



异构无线传感器网络中一种可恢复数据的安全聚集算法^{*}

石鲁生^{1,2}, 朱慧博¹, 陈 林¹

(1. 宿迁学院计算机科学系 宿迁 223800;

2. 南京航空航天大学计算机科学与技术学院 南京 210016)

摘 要: 现有无线传感器网络的安全聚集算法能耗开销大, 聚集类型单一, 提出一种针对异构无线传感器网络的可恢复数据的安全聚集算法。算法使用基于椭圆曲线的同态加密技术实现数据隐私保护, 利用高效的签名聚集方案为数据完整性和真实性的验证提供可靠保障。算法独特的数据恢复功能, 使聚集节点可在得到聚集结果的同时恢复聚集前的原始数据, 方便后续操作, 也丰富了聚集类型。算法充分利用异构无线传感器网络中的节点差异, 将大量计算工作转移至高资源节点, 提高了执行效率。仿真实验和对比分析表明, 算法安全性好、效率高, 虽然单次聚集过程的通信量稍大, 但数据恢复节省了后续工作的开销, 整体能耗实际有所降低。

关键词: 无线传感器网络; 数据恢复; 数据聚集; 隐私保护; 异构

doi: 10.3969/j.issn.1000-0801.2013.11.005

Security Data Aggregation with Recoverable Data in Heterogeneous Wireless Sensor Network

Shi Lusheng^{1,2}, Zhu Huibo¹, Chen Lin¹

(1. Department of Computer Science, Suqian College, Suqian 223800, China;

2. College of Computer Science and Technology, Nanjing University of

Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: Recently, many security aggregation algorithms in wireless sensor network have high communication overhead and the usage of aggregation functions is constrained. A secure data aggregation algorithm with recoverable data in heterogeneous wireless sensor network was proposed. The algorithm uses homomorphism encryption techniques based on elliptic curve to address data privacy protection, and uses an efficient aggregate signature scheme to ensure data integrity and authenticity. The unique data recovery function of this algorithm can recover individual data together with getting the aggregated results, and can facilitate the follow-up operation, and enrich the aggregate type. The algorithm takes full advantage of the difference of nodes in heterogeneous wireless sensor network, and diverts large number of calculation work to h-sensors, this approach improves the efficiency of the implementation. Simulation and comparative analysis show that algorithm has high safety and high efficiency, although the communication overhead of single aggregate process is high, data recovery process saves the overhead of the follow-up work, and the overall energy consumption is actually reduced.

Key words: wireless sensor network, data recovery, data aggregation, privacy-preserving, heterogeneous

^{*} 国家自然科学基金资助项目(No.60673127), 国家高技术研究发展计划(“863”计划)基金资助项目(No.2007AA01Z404), 江苏高校优势学科建设工程资助项目“物联网与控制技术”, 江苏省宿迁学院重点科研基金资助项目(No.2012KY14)



1 引言

近年来,无线传感器网络(wireless sensor network, WSN)越来越受到人们的关注。无线传感器网络由微型、低成本、低功耗的微传感器组成,这些传感器可以通过无线通信协同工作,进行数据监测和处理。目前,无线传感器网络的应用领域已快速扩展至军事、救灾、环境、医疗、家居等众多领域。在很多应用场景下,不同感知能力、计算能力、通信能力以及不同能量储备的传感器常需要相互配合开展工作,这种由不同类型传感器组成的网络称为异构无线传感器网络(heterogeneous wireless sensor network)^[1]。相对于相同类型传感器组成的同构无线传感器网络(homogeneous wireless sensor network),异构无线传感器网络能满足更多的实际需求^[2]。

数据收集是无线传感器网络投入实际应用后的主要功能^[3],由于资源受限的特征突出,各种数据收集算法一直如何将如何延长网络生命周期、降低能耗作为重要的设计目标。

硬件方面,植入高资源节点,构建异构无线传感器网络是延长网络生命周期的有效方法。在异构无线传感器网络中,由少量高资源节点充当簇头,构成上层网络,负责收集数据和执行查询任务,并可与基站进行高速通信;大量资源受限的一般节点形成下层网络,负责数据采集工作,并将采集数据传输至簇头。这种两层传感器网络具有寿命长、易扩展等优点,是无线传感器网络的重要发展方向^[4]。

