doi:10.3969/j.issn.1000-436X.2012.10.003

无线传感器网络中基于隐私保护元的数据聚合机制

曾玮妮[1,2]，林亚平[2]，何施茗[2]，余建平[3]

（1. 中国船舶重工集团公司 第 716 研究所，江苏 连云港 222006；2. 湖南大学 信息科学与工程学院，湖南 长沙 410082；
3. 湖南师范大学 数学与计算机科学学院，湖南 长沙 410082）

摘 要：提出对聚合中的传感数据提供隐私保护的分布式机制。基于同余的代数特性定义了隐私保护元，无需通信即可实现传感数据的隐私性，且聚合值在簇内得以准确还原。给出了隐私保护元生成方法，该方法无需通信，且支持动态变化的聚合节点。分析表明，与集中式机制相比，避免了基站获取隐私数据及单点失效问题，对分组丢失环境有着更强的健壮性，且通信开销更低；与分布式机制相比，在提高隐私保护有效性的同时通信开销更低。

关键词：传感器网络；数据聚合；隐私保护；同余；隐私保护元

中图分类号：TP393；TP309 **文献标识码**：A **文章编号**：1000-436X(2012)10-0016-10

Data aggregation based on the privacy-preserving element in wireless sensor networks

ZENG Wei-ni[1,2], LIN Ya-ping[2], HE Shi-ming[2], YU Jian-ping[3]

(1. The 716th Research Institute, China Shipbuilding Industry Corporation, Lianyungang 222006, China;
2. College of Information Science and Engineering, Hunan University, Changsha 410082, China;
3. College of Mathematics and Computer Science, Hunan Normal University, Changsha 410082, China)

Abstract: A distributed mechanism was proposed to protect the data privacy during the data aggregation phase. The contributions of this mechanism are: 1) Privacy-preserving element taking advantage of the algebraic properties of congruence was defined. In privacy- preserving elements, privacy data could be preserved without the extra data exchange, and the aggregation result could be recovered from the perturbed data in the cluster head. 2) A flexible method for generating the privacy- preserving element was given. Thus, nodes could generate their privacy-preserving element without the extra data exchange, and the method was adapted to the dynamic reporting nodes. Extensive analysis showed that: compared with the centralized mechanism, the proposed mechanism has a better resistance to data loss, can avoid the single point problem and also consumes less communication overhead; compared with the other distributed mechanisms, the proposed mechanism is able to preserve privacy more efficiently while consuming less communication overhead.

Key words: sensor network; data aggregation; privacy preserving; congruence; privacy-preserving element

收稿日期：2011-03-22；**修回日期**：2011-08-31

基金项目：国家自然科学基金资助项目(60973031, 60903168)；国家教育部博士点基金资助项目(20100161110025)；湖南省教育厅资助科研项目(10B062)；湖南师范大学青年优秀人才培养计划基金资助项目(ET51102)

Foundation Items: The National Natural Science Foundation of China (60973031, 60903168); The PhD Programs Foundation of Ministry of Education of China (20100161110025); The Scientific Research Fund of Hunan Provincial Education Department of China(10B062); The Program for Excellent Talents in Hunan Normal University (ET51102)

1　引言

由于传感器节点能量的有限，传感器网络（sensor network）通常在网内对所采集的数据进行聚合处理，再将聚合结果发送给基站以减少传输能耗[1]。当传感器网络应用于民用领域中的敏感性数据监测时，感知对象通常不希望与其生活、健康等隐私信息相关的数据暴露，因此，节点所采集的数据需满足对其他节点的隐私性（即使得该节点以外的任何节点都不能获取其传感数据）[2]。然而，传统加密体系不能在保证数据隐私性的同时支持数据聚合；基于安全多方计算等技术的隐私保护方案由于开销昂贵也不适用于传感器网络[2]。数据聚合对传感数据的隐私性保护提出了新的挑战，亟待研究新的技术解决这一矛盾。

求和是一种基础的聚合函数，因为求均值及方差等函数均可以转化为求和函数[3]。实现了求和中的数据隐私保护则意味着实现了这一系列函数中的隐私保护。目前针对求和中的隐私保护问题已有一些研究工作[2~12]。这些工作通过隐藏传感数据实现其隐私保护，这就需要从隐藏数据中恢复出聚合值。隐藏技术的不同使得聚合值的恢复方式也不尽相同，按照是否可以从网内恢复出聚合值，可以将已有机制分为以下 2 类。

第 1 类机制由基站集中管理，聚合值不能在网内恢复。早期工作有 Castelluccia 等提出的机制[3]，该机制中各节点与基站共享秘密数 k，其发送的数据为隐藏后的数据$(d+k) \bmod M$（d 为传感数据）；当基站收到隐藏数据的聚合值后，减去相应的 k 恢复聚合值。由于基站必须知道哪些节点参与了聚合才能恢复出聚合值，该机制存在以下不足：1)当只有部分节点参与聚合时，需要上传 ID 信息。2)即使所有节点参与聚合，理论上无需上传 ID 信息，而一旦发生了分组丢失，聚合值将不能有效恢复[4]。3)如果敌方获取了秘密数及隐藏数据的范围，则可以猜测出相应传感数据的范围。针对上述问题，Castelluccia 等[5]、Feng 等[6]分别提出了加强机制，这些机制通过动态地生成参数 k 解决了问题 3)。Feng 等还通过一种折衷策略优化了问题 1)，然而，依然需要额外的 ID 传输开销[6]。此外，文献[7]和文献[8]也基于类似技术提出了由基站集中管理的机制。对上述机制而言，由于节点 ID 不能参与数据聚合，上传 ID 以解决数据分组丢失问题的方法因通信开销昂贵并不可行。此外，这些机制不能对基站保持传感数据的隐私性，这一问题在基站被俘获时尤为严重。

第 2 类机制通过节点协作分布式实现传感数据的隐私保护，聚合值可以在网内恢复，避免了第一类机制存在的问题。然而，依然存在不足。这类机制有 He 等提出的 CPDA（cluster-based private data aggregation）和 SMART（slice- mix- aggregate）[2]。CPDA 采取多项式技术，各节点需要与所有簇成员进行信息交互才能实现隐私保护，其隐私保护力度（所能容忍的被俘获节点数）及通信开销均随簇大小 m_c 的增长而增长；SMART 则通过将数据切分为 J 份并分发给不同邻居节点实现隐私保护，其隐私保护力度和通信开销随着 J 的增长而增长。因此，不能一味通过增大 m_c 和 J 的取值来提高两者的隐私保护力度；此外，这些机制难于同实现数据完整性保护的安全聚合机制兼容。为实现聚合值的完整性鉴别，He 等对 CPDA 和 SMART 分别进行了扩展，引入监督思想，基于冗余传输提出了机制 iPDA[9] 和 iCPDA[10]，然而，新的机制引发了更高的系统开销；且由于节点对间传输的隐私保护信息需要对其他节点保持机密性，依然不能实现成员节点间传输数据的完整性鉴别。在 Conti 提出的机制中，每对孪生节点共享多个双密钥，节点根据双密钥的使用情况隐藏传感数据，其隐私保护力度同样受限于通信开销[4]。Huang 等则基于异或及散列运算提出了与 Conti 的机制类似的机制[11]，然而，Huang 所提出的机制只适应于参与聚合的节点固定情况，而在实际应用中参与聚合的节点可能动态变化。Zeng 等基于同余的代数特性构造了隐私保护函数，在此基础上提出了隐私保护机制[12]，该机制同样难以兼容于实现数据完整性保护的安全聚合机制。

