9 与理论分析相符，可以看到，在篡改率为 20%以下，同时分组丢失率较高的情况下，水印识别率依然很高，可以证明水印方案具有较高的顽健性。在超过一定的篡改率后水印的识别率会迅速下降，也证明了本水印方案具有一定的脆弱性，适合用于完整性验证方案中。

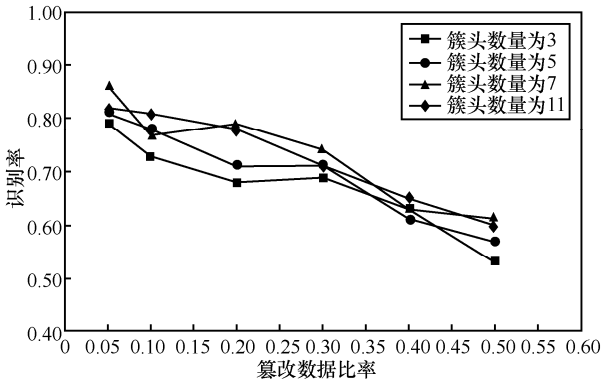

图 9　水印识别率

在节点丢失分组时，由于在分片操作之前会对数据进行处理，数据分片不会出现(0,0)的情况。在簇头进行聚集时，如果簇内某个节点数据分组丢失，在按顺序进行排列组合成图像时，这 2 个像素点的值就会直接设置为 0，在基站处如果发现(0,0)对的存在则认为数据分组丢失。该传感器的数据需要重新发送，并不对其进行水印提取处理。

6　结束语

本文基于可逆数字水印提出了一个新的完整性认证融合协议。经过实验对比，本文方案具有高效、低能耗、高识别率的特性，同时具有可以在加密融合数据出错但水印完好的情况下恢复原始数据的能力。与其他使用基于数字签名或聚集 MAC 的方案相比，本文方案具有更高的安全性，同时节省更多的通信开销，在网络内平均簇规模相近的情况下有更低的时延，节省了大量的网络资源。本文方案实现了高机密性及完整性验证，同时降低了能耗，在一定程度上解决了无线传感网隐私保护的高能耗与资源受限的对立问题。

参考文献:

[1] 李建中, 李金宝, 石胜飞. 传感器网络及其数据管理的概念、问题与进展[J]. 软件学报, 2003, 14(10): 1717-1727.
LI J Z, LI J B, SHI S F. Concepts, issues and advance of sensor networks and data management of sensor networks[J]. Journal of Software, 2003,14(10):1717-1727.

[2] 董晓蕾. 物联网隐私保护研究进展[J]. 计算机研究与发展, 2015, 52(10):2341-2352.
DONG X L. Advances of privacy preservation in Internet of things[J]. Journal of Computer Research and Development, 2015, 52(10): 2341-2352.

[3] 白乐强, 李玲, 钱施光, 等. 基于椭圆模型的无线传感器网络源位置隐私保护算法[J]. 控制与决策, 2017, 32(2):255-261.
BAI L Q, LI L, QIAN S G, et al. Source-location privacy protection algorithm in WSN based on ellipse model[J]. Control and Decision,2017, 32(2):255-261.

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

[5] 付帅, 姜奇, 马建峰. 一种无线传感器网络隐私保护数据聚合方案[J]. 计算机研究与发展, 2016, 53(9):2030-2038.
FU S, JIANG Q, MA J F. A privacy-preserving data aggregation scheme in wireless sensor networks[J]. Journal of Computer Research and Development, 2016, 53(9): 2030-2038.

[6] 苘大鹏, 王臣也, 杨武, 等. 低能耗的无线传感器网络隐私数据融合方法[J]. 清华大学学报（自然科学版）, 2017, 57(2):213-219.
MAN D P, WANG C Y,YANG W, et al. Energy-efficient cluster-based

privacy data aggregation for wireless sensor networks[J].Journal of Tsinghua University(Science and Technology), 2017, 57(2): 213-219.

[7] 丁超, 杨立君, 吴蒙. 一种同时保障隐私性与完整性的无线传感器网络可恢复数据聚合方案[J]. 电子与信息学报, 2015, 37(12): 2808-2814.
DING C, YANG L J, WU M. A recoverable privacy preserving integrity assured data aggregation scheme for wireless sensor networks[J]. Journal of Electronics and Information Technology, 2015,37(12): 2808-2814.

[8] GUO H P, LI Y J, JAJODIA S. Chaining watermarks for detecting malicious modifications[J]. Information Sciences, 2007, 177(1): 281-298.

[9] GUAN T H, CHEN Y H. A node clone attack detection scheme based on digital watermark in WSN[C]//First IEEE International Conference on Computer Communication and the Internet.2016:257-260.

[10] HAMEED K, KHAN M S, AHMED I, et al. A zero watermarking scheme for data integrity in wireless sensor networks[C]//19th International Conference on Network Based Information Systems.2016, 56: 119-126.

[11] KHAN A, SIDDIQA A, MUNIB S, et al. A recent survey of reversible watermarking techniques[J]. Information Sciences, 2014, 27(9): 251-272

[12] LFTIKHAR S, KAMRAN M, MUNIR E U, et al. A reversible watermarking technique for social network datasets for enabling data trust in cyber, physical, and social computing[J]. IEEE Systems Journal, 2017, 11(1):197- 206.

[13] SHI X, XIAO D. A reversible watermarking authentication seheme for wireless sensor networks[J]. Information Sciences, 2013, 240(8): 173- 183.

[14] GNAWALI O, FONSECA R, JAMIESON K, et al. Collection tree protocol[C]//The 7th ACM Conference on Embedded Networked Sensor Systems.2009:1-14.

[15] HEIDARI-BATENI G, MCGILLEM C D. A Chaotic direct sequence spread spectrum communication system[J]. IEEE Transactions on Communications, 1994,42(2-4): 1524-1527.

[16] LIU X X, GUO Y C, SUN C. A novel data integrity protection algorithm based on grouping negotiation and watermarking for WSN[J]. Journal of Computational Information Systems, 2015, 11(7): 2693-2700.

[17] TIAN J. Reversible data embedding using a difference expansion[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003,13(8):890-896.

[18] MEULENAER G D, GOSSET F, STANDAERT F X, et al. On the energy cost of communication and cryptography in wireless sensor networks[C]//IEEE International Conference on Wireless and Mobile Computing, Networking and Communications.2008:580-585.

[19] MYKLETUN E, GIRAO J, WESTHOFF D. Public key based cryptoschemes for data concealment in wireless sensor networks[C]//IEEE International Conference on Communications.2006:2288-2295.

[20] YANG L, DING C, WU M. RPIDA: recoverable privacy preserving integrity-assured data aggregation scheme for wireless sensor networks[J]. KSII Transactions on Internet and Information Systems,2015,37(12):2808-2814.

[作者简介]

蒋文贤（1974-），男，福建漳州人，华侨大学副教授，主要研究方向为物联网安全、网络协议等。

张振兴（1991-），男，黑龙江双鸭山人，华侨大学硕士生，主要研究方向为网络安全、隐私保护技术等。

吴晶晶（1975-），女，福建漳州人，博士，泉州师范学院教授，主要研究方向为无线传感器网络、数据挖掘和大数据管理和分析等。