软件方面,使用数据聚集技术是降低能耗的重要手段。传统的数据聚集方法^[5-7]虽然降低了无线传感器网络的通信开销,但没有解决聚集过程中的安全性问题,不具备实用价值,因此各种安全聚集算法应运而生。DADPP^[8]、ESPART^[9]等是具备隐私保护能力的聚集方法,SIES^[10]和iCPDA^[11]则是兼顾隐私保护和完整性验证的聚集方案。DADPP通过向原始数据中添加随机种子和私有随机数进行扰动,达到隐私保护的目的;ESPART通过对原始数据进行切片和加密传输来保护数据隐私;SIES算法使用同态加密函数保护数据隐私,采用SECOA^[12]思路验证聚集结果的完整性;iCPDA算法在隐私保护和完整性验证中分别使用了安全多方计算方法和同行监督机制。增加了隐私保护和完整性验证之后的聚集算法出现了新的问题:一是原本降低了的通信开销大增;二是聚集类型受限严重,很多算法仅支持SUM一种。

本文提出的异构无线传感器网络的数据聚集算法,在

保护数据隐私以及为数据的完整性和真实性提供有效验证的基础上,特别设计了数据恢复机制,从而使基站或高资源节点在得到聚集结果的同时,能够通过该机制精确、有效地恢复聚集前的原始数据。这些原始数据的获得让基站或高资源节点在执行其他后续聚集操作时,类型不再受限,同时由于聚集过程中的通信量大为减少,也降低了整个网络的能耗开销。

2 系统模型

2.1 网络模型

假设异构无线传感器网络采用基于分簇的两层结构,由以下3个部分组成。

- 一个基站(base station, BS),拥有强大的计算和通信能力、足够大的存储空间、稳定的电力供应,并采取了严密的防护措施。
- 少量高资源(h-sensor, HS)节点,它们充当簇头,是两层结构中的上层,主要负责收集簇内节点采集到的数据,并聚集转发给基站。令网络中簇的数目为 n ,簇头节点集合为 $H=\{H_1, \dots, H_n\}$ 。
- 大量低资源(l-sensors, LS)节点,它们充当簇中的一般成员,是两层结构中的下层,主要负责采集监测区域内的感知数据,并发送至簇头节点。以 H_i 为簇头的簇内一般传感器节点 j 表示为 L_{ij} ,其原始感知数据用 d_{ij} 表示。

2.2 攻击模型

鉴于BS不易被捕获,假设其是安全可信的,则依照严重程度将攻击分为以下3种。

- 窃听无线通信。攻击者未捕获任何节点,但通过窃听网络中的无线通信获取或伪造数据。
- 捕获LS节点。攻击者可以获取或篡改被捕获LS节点的感知数据,亦可攻击被捕获LS节点转发的感知数据。
- 捕获HS节点。攻击者可以获取被捕获HS节点所在簇内所有LS节点的感知数据,并可篡改HS节点上报给基站的中间聚集结果。

2.3 密钥预分配

异构无线传感器网络部署前,BS和HS节点的信息易知,BS首先根据EC-EG方案^[13]生成密钥对 (P_{BS}, R_{BS}) ,再根据Boneh^[14]等的方案为 H_i 生成密钥对 (P_{H_i}, R_{H_i}) 。其中, P_{BS} 为所有BS和HS节点共享的公钥, P_{H_i} 是BS与节点 H_i 共享的

公钥, P_{BS} 和 R_{H_i} 则分别为 BS 和 H_i 的私钥。

BS 预先装载自身的密钥对 (P_{BS}, R_{BS}) 和每个 HS 节点 H_i 的公钥 P_{H_i} 。每个 HS 节点 H_i 除装载自身的密钥对 (P_{H_i}, R_{H_i}) 外, 还将装载 P_{BS} 和一个用于验证签名的散列函数 $H(\cdot)$ 。

待网络部署完毕, 各分簇形成后, 为保护每个簇内节点 L_{ij} 和其簇头 H_i 之间的通信, 同样由基站为它们生成一个密钥对 $(P_{L_{ij}}, R_{L_{ij}})$ 。

