无线传感器网络隐私保护数据聚集技术

张晓莹[1,2]，彭辉[3]，陈红[1,2]

（1. 中国人民大学信息学院，北京 100872；2. 中国人民大学数据工程与知识工程教育部重点实验室，北京 100872；
3. 工业和信息化部电子第五研究所，广东 广州 510000）

摘 要：对无线传感器网络隐私保护数据聚集技术的研究现状与进展进行了综述。首先介绍研究相关的基础知识，包括网络模型、攻击模型和性能评估指标；然后按照同态加密、数据扰动、切分重组、泛化、安全多方计算等隐私保护技术对现有研究成果进行分类，详细阐述了具有代表性的协议的核心技术，对比分析了的各协议的性能；最后，对未来研究方向进行了展望。

关键词：隐私保护；数据聚集；无线传感器网络；物联网

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000-436x.2018101

State-of-the-art survey of privacy-preserving data aggregation in wireless sensor networks

ZHANG Xiaoying[1,2], PENG Hui[3], CHEN Hong[1,2]

1. School of Information, Renmin University of China, Beijing 100872, China
2. Key Laboratory Data Engineering and Knowledge Engineering of Ministry of Education, Renmin University of China, Beijing 100872, China
3. The Fifth Electronic Research Institute of MIIT, Guangzhou 510000, China

Abstract: A state-of-the-art survey of privacy-preserving data aggregation techniques in wireless sensor networks was reviewed. Firstly, preliminaries were introduced, including network models, adversary models, and performance evaluation metrics. Secondly, existing related work was classified into several types according to privacy preservation techniques, such as homomorphic encryption, data perturbation, slicing-mixing technique, generalization, secure multiparty computation, and the key mechanisms of typical protocols were elaborated and analyzed. Finally, the promising future research directions were discussed.

Key words: privacy preservation, data aggregation, wireless sensor networks, internet of things

1 引言

无线传感器网络[1]（以下简称传感器网络）是由大量微型传感器节点通过自组织方式形成的多跳分布式网络系统，通过传感器节点感知、计算、传输数据为人们提供服务，允许人们在任何时间、任何地点和任何环境下获取大量重要的信息。例如，数据聚集是传感器网络向用户提供的基本但重要的查询服务之一[2]。常见的聚集查询类型有求和、求极值、求平均值、计数等。作为物联网的重要组成部分，近年来，传感器网络已经被广泛应用在军事国防、智能家居、卫生医疗等重要领域，但是在多个关键性领域的实际应用与部署过程中暴露出严重的隐私泄露问题，例如，在智能电网中，供电公司通过传感器网络下发求

收稿日期：2017−11−08；**修回日期**：2018−04−08

通信作者：陈红，chong@ruc.edu.cn

基金项目：国家自然科学基金资助项目（No.61532021, No.61772537, No.61772536, No.61702522）；国家重点研究发展计划基金资助项目（No.2016YFB1000702）

Foundation Items: The National Natural Science Foundation of China (No.61532021, No.61772537, No.61772536, No.61702522), The National Key R & D Program of China (No.2016YFB1000702)

和聚集命令获取某个小区在用电高峰期的总用电量；智能电表读取家庭用电信息后通过传感器网络传回数据。这些数据属于个人和家庭隐私，一旦在聚集过程中泄露，就会泄露家里是否有人、何时无人等敏感信息。传感器网络在实际应用中暴露出的隐私问题会泄露监测对象的重要信息，甚至会威胁到监测对象的安全，这极大地阻碍了传感器网络的广泛应用。因此，研究传感器网络隐私保护技术对传感器网络和物联网的发展具有积极意义。

传感器网络隐私保护数据聚集技术的目标是：在数据聚集的过程中，有效控制非法用户对网络敏感信息的访问，防止网络敏感信息的泄露，同时尽可能地减少能量消耗，降低节点通信成本和计算代价，提高聚集结果的精确性和可靠性。

传感器网络具有资源有限、自组织、多跳等特征，这些特征使隐私保护数据聚集的实现面临着节点的计算能力和通信能力有限、网络攻击方式多样化、单纯的数据加密机制不适用等难题，给隐私保护数据聚集技术的研究带来了严峻的挑战。

1) 节点资源受限导致高能耗的安全技术无法适用。传感器节点的能量、通信范围、计算能力、存储空间等资源都非常有限。高能耗的安全技术产生频繁的通信和复杂的计算，必将造成网络能量很快消耗殆尽、缩短网络的生命周期。因此，如何实现低通信量和低计算量的隐私保护技术，最大程度地减少能量开销，延长网络生命周期，是研究传感器网络隐私保护数据聚集技术面临的首要挑战。

2) 网络的开放性导致攻击方式多样化。传感器节点一般通过飞机播散等方式被随机部署到无人值守的应用环境中，使人们无法预知节点的位置、邻居关系以及攻击者等信息，节点间的无线通信容易受到窃听、篡改、恶意代码注入等多种攻击的影响。因此，如何设计能够抵御复杂多变的网络攻击的隐私保护技术，是研究传感器网络隐私保护数据聚集技术面临的另一挑战。

3) 网内聚集使得网络隐私保护难度增加。传感器网络作为一种分布式网络系统，其拓扑结构复杂，主要以网内聚集（in-network aggregation）的方式实现数据聚集。这种方式虽然能够去掉冗余数据，减少网络通信，但是其可行性是建立在获取节点数据的基础上，这导致单纯的数据加密机制不能满足数据网内聚集的要求，增加了隐私保护的难度。因此，如何平衡聚集性能和隐私保护需求之间的矛盾，设计出适用于传感器网络聚集的隐私保护技术是传感器网络隐私保护数据聚集技术研究面临的重要挑战。

隐私保护数据聚集技术由 Joao 等[3]于 2005 年提出，已逐渐得到学术界的广泛关注。本文系统总结了现有的传感器网络隐私保护数据聚集技术研究成果，按照所采用的隐私保护技术对现有研究成果进行了分类，详细阐述了具有代表性的协议的核心技术，分析比较了各协议的主要优缺点，最后指出了未来的研究方向。

2　基础知识

为了便于读者理解，本节针对传感器网络隐私保护数据聚集技术研究涉及的常用基础知识进行简要介绍。

2.1　网络模型

网络模型是对传感器网络所采用的拓扑结构的抽象，直接影响传感器网络数据聚集的方式。常见的传感器网络主要有 2 种，分别是节点相似的传感器网络（wireless sensor networks with similar nodes）和两层传感器网络（two-tiered wireless sensor networks）。

节点相似的传感器网络由 2 种节点组成，分别是基站（sink）和传感器节点，网络结构如图 1 所示。基站负责向网络下发用户的命令，并将执行结果返回用户。传感器节点负责采集、传输数据，路由路径上的中间节点还需要根据查询类型执行计算、融合等操作。在该网络模型中，基站较少，通常只有一个，而传感器节点往往有成百上千个。传感器节点之间是对等的关系，具有相同的初始能量、存储空间、通信和计算能力。除了基站，其他所有传感器节点的资源都是有限的。

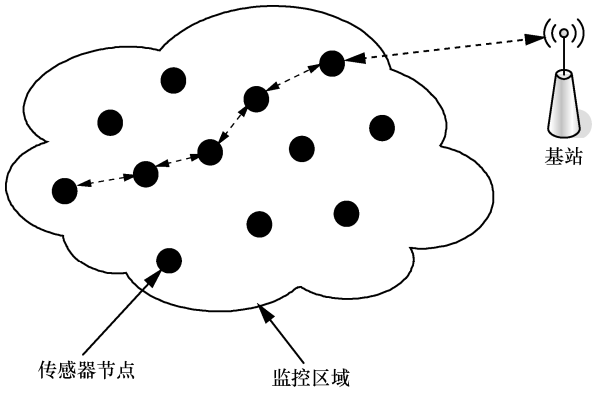

图 1　节点相似的传感器网络结构

如果在节点相似的传感器网络中引入一种特殊的节点——管理节点（又称存储节点，master node），就构成了两层传感器网络，其网络结构如图 2 所示，大量的传感器节点位于网络的底层，少量的管理节点位于网络的上层。与节点相似的传感器网络不同的是，在两层传感器网络中，基站不再将用户的命令广播到网络中，而是只下发到管理节点，传感器节点也不再将数据传输到基站，而是周期性地采样并定期上传数据到所属的管理节点。管理节点负责存储其管辖范围内传感器节点的数据，执行来自基站的命令。相对于传感器节点，基站与管理节点都属于高资源节点，其资源不受限制。