为有效解决数据聚合中的隐私保护问题，所提出机制应满足以下需求：① 实现传感数据的隐私性；② 保证聚合值的准确性；③ 能量有效，且当聚合节点动态变化时依然有效；④ 与其他安全数据聚合机制兼容。已有工作不能很好地满足上述需求，难于实际使用。本文致力于研究新的数据隐藏技术，主要创新和贡献如下。

1) 基于同余的代数特性定义了隐私保护元，各节点利用其隐私保护元，无需额外发送消息即可隐藏其传感数据以实现隐私性保护；而簇头一旦收到了簇内节点隐藏后的传感数据，通过模加运算即可

恢复出簇内聚合值。

2) 给出了一种使得节点可以独立、动态地生成其隐私保护元的方法。该方法基于散列运算和取模运算，易于实现，且无需额外通信交互。此外，该方法使节点不仅可以根据动态变化的数据聚合，参与节点动态地生成其隐私保护元，而且在参与聚合的节点相同时也可以生成不同的隐私保护元，保证了数据隐藏的安全性和灵活性。得益于动态变化的隐私保护元，节点通过异或运算即可实现簇内聚合值的机密性保护，且支持聚合值的完整性鉴别。

3) 基于所定义的隐私保护元及其生成方法，提出了分布式机制 DAPE（data aggregation mechanism based on privacy-preserving element）。DAPE 属于第二类机制，它不仅避免了第一类机制固有的问题，还具有更低的通信开销。而与同类机制相比，DAPE 不仅在提高隐私保护有效性的同时有着更低的通信开销，且无需额外开销即可与实现数据完整性鉴别的安全聚合机制，如文献[13]和文献[14]中机制兼容。

2 系统模型及相关假设

本文考虑典型的传感器网络，即由大量低耦合的传感器节点（简称节点）自组织而成的静态网络。节点类型如伯克利的 MICA 节点，它们通常配有 8MHz 的处理器，128KB 的 ROM，4KB 的 RAM。因此，虽然节点资源严格受限，但是拥有的空间足够用来存放数字节的隐私保护信息，且拥有足够的计算能力进行简单的计算操作如散列运算。网络部署后形成双层簇结构[15]，各簇成员知道所在簇的成员关系。

假设敌方可能俘获任何节点，且可以获取该节点所有的秘密信息。本文采用对偶密钥实现初始化中节点对之间信息传输的安全性，对偶密钥管理不是本文的研究内容，目前已有较多研究成果，在此基础上假设节点对间对偶密钥具有互异性[16,17]。尽管传感数据具有不同的数据类别，由于非整型数据可以转换为整型数据，且整型数据在存储和传输上通常更为有效，同文献[6]，假设参与数据聚合的传感数据为整型数据，且在 0 和上界 $d_{\max}$ 之间变化。

3 理论基础

本文以簇为聚合的基本单位，记簇内节点数为 n，并以从 1 标记到 n 的簇内 ID 表示各节点。相邻两次数据汇报间的间隔为一个阶段。在各阶段，节点可能汇报数据，也可能不汇报数据，为便于描述，记簇 C_a 中参与聚合的节点集合为 C'_a，C'_a 大小为 m（$m \leqslant n$）。为实现传感数据的隐私保护和聚合值的簇内恢复，定义了隐私保护元。隐私保护元的生成需要用到 P-序列，首先给出其定义。

定义 1 (P-序列) 任意节点 $b(b \in C'_a)$ 的 P-序列 P^b 是由 m 个整数构成的集合，按照簇内 ID 将其记为 $P^b = \{p_c^b, c \in C'_a\}$。$P^b$ 满足 $(\sum_{c \in C'_a} p_c^b) \bmod g = 0$，其中，$g = d_{\max} n$，$d_{\max}$ 为传感数据的上界。

各节点都对应一个秘密的 P-序列。节点的 P-序列用于生成其簇成员的隐私保护元。接下来给出隐私保护元的定义。

定义 2 (隐私保护元 R) 任意节点 $b(b \in C'_a)$ 的隐私保护元 $R^b = (\sum_{c \in C'_a} p_b^c) \bmod g$，其中，$p_b^c$ 为节点 $c(c \in C'_a)$ 的 P-序列中下标为 b 的元素。

接下来给出性质 1，性质 1 表明隐私保护元可以有效实现传感数据的隐私保护及簇内聚合值的准确还原。为便于描述，记节点 b 的传感数据为 d^b。

性质 1

1) 对于任意 C'_a，必有 $(\sum_{b \in C'_a} R^b) \bmod g = 0$；

2) 若 $(\sum_{b \in C'_a} d^b) \leqslant g - 1$，则 $(\sum_{b \in C'_a} (d^b + R^b)) \bmod g = \sum_{b \in C'_a} d^b$。

证明 1) $\because$ 对于 $\forall b \in C'_a$ 均有 $(\sum_{c \in C'_a} p_c^b) \bmod g = 0$，

$$
\begin{aligned}
&\therefore (\sum_{b \in C'_a} R^b) \bmod g \\
&= [\sum_{b \in C'_a} (\sum_{c \in C'_a} p_b^c) \bmod g] \bmod g \\
&= (\sum_{c \in C'_a} \sum_{b \in C'_a} p_b^c) \bmod g \\
&= [\sum_{c \in C'_a} (\sum_{b \in C'_a} p_b^c) \bmod g] \bmod g \\
&= (\sum_{c \in C'_a} 0) \bmod g = 0 。
\end{aligned}
$$

2)

$$
\begin{aligned}
&(\sum_{b \in C'_a} (d^b + R^b)) \bmod g \\
&= (\sum_{b \in C'_a} d^b + \sum_{b \in C'_a} R^b) \bmod g \\
&= (\sum_{b \in C'_a} d^b) \bmod g + (\sum_{b \in C'_a} R^b) \bmod g \\
&= \sum_{b \in C'_a} d^b 。
\end{aligned}
$$

算例 1 以 $C'_a = \{1, 2, 3\}$ 给出性质 1 的算例。设 g=12 626，各节点的传感数据及 P-序列如表 1 所示。节点 1 用来计算其隐私保护元的 P-序列元素为表 1 中划横线的数据。