3 可恢复数据的安全聚集算法

异构无线传感器网络中, 可恢复数据的安全聚集算法的目的在于充分利用异构无线传感器网络的特点, 在不增大甚至降低整个网络通信开销的基础上实现安全的数据聚集, 同时通过在基站和高资源节点恢复各传感器原始数据的方法, 使得后续操作类型不再受限。

在数据聚集过程中, 簇头和基站均利用基于椭圆曲线的密码系统 EC-EG, 通过加法同态加密技术, 用生成的公共密钥完成隐私保护的数据聚集。同时利用基于双线性映射的高效聚合签名方案, 将一组不同的签名合并到一个聚合签名中, 由此可以根据签名进行有效的安全验证, 进而实现安全的数据聚集。

独特的数据恢复功能在加密聚合前, 先将原始数据与若干个 0 组成的二进制数进行简单连接, 加密聚合后, 再解密聚合结果, 并从中取出相应位置上的二进制数, 恢复原始数据。数据恢复功能的设计让异构无线传感器网络中占据资源优势的基站和少量高资源节点在得到聚集结果的同时, 可以恢复聚集前的原始数据, 从而突破了大部分安全聚集算法中聚集类型严重受限的弊病。

算法由 3 部分组成: 簇内数据收集和聚集、簇头加密和签名传输、基站聚集和安全验证。

3.1 簇内数据收集和聚集

具体步骤如下。

(1) LS 节点 L_{ij} 发送加密的 d_{ij} 和签名 s_{ij} 给对应的 HS 节点 H_i 。

(2) H_i 接收到加密信息后, 利用 L_{ij} 的签名 s_{ij} 验证 d_{ij} 的真实性。

(3) 在一定的时间周期内, H_i 收集完簇内所有 LS 节点的感知数据后, 执行簇内聚集, 并将聚集结果 d_i 作为自身数据。

3.2 簇头加密和签名传输

具体步骤如下。

(1) 加密簇头节点 H_i 的 d_i : $m_i = d_i || 0^t$, 其中 $||$ 表示简单连接, 0^t 表示 t 个 0 组成的二进制数, $t = l \times (i-1)$, l 为传输信息中有效感知数据的比特数。

(2) 计算 H_i 的密文: $c_i = (r_i, a_i) = (k_i + G, M_i + k_i \times Y)$, 其中 k_i 为 $[1, Z]$ 内的随机数, $Z, G, Y \in P_{BS}$, $M_i = \text{map}(m_i) = m_i \times G$, $\text{map}(\cdot)$ 为一个将值 m 映射为椭圆曲线点 M 的函数, 满足加法同态性质。

(3) 计算 H_i 的签名: $s_i = R_{H_i} \times H(d_i)$, 其中 $H(\cdot)$ 为节点 H_i 预装的散列函数。

(4) H_i 向基站发送数据对 (c_i, s_i) 。

3.3 基站聚集和安全验证

具体步骤如下。

(1) 所有簇头节点的聚集数据并非一跳直接传输至基站, 如果一个簇头节点接收到其他一个或多个簇头的聚集结果, 那么将把接收到的所有密文和签名对应的与自身的密文和签名求和, 得到新的密文、签名数据对, 然后再向基站发送。因此基站最终聚集后将得到结果 (C, S) , 其中 $C = (R, A) = (\sum_{i=1}^n r_i, \sum_{i=1}^n a_i)$, $S = \sum_{i=1}^n s_i$ 。

(2) 解密 C 得 M' : $M' = -x \times R + A = \sum_{i=1}^n M_i = M_1 + M_2 + \dots + M_n$,

其中 $x \in R_{BS}$ 。

(3) 从 M' 获得 m' : $m' = \text{rmap}(M') = m_1 + m_2 + \dots + m_n$, 其中 $\text{rmap}(\cdot)$ 为 $\text{map}(\cdot)$ 的反函数。

(4) 恢复 d_i : 利用解密函数 $\text{Decode}(m', n, l): d_i = m'[(i-1) \times l, i \times l - 1]$ 恢复并获取 d_i , 其中 $i = 1, 2, \dots, n$, d_i 为二进制数 m' 的第 $(i-1) \times l$ 位至 $i \times l - 1$ 位上的数字所构成的二进制数。