现有的传感器网络隐私保护数据聚集协议主要基于节点相似的传感器网络，也有少数基于两层传感器网络。

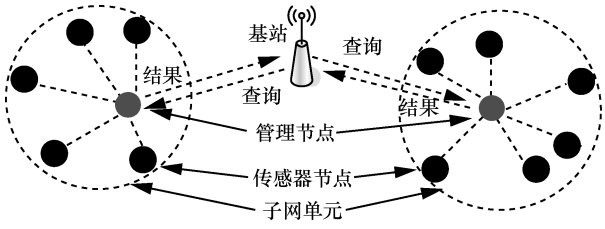

图 2 两层传感器网络结构

2.2 攻击模型

攻击模型是对攻击者可能采取的攻击行为的抽象描述。在传感器网络中，通常假设基站是可信的，否则整个网络都不可信。根据现有的研究工作，从攻击方式的角度将攻击模型大致分为诚实但好奇模型（honest but curious model）[4]和恶意攻击模型（malicious model）[5]。

在诚实但好奇模型中，所有节点都会严格按照协议的规则处理数据，但这些节点拥有一颗“好奇心”，试图通过窃听无线链路、查看其转发的数据等方式获得其他节点的敏感信息。在该模型中，攻击者只关注敏感信息的内容，但不会改变敏感信息。

在恶意攻击模型中，节点不再严格遵守协议规则，而是试图通过向网络中注入虚假信息、恶意修改或删除真实信息等方式影响最终的查询结果。在该模型中，攻击者将恶意篡改敏感信息，对网络安全的威胁更大。

现有的传感器网络隐私保护数据聚集协议主要解决诚实但好奇模型中隐私泄露问题，但恶意攻击模型中的信息篡改问题也逐渐受到研究人员的关注。

2.3 性能评估

现有相关研究工作主要从以下 5 方面评估传感器网络隐私保护数据聚集协议的性能。

1) 通用性

常用的聚集类型很多，如求和、计数、求极值、求方差、求分位数等。协议所支持的聚集类型反映该协议的通用性，支持的类型越多，协议的通用性越高。

2) 隐私性

传感器网络中节点的感知数据属于敏感信息。隐私性要求协议能够有效地防止敏感信息被非法用户获取。隐私性一般使用攻击者根据掌握的知识成功推测出敏感信息的概率来评估。推测出敏感信息的概率越低，协议的隐私性越强。

3) 完整性

广义完整性的目标是保证敏感信息在节点采集、网络传输和计算处理的过程中不被恶意改变。自组织多跳是传感器网络的特征。感知数据从采集节点到基站往往需要经过传输路径上其他节点的转发，有时还需要进行轻量级的计算。广义完整性要求协议能够保证感知数据被如实地采集、转发和计算。由于完整性直接影响最终结果，因此，通常所说的完整性是指结果完整性，即基站收到的最终结果应该包含真实的结果，禁止攻击者恶意修改、删除结果和注入非法信息。完整性一般通过基站成功检测出不完整结果的概率来评估。检测出不完整结果的概率越高，协议的完整性越强。

4) 高效性

传感器网络的能量非常有限。文献[6]研究显示节点通信和计算，特别是前者，是消耗能量的主要因素。网络的剩余能量直接决定了网络的生命周期。高效性一般使用节点的通信成本和计算代价来评估。通信成本和计算代价越低，节点执行效率越高，协议越高效。

5) 精确性

理想的情况下，真实结果与计算结果是等价的。但是为了权衡各项评估指标，有时会牺牲一定的结果精度。此外，节点失效、信号冲突等特殊情况都可能导致最终结果产生误差。精确性一般使用实际的查询结果与正确的查询结果之间的误差来评估。误差越小，协议的精确性越高。一般地，要求协议在满足其他各项评估指标的前提下，保证查询结果在可接受的误差范围内尽可能精确。

3　隐私保护数据聚集技术

现有隐私保护数据聚集协议采用的隐私保护技术主要分为同态加密（homomorphic encryption）、数据扰动（data perturbation）、切分重组（slicing-mixing technique）、泛化（generalization）和安全多方计算（secure multiparty computation），另外还有其他隐私保护技术，如匿名技术（anonymization）、前缀成员验证技术（prefix membership verification）等。此外，还有少数研究工作只关注了结果完整性问题。本节将对代表性协议进行详细的阐述和分析。

3.1　同态加密技术

同态加密[7]技术是一类特殊的密码技术，它允许对密文直接进行代数运算，得到的结果仍然是密文形式，对该密文解密后所得的结果与对明文进行同样的代数运算得到的结果一致。假设 R 和 S 是 2 个域，加密函数 $E:R\to S$，解密函数 $D:S\to R$，E 具备同态性当且仅当存在有效算法 $@$，对任意 $a\in R$、$b\in R$，都有 $a@b=D\left(E\left(a\right)@E\left(b\right)\right)$。同态加密技术的这一特性允许以密文的形式直接处理信息，中间过程不需要解密，一定程度上降低了敏感信息在中间处理环节泄露的风险。常见的同态加密有加法同态（additive homomorphism）和乘法同态（multiplicative homomorphism），因此，主要解决加法类数据聚集的隐私保护问题。

CDA 协议[3,8]是较早研究传感器网络隐私保护数据聚集的协议。该协议采用 Domingo-Ferrer 提出的同态加密算法[9]建立端到端加密机制，在保护节点感知数据的同时实现网内聚集。Domingo- Ferrer 的方法需要预先设置参数：正整数 j；多因子大整数 g；密钥 $k=\left(r,g'\right)$；安全等级 $\log_{g'}g$。感知数据 d 被随机拆分成 $d_1,d_2,\cdots,d_j$ 并满足：$d=\sum_{i=1}^{j}d_i \bmod g'$。节点按照 $E_k\left(d\right)=(d_1r \bmod g,\ d_2r^2 \bmod g,\cdots,\ d_jr^j \bmod g)$ 加密数据后上传。中间节点直接聚集密文后继续上传。基站收到后按照 $D_k\left(E_k\left(d\right)\right)=\sum_{i=1}^{j}d_i \bmod g'$ 解密，得到最终聚集结果。CDA 协议通过同态加密技术直接对密文进行聚集处理，既保护了数据的隐私性，又避免了逐跳加密带来的复杂计算和时间延迟。

文献[10]从软件工程的角度分析了传感器网络中的隐私保护数据聚集问题，构建了隐私保护数据聚集 UML（unfiled modeling language）模型，并且提出一种动态隐私保护数据聚集协议 DyDAP。该协议还设计出一种基于离散时间控制理论[11]的动态网内数据融合机制，用于减少节点间的通信量，避免网络拥塞。

文献[12]提出一种同态流密码策略，支持在密文上直接聚集。该策略本质上是一次一密[13]，使用模加（modular addition）操作代替流密码中的异或操作。同态流密码是一种轻量级的加密技术，其计算代价较小。但是文献[12]对明文长度有特殊限制，否则影响结果的正确性。

一些研究对文献[12]的工作进行了改进。文献[14]利用承诺树[15]让每个节点检查聚集结果是否包含自己的数据，并将自己的认证码发送至基站，由基站做最终地验证。文献[16]通过构建加密的聚集校验和实现对聚集结果的端到端认证。与采用逐跳认证的协议[17-19]相比，端到端认证能够节省节点的通信开销。文献[20]解决了文献[12]数据丢失问题，采用 cascaded ridesharing 容错机制[21]，在节点与基站之间建立多条聚集路径，保证基站能够接收到每一个数据。

IPHCDA 协议[22]是一种适用于层次化传感器网络的安全数据聚集协议。它将基于椭圆曲线密码体制的同态加密技术[23]轻量化，既降低了节点计算复杂度，又保证了聚集过程中不会泄露感知数据。IPHCDA 协议将网络划分成若干组，先进行低层次的组内聚集，然后进行高层次的组间聚集。在组间聚集之前，聚集节点根据各组的聚集结果计算出所在组的消息验证码（MAC, message authentication code）一起发送到基站。基站根据 MAC 信息验证各组聚集结果的完整性。IPHCDA 协议还支持节点级别的完整性验证，但要求节点传输各自的 MAC 信息，这导致网络通信代价大幅增加。