以节点 1 给出隐私保护元的计算过程：R^1=(3 654+2 379+4 717)mod 12 626=10 750。类似地，其他节点可以获得其隐私保护元，如表 1 所示。不难验算得(R^1+R^2+R^3) mod 12 626=0，与性质 1 一致。

接下来以节点 1 给出传感数据的隐藏过程：$D^1=(d^1+R^1)\bmod g=(110+10\,750)\bmod 12\,626=10\,860$。类似地，其他节点可得其隐藏后的传感数据，如表 1 所示。于是：$D=(D^1+D^2+D^3)\bmod 12\,626=(10\,860+11\,569+3\,180)\bmod 12\,626=357$。由于 $d=d^1+d^2+d^3=110+69+178=357$，可见 $D=d$，与性质 1 一致。

表 1　　性质 1 的算例

节点 b	P-序列	d^b	R^b	D^b
节点 1	{3 654, 2 319, 6 653}	110	10 750	10 860
节点 2	{2 379, 5 114, 5 133}	69	11 500	11 569
节点 3	{4 717, 4 067, 3 842}	178	3 002	3 180

注 d^b：节点 b 的传感数据；R^b：节点 b 的隐私保护元；D^b：节点 b 隐藏后的传感数据

4　数据聚合中的隐私保护机制

DAPE 利用隐私保护元实现传感数据的隐私保护和聚合值的有效恢复。如图 1 所示，该机制包括初始化和数据汇报 2 部分，其中，初始化部分仅在网络部署后实施，数据汇报部分则反复运行。接下来给出详细的机制实现。

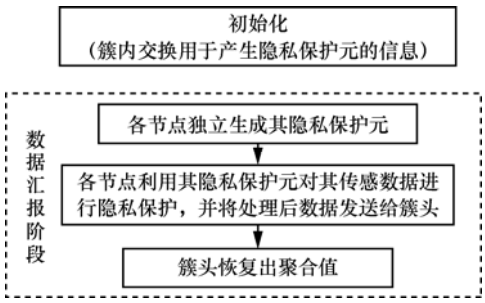


图 1　机制 DAPE 框架

4.1　初始化

在初始化过程中，各节点生成并分发用于生成其 P-序列的种子（P-序列的生成过程见 4.2 节）。此后，任意节点对(b, c)将共享且仅共享 2 个种子：$\{r_c^b, r_b^c\}$；任何节点都不能获得其他节点对间共享的种子。以簇 C_a 进行具体的过程描述，并记 b 与 c 间的对偶密钥为 $K_{b,c}$。

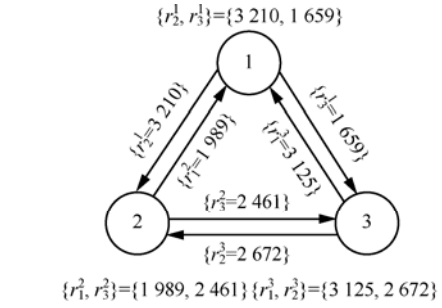
Step1　任意节点 b 随机生成 $\{r_c^b(c\neq b,\ 1\leqslant c\leqslant n)\}$ 作为生成其 P-序列的种子，其中，$\forall r_c^b(c\neq b,\ 1\leqslant c\leqslant n)$ 满足 $r_c^b<g$。接下来，节点 b 将 $\{r_c^b\}_{K_{b,c}}$ 发送给相应的节点 c ($c\neq b,\ 1\leqslant c\leqslant n$)。

Step2　任意节点 b 存储其生成的种子 $\{r_c^b(c\in C_a,\ c\neq b)\}$ 及收到的种子 $\{r_b^c(c\in C_a, c\neq b)\}$。为便于理解上述过程，以包含节点{1,2,3}的簇给出算例 2 如下。

算例 2　取 g=4 095，如图 2(a)所示，首先，各节点分别独立产生用于生成其 P-序列的 2 个种子。如节点 1 生成的种子为 $\{r_2^1, r_3^1\}=\{3\,210, 1\,659\}$。

接下来，如图 2(a)所示，各节点将其生成的种子发送给相应的簇成员。如节点 1 将{3 210}和{1 659}分别发送给节点 2 和节点 3。

最后，如图 2(b)所示，各节点存储所生成和接收的种子。如节点 1 所存储的种子为：$\{r_2^1, r_3^1\}\cup\{r_1^2, r_1^3\}=\{3\,210, 1\,659\}\cup\{1\,989, 3\,125\}$。从图 2(b)不难发现，任意节点对仅共享 2 个种子，如节点 1 和节点 2 所共享的种子为 3 210 和 1 989。



(a) 节点间种子交换过程

1　$\{r_2^1, r_3^1\}$ $\{r_1^2, r_1^3\}$ ={3 210, 1 659}　{1 989, 3 125}

2　$\{r_1^2, r_3^2\}$ $\{r_2^1, r_2^3\}$ ={1 989, 2 461}　{3 210, 2 672}

3　$\{r_1^3, r_2^3\}$ $\{r_3^1, r_3^2\}$ ={3 125, 2 672}　{1 659, 2 461}

(b) 各节点所存储的秘密种子

图 2　初始化过程的算例

4.2　数据汇报

首先将要用到的符号解释如下。

C_a'：簇 C_a 中参与聚合的节点集合；

r_c^b：由节点 b 生成且仅与节点 c 共享的种子；

r_b^c：由节点 c 生成且仅与节点 b 共享的种子；

p_c^b：节点 b 的 P-序列元素，并仅与节点 c 共享；

$H(\cdot)$：单向散列函数，其函数值的字长不小于

传感数据的字长；

d^b：节点 b 的传感数据；

R^b：节点 b 的隐私保护元；

D^b：节点 b 隐藏后的传感数据。

在各阶段，节点隐藏其传感数据并发送给簇头，由簇头恢复聚合值。以 C'_a（本文目的在于隐私保护，不再讨论 C'_a 的形成过程）进行描述，并仅描述 $m \geqslant 3$ 的情况；如果 $m<3$，则同 SMART[2]，各节点对数据进行切分和分发，不再赘述。

Step1（簇内数据隐藏） 任意节点 b 首先根据种子 $r_c^b (c \in C'_a, c \neq b)$ 计算其 P-序列元素 p_c^b，进而求出其 P-序列元素 p_b^b，具体计算如下

$$p_c^b = H(r_c^b, s) \bmod g \quad (c \in C'_a, c \neq b)$$

$$p_b^b = g - (\sum_{c \in C'_a, c \neq b} p_c^b) \bmod g$$

接下来，节点 b 根据种子 $r_b^c (c \in C'_a, c \neq b)$ 获取节点 c 的 P-序列元素 p_b^c；进而利用 $\{p_b^c (c \in C'_a, c \neq b)\}$ 和 p_b^b 生成其隐私保护元 R^b。

$$p_b^c = H(r_b^c, s) \bmod g \ (c \in C'_a, c \neq b)$$

$$R^b = (\sum_{c \in C'_a} p_b^c) \bmod g$$

最后，b 利用 R^b 隐藏 d^b：$D^b = (d^b + R^b) \bmod g$，并将 $\{D^b, b\}$ 发送给簇头。

Step1 中任意节点 b 产生的 $\{p_c^b (c \in C'_a)\}$ 为 P-序列，以下进行证明。

$$(p_b^b + \sum_{c \in C'_a, c \neq b} p_c^b) \bmod g$$

$$= [(g - (\sum_{c \in C'_a, c \neq b} p_c^b) \bmod g) + \sum_{c \in C'_a, c \neq b} p_c^b] \bmod g = 0$$