(5) 验证 d_i : 基站根据已经加密的各签名信息, 检查等式 $e(S, g_2) = \prod_{i=1}^n e(H(r_i), P_{H_i})$ 是否成立。其中 e 是双线性映射, g_2 用于生成 e 中的素数阶循环群 G_2 。如果等式成立, d_i 的完整性和真实性得以验证, 基站将接受所有 d_i ; 否则拒绝。

3.4 数据恢复示例

假设分层异构无线传感器网络如图 1 所示。网络中有一个 BS, 4 个分别以 HS 节点 H_1, H_2, H_3 和 H_4 为簇头的簇, 每个簇包含数量不等的 LS 节点。以 H_2 所在簇为例, 共有 $L_{21}, L_{22}, L_{23}, L_{24}$ 和 L_{25} 5 个 LS 节点, 其他簇类似。

假设 BS 发出一个 average 查询请求, 聚集工作启动。设 H_2 所在簇内 5 个 LS 节点的感知数据 $d_{21}=5, d_{22}=6, d_{23}=4, d_{24}=3, d_{25}=2$, H_2 接收到这些加密的感知数据后, 执行簇内

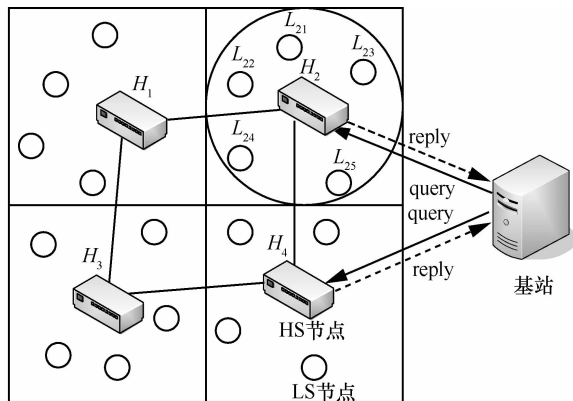


图1 一个分层异构无线传感器网络

average 聚集,得到 $d_2=4$ 。其他簇类似,令其分别得到 $d_1=5$ 、 $d_3=2$ 和 $d_4=7$ 。

根据 d_1 、 d_2 、 d_3 和 d_4 的值,令 $l=3$ 即可满足有效数据的传输需求。 H_2 加密 d_2 得到 $m_2=d_2 \parallel 0^3=(100)_2 \parallel (000)_2=(100000)_2$,然后计算密文 c_2 和签名 s_2 ,并将 (c_2, s_2) 发往 BS。其他 HS 节点类似,可得 $m_1=(101)_2$ 、 $m_3=(010000000)_2$ 、 $m_4=(111000000000)_2$ 。

BS 将获得的所有 HS 节点的密文和签名聚集后,得到 (C, S) ,解密 C 可得 $M'=M_1+M_2+M_3+M_4$,再利用 $rmmap()$ 函数得到 $m'=m_1+m_2+m_3+m_4=(111010100101)_2$,然后可以恢复 d_1 、 d_2 、 d_3 和 d_4 :

$$d_1=m'[(1-1) \times 3, 1 \times 3-1]=(111010100101)_2[0,2]=(101)_2=5 \quad (1)$$

$$d_2=m'[(2-1) \times 3, 2 \times 3-1]=(111010100101)_2[3,5]=(100)_2=4 \quad (2)$$

$$d_3=m'[(3-1) \times 3, 3 \times 3-1]=(111010100101)_2[6,8]=(010)_2=2 \quad (3)$$

$$d_4=m'[(4-1) \times 3, 4 \times 3-1]=(111010100101)_2[9,11]=(111)_2=7 \quad (4)$$

最后 BS 根据等式 $e=(S, g_2)=\prod_{i=1}^n e(H(r_i), P_{H_i})$ 验证 d_1 、 d_2 、 d_3 和 d_4 的真实性与完整性,以决定接受或拒绝它们。

4 主要性能分析与仿真

针对本文提出的算法,首先分析了安全性及数据恢复性质,然后通过仿真,展示了算法在最短查询周期和通信开销两个方面的表现。仿真中,选择了只实现简单网内聚集的 TAG^[15]算法和使用分簇结构并同时实现隐私保护和完整性验证功能的 iCPDA 算法与本文算法进行比较。