SIES 协议[24]的目标是：在高效完成网内聚集的同时，保证敏感信息的隐私性、完整性和时效性。SIES 协议结合多种方法来实现上述目标：加法类同态加密技术支持密文形式的聚集，有效地防止了聚集过程泄露节点数据；密钥共享机制[25]增加了攻击者获取正确密钥的困难程度，因而能够检测出不完整的结果，保证数据来源真实可靠；可认证的广播协议 μTesla [26]可以抵御面向查询者的伪装攻击；随时间变化的密钥能够抵御重放攻击。

文献[27]提出一种端到端的安全数据聚集协议。该协议使用基于椭圆曲线密码体制的EIGamal 同态加密技术[28]。首先将每个感知数据映射成椭圆曲线上的一点，然后对点执行同态加密聚集。在聚集时，节点采用改进后的椭圆曲线数字签名技术[29]为数据生成签名，与加密的聚集结果一起上传到基站。基站根据签名判断聚集结果是否完整。

SDA-HP 协议[30]使用对称同态加密技术[31]保护数据隐私，结合同态 MAC 技术[32]验证结果的完整性。与之前基于同态加密技术的聚集协议不同，SDA-HP 协议不直接加密每个感知数据，而是先将每个感知数据拆分成 d 个子数据，d 的值越大，隐私性越强，但是节点的存储代价、计算代价和通信代价也越大。

还有一些相关研究工作[33-34]也采用同态加密技术。此外，文献[35-39]将同态加密技术应用到智能医疗、智能电网、移动感知领域中。在上述隐私保护数据聚集协议中，基站只能得到聚集结果，不能得到每个节点的感知数据，这导致协议只能适用于单一或有限的聚集类型。文献[40-43]研究了支持多种数据聚集的隐私保护机制。文献[40]提出一种可还原的隐私保护数据聚集协议 RCDA。基站能够从聚集后的数据中还原出原始的感知数据。根据原始数据，基站不仅可以检验结果的完整性与真实性，而且支持任何类型的聚集操作。文献[41]设计了一种环型数据结构实现数据聚集，采用伪随机机制实现匿名通信，使用同态加密技术加入噪声，支持求和、求极值聚集类型。文献[43]提出一种多功能安全数据聚集协议 MODA，利用同态加密机制将敏感信息保存到向量中，不仅能够保护感知数据，还可以保护序列信息和上下文信息。MODA 协议虽然能够得到精确的查询结果，但是通信代价较高。

3.2 数据扰动技术

数据扰动技术是一种数据失真技术，最早被应用在统计披露控制（statistics disclosure control）[44-45]领域。其基本思想是随机产生一个或多个扰动因子，通过一定的运算将其与原始数据融合，从而隐藏敏感信息，同时保持某些数据特征不变，使经过扰动处理得到的统计信息与根据原始数据得到的统计信息之间没有明显的差异。相比于同态加密技术，数据扰动技术实现起来更简单、高效。

CPDA 协议[46-47]是最早基于数据扰动技术解决隐私保护数据聚集问题的协议。该协议借助数据扰动技术和多项式性质，在不泄露节点敏感数据的情况下，经过多项式变换求解出正确的聚集结果。CPDA 协议具体包含 3 个阶段：网络分簇阶段、簇内聚集阶段和簇间聚集阶段。在网络初始阶段，每个节点按照投票机制随机成为簇头节点或成员节点，并将网络分成若干簇。假设一个簇有 m 个节点 $s_0, s_1, \cdots, s_{m-1}$，在簇内聚集阶段，每个节点 s_i 首先随机产生一个公开种子 x_i 和 $m-1$ 个私有扰动因子 $r_1^i, \cdots, r_{m-1}^i$，然后根据当前的感知数据 d_i 和扰动策略为簇内其他节点 $s_j\left(j \neq i\right)$ 产生一个扰动数据 $v_j^i = d_i + r_1^i x_i + r_2^i x_i^2 + \ldots + r_{m-1}^i x_i^{m-1}$，将 v_j^i 加密并发送至相应的节点 s_j。s_j 解密所有的 v_j^i 后计算 $F_j = \sum_{i=0}^{m-1} v_j^i$。所有成员节点 s_i 将 F_i 发送给簇头。簇头首先计算出 $F = \sum_{i=0}^{m-1} F_i$，然后根据 m 个公开种子构建一个 $m \times m$ 的矩阵 $\boldsymbol{G}^{-1}$，最后计算 $\boldsymbol{U} = \boldsymbol{G}^{-1} \times F = \left(D, R_1, \cdots R_{m-1}\right)^{\mathrm{T}}$，显然 $D = \sum_{i=0}^{m-1} d_i$ 是簇内的聚集结果。在簇间聚集阶段，簇头将各自簇内聚集结果沿着路由树聚集并上传到基站。CPDA 协议的数据隐私性与簇内节点数量有关。另外，多项式计算不仅会增加簇头节点的计算复杂程度，而且会限制协议的通用性，使协议只适用于加法类聚集。

文献[48]提出了一系列基于数据扰动的隐私保护聚集查询协议，分别是基本扰动机制 BSP、基于完全报告的扰动机制 FSP、最优自适应的扰动机制 O-ASP、分布式自适应的扰动机制 D-ASP。这些协议只适用于加法类聚集。

MDPA 协议[49]研究多维数据的隐私保护聚集处理技术。节点使用扰动技术将多维数据按转换成一维数据。聚集节点直接对这些数据进行聚集，并且将加密后的聚集结果发送至基站。基站按照事先约定的参数还原出每一维的聚集结果。MDPA 协议仅对加法类聚集有效。

文献[50]关注了两层传感器网络中的隐私保护数据聚集问题，按照恶意节点是否协作攻击，分别提出不共谋的隐私保护聚集协议 PDAAS 和抵御共谋的隐私保护聚集协议 PDACAS。在 PDAAS 协议中，每个节点与基站和簇头共享不同密钥。节点将扰动因子有序添加到感知数据中，簇头与基站逆向

解密得到聚集结果。为了抵御基站与簇头节点之间的共谋攻击，文献[50]进一步提出了 PDACAS 协议。在 PDACAS 协议中，每个传感器节点拥有一个独立的密钥环（key ring）。节点根据密钥环生成多个扰动因子，将感知数据沿着簇内虚拟循环列表传输 2 次，完成扰动因子的添加和去除，同时得到簇内聚集结果。两次簇内传输会产生较大通信量。

PEQ 协议[51]利用扰动矩阵将节点原始数据隐藏到构造的列向量中。基站基于矩阵的非奇异性求解出方程组的唯一解，即全网的感知数据，根据聚集类型计算出精确的结果。PEQ 协议不受聚集类型的限制。当节点数量较多时，节点传输扰动列向量会产生大量通信开销。

3.3　切分重组技术

切分重组技术最早由文献[46-47]提出，其核心思想是每个参与者将自己的数据表示成若干子数据的和，随机地与其他参与者交换子数据，参与者计算出收到的子数据之和，使用该值伪装成自己的原始数据，称该值为伪数据。一个节点的伪数据是根据多个参与者的子数据计算得到的，已经与该节点的原始数据没有明显联系。由于子数据只是原始数据的一小部分，即使被攻击者获得，也无法从子数据逆推出原始数据。切分重组的特点决定了它主要应用于加法类聚集。