可见，$\{p_c^b (c \in C'_a)\}$ 符合 P-序列的定义，也因此，R^b 满足隐私保护元的定义。

Step2（簇内聚合） 簇头在获取了 C'_a 中各节点所发送的数据，即获取了 $\{\{D^b, b\} (b \in C'_a)\}$ 后，可恢复簇内聚合值 D，过程如下：

$$D = (\sum_{b \in C'_a} D^b) \bmod g$$

由性质 1 可知，$D = (\sum_{b \in C'_a} D^b)$。

记簇头收到其他簇所发送的数据为 $\tilde{D}$。接下来，簇头计算最终聚合值：$D_a = D + \tilde{D}$，并将其发送给下一跳节点。

算例 3（数据汇报过程）如图 3 所示，以 $C'_1 = \{1,2,3\}$ 给出数据汇报过程的算例，并设节点 1~3 的传感数据分别为 137、516 及 338，所处阶段 s 为 1。节点根据其种子及 $H(\cdot)$ 易于获取相应的 P-序列元素，给定这些值，如图 3 (a)所示，带下划线的数据为节点 1 所能获取的数据。

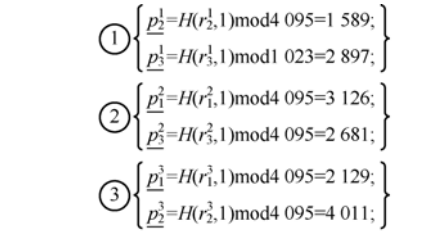
首先以节点 1 给出 R^1 的生成过程，如图 3(b)所示：利用 p_2^1 和 p_3^1 获取 p_1^1；进而利用 p_1^1、p_1^2 和 p_1^3 获取 R^1。类似地，节点 2 和 3 分别获取 R^2 和 R^3。

接下来，如图 3(c)所示，各节点利用其隐私保护元隐藏其传感数据并发送给簇头。例如，节点 1 利用 R^1 隐藏其传感数据 d^1，得到 $D^1 = 906$；节点 1 仅将 $\{D^1, 1\}$ 发送给簇头。类似地，节点 2 和 3 分别将 $\{D^2, 2\}$ 和 $\{D^3, 3\}$ 发送给簇头。从上述过程易于发现，由于采用了数据隐藏，敌方无法从各节点发送给簇头的数据中推测出其传感数据。

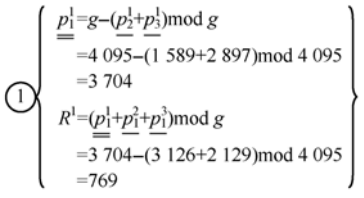
最后，如图 3 (c)所示，簇头根据 D^1、D^2 和 D^3 计算得 D。显然，$D = d$，这意味着簇内聚合值在簇头处得到了准确还原。

4.3 相关讨论

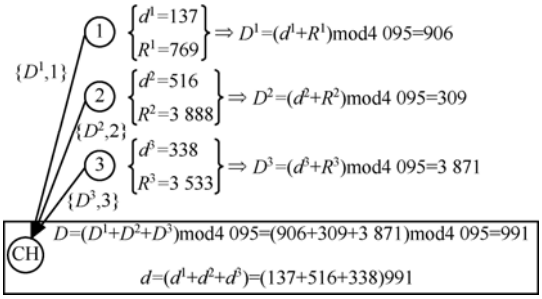
以明文发送 $\{D^b, b\}$ 并不会影响传感数据 d^b 的隐私性（分析见第 5.1 节）。考虑到有些应用场合不仅需要实现传感数据的隐私性，还需要保证簇内聚合值的机密性，而敌方如果获取了簇内各个 D^b，则可以获取簇内聚合值，采取以下方法实现聚合值的机密性保护。



(a) 节点1~3的种子所对应的P-序列值



(b) 节点1生成其隐私保护元



(c)CH 接收各节点发送的隐藏数据并获取聚合值

图 3 数据汇报过程的算例（CH 代表簇头）

簇内节点共享簇密钥 K_a，任意节点 b 在获得 D^b 后，利用 K_a 将 D^b 加密为 $D^b \otimes K_a$（$\otimes$ 为异或操作）并发送至簇头。簇头在收到了 $\{D^b \otimes K_a, b\}$ 后，首先计算 $D^b \otimes K_a \otimes K_a$ 以获取 D^b；之后按照 Step 2 操作即可获取聚合值。而敌方由于不能获取 K_a，不能还原出 D^b，必不能获取该簇的聚合值。

得益于动态变化的隐私保护元，上述方案中的 K_a 可以有效对抗已知明文攻击：假设敌方获取了 d^c，并获取了密文 $D^c \otimes K_a$，由于敌方不能获取 R^c，必不能由此获取 K_a。敌方只有俘获了某个簇成员才能获得 K_a；而此时虽然敌方可以获取各个 D^b，进而获取聚合值，如 5.1 节所分析，敌方并不能因此获取节点的隐私数据。值得一提的是，即使采用加密体系如 RC5 加密 D^b 以实现聚合值的机密性保护，只要簇密钥暴露了（簇内一个节点被俘获则簇内密钥将被暴露），聚合值一样会暴露。也就是说，传统加密体系在节点被俘获问题上并不会比上述方案更有效。因而，选择计算更有效的上述方案。关于被俘获节点的检测，可以参考文献[18]；关于节点被俘获所引发的簇密钥暴露问题，文献[19]给出了新的方法，不再详述。

最后讨论聚合值的完整性鉴别。由于无论以明文还是按照上述方法发送 $\{D^b, b\}$，簇内节点均可以获取簇头处理的数据，各节点都可以监督簇头的聚合操作。也因此，即使簇头被俘获了，簇头篡改聚合值的行为将被监测到。这意味着 DAPE 无需额外开销，即可实现数据完整性鉴别的安全聚合机制，如文献[13]和文献[14]中机制兼容。不再赘述完整性鉴别的具体过程。

5　性能评估

本节首先评估隐私保护有效性和数据聚合准确性，接下来评估系统开销。DAPE 中簇内参与聚合的节点数为 m，为便于比较，在 5.3 节及 5.4 节的开销评估中，将 CPDA 和 Conti 的机制的簇大小统一记为 m。