4.1 安全性

根据第 2.2 节的攻击模型,分析本算法在安全性方面的表现。

(1) 无线通信遭窃听

此时算法的安全性能能够得到保障。因为簇内和簇间的

通信都进行了加密处理,只窃听无线通信,攻击者无法破解。此外,由于算法要求所有传输信息必须具备相应节点的签名,而攻击者没有密钥无法伪造签名,因此不可能在通信链路中篡改或注入虚假信息。

(2) LS 节点被捕获

如果攻击者将被捕获的 LS 节点伪装成正常节点参与聚集,或者发送较为合理的伪装数据参与聚集,目前的算法都无法检测,不过这种攻击的危害性很小。在本算法中,除被捕获 LS 节点以外,攻击者无法假冒其他节点的信息,也不能篡改被捕获节点转发的信息,其原因是无法伪造相应的签名。

(3) HS 节点被捕获

如果攻击者捕获了 HS 节点,情况将比较严重。但由于本算法中使用了椭圆曲线加密技术,簇内聚集时,如果没有关于椭圆曲线点的加法函数,就无法完成聚集,这意味着对椭圆曲线构造方法一无所知的攻击者,无法完成任何未经授权的聚集。

在应对共谋攻击方面,由于采用了共享密钥以及签名机制,即使在网络节点平均密度较低时,本文算法仍然较容易发现共谋攻击,而且节点密度越大,发现共谋攻击的能力越强。假设网络中的节点均匀分布,当节点通信半径 $R=50$ m、平均节点密度取不同值时,本文算法与 iCPDA 算法应对共谋攻击的能力^[11]如图 2 所示。

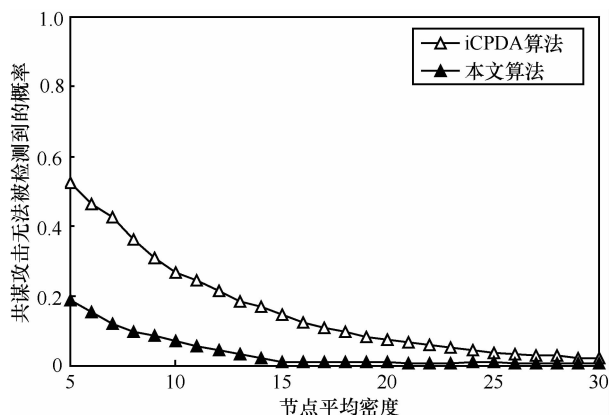


图2 本文算法与 iCPDA 算法应对共谋攻击的能力

通过以上分析可以看出,在各种攻击面前,算法表现出非常好的安全性能。值得特别指出的是,与 iCPDA 算法只能验证聚集结果的完整性不同,本文算法通过签名机制可以验证所有原始数据的真实性和完整性,这为恢复数据后其他操作的进行提供了可靠的保障。

4.2 数据恢复

第 2.4 节的示例表明, 基站在获得最终结果的同时, 可以恢复所有簇头的聚集结果。如果它们通过了安全验证, 那么在一些精度要求不高的应用环境中, 很多后续操作已经可以执行。因为同一簇内 LS 节点的地理位置相近, 所采集数据在数值上相似甚至重复的情况非常普遍, 可令各簇的聚集结果(如平均值)作为本簇值的代表, 这样基站便可轻松获得网络中全部感知数据近似的最大值、最小值或总和。

对精度要求较高的场合, 可以借助 HS 节点的帮助完成各种后续操作。由于簇内聚集过程中 HS 节点也可同样还原簇内各 LS 节点的原始数据, 并进行验证, 因此基站如需其他聚集结果, 只要命令每个 HS 节点执行指定聚集函数即可。为充分利用 HS 节点强大的计算能力, 聚集函数可以在网络部署之前, 以防篡改形式先行装入 HS 节点。尽管这样可能导致 HS 节点硬件成本上升, 但由于此时大部分计算开销已被转移至 HS 节点, LS 节点的设计将变得非常简单, 成本大大降低。在 LS 节点数量占绝对优势的异构无线传感器网络中, 整体硬件成本实际上降低了。