SMART 协议[46-47]是最早基于切分重组技术的隐私保护聚集查询协议。它的基本思想是：节点将每个感知数据切分成若干数据片（data slices），并且将这些数据片发送给随机选择的邻居节点，节点重新组合收到的数据片得到伪数据，将其作为本节点的感知数据直接参与传输和聚集。伪数据并非真实的感知数据，因此，能够在不加密的情况下直接参与聚集，提高了聚集的效率。SMART 协议包含 3 个阶段：切分阶段、重组阶段和聚集阶段。假设网络有 n 个节点，每个感知数据被切分成 $J(J>1)$ 片。每个节点 s_i 将采集的数据 d_i 切分成 J 个分组，从 h 跳邻居节点中随机选择 $J-1$ 个，s_i 自己保留一个，并将其余数据片加密后分别发送给选择的邻居节点。s_j 将收到的数据片重新组合得到 $r_j=\sum_{i=1}^{n}d_{ij}$。s_i 直接将 r_i 向上转发并聚集，直到基站收到最终的聚集结果。在 SMART 协议中，数据的隐私性与数据分组数量 J 有关。此外，同一时间过多的节点通信还会导致网络阻塞和冲突，造成结果响应时间延长和结果精确度降低。为了解决上述问题，很多研究工作从数据分组数量和数据碰撞 2 个方面对 SMART 协议进行了改进，下面详细介绍这些工作[52-60]。

为了减少数据分组的数量 EEHA 协议[52]只允许叶子节点对感知数据进行切分处理。ESMART 协议[53]也只允许叶子节点对感知数据进行切分处理，并且数据分组数量是区间 $[2,J]$ 中的一个随机整数。HEEPP 协议[54]在 ESMART 协议的基础上增加了数据查询阶段，防止聚集节点丢失数据。在 SESDA 协议[55]中，数据分组的数量由节点已收到的数据片数量动态确定。ESPART 协议[56]通过控制节点的出入度减少切分重组产生的数据分组，并设定了最小出入度。D-SMART 协议[58]也采用动态切分技术，按照数据的重要性将感知数据分为普通、重要和机密 3 个等级，对应的数据分组数依次为 2、3、4。文献[57]提出了隐私性与效率的平衡模型 BPDA。接收数据分组的节点是根据平衡模型选择的，这与 SMART 协议的随机选择机制不同。BPDA 模型保证了数据分组优先发送给隐私性较低的节点。

为了解决切分重组技术造成的数据碰撞问题，文献[59-60]引入 5 种优化因子降低碰撞率、减少碰撞造成的损失。在降低碰撞率方面，加入随机分组因子和局部因子；在减少碰撞损失方面，加入小数据因子、正负因子和补偿因子。随机分组因子使得各数据分组在一定时间分组内随机传输，避免形成数据分组的传输高峰。局部因子允许切分失败的节点直接将感知数据以整体的形式发送给邻居节点。小数据因子限制每个数据分组的取值范围，保证数据损失不超过设定的最大丢失数据值。正负因子使得数据分组以“正”“负”形式交替出现。补偿因子会在聚集阶段根据发送丢失率进行一定的补偿。随机分分组因子、小数据因子和正负因子 3 种策略不会增加通信成本，局部因子策略一定程度上可以减少通信量，而补偿因子策略不仅会带来额外的通信开销，还会加重冲突碰撞情况。

PriSense 协议[62]是 SMART 协议在移动网络的应用，提出 3 种接收数据片节点的选择方案，分别是全网随机选择、从一跳邻居中选择和从 h 跳邻居中选择。PriSense 协议不仅支持加法类聚集，还支持非线性聚集。

iPDA 协议[63]在 SMART 协议的基础上，通过构建多棵不相交聚集树，引入冗余信息策略验证聚

集结果的完整性。文献[64]结合 CPDA 与 SMART 协议，提出一种基于簇内监督的可验证的隐私保护数据聚集协议 iCPDA，其完整性验证的有效性取决于网络拓扑结构。

以上研究工作主要解决快照式的数据聚集，文献[65]针对连续式数据聚集，在 SMART 协议基础上提出一种安全有效的隐私保护聚集协议 PECDA。PECDA 协议只要求叶子节点进行数据切分，利用公钥机制在邻居节点之间建立一条安全通道保护感知数据，再基于数据的时间相关性过滤掉冗余数据，减少连续聚集过程中产生的通信量。

3.4 泛化技术

泛化技术的核心思想是将精确的数据模糊化，使攻击者很难凭借模糊后的数据确定原始数据。模糊后的数据保留了原始数据的特征信息，因此可以根据特征信息完成一些对结果精度要求不高的查询任务。泛化技术虽然可以保护信息的精确值，但也泄露了一定的特征信息，此外还会影响结果的精确性，多用于近似聚集。

ESPDA 协议[66]将节点数据转换成模式代码（pattern codes）参与聚集，避免感知数据在网络中传输。PHA 协议[67]是一种基于直方图泛化技术的通用隐私保护数据聚集方案，支持多种近似聚集。基本思想是用直方图的某一区间表示节点感知数据。直方图是感知数据的泛化，由于 PHA 协议根据直方图估算聚集结果，估算结果存在误差。经分析可知，值域的划分粒度直接影响协议的隐私性、高效性和精确性。文献[68]在 PHA 系列协议的基础上增加了恶意聚集行为检测机制。在 PHA 方案中，基站只能粗略地统计出网络数据的分布情况，无法知道每个节点的数据情况。为了能够反映节点与数据的关系，文献[69]提出一种基于参照矩阵的通用隐私保护聚集协议 PGAQ。

3.5 安全多方计算技术

安全多方计算[70]允许多个互不信任的参与方按照特定的方式协同完成计算任务。在这个过程中，每个参与方提供一个或多个输入，除了最终的输出，每个参与方均不知道其他参与方的输入信息。该技术确保了输入的独立性和计算的正确性。

文献[71]综合运用了安全多方计算与数据扰动技术保护节点数据。采用 CPDA 协议的建簇机制将网络划分成多个簇，为每个簇随机建立一个哈密顿圈（hamiltonian circuit）[72]。节点在路由过程中控制扰动信息的增减，从而在隐藏感知数据的情况下计算出聚集结果。由于数据需要在簇内进行 2 次环路传输，并且哈密顿圈上的节点位置关系并非物理的，加重了网络通信负担。RPDA 协议[73]是一种基于轮转机制的低能耗隐私保护聚集协议。每个簇根据节点之间的对应关系建立轮转环路。轮转过程中，从粗头开始，簇内节点依次计算自己的轮转数据，最终返回簇头。簇头去掉扰动得到簇内聚集结果后执行自下而上的簇间聚集。

3.6 其他隐私保护技术

匿名技术可以消除身份标识，同时保留原始信息[74]。KIPDA 协议[75]引入伪装数据（camouflage value）对感知数据匿名处理，适用于求极值聚集。该协议的基本思想是：为每个节点构造一个长为 k 的消息集合，包含 $k-1$ 个伪装数据和 1 个真实数据，攻击者从消息集合中分辨出真实数据的概率为 $\frac{1}{k}$，即满足 k-不可辨识性（k-indistinguishability）。KIPDA 协议的隐私保护强度与消息集合长度 k 有关。DCSPDA 协议[76]借鉴 KIPDA 协议的思想，解决传感器网络中多媒体数据的隐私保护聚集问题。

前缀成员验证技术早期应用于跨域协作防火墙（cross-domain cooperative firewall）领域。文献[77]首次提出前缀成员验证技术，文献[78]对其进行了改进。文献[79]基于前缀成员验证技术提出一种适用于两层网络模型的隐私保护数据聚集协议，将值与值之间的大小关系判定转换成值与集合的包含关系判定，支持极值聚集。编码的传输会增加节点的通信开销。

PIP 协议[80]综合运用多项式内插技术（polynomial interpolation）[81]、同态加密技术和数据扰动技术，保护隐私性和完整性。协议的主要思想是：节点将感知数据 d 分成 k 份 $d_1,d_2,\cdots,d_k$，迭代使用多项式内插技术依次构造出 1 阶至 k 阶多项式，d_i 隐藏在相应阶数的多项式中。对于一个 k 阶多项式，只有获取多项式上的至少 $k+1$ 个点才可以正确重构出多项式的表达式。多项式内插技术的迭代增加了节点的计算代价。

文献[82]提出一种基于多项式回归的隐私保护聚集协议 PRAD，支持加法类聚集。为了减少通信量，节点将 n 个感知数据拟合成一个 $m(n>m)$ 阶多项式函数，加入扰动因子后直接用多项式函数系数进行聚集。基站从聚集的多项式系数中去除扰动因