5.1　隐私保护有效性

集中式机制如 FSP（fully reporting SP-based）及 D-ASP（distributed adaptive SP-based）[6]中节点利用与基站共享的秘密数实现隐私保护，当基站被俘获时，其数据隐私将被暴露。对于各分布式机制而言，隐私保护有效性与被俘获节点/节点对间通信链路的暴露有关。在传感器网络中，节点对间信息传输的机密性通过对偶密钥加密实现。目前已有研究可以保证被俘获节点不会对其他节点间对偶密钥造成影响[16]，因此，节点对间加密链路的暴露等价于节点被俘获，也因此，接下来仅分析节点被俘获对典型的分布式机制 DAPE、CPDA[2]、SMART[2]及 Conti 的机制[4]所造成的影响。

DAPE 中任意的节点 b 利用其隐私保护元 R^b 对其传感数据 d^b 进行隐私保护，因此，敌方如果不能获取 R^b，则不能获取 d^b。1）假设敌方侥幸获取了某个阶段 s_0 的 d^b（通过攻破 DAPE 以外的方式），并获取了这一阶段的 D^b。虽然此时敌方可以获取 s_0 的 R^b（根据 $D^b = (d^b + R^b) \bmod g$），然而，只要种子或阶段数 s 的取值不重复，那么 s_0 所使用的 R^b 并不会确切地在某个阶段 s_0' 被重复使用，这意味着敌方不能由此获取节点 b 在任何其他阶段的隐私数据。而在传感器节点生命周期内，易于做到 s 的取值不重复；且即使 s 的取值存在重复的可能性，还可以通过更新种子满足这一条件。此外，由于 R^b 在各阶段都得到了更新，且由于散列函数的随机性，各阶段的 R^b 不存在关联性，敌方不能通过任何阶段 s_0 的 R^b 获取其他阶段的 R^b。最后，由于 R^b 并非某个散列值，而是多个散列值运算后的结果，敌方即使获取了某个 R^b，也不能获取生成该 R^b 的相应的秘密数的散列值，避免了敌方通过强力攻击获取各节点的秘密种子。可见，在这一攻击假设下，DAPE 是安全的。2）R^b 是基于 b 与 C_a' 中各节点所共享的秘密种子生成的。因此，敌方只有获取了 b 的所有秘密种子才能获取其各阶段的 R^b。由于任何节点对间所共享的种子与其他节点对间所共享的种子互异，敌方只有俘获了 C_a' 中所有节点才能获取足够的种子信息进而获取各阶段的 R^b。于是，DAPE 所能容忍的被俘获节点数为$(m-1)$。

CPDA 中所有参与聚合的节点成簇，任意节点 b 的数据隐私暴露当且仅当其所在簇成员串谋。记 CPDA 的簇大小为 m_c，则其所能容忍的被俘获节点数为 $(m_c - 1)$。SMART 中任意节点 b 的数据隐私暴露当且仅当其入度与出度节点均被俘获。因此，SMART 所能容忍的被俘获簇节点的平均数目为 $3(J-1)/2$。Conti 的机制中的各节点与簇内成员共享 A 个双密钥，每轮数据汇报使用 $V(V \leqslant A)$个。记其簇大小为 C，被俘获的节点数为 w，则节点的数据隐私被暴露的概率为 $[(2w-1)/(C-1)]^V$。对于 Conti 的机制而言，即使敌方只俘获了 2 个簇节点，仍然

有机会获取节点的数据隐私。

综上，如果 $m>m_c$，那么 DAPE 比 CPDA 可以容忍更多的被俘获节点，即有着更强的隐私保护力度。如果 $m>3(J-1)/2$，则 DAPE 比 SMART 有着更强的隐私保护力度。而即使 $m=C$，DAPE 的隐私保护有效性也要高于 Conti 的机制。

5.2 数据聚合准确性

对于 DAPE、CPDA、SMART、Conti 的机制及 FSP、D-ASP 而言，如果所有消息均发送成功了，那么基站所获取的聚合值均为准确的聚合值（性质 1 保证了 DAPE 具有这一性能）。然而，数据分组在实际传输中可能被丢失或损害，将对这些机制造成不同的影响，以下进行具体分析。

对于 FSP 及 D-ASP，由于不是所有数据后都附加了源节点 ID，如果簇内发生传输失败，簇头将无法检测到哪些分组丢失；如果簇间发生传输失败，如分组丢失，由于基站同样无法获取丢失数据分组的信息，将无法确定使用哪些秘密数进行数据还原。因此，即使只有一个分组丢失，基站也无法还原所收到数据的聚合值。这一问题可以通过在每一个数据分组后附上源节点 ID 进行解决，然而，由于节点 ID 不能参与数据聚合，该方法可能引发昂贵的额外通信开销，可行性不强。

对于 DAPE，CPDA 及 Conti 的机制而言，如果簇内发生传输失败，簇头根据成功接收的数据分组中的 ID 信息即可检测到哪些分组丢失。因此，各簇向其他簇发送的总是准确的聚合值。也因此，即使簇间存在分组丢失等失效传输，基站也能获取数据的准确聚合结果。SMART 可以扩充为这一类情况。而由于 CPDA、SMART 及 Conti 中节点需要发送的数据多于 DAPE（详见 5.3 节），在数据分组传输失效率相同且数据发送期限相同的前提下，DAPE 将能发送更多的数据分组。也因此，就数据聚合准确度而言，DAPE 最为适合信道脆弱的传感器网络。

5.3 通信开销

本节分析和比较各机制在数据汇报阶段的通信开销。为便于描述，记传感数据长 L_{sen} bit；网络节点数为 N，节点的全局 ID 长 l_{glo} ($l_{\text{glo}}=\lceil\log N\rceil$) bit；DAPE 的簇节点数为 n，记簇内 ID 长 l_{clu} ($l_{\text{clu}}=\lceil\log n\rceil$)bit；D-ASP 中的 $list_b$ 列表（节点 ID 构成）长 $L_{\{\text{ID}\}}$ bit。为便于分析和比较，同文献[6]中，假定网络部署后形成多个单跳簇。必须要说明的是，即使是多跳簇，也不会影响 DAPE 在通信上的优势，因为如同下文分析的，DAPE 中各节点仅需发送一个数据分组，且分组长小于其他机制。由于 DAPE、CPDA、SMART 及 Conti 的机制的簇间通信开销与没有提供隐私保护的机制一样，额外的通信开销仅在簇内通信中产生，接下来仅分析其簇内通信开销。