数据恢复功能完全突破了以往由于使用各种安全机制所导致的聚集算法对聚集类型的限制, 同时也节省了执行其他聚集工作的计算和通信开销, 进而从总体上降低了网络中的能量消耗, 延长了网络寿命。

4.3 查询周期

本文使用最终聚集结果的准确性衡量算法查询周期的长短, 即时间效率。记基站聚集结果与由真实数据所得聚集结果的比值 AR 为聚集算法的准确性, 理想情况下, $AR=1$ 。在现实环境中, 如果所有数据的收集、传输、加密和聚集工作都能在指定查询周期内顺利完成, 则正确算法的 AR 值应该接近或达到 1, 如果因查询周期结束, 一些数据的处理工作没有完成, 则必然导致准确性降低, 且查询周期越短, 准确性越差。另外, 较长的查询周期还可以减少无线信道内碰撞造成的数据丢失, 提高准确性。因此, 如果某时间点之后, 算法的 AR 值一直稳定在 1 附近, 则该时间点就是算法近似的最小查询周期。

利用 TOSSIM 仿真环境, 将 500 个传感器节点随机部署在一个指定的区域内, 分别模拟执行 TAG 算法、iCPDA (p_c 分别取 0.1、0.2、0.3) 算法和本文算法 (n 分别取 50、100、150) 各 50 次, 计算平均值, 得到查询周期和通信开销的结果分别如图 3 和图 4 所示。其中, p_c 是 iCPDA 算法中节点成为簇头节点的概率, n 为本文算法中簇头节点的个数, 当

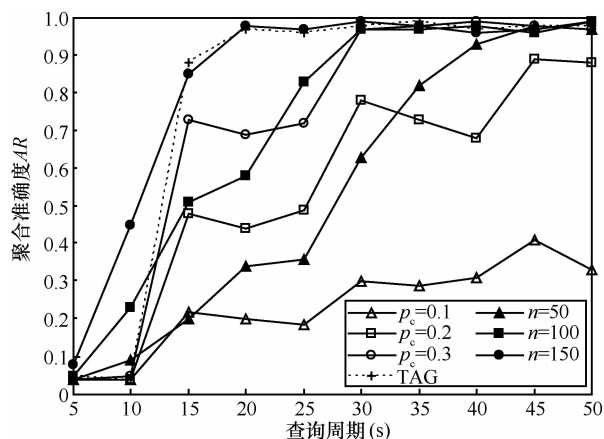


图3 3种算法的查询周期

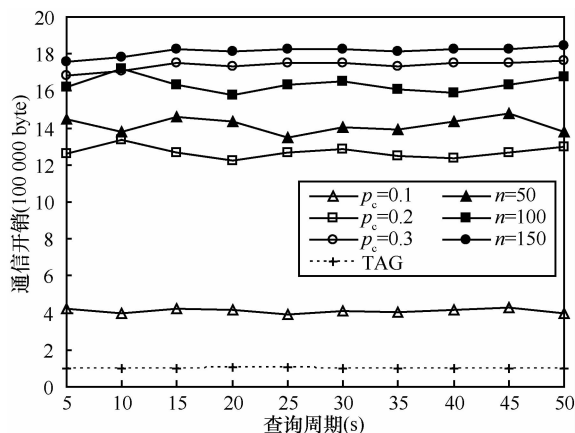


图4 3种算法的通信开销

p_c 分别取 0.1、0.2 和 0.3 时, iCPDA 算法中簇头节点的个数刚好为 50、100 和 150, 与 n 的取值一一对应。

对于本文的算法, 在 $n=150$ 时, 其查询周期大约为 20 s, 基本与不带隐私保护和完整性验证功能的 TAG 算法相当, 这是因为此时网内 HS 节点数量较多, 每个簇内的成员较少, 利用 HS 节点的资源优势, 簇内数据收集、加密、聚集等工作得以在较短时间内完成, 从而缩短了整个网络的查询周期; 当 $n=100$ 和 50 时, 本文算法的查询周期分别增大至 30 s 和 45 s 附近, 这说明随着 HS 节点数量的减少, 簇内数据收集和处理的的工作量增大, 延长了查询周期。虽然 iCPDA 算法的查询周期随 p_c 值的增大而减小, 本文算法的查询周期也随 n 值的增大而减小, 两者趋势相同, 但本文算法对应的查询周期更短, 且优势明显。正是由于充分利用了 HS 节点强大的计算、通信能力, 本文算法不但得到了比 iCPDA 算法更高的安全保障, 而且提高了时间效率。