子得到多项式函数，最后基于该多项式函数计算出近似的聚集结果。

文献[83]基于 Z-O（zero-one）编码比较技术（又称为 0-1 编码比较技术）[84] 提出一种面向两层网络模型的隐私保护极值聚集协议 EMQP。Z-O 编码比较技术的基本思想是将数值大小的比较转换为集合交集是否为空的判断。节点为感知数据构造 Z 码集合和 O 码集合。管理节点利用 Z-O 编码的性质进行判断，返回聚集结果。与前缀成员验证技术类似，Z-O 码的传输也会增加节点的通信代价。为了降低节点通信代价，文献[85]对 EMQP 协议进行了改进，要求节点随机选择其中一个码集合存储到管理节点。虽然随机选择机制一定程度上降低了节点通信量，但是降低了结果的精确度。

文献[86]基于共享和签名策略提出 2 种端到端加密方案，但仍存在一些缺点。一方面，聚集节点的通信负担较大，能量消耗比普通节点快得多；另一方面，方案假设聚集节点与基站能够直接通信，但实际应用中节点的通信范围是有限的。

3.7　完整性验证技术

上述研究成果重点关注了数据聚集过程中敏感信息的隐私性，少数研究成果在实现隐私保护的前提下进一步关注了结果的完整性，但有些研究工作只关注恶意攻击模型中的结果完整性问题。文献[17-18]针对聚集节点和普通传感器节点被俘获情况，提出一种“聚集—提交—证明”的安全聚集框架。基站与聚集节点根据承诺信息（commitment）对聚集结果进行交互式验证。SecureDAV 协议[87]采用节点签名机制验证结果的完整性。SDAP 协议[19]遵循“分而治之”和“谁提交谁证明”的原则，实现安全逐跳数据聚集。上述研究主要针对实时聚集的完整性问题，文献[88-89]依据变化模式的发生情况提出适用于连续聚集的结果验证机制。

4　对比分析

近年来，传感器网络隐私保护数据聚集技术已经成为研究热点，受到学术界的广泛关注。本节首先总体分析了各隐私保护技术的优缺点（见表 1），然后针对不同的隐私保护数据聚集协议，从协议所采用的主要隐私保护技术、网络模型、攻击模型、通用性、隐私性、完整性、高效性、精确性等方面进行了对比分析。

1) 从总体上看，现有的相关研究成果往往局限于某一种或某一类的聚集，均未较好地平衡隐私性、完整性、高效性和精确性之间的关系。同态加密技术能够在不解密的情况下直接聚集密文，但隐私性完全依赖于同态加密函数的复杂程度。函数越复杂，隐私性越高，但计算代价也越高。数据扰动技术将扰动因子与敏感信息融合，实现原理比较简单，但是为了提高隐私性，往往会增加扰动因子添加与去除的复杂程度，直接加重了节点计算代价。切分重组技术中的伪数据彻底掩盖了原始信息，然而数据片的传输不仅增加了节点通信量，还导致簇内数据碰撞的频繁发生。泛化技术使用模糊区间代替精确值，但是泄露了一定的特征信息。泛化技术能够支持多种聚集类型，但是聚集结果不精确。安全多方计算技术的实现依赖于多个参与者，一定程度上增加了隐私泄露的风险。匿名技术让伪装数据与敏感数据混淆在一起，增加敏感数据的辨识难度。但是由于数据不再加密，攻击者仍然能够以一定的概率推测出敏感数据。此外，所需伪装数据量远多于敏感数据，增加了通信量。前缀成员验证技术和 Z-O 编码比较技术将一个敏感数据表示成 2 个码值，多项式内插技术将一个感知数据分散隐藏到多个多项式中，多项式回归技术将多个敏感数据拟合成一个多项式，均很好地实现了隐私保护，但分别存在一些通信开销大、计算复杂、结果不精确等问题缺点。

2) 基于同态加密技术的数据聚集协议，在网络模型方面，均以节点相似的传感器网络为研究背景；在攻击模型方面，除了个别研究[3,9-10,12,20,43]只能抵御诚实但好奇模型，其他研究成果均能够抵御诚实但好奇模型和恶意攻击模型；在通用性方面，受同态加密函数构造特征的限制，大部分协议只适用于加法类聚集，只有极少数协议，如 RCDA 协议、MODA 协议，适用于任何类型的聚集；在隐私性方面，早期研究中同态加密函数构造过于简单，隐私性较弱，而后期研究采用椭圆曲线密码机制等复杂同态加密技术，使隐私性有所提高；在完整性方面，早期研究只关注了诚实但好奇模型中的隐私泄露问题，随着恶意攻击模型中的信息篡改问题逐渐受到关注，很多协议在聚集过程中附加简单的冗余信息验证聚集结果的完整性，但是只有少数研究[22,40]能够实现节点级别的完整性验证；在高效性方面，同态加密函数的复杂程度直接影响了节点计

表 1 各隐私保护技术的优缺点

隐私保护技术	主要优点	主要缺点
同态加密技术	能够直接聚集密文	同态加密函数的构造复杂
		仅支持加法类聚集
数据扰动技术	实现简单	扰动的管理复杂
切分重组技术	隐私性较强	通信开销较大
		容易发生数据碰撞
泛化技术	支持多种聚集类型	结果不精确
		泄露敏感数据的特征信息
安全多方计算技术	结果精确	实现依赖于其他参与者
匿名技术	无需加密	通信开销较大
		存在隐私泄露风险
前缀成员验证技术	隐私保护能力较强	仅支持极值聚集
		通信开销较大
Z-O 编码比较技术	隐私性较强	仅支持极值聚集
		通信开销较大
多项式内插技术	隐私性较强	多项式计算复杂
		通信开销较大
多项式回归技术	隐私性较强	结果不精确

算代价，间接影响节点通信成本，函数越复杂，计算代价越高，函数产生的消息越多，通信成本越高；在精确性方面，除了研究[12,14,16,20]由系统参数 M 决定，其他均能得到精确的聚集结果。

3) 基于数据扰动技术的数据聚集协议，在网络模型方面，大部分协议采用节点相似的传感器网络，只有文献[50]采用两层传感器网络模型；在攻击模型方面，所有研究均只关注诚实但好奇模型，没有考虑恶意攻击模型；在通用性方面，与基于同态加密的聚集协议类似，大部分协议只适用于加法类聚集，只有 PEQ 协议适用于任何类型的聚集；在隐私性方面，扰动与原始数据的融合方式决定了协议的隐私性，融合方式越复杂，隐私性越强，如研究[46-47,49-51]采用多项式或维度变换或矩阵等复杂方法融合数据，因而隐私性较强；在完整性方面，由于协议只关注了诚实但好奇模型，所以无法验证结果完整性；在高效性方面，融合方式的复杂程度直接影响到节点的计算代价，融合方式越复杂，计算代价越高，有些协议[46-48,50-51]需要传输多项式、矩阵或多次传输，导致节点成本较高；在精确性方面，现有研究成果均能保证结果是精确的。此外，MPDA 协议采用降维技术实现多维数据的聚集。

4) 基于切分重组技术的数据聚集协议，在网络模型方面，均采用节点相似的传感器网络；在攻击模型方面，大部分协议只能抵御诚实但好奇模型，只有 iPDA 协议和 iCPDA 协议能够同时抵御诚实但好奇模型和恶意攻击模型；在通用性方面，由切分重组技术的原理决定，现有研究仅支持加法类聚集；在隐私性方面，节点的感知数据被分成若干数据分组，被分散到多个邻居节点的伪数据中，只有攻击者获得该节点发送和收到的所有消息，才能计算出它的感知数据，但这个概率非常小，因此大部分基于切分重组的聚集协议具有较强的隐私性，但是 EEHA 协议和 ESMART 协议中只有叶子节点才进行切分，这 2 个协议的隐私性较弱；在完整性方面，只有 iPDA 协议和 iCPDA 协议能够验证结果完整性，但二者的验证机制均存在一定的局限性，如 iPDA 协议取决于不相交树中至少存在一个正确的聚集结果，iCPDA 协议取决于可信节点与恶意节点能够一跳通信；在高效性方面，虽然很多研究[52-53,55-60]对 SMART 协议进行了改进，但数据分组的传输仍然导致节点通信成本较高，由于节点只进行简单的加减运算，因此计算代价较低；在精确性方面，数据分组的传输还容易造成数据碰撞，影响结果的精确度，而 HEEPP 协议中的数据查询阶段，允许节点重新提交丢失的数据，保