DAPE 中任意节点 b 的通信开销源于将 $\{D^b,b\}$ 发送给簇头，其中，D^b 的数据范围为 $[0,g-1]$。由于 $g=d_{\max}n$，而 $\lceil\log n\rceil=l_{\text{clu}}$，且 $\lceil\log d_{\max}\rceil=L_{\text{sen}}$，于是，$D^b$ 长 $(L_{\text{sen}}+l_{\text{clu}})$ bit，则 $\{D^b,b\}$ 长 $(L_{\text{sen}}+2l_{\text{clu}})$ bit。值得注意的是，虽然 DAPE 的隐私保护有效性与 $m(m\leqslant n)$成正比，而 m 随 n 的增长而增长，这意味着 n 越大则隐私保护有效性越高，由于 $l_{\text{clu}}=\lceil\log n\rceil$，通信开销随 n 的增长是缓慢增长的。可见，DAPE 的隐私保护有效性并没有受限于通信开销。

CPDA 中的任意节点 b 需要将隐藏后的传感数据 $\{V_c^b,b\}$ 发送给任意簇成员 c，其中，$\left|V_c^b\right|\geqslant L_{\text{sen}}$；$b$ 还需要将隐藏后的传感数据 $\{F_b,b\}$ 发送给簇头，其中，$\left|F_b\right|\geqslant(L_{\text{sen}}+l_{\text{clu}})$。于是，各节点总的通信开销不小于 $[m(L_{\text{sen}}+l_{\text{glo}})+l_{\text{clu}}]$ bit。

SMART 中节点将其传感数据分为 J 块（每个块数据的长 L_{sen} bit），并将其中的$(J-1)$块分别发送给$(J-1)$个邻居节点。此外，该节点将所收到的数据及所保留的块数据进行聚合并发送给下一跳节点，该数据长为 $(L_{\text{sen}}+l_{\text{clu}})$ bit。因此，各节点至少需要发送 J 个消息分组，总的通信开销大于 $(JL_{\text{sen}}+l_{\text{clu}})$ bit。

Conti 的机制中的任意节点 b 在汇报其传感数据前需要发送 2 条 $\{S,\{s_i,H(k_i)\}\}$ 以确定双密钥的使用情况，如果孪生节点所共享的双密钥互异，则该信息的平均长度为 $(Am/4)L_{\text{sen}}$ bit（A 为节点所拥有的双密钥数目，$A\geqslant 2$）；否则，大于这一长度。之后，节点 b 利用其相应的双密钥隐藏其传感数据，最终将隐藏结果 $\{d_b+H(seed,k_i)\}$ 发送给簇头。因此，各节点的通信开销不小于 $[1+(Am/2)]L_{\text{sen}}$ bit。

FSP 中任意节点 b 的通信开销源将 $\{\hat{D}_b,\hat{A}_b\}$ 发送给簇头。$\hat{D}_b$ 和 $\hat{A}_b$ 的数据范围均为 $[0,q-1]$。由于 $q>\max\{2N,\ 2^{L_{\text{sen}}-1}\}$，于是，各节点总的通信开销为

表 2　　各机制中任意节点的簇内通信开销

机制名	消息至 CH/数目	消息至其他节点/数目	消息长度（不含分组头）/bit	总的开销（不含分组头）/bit
CPDA	$\{F_b, ID\}$ /1	$\{V_c^b, ID\}$ /$(m-1)$	$\lvert\{F_b, ID\}\rvert \geqslant (L_{\text{sen}} + l_{\text{clu}} + l_{\text{glo}})$ $\lvert\{V_c^b, ID\}\rvert \geqslant (L_{\text{sen}} + l_{\text{glo}})$	$\geqslant [m(L_{\text{sen}} + l_{\text{glo}}) + l_{\text{clu}}]$
SMART	—	$\{S_{b,c}\}$ /$(J-1)$; $\{S_b\}$ /1	$\lvert\{S_{b,c}\}\rvert = L_{\text{sen}}$, $\lvert\{S_b\}\rvert > L_{\text{sen}}$	$> (JL_{\text{sen}} + l_{\text{clu}})$
FSP	$\{\hat{D}_b, \hat{A}_b\}$ /1	—	$\lvert\{\hat{D}_b, \hat{A}_b\}\rvert = 2\max\{L_{\text{sen}}, l_{\text{glo}} + 1\}$	$2\max\{L_{\text{sen}}, l_{\text{glo}} + 1\}$
D-ASP	$\{\hat{D}_b, \hat{A}_b, ID_{\text{glo}}\}$ 或$\{\hat{D}_b, \hat{A}_b\}$ /1	控制信息	$\lvert\{\hat{D}_b, \hat{A}_b, ID_{\text{glo}}\}\rvert = (2\max\{L_{\text{sen}}, l_{\text{glo}} + 1\} + l_{\text{glo}})$	$(2\max\{L_{\text{sen}}, l_{\text{glo}} + 1\} + l_{\text{glo}})$
Conti	$\{d_b + H(seed, k_i)\}$ /1	$\{S, \{s_i, H(k_i)\}\}$ /2	$\lvert\{d_b + H(seed, k_i)\}\rvert = L_{\text{sen}}$ $\lvert\{S, \{s_i, H(k_i)\}\}\rvert = AmL_{\text{sen}}/4$	$[[1 + (Am/2)]L_{\text{sen}}$
DAPE	$\{D_b, ID'\}$ /1	—	$\lvert\{D_b, ID'\}\rvert = (L_{\text{sen}} + 2l_{\text{clu}})$	$(L_{\text{sen}} + 2l_{\text{clu}})$

注：m: 协作进行隐私保护的节点数；J: 数据分块数；A: 节点拥有的双密钥数目，$A \geqslant 2$；l_{glo}：节点全局 ID 长度；l_{clu}：节点的簇内 ID 长度；$|\{M\}|$: 消息 M 的长度。

$2\max\{L_{\text{sen}}, (l_{\text{glo}} + 1)\} \geqslant 2L_{\text{sen}}$ bit。D-ASP 中任意节点 b 发送给簇头的消息为 $\{\hat{D}_b, \hat{A}_b, list_b(\text{ID list})\}$，因此，总的通信开销为 $2 \times \max\{L_{\text{sen}}, (l_{\text{glo}} + 1)\} + L_{\{\text{ID}\}}$ bit。

表 2 总结了上述机制的通信开销。由于 $J \geqslant 3$，$l_{\text{glo}} > l_{\text{clu}}$，$m \geqslant 3$，$A \geqslant 2$，易知 DAPE 的通信开销比其他分布式机制要低。$2\max\{L_{\text{sen}}, (l_{\text{glo}} + 1)\} < (L_{\text{sen}} + 2l_{\text{clu}})$ 成立的条件是 $L_{\text{sen}} < 2l_{\text{clu}}$，而即使 $l_{\text{clu}} = 5$（可支持大小为 32 的簇），要想满足 $L_{\text{sen}} < 2l_{\text{clu}}$，需满足 $d_{\max}$ <1 024 或 N<512，可见 $L_{\text{sen}} < 2l_{\text{clu}}$ 的成立受限于实际情况。也就是说，一般情况下，DAPE 在通信上比 FSP 更为有效，则显然 DAPE 比 D-ASP 在通信上更为有效。