4.4 通信开销

已有大量研究证明, 在无线传感器网络中数据通信的



能量消耗远大于计算开销,而且本文算法中的大部分计算工作已经转移至计算能力强大的 HS 节点,因此完全可以使用通信开销衡量整个网络的能耗。

3 种算法的通信开销与查询周期关系不大,其中 TAG 算法通信开销最低,因为其功能最简单。iCPDA 与本文算法的通信开销都随着 p_c 或 n 值的增大而增大,因为此时会有更多的簇,需要更多的数据传输,可见在异构无线传感器网络中,并非 HS 节点越多越好。具体来说,除 $n=50$ 时本文算法的通信开销超出对应 iCPDA 算法较多外,其余只多出少许,相差不大。本文算法通信量较大,主要是算法中所传输的数据分组信息丰富、长度较长所致。考虑到本文算法可以提供更高级别的安全保障以及数据恢复为后续工作节省的能量消耗,聚集过程中的通信开销是可以接受的,综合衡量应该比 iCPDA 算法有所降低。

5 结束语

目前的无线传感器网络中,低能耗的聚集算法安全性不足,安全聚集算法又带来高能耗和聚集类型单一等问题,本文在更适应实际应用需求的异构无线传感器网络中,提出了一个带数据恢复功能的安全聚集算法。

算法较好地实现了数据的隐私保护,并具备验证数据真实性和完整性的功能。算法特殊的数据恢复能力,使聚集节点能够恢复聚集前的原始数据。利用异构无线传感器网络中的节点差异,算法还尽可能将计算开销从 LS 节点向 HS 节点转移,以提高效率、降低 LS 节点的能耗。通过性能分析和仿真实验,验证了算法的高效性和安全性,虽然仅从一次聚集过程看,通信量稍大,但恢复的原始数据可为后续聚集节省不少开销,因此实际能耗是令人满意的。

鉴于无线传感器网络能量受限的突出特征和异构网络中节点拥有强大的计算和通信能力的特点,如何进一步降低单次聚集过程的能耗、更加充分利用节点等将是以后努力的方向。

参考文献

- 1 Duarte-Melo E J, Liu M Y. Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks. Proceedings of the GLOBECOM 2002, New York, USA, 2002:21~25
- 2 Yarvis M, Kushalnagar N, Singh H, *et al.* Exploiting heterogeneity in sensor networks. Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM 2005), Miami, FL, USA, 2005:878~890
- 3 Malhotra B, Nikolaidis I, Nascimento M A. Aggregation convergecast scheduling in wireless sensor networks. Wireless Network, 2011, 17(2): 319~335
- 4 Desnoyers P, Ganesan D, Li H, *et al.* PRESTO: a predictive storage architecture for sensor networks. Proceedings of the Tenth Conference on Hot Topics in Operating Systems(HotOS-X), Santa Fe, New Mexico, USA, 2005:231~236
- 5 Madden S, Franklin M J, Hellerstein J M. TAG: a tiny aggregation service for Ad Hoc sensor networks. Proceedings of the 5th Symposium on Operating Systems Design and Implementation, New York, USA, 2002: 131~146
- 6 Deshpande A, Nath S, Gibbons P B, *et al.* Cache-and-query for wide area sensor databases. Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data, San Diego, CA, USA, 2003:503~514
- 7 Tang X, Xu J. Extending network lifetime for precision constrained data aggregation in wireless sensor networks. Proceedings of the IEEE INFOCOM, Barcelona, Catalunya, Spain, 2006: 755~766
- 8 Yao J B, Wen G J. Protecting classification privacy data aggregation in wireless sensor networks. Proceedings of the 4th International Conference on Wireless Communication, Networking and Mobile Computing (WiCOM), Dalian, China, 2008:1~5
- 9 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, 2011, 34(5):792~800
- 10 Papadopoulos S, Kiayias A, Papadias D. Secure and efficient in-network processing of exact SUM queries. Proceedings of the 27th International Conference on Data Engineering (ICDE), Hannover, Germany, 2011:517~528
- 11 He W, Liu X, Nguyen H, *et al.* A cluster-based protocol to enforce integrity and preserve privacy in data aggregation. Proceedings of the 29th IEEE International Conference on Distributed Computing Systems Workshops, Montreal, QC, Canada, 2009: 14~19
- 12 Nath S, Yu H, Chan H. Secure outsourced aggregation via one way chains. Proceedings of the ACM SIGMOD International Conference on Management of Data, Rhode Island, USA, 2009:31~34
- 13 Mykletun E, Girao J, Westhoff D. Public key based crypto schemes for data concealment in wireless sensor networks. Proceedings of the 2006 IEEE International Conference on Communications (ICC 2006), Istanbul, Turkey, 2006:2288 ~ 2295
- 14 Boneh D, Gentry C, Lynn B, *et al.* Aggregate and verifiably encrypted