证得到精确的结果。

5) 基于泛化技术的数据聚集协议，在网络模型方面，均采用节点相似的传感器网络；在攻击模型方面，大部分协议只关注诚实但好奇模型，只有文献[68]同时考虑诚实但好奇模型和恶意攻击模型；在通用性方面，大部分协议保留了每个感知数据的取值范围，根据该范围可以执行任何类型聚集，只有 ESPDA 协议仅支持极值聚集；在隐私性方面，现有研究成果均对感知数据进行模糊化处理，较好地保护了敏感信息；在完整性方面，只有文献[68]给出结果完整性的判断规则，但这仅是结果满足完整性的必要条件，而非充分条件；在高效性方面，现有协议只进行简单的计算，由基站进行复杂的结果计算，因此，计算代价较低，除了 ESPDA 协议只传输感知数据的模式代码，其他文献[67-69]均需要传输直方图或向量，通信成本较高；在精确性方面，泛化技术的本质决定了只能获得近似的聚集结果。

6) 基于安全多方计算技术的数据聚集协议，在网络模型方面，均采用节点相似的传感器网络；在攻击模型方面，只研究了诚实但好奇模型中的隐私泄露问题；在通用性方面，目前现有协议只支持加法类聚集；在隐私性方面，攻击者想要获得一个节点的感知数据，必须同时俘获该节点的邻居节点，而这个可能性非常小，因此具有较强的隐私性；在完整性方面，目前现有协议无法验证结果是否完整；在高效性方面，RPDA 协议大部分节点只需传输一次数据，没有额外的通信，通信成本较低，而文献[71]需要沿哈密顿圈传输 2 次数据，通信成本较高，由于多个参与者协同计算出结果，RPDA 协议和文献[71]计算成本均较低；在精确性方面，现有协议能够得到精确的聚集结果。

5　未来工作展望

目前，传感器网络隐私保护数据聚集技术已经成为研究热点，虽然取得了一定的研究成果，但是仍然还有很多具有挑战的问题亟待进一步研究。

1) 各性能之间的优化均衡

隐私性、完整性、高效性和精确性四者之间存在此消彼长的关系。隐私性要求尽可能减少消息中包含的信息量，但只有足够多的信息量才能够得到精确的结果和发现不完整结果；高效性要求协议尽可能降低通信和计算成本，但只有复杂的保护机制和一定的冗余信息才能保护敏感信息和验证结果的完整性。传感器网络隐私保护数据聚集协议的优化目标是在隐私性、完整性、高效性和精确性之间取得平衡，即在保证较高的隐私性和完整性的前提下，减少通信与计算代价，提高结果精确度。现有研究成果虽然提出了一些平衡策略，但仍不能满足实际应用的需求，还需要深入研究。实现隐私性、完整性、高效性、精确性之间优化均衡的重点在于隐私保护机制的轻量化，其中重点研究方向包括轻量级数据同态加密技术、轻量级保序加密机制等。

2) 复杂聚集的隐私保护技术

随着传感器技术的不断进步，单个传感器节点可以感知多种属性信息。例如，在智能家居中，智能传感器可以同时感知温度、湿度、光照等信息。与此同时，用户需求日趋复杂化，从单维数据到多维数据，从快照式聚集到连续式聚集。现有研究成果主要研究了较为简单的单维、快照式聚集的隐私保护技术，对于难度加大的多维、连续式聚集的隐私保护技术则极少研究。在多维、连续式数据聚集中，节点的计算量和网络传输的数据量呈现大幅增长，基于数据分组重组、复杂加密等机制的隐私保护方法不再适用。如果直接将现有研究成果应用在多维、连续式聚集的场景中，势必造成通信成本和计算代价的快速增加，甚至引发路由风暴、通信延迟等问题，影响网络的正常运行。因此，研究多维聚集、连续式聚集等复杂聚集的隐私保护技术是传感器网络应用发展的需要，也是未来的重点研究方向。重点研究方向有多维聚集和连续聚集中的隐私保护数据压缩编码技术、隐私保护数据重用策略等。

3) 基于上下文的隐私保护聚集技术

“互联网+”的出现推动了传感器网络在智慧城市、智能交通、数字医疗等重要领域的广泛应用，这些领域中的数据通常具有上下文信息。常见的上下文信息有位置信息、时间信息等。位置信息能够反映出数据的来源、去向以及移动轨迹，时间信息能够反映出数据何时被数据源采集、何时传输到接收方。现有研究成果主要关注感知数据本身的隐私性，对基于上下文的隐私保护聚集技术研究基本还是空白。某个监测对象的上下文信息一旦泄露，攻击者就可以通过数理统计、时序分析等背景知识攻击手段掌握该对象的变化规律，一方面直接带来了严重的安全威胁，另一方面也增大了传统攻击方式的成功率。因此，研究基于上下文的隐私保护聚集

技术对更好地保护监测对象的安全具有重要意义。

4) 低能耗的隐私保护数据聚集完整性验证技术

完整性验证是隐私保护的一个重要方面，在保护数据隐私性的同时也要保证数据的完整可靠。现有研究工作对数据聚集结果完整性验证方面的关注较少，已有技术主要是在隐私保护之外再进行完整性验证，额外增加了通信和计算处理步骤，增大了网络能耗。考虑到传感器节点能量有限是传感器网络的突出特点，设计低能耗的隐私保护数据聚集完整性验证机制，使用尽量少的通信量和计算量实现结果的完整性验证，对于提高传感器节点的寿命、延长传感器网络的生命周期具有重要意义。研究低能耗的数据聚集完整性验证技术是传感器网络隐私保护需要解决的关键科学问题之一。目前，相关研究重点是设计与数据隐私保护机制结合的完整性验证机制，以取代冗余度较大的专用结果完整性验证策略。

5) 共谋攻击模型下的隐私保护数据聚集技术

共谋攻击是传感器网络中攻击强度高的一类攻击，攻击者同时俘获多个传感器节点，并依靠多个俘获节点之间的信息交换来形成共谋关系，以推测加密公钥私钥、数据隐藏策略、数据分组流向、数据汇聚模式、完整性校验策略等核心隐私保护机制，从而实现对安全机制的破解，获取网络敏感数据。共谋攻击危害性大、防御难度高，是传感器网络隐私保护技术研究中的难点问题，现有研究成果对共谋攻击的涉及还很少。共谋攻击模型下的隐私保护数据聚集技术的研究重点是引入非确定性的数据混淆机制，使攻击者必须俘获大量的节点才能破解安全机制，降低共谋攻击成功的概率。

6) 新型网络中的隐私保护数据聚集技术

随着传感器网络技术的快速发展和普及应用，出现了智能汽车传感器网络、智能家居传感器网络、智能电力传感器网络等新型网络。由于应用需求和网络场景的差异，不同类型的网络对隐私保护数据聚集技术提出了不同的要求。例如：智能汽车传感器网络中，对隐私保护协议能耗的约束比较小，但是对数据传输实时性的要求非常高；在智慧医疗传感器网络中，体征监测数据直接影响治疗措施的选择，因此，对监测数据的精确性和抗篡改性有很高的要求；在智能电力传感器网络中，对大规模和远距离场景下的隐私保护性能提出了额外的要求。因此，根据各类新型网络的特点和需求，设计专用的隐私保护数据聚集协议是未来研究的重点方向之一。典型的研究方向包括高实时性隐私保护数据聚集技术、数据聚集正确性校验技术和篡改防御技术、容侵容错数据聚集技术、隐私保护近似聚集技术等。

6 结束语

作为物联网的重要组成部分，传感器网络已经被广泛应用在许多重要领域。但是在多个关键性领域的实际应用与部署过程中暴露出了严重的隐私泄露问题。传感器网络资源有限、自组织、多跳等特征给隐私保护数据聚集技术的研究带来了严峻的挑战。本文围绕同态加密、数据扰动、切分重组、泛化、安全多方计算等隐私保护技术对现有传感器网络隐私保护数据聚集研究成果进行了详细的阐述和分析。最后，对今后的研究工作进行了展望。

参考文献：

[1] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, et al. Wireless sensor networks: a survey[J]. Computer Networks, 2002, 38(4): 393-422.