DAPE 的通信开销与 L_{sen} 及 l_{clu} 有关。为了直观地展示 DAPE 在不同的 L_{sen} 及 n 取值下相对其他机制的通信有效性，以单跳簇给出算例 4 如下。

算例 4　（节点的通信开销）：CPDA 和 SMART 的通信开销分别随 m 和 J 的增长而线性增长，机制的提出者将 m 和 J 的取值推荐为 3（此时两者能容忍 2 个被俘获节点），按照推荐值计算两者开销。Conti 的通信开销与 A($A \geqslant 2$)及 m 相关，取 A=2 且同样取 m=3 进行计算。DAPE 的通信开销与 m 无关，表 3 给出了各机制在 L_{sen} 及 n 变化时开销的变化情况，此时全局 ID 随簇内节点数的变化而变化。

从表 3 可以直观看出，DAPE 的通信开销是轻量的，其随簇大小 n 的增长而缓慢增长，这是由于 $l_{\text{clu}} = \log\lceil n \rceil$；其随 L_{sen} 的增长而线性增长，然而，其随 L_{sen} 增长而增长的速度小于其他机制。虽然其他机制中参数的选取均为最小值，DAPE 仍然比其他机制具有更低的通信开销，特别是与分布式机制相比，通信上的优势更为明显。值得一提的是，DAPE 的通信开销与 m 无关，即使 m=n，其通信开销也是一样的，而其他机制如果取 m=n，通信开销将迅速增长。此外，如果增大 A，Conti 的机制在隐私保护有效性增强的同时，开销同样会迅速增大。可见，DAPE 比已有分布式机制有着更高的隐私保护有效性，且通信也更为有效。

表 3　各节点簇内通信开销的算例（单位 bit）

参数值	CPDA	SMART	FSP	Conti	DAPE
n=8 ($l_{\text{clu}} = 3$), $L_{\text{sen}} = 11$	71	36	$\geqslant 22$	44	17
n=12 ($l_{\text{clu}} = 4$), $L_{\text{sen}} = 11$	71	37	$\geqslant 22$	44	19
n=16 ($l_{\text{clu}} = 4$), $L_{\text{sen}} = 11$	71	37	$\geqslant 22$	44	19
n=20 ($l_{\text{clu}} = 5$), $L_{\text{sen}} = 11$	71	38	$\geqslant 22$	44	21
n=20 ($l_{\text{clu}} = 5$), $L_{\text{sen}} = 12$	74	41	$\geqslant 24$	48	22
n=20 ($l_{\text{clu}} = 5$), $L_{\text{sen}} = 13$	77	44	$\geqslant 26$	52	23

注：CPDA 和 Conti 机制中协作进行隐私保护的节点数 m 取 3；SMART 中，J=3；A=2。

5.4　存储和计算开销

5.4.1　*存储开销*

DAPE 中节点需要存储 $2(n-1)$个种子，开销为 $2(n-1)(L_{\text{sen}} + l_{\text{clu}})$ bit。CPDA 中的种子是临时生成的；SMART 利用数据切分技术实现隐私保护，因此，两者无需额外的存储开销，然而，以高的通信

开销为代价。Conti 的机制中各节点需要存储 K 个密钥，存储开销为 KL_{sen} bit。FSP 及 D-ASP 中节点需要存储 2 个种子，开销为 $2\max\{L_{\text{sen}},(l_{\text{glo}}+1)\}$ bit。

综上，DAPE 的存储开销低于 Conti 的机制，高于其他机制。由于 n 为簇大小，DAPE 的存储开销仍然是合适的。例如：1）取 $L_{\text{sen}}=11$ bit（传感数据范围为 0~2 047），n=8($l_{\text{clu}}=3$ bit)，则存储开销为 25byte。2）仍然取 $L_{\text{sen}}=11$ bit，则即使 n=20（此时 l_{clu} 为 5bit），存储开销为 76 B。3）仍然取 n=20，取 $L_{\text{sen}}=16$ bit（此时传感数据范围为 0~16 383），存储开销为 100byte。节点数目为 20 的簇已经是较大的簇了，且 0~16 383 可以包含常见的传感数据范围，而此时的存储开销仅为 100byte，可见 DAPE 的存储开销是适合的。

5.4.2 计算开销

DAPE 分为初始化和数据汇报 2 部分：1）初始化中各节点将种子加密发送给簇成员，并解密收到种子，总的计算开销为 2(n−1)次加/解密。可见，初始化的计算开销是合适的。2）在数据汇报部分，各节点通过散列运算获取 2(m−1)个 P-序列元素值；并利用其隐私保护元隐藏传感数据，总的计算开销为 2(m−1)次散列运算及复杂度为 2o(m) 的四则运算。簇头对所收到的数据进行复杂度为 o(m) 的四则运算。如果需要实现聚合值的机密性，则普通节点及簇头只需分别增加 1 次及(m−1)次异或运算即可。

CPDA 中节点分别加密发送给簇成员的数据，解密收到的数据并进行四则运算，最终值加密发送给簇头，总的计算开销为 2m 次加/解密及复杂度为 2o(m) 的四则运算；簇头在解密收到的成员数据后，通过高斯消去法还原聚合值，其计算开销为 m 次加/解密、1 次矩阵求逆。

SMART 中节点将其传感数据切分为 J 份并将其中的(J−1)份加密发送给邻居节点，还需要将收到的数据解密求和，其计算开销为 2J 次加/解密及复杂度为 2o(J) 的四则运算。

Conti 的机制中节点对 A 个双密钥进行 2 次散列运算，再利用运算值进行传感数据的隐藏保护，因此，其计算开销为 2A 次散列运算，复杂度为 o(A) 的四则运算，4 次加/解密。此外，簇头需要解密所收到的数据并求和，计算开销为 m 次加/解密及复杂度为 o(m) 的四则运算。

表 4 存储开销和数据汇报阶段的计算开销

	CPDA	SMART	Conti 的机制	FSP/D-ASP	DAPE
存储开销/bit	—	—	KL_{sen}	$2\max\{L_{\text{sen}},(l_{\text{glo}}+1)\}$	$2(n-1)(L_{\text{sen}}+l_{\text{clu}})$
计算开销(节点)	2 次加/解密；复杂度为 o(m)	2J 次加/解密；复杂度为 2o(J)的四则运算	2A 次散列运算复杂度为 o(A)的四则运算；4 次加/解密	1 次散列运算；复杂度为 o(m)的四则运算	2(n−1)次散列运算；复杂度为 2o(m)的四则运算；1 次异或操作
计算开销(簇头)	1 矩阵求逆；m 次解密	—	m 次加/解密；复杂度为 o(m)的四则运算	复杂度为 o(m)的四则运算	复杂度为 o(m)的四则运算；(m−1)次异或操作