(下转第 37 页)

- 10 Perillo M, Cheng Z, Heinzelman W. On the problem of unbalanced load distribution in wireless sensor networks. Proceedings of the IEEE GLOBECOM Workshops on Wireless Ad Hoc and Sensor Networks, Dallas, USA, 2004: 74~79
- 11 Li J, Mohapatra P. An analytical model for the energy hole problem in many to one sensor networks. Proceedings of the IEEE Vehicular Technology Conference, Dallas, USA, 2005: 2721~2725
- 12 Olariu S, Stojmenovic I. Data-centric protocols for wireless sensor networks. Handbook of Sensor Networks: Algorithms and Architectures. Wiley, 2005
- 13 Lian J, Naik K, Agnew G. Data capacity improvement of wireless sensor networks using non-uniform sensor distribution. International Journal of Distributed Sensor Networks, 2006, 2(2): 121~145
- 14 Olariu S, Stojmenovic I. Design guidelines for maximizing lifetime and avoiding energy holes in sensor networks with uniform distribution and uniform reporting. Proceedings of the IEEE INFOCOM, Barcelona, Spain, 2006: 1~12
- 15 吴小兵, 陈贵海. 无线传感器网络中节点非均匀分布的能量空洞问题. 计算机学报, 2008, 31(2): 254~262
- 16 Song C, Liu M, Gong H G, *et al.* ACO-based algorithm for solving energy hole problems in wireless sensor networks. Journal of Software, 2009, 20(10): 2729~2743
- 17 刘安丰, 阳国军, 陈志刚. 基于不等簇半径轮换工作的传感器网络能量空洞避免研究. 通信学报, 2010, 31(1): 1~8
- 18 Zeng Z W, Chen Z G, Liu A F. Energy hole avoidance for WSN based on adjust transmission power. Chinese Journal Computer, 2010, 33(1): 12~22
- 19 Liu A F, Wu X Y, Chen Z G, *et al.* Research on the energy hole problem based on unequal cluster-radius for wireless sensor networks. Computer Communications, 2010, 33(3): 302~32

[作者简介]



陆春龙, 男, 常州大学硕士研究生, 主要研究方向为系统综合节能理论及应用研究。



曹玉春, 男, 博士, 常州大学副教授, 主要研究方向为能源环境领域的多相流、燃烧和数值计算。



乐光学, 男, 博士, 嘉兴学院教授, 主要研究方向为计算机网络与分布式计算、无线网络技术。

(收稿日期: 2013-09-10)

(上接第 28 页)

signatures from bilinear maps. Proceedings of the 22nd International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt 2003), Warsaw, Poland, 2003: 416~432

- 15 Madden S, Franklin M J, Hellerstein J M. TAG: a tiny aggregation service for Ad Hoc sensor networks. Proceedings of the 5th Symposium on Operating Systems Design and Implementation, New York, USA, 2002: 131~146

[作者简介]



石鲁生, 男, 宿迁学院副教授, 主要研究方向为信息安全、无线传感器网络。



朱慧博, 女, 宿迁学院副教授, 主要研究方向为无线传感器、高频功率电子变换技术。



陈林, 男, 宿迁学院副教授, 主要研究方向为 Web 服务和语义 Web 服务。

(收稿日期: 2013-06-22)