[2] SAMUEL M, FRANKLIN M J, HELLERSTEIN J M, et al. TAG: A tiny aggregation service for ad-hoc sensor networks[J].OSDI, 2002, 36(SI): 131-146.

[3] GIRÃO J, WESTHOFF D, SCHNEIDER M. CDA: Concealed data aggregation for reverse multicast traffic in wireless sensor networks[C].ICC.2005: 3044-3049.

[4] GOLDREICH O. Foundations of cryptography: a primer[M]. Boston: Now Publishers Inc, 2005.

[5] SHENG B, LI Q. Verifiable privacy-preserving range query in two-tiered sensor networks[C].INFOCOM. 2008: 46-50.

[6] SZEWCZYK R, FERENCZ A. Energy implication of network sensor designs[EB]. 2016.

[7] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of secure computation, 1978, 4(11): 169-180.

[8] WESTHOFF D, GIRÃO J, ACHARYA M. Concealed data aggregation for reverse multicast traffic in sensor networks: Encryption, key distribution, and routing adaptation[J]. IEEE Trans. Mob. Comput. 2006, 5(10): 1417-1431.

[9] DOMINGO-FERRER J. A provably secure additive and multiplicative privacy homomorphism[C]//ISC.2002: 471-483.

[10] SICARI S, GRIECO L A, BOGGIA G, et al. DyDAP: a dynamic data aggregation scheme for privacy aware wireless sensor networks[J]. Journal of Systems and Software, 2012, 85(1): 152-166.

[11] MASTROCRISTINO T, TESORIERE G, GRIECO L A, et al. Congestion control based on data-aggregation for wireless sensor networks[C]//International Symposium on Industrial Electronics. 2010: 3386-3391.

[12] CASTELLUCCIA C, MYKLETUN E, TSUDIK G, et al. Efficient aggregation of encrypted data in wireless sensor networks[C]// MobiQuitous. 2005: 109-117.

[13] VERNAM G S. Cipher printing telegraph systems for secret wire and radio telegraphic communications[J]. Transactions of the American In-

stitute of Electrical Engineers, 1926, 45(2): 295-301.
[14] CRISTOFARO E D. A Secure and Privacy-Protecting Aggregation Scheme for Sensor Networks[C]//WOWMOM.2007: 1-5.
[15] CHAN H, PERRIG A, SONG D. Secure hierarchical in-network aggregation in sensor networks[C].ACM Conference on Computer and Communications Security. 2006: 278-287.
[16] CASTELLUCCIA C, CHAN A, MYKLETUN E, et al. Efficient and provably secure aggregation of encrypted data in wireless sensor networks[J]. TOSN, 2009, 5(3): 20:1-20.
[17] PRZYDATEK B, SONG D, PERRIG A. SIA: secure information aggregation in sensor networks[C]//SenSys.2003: 255-265.
[18] CHAN H, PERRIG A, PRZYDATEK B, et al. SIA: secure information aggregation in sensor networks[J]. Journal of Computer Security, 2007, 15(1): 69-102.
[19] YANG Y, WANG X, ZHU S, et al. SDAP: A secure hop-by-hop data aggregation protocol for sensor networks[J].ACM Trans. Inf. Syst. Secur. , 2008, 11(4): 18:1-18:43.
[20] ISKANDER M K, LEE A J. Privacy and robustness for data aggregation in wireless sensor networks[C]//ACM Conference on Computer and Communications Security. 2010: 699-701.
[21] GOBRIEL S, KHATTAB S, MOSSÉ D, et al. RideSharing: fault tolerant aggregation in sensor networks using corrective actions[C]//SECON. 2006: 595-604.
[22] OZDEMIR S, XIAO Y. Integrity protecting hierarchical concealed data aggregation for wireless sensor networks[J]. Computer Networks, 2011, 55(8): 1735-1746 .
[23] DAN B, GOH E J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts[C]//TCC.2005: 325-341.
[24] PAPADOPOULOS S, KIAYIAS A, PAPADIAS D. Secure and efficient in-network processing of exact SUM queries[C]//ICDE. 2011: 517-528.
[25] MENEZES A J, OORSCHOT P V, VANSTONE S A. Handbook of applied cryptography[M]. Florida: CRC Press, 1996.
[26] PERRIG A, SZEWCZYK R, WEN V, et al. SPINS: Security Protocols for Sensor Networks[J]. Wireless Networks, 2002, 8(5): 521-534.
[27] KUMAR V, MADRIA S K. Secure hierarchical data aggregation in wireless sensor networks: performance evaluation and analysis[C]//MDM. 2012: 196-201.
[28] MYKLETUN E, GIRÃO J, WESTHOFF D. Public key based crypto schemes for data concealment in wireless sensor networks[C]//ICC. 2006: 2288-2295.
[29] SUN H M, LIN Y H, HSIAO Y C, et al. An efficient and verifiable concealed data aggregation scheme in wireless sensor networks[C]//ICESS. 2008: 19-26.
[30] ZHOU Q, YANG G, HE L. An efficient secure data aggregation based on homomorphic primitives in wireless sensor networks[J]. IJDSN, 2014(7): 962925
[31] CHAN C F. Symmetric-key homomorphic encryption for encrypted data processing[C]//ICC. 2009: 1-5.
[32] AGRAWAL S, DAN B. Homomorphic MACs: MAC-based integrity for network coding[C]//ACNS 2009: 292-305.
[33] MERAD B O R, SENOUCI S M, FEHAM M. Secure and efficient verification for data aggregation in wireless sensor networks[J]. Journal of Network Management, 2018(28).: e2000
[34] SHIM K A, PARK C M. A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks[J]. IEEE Trans. Parallel Distrib. Syst, 2015, 26(8): 2128-2139.
[35] ARA A, AL-RODHAAN M, YUAN T, et al. A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems[J]. IEEE Access, 2017(5):12601-12617.
[36] ZHU H, GAO L, LI H. Secure and privacy-preserving body sensor data collection and query scheme[J]. Sensors 2016, 16(2): 179.
[37] XIE K, NING X, WANG X, et al. An efficient privacy-preserving compressive data gathering scheme in WSNs[J]. Inf. Sci. 2017(390): 82-94.
[38] TONYALI S, AKKAYA K, SAPUTRO N, et al. Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems[J]. Future Generation Comp. Syst. 2018(78): 547-557.
[39] ZHANG L, WANG X, LU J, et al. An efficient privacy preserving data aggregation approach for mobile sensing[J]. Security and Communication, 2016, 9(16): 3844-3853
[40] 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 Trans. Parallel Distrib. Syst., 2012, 23(4): 727-734.
[41] ZHANG K, HAN Q, CAI Z, et al.RiPPAS: a ring-based privacy-preserving aggregation scheme in wireless sensor networks[J]. Sensors, 2017, 17(2): 300.
[42] ZHONG H, SHAO L, CUI J, et al. An efficient and secure recoverable data aggregation scheme for heterogeneous wireless sensor networks[J]. J. Parallel Distrib. Comput, 2018(111): 1-12.
[43] ZHANG P, WANG J, GUO K, et al. Multi-functional secure data aggregation schemes for WSNs[J]. Ad Hoc Networks, 2018(69): 86-99.
[44] ADAM N R, WORTMANN J C. Security-control methods for statistical databases: a comparative study[C]//ACM Comput. Surv.1989, 21(4): 515-556
[45] XIAO X, TAO Y, CHEN M. Optimal Random perturbation at multiple privacy levels[J]. PVLDB 2009, 2(1): 814-825.
[46] HE W, LIU X, NGUYEN H, et al. PDA: privacy-preserving data aggregation in wireless sensor networks[C]//INFOCOM. 2007: 2045-2053.
[47] HE W, LIU X, NGUYEN H, et al. PDA: privacy-preserving data aggregation for information collection[J]. TOSN 2011, 8(1): 6:1-6:22.
[48] FENG T, WANG C, ZHANG W, et al. Confidentiality protection for distributed sensor data aggregation[C]//INFOCOM 2008: 56-60.
[49] LIN X, LU R, SHEN X. MDPA: multidimensional privacy-preserving aggregation scheme for wireless sensor networks[J].Communications and Mobile Computing, 2010, 10(6): 843-856.
[50] YAO Y, LIU J, XIONG N N. Privacy-preserving data aggregation in two-tiered wireless sensor networks with mobile nodes[J]. Sensors, 2014, 14(11): 21174-21194.
[51] HAI V, NGUYEN T, MITTAL N, et al. PEQ: a privacy-preserving scheme for exact query evaluation in distributed sensor data networks[C]//SRDS. 2009: 189-198.
[52] LI H, LIN K, LI K. Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks[J]. Computer Communications 2011, 34(4): 591-597.
[53] LI C, LIU Y. ESMART: energy-efficient slice-mix-aggregate for wireless sensor network[J]. IJDSN, 2013.
[54] LIU C, LIU Y, ZHANG Z, et al. High energy‐efficient and privacy‐preserving secure data aggregation for wireless sensor networks[J]. International Journal of Communication Systems, 2013, 26(3): 380-394.
[55] 王涛春, 秦小麟, 刘亮, 等. 无线传感器网络中安全高效的空间数据聚集算法[J]. 软件学报, 2014, 25(8): 1671-1684.
WANG T C, QIN X L, LIU L, et al. Secure and Energy-Efficient Spatial Data Aggregation Algorithm in Wireless Sensor Networks[J]. Journal of Software, 2014 ,25(8):1671-1684.
[56] 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. 计算机学报[J], 2011, 34(5): 792-800.
YANG G, WANG A Q, CHEN Z D, et al. An Energy-Saving Privacy-Preserving Data Aggregation Algorithm[J].Chinese Journal of Computers, 2011,34(5):792-800
[57] ZHANG C, LI C, ZHAO Y. A balance privacy-preserving data aggregation model in wireless sensor networks[J]. International Journal of