FSP 及 D-ASP 中节点首先对其秘密数进行散列运算；之后，利用运算值进行传感数据的隐藏保护，各节点的计算开销为 1 次散列运算、复杂度为 o(m) 的四则运算；簇头的计算开销为复杂度为 o(m) 的四则运算。

表 4 总结了各机制的存储开销和数据汇报阶段的计算开销，其中，DAPE 的计算开销是按照实现了聚合值的机密性保护评估的。从表 4 可以看出，DAPE 的存储开销低于 Conti 的机制，高于其他机制；计算开销高于 FSP 及 D-ASP，低于其他机制。然而，如同前文分析的，DAPE 的存储和计算开销仍然是轻量的，适合于传感器网络。

6 结束语

本文提出了一种对聚合中的传感数据提供隐私保护的机制 DAPE。基于构造的隐私保护元，DAPE 中节点无需额外的信息交互即可实现其传感数据的隐私保护，且簇内聚合值可以在簇内得到有效还原。因此，与可以在网内实现聚合值还原的其他机制相比，DAPE 在提高隐私保护有效性的同时在通信上更为有效，且还可以兼容于实现数据完整性鉴别的安全聚合机制；与需要由基站恢复聚合值的机制相比，DAPE 能够更好地适应脆弱的无线通信信道，且在通信方面更为有效。虽然 DAPE 的存储和计算开销高于部分已有机制，由于存储开销仅与簇节点数 n 正相关，而节点的计算开销主要源于(m−1)次散列运算（$m\leqslant n$），因此，DAPE 的存储和计算开销仍然是轻量的。可见，DAPE 更适用于资源有限且应用相关的传感器网络。

参考文献：

[1] TANG X, XU J. Extending network lifetime for precision constrained data aggregation in wireless sensor networks[A]. Proceedings INFOCOM 2006: 25th IEEE International Conference on Computer Communications[C]. Piscataway, USA, 2006. 131-146.

[2] HE W, LIU X, NGUYEN H, *et al*. PDA: privacy-preserving data aggregation in wireless sensor networks[A]. Proceedings INFOCOM 2007: 26th IEEE International Conference on Computer Communications[C]. Piscataway, USA, 2006. 165-168.

[3] CASTELLUCCIA C, MYKLETUN E, TSUDIK G. Efficient aggregation of encrypted data in wireless sensor networks[A]. MobiQuitous 2005: Second Annual International Conference on Mobile and Ubiquitous Systems Networking and Services[C]. San Diego, California, USA, 2005. 109-117.

[4] CONTI M, ZHANG L, ROY S, *et al*. Privacy-preserving robust data aggregation in wireless sensor networks[J]. Security and Communication Networks, 2009,2(2):195-213.

[5] CASTELLUCCIA C, CHAN A, MYKLETUN E, *et al*. Efficient and provably secure aggregation of encrypted data in wireless sensor networks[J]. ACM Transactions on Sensor Networks, 2009,5(3):1-36.

[6] FENG T, WANG C, ZHANG W, *et al*. Confidentiality protection schemes for data aggregation in sensor networks[A]. Proceedings INFOCOM 2008: 27th IEEE International Conference on Computer Communications[C]. Piscataway, USA, 2008. 131-146.

[7] WESTHOFF D, GIRAO J, ACHARYA M. Concealed data aggregation for reverse multicast traffic in sensor networks: encryption, key distribution, and routing adaptation[J]. IEEE Transactions on Mobile Computing, 2006,5(10):1417-1431.

[8] BISTA R, CHONJU C, SONG M, *et al*. Preserving privacy and assuring integrity in data aggregation for wireless sensor networks[A]. 2010 IEEE International Conference on Networked Embedded Systems for Enterprise Applications, NESEA 2010[C]. Soochow, China, 2010. 128-237.

[9] HE W, LIU X, NGUYEN H, *et al*. Abdelzaher. iPDA: an integrity-protecting private data aggregation scheme for wireless sensor networks[A]. Proceedings IEEE Military Communications Conference MILCOM[C]. Washington, DC, USA, 2008. 1-7.

[10] HE W, LIU X, NGUYEN H, *et al*. A cluster-based protocol to enforce integrity and preserve privacy in data aggregation[A]. Proceedings of the 29th IEEE International Conference on Distributed Computing Systems Workshops[C]. Anchorage, Alaska, 2009. 14-19.

[11] HUANG S, SHIEH S, TYGAR J. Secure encrypted-data aggregation for wireless sensor networks[J]. Wireless Networks, 2010,16(4): 915-927.

[12] ZENG W, LIN Y, WANG L. Privacy-preserving data aggregation based on the p-function set in wireless sensor networks[A]. Proceedings of the 2010 IEEE 10th International Conference on Computer and Information Technology (CIT 2010)[C]. Bradford, United Kingdom, 2010. 2831-2836.

[13] BEKARA C, LAURENT-MAKNAVICIUS M. A secure aggregation protocol for cluster-based wireless sensor networks with no requirements for trusted aggregator nodes[A]. NGMAST 2007 - The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies, Proceedingss[C]. Piscataway, USA, 2007. 1-10.

[14] SUAT O, CAM H. Integration of false data detection with data aggregation and confidential transmission inwireless sensor networks[J]. IEEE/ACM Transactions on Networking, 2010,18(3):736-749.

[15] GUAN X, GUAN L, WANG X. A novel energy efficient clustering technique based on virtual hexagon for wireless sensor networks[J]. International Journal of Innovative Computing, Information and Control, 2011, 7(4):1891-1904.

[16] ZHANG W, TRAN M, ZHU S, *et al*. A random perturbation-based scheme for pairwise key establishment in sensor networks[A]. MobiHoc'07: Proceedings of the Eighth ACM International Symposium on Mobile Ad Hoc Networking and Computing[C]. New York, USA, 2007. 90-99.

[17] ALI F, MEHDI B, HOSSEIN S, *et al*. A high performance and intrinsically secure key establishment protocol for wireless sensor networks[J]. Computer Networks, 2011,55(8):1849-1863.

[18] MUKHERJEE P, SEN S. Comparing reputation schemes for detecting malicious nodes in sensor networks[J]. Computer Journal, 2011,54(3): 482-489.

[19] WEN M, ZHENG Y, YE W, *et al*. A key management protocol with robust continuity for sensor networks[J]. Computer Standards & Interfaces, 2009,31(4): 642-647.

作者简介：

曾玮妮（1982-），女，湖南邵阳人，博士，中国船舶重工集团公司第 716 研究所高级工程师，主要研究方向为传感器网络。

林亚平（1955-），男，湖南邵阳人，博士，湖南大学教授、博士生导师，主要研究方向为通信网络和机器学习。

何施茗（1986-），女，湖南永州人，湖南大学博士生,主要研究方向为无线网络。

余建平（1979-），男，湖南怀化人，博士，湖南师范大学副教授，主要研究方向为传感器网络及群体智能。