Distributed Sensor Networks, 2015, 501: 937280.
[58] WANG J, CHEN Y. Research and improvement of wireless sensor network secure data aggregation protocol based on SMART[J]. International Journal of Wireless Information Networks, 2018 (11):1-9.
[59] 杨庚, 李森, 陈正宇,等. 传感器网络中面向隐私保护的高精确度数据融合算法[J]. 计算机学报, 2013, 36(1): 189-200.
YANG G, LI S, CHEN ZY, et al. High-Accuracy and Privacy-Preserving Oriented Data Aggregation Algorithm in Sensor Networks[J].Chinese Journal of Computers, 2013,36(1):189-200
[60] YANG G, LI S, XU X, et al.Precision-enhanced and encryption-mixed privacy-preserving data aggregation in wireless sensor networks[J]. IJDSN ,2013.
[61] XU Y, LEE W, XU J, et al. Processing window queries in wireless sensor networks[C]//ICDE. 2006:70-70.
[62] SHI J, ZHANG R, LIU Y, et al. PriSense: privacy-preserving data aggregation in people-centric urban sensing systems[C].INFOCOM. 2010: 758-766.
[63] HE W, NGUYEN H, LIU X, et al. iPDA: an integrity-protecting private data aggregation scheme for wireless sensor networks[C]// MILCOM. 2008: 1-7.
[64] HE W, LIU X, NGUYEN H, et al. A cluster-based protocol to enforce integrity and preserve privacy in data aggregation[C]//ICDCS Workshops. 2009: 14-19.
[65] WANG T, QIN X, DING Y, et al. Privacy-preserving and energy-efficient continuous data aggregation algorithm in wireless sensor networks[J]. Wireless Personal Communications, 201, 98(1): 665-684.
[66] HASAN ÇAM, SUAT ÖZDEMIR, PRASHANT NAIR, et al. Energy-efficient secure pattern based data aggregation for wireless sensor networks[J]. Computer Communications 2006, 29(4): 446-455.
[67] ZHANG W, WANG C, FENG T. GP2S: Generic Privacy-Preservation Solutions for Approximate Aggregation of Sensor Data [C]//PerCom. 2008: 179-184.
[68] WANG C, WANG G, ZHANG W, et al. Reconciling privacy preservation and intrusion detection in sensory data aggregation[C]//INFOCOM. 2011: 336-340.
[69] 范永健, 陈红, 张晓莹,等. 无线传感器网络中隐私保护通用近似查询协议[J]. 计算机学报, 2014, 37(4): 915-926.
FAN YJ, CHEN H, ZHANG XY, et al. Privacy-Preserving Generic Approximate Query in Wireless Sensor Networks[J]. Chinese Journal of Computers, 2014,37(4):915-926
[70] SCHNEIER B P.Applied cryptography - protocols, algorithms, and source code in C[M]. 2nd ed, New Jersey: Wiley, 1996.
[71] 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.
[72] CHOI H, ZHU S, PORTA T F L. SET: Detecting node clones in sensor networks[C]//SecureComm. 2007: 341-350.
[73] ZHANG X, CHEN H, WANG K, et al. Rotation-based privacy-preserving data aggregation in wireless sensor networks[C]//ICC 2014: 4184-4189.
[74] RAGHUNATHAN B. The complete book of data anonymization: from planning to implementation[M]. Florida: CRC Press, 2013.
[75] GROAT M M, HE W, FORREST S. KIPDA: k-indistinguishable privacy-preserving data aggregation in wireless sensor networks[C]// INFOCOM. 2011: 2024-2032.
[76] WU D, YANG B, WANG H, et al. Privacy-preserving multimedia big data aggregation in large-scale wireless sensor networks[J]. TOMCCAP, 2016, 12(4s): 60:1-60:19.
[77] CHENG J, YANG H, WONG S H Y, et al. Design and implementation of cross-domain cooperative firewall[C].ICNP. 2007: 284-293.
[78] LIU A X, CHEN F. Collaborative enforcement of firewall policies in virtual private networks[C]//PODC. 2008: 95-104.
[79] YAO Y, XIONG X, PARK Y H, et al. Privacy-preserving max/min query in two-tiered wireless sensor networks[J]. Computers & Mathematics with Applications 2013, 65(9): 1318-1325.
[80] KUMAR V, MADRIA S. PIP: privacy and integrity preserving data aggregation in wireless sensor networks[C]//SRDS. 2013: 10-19.
[81] PARAKH A, KAK S. Recursive secret sharing for distributed storage and information hiding[C]//ANTS. 2009: 1-3.
[82] OZDEMIR S, PENG M, XIAO Y. PRDA: polynomial regression-based privacy-preserving data aggregation for wireless sensor network[J]. Communications and Mobile Computing, 2015,15.4 (2015): 615-628.
[83] DAI H, YANG G, QIN X. EMQP: An energy-efficient privacy-preserving MAX/MIN query processing in tiered wireless sensor networks[J].IJDSN, 2013.
[84] LIN H Y, TZENG W G. An efficient solution to the millionaires' problem based on homomorphic encryption[C]//ACNS.2005: 456-466.
[85] DAI H, WEI T, HUANG Y, et al. Random secure comparator selection based privacy-preserving max/min query processing in two-tiered sensor networks[J]. Sensors 2016: 6301404:1-6301404:13.
[86] ALGHAMDI W Y, WU H, KANHERE S S. Reliable and secure end-to-end data aggregation using secret sharing in WSNs[C]//IEEE Wireless Communications and Networking Conference. 2017: 1-6.
[87] MAHIMKAR A, RAPPAPORT T S. SecureDAV: a secure data aggregation and verification protocol for sensor networks[C]//GLOBECOM. 2004: 2175-2179.
[88] YU L, LI J, CHENG S, et al. Secure continuous aggregation via sampling-based verification in wireless sensor networks[C]//INFOCOM. 2011: 1763-1771.
[89] YU L, LI J, CHENG S, et al. Secure continuous aggregation in wireless sensor networks[J]. IEEE Trans. Parallel Distrib. Syst., 2014, 25(3): 762-774.

[作者简介]

张晓莹（1987−），女，山东临沂人，博士，中国人民大学工程师，主要研究方向为物联网数据管理、隐私保护等。

彭辉（1986−），男，山东曲阜人，博士，工业和信息化部电子第五研究所工程师，主要研究方向为物联网数据管理、隐私保护等。

陈红（1965−），女，江西鄱阳人，博士，中国人民大学教授、博士生导师，主要研究方向为数据库、数据仓库、物联网等。