软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2014,25(8):1671−1684 [doi: 10.13328/j.cnki.jos.004663]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

无线传感器网络中安全高效的空间数据聚集算法*

王涛春[1,2], 秦小麟[1], 刘 亮[1], 丁有伟[1]

[1](南京航空航天大学 计算机科学与技术学院,江苏 南京 210016)

[2](安徽师范大学 数学计算机科学学院,安徽 芜湖 241003)

通讯作者: 秦小麟, E-mail: qinxcs@nuaa.edu.cn

摘 要: 提出了一种传感器网络中安全高效的空间数据聚集算法 SESDA(secure and energy-efficient spatial data aggregation algorithm).SESDA 基于路线方法实现数据聚集,由于算法沿着已设计好的路线执行聚集请求和数据聚集,使得 SESDA 不受网络拓扑结构的影响,适用于网络拓扑结构动态变化的传感器网络,且节省了网络拓扑结构的维护消耗.此外,针对过多加/解密操作对节点能量急剧消耗的特点,SESDA 通过安全通道传输感知数据来保证数据的隐私性,避免了节点之间在数据传输过程中需要对感知数据进行加/解密操作,不仅可以节约节点大量的能量从而延长网络寿命,而且使得数据聚集具有很小的处理延迟,因而获得较高的聚集精确度.理论分析和实验结果显示,SESDA 具有低通信量、低能耗、高安全性和高精确度的特点.

关键词: 数据聚集;隐私保护;安全通道;拓扑结构无关;切片技术

中图法分类号: TP393

中文引用格式: 王涛春,秦小麟,刘亮,丁有伟.无线传感器网络中安全高效的空间数据聚集算法.软件学报,2014,25(8):1671−1684. http://www.jos.org.cn/1000-9825/4663.htm

英文引用格式: Wang TC, Qin XL, Liu L, Ding YW. Secure and energy-efficient spatial data aggregation algorithm in wireless sensor networks. Ruan Jian Xue Bao/Journal of Software, 2014,25(8):1671−1684 (in Chinese). http://www.jos.org.cn/1000-9825/4663.htm

Secure and Energy-Efficient Spatial Data Aggregation Algorithm in Wireless Sensor Networks

WANG Tao-Chun[1,2], QIN Xiao-Lin[1], LIU Liang[1], DING You-Wei[1]

[1](College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

[2](College of Mathematics and Computer Science, Anhui Normal University, Wuhu 241003, China)

Corresponding author: QIN Xiao-Lin, E-mail: qinxcs@nuaa.edu.cn

Abstract: This paper proposes a secure and energy-efficient spatial data aggregation algorithm for sensor networks (SESDA for short). SESDA is an itinerary-based algorithm to achieve data aggregation. Owing to the well-designed itinerary for aggregate request propagation and data aggregation, SESDA is not susceptible to network topology and thus suitable for sensor networks with transient network topology, hence improves energy efficiency. In addition, to counter dramatic energy consumption caused by heavy encryption/decryption operations, SESDA uses secure channel to obtain data privacy. SESDA needs no encryption/decryption operations during data aggregation, which significantly reduces the energy consumption, prolongs the lifetime of sensor networks, and achieves high accuracy of aggregation results due to small delivery delay. Theoretical analysis and experimental results show that SESDA has low traffic and energy consumption, high safety and accuracy.

Key words: data aggregation; privacy-preserving; secure channel; infrastructure-free; slicing technology

* 基金项目: 国家自然科学基金(61373015, 61370050, 41301407); 中国博士后基金(2013M540447); 教育部高等学校博士学科点专项科研基金(20103218110017); 江苏高校优势学科建设工程资助项目(PAPD); 中央高校基本科研业务费专项基金(NP2013307); 安徽高校省级自然科学研究项目(KJ2012Z120)

收稿时间: 2014-02-09; 定稿时间: 2014-04-29

无线传感器网络(wireless sensor networks,简称 WSNs)是由大量部署在物理世界的传感节点通过无线通信方式形成的多跳自组织网络系统,在环境监控、医疗卫生、智能交通和国防等领域具有广泛的应用[1,2].传感节点一般具有能量、计算和存储等资源受限特征,特别是由电池供电,且难以更换,因此,节省能耗、延长网络使用寿命是 WSNs 研究所面临的重要挑战.WSNs 一般通过数据聚集[3−7]减少通信量以节省能耗.然而在很多应用中,WSNs 面临严重的隐私泄漏问题,例如在医疗卫生领域,监控病人的健康信息被恶意窥探等.如何保证感知数据的隐私性,是拓展 WSNs 应用领域的关键因素,是 WSNs 研究中的一个热点问题.

现有的隐私保护数据聚集算法一般基于某种网络拓扑结构(树或簇)实现聚集请求和数据聚集,由于传感节点的易损耗性,且易受周围环境的影响,节点容易发生失效、移动等情况,使得 WSNs 结构频繁发生变化,导致维护网络拓扑结构的代价太大.文献[8]提出了一种结构无关的基于路线的算法 IWQE,能够有效地减少网络拓扑结构维护能耗,降低网络拓扑变化带来的影响,但 IWQE 没有考虑感知数据的隐私性.此外,已有算法主要通过加密来保证感知数据的隐私性,但过多的加/解密操作将造成严重的延迟和能量消耗.文献[9]提出了一种新的隐私保护的加聚集算法,其主要思想是:Sink 与每个节点共享一个随机数(密钥),每个节点将随机数加到自身感知数据上,其余操作与基本的数据聚集算法一致,Sink 通过减去与所有节点共享的随机数得到真实的聚集结果.虽然算法不需要进行加/解密操作,但部分节点由于通道冲突没有完成数据传输,而 Sink 又很难追踪到这些节点,因此,该算法的聚集结果可能由于减去多余的随机数而产生较大的偏差.

针对这些问题,本文提出一种安全而高效的空间数据聚集算法 SESDA(secure and energy-efficient spatial data aggregation algorithm).SESDA 在安全链接邻居节点之间建立安全通道(共享随机数),所有数据通过安全通道传输,因此数据不需要加/解密,节省了大量计算能耗.另外,根据聚集区域设定好理想路线,从起始聚集节点出发,广播聚集请求,聚集数据节点的感知数据,并将部分聚集结果沿着理想路线传给下一个聚集节点.如此继续,直到聚集区域的最后一个聚集节点,得到最终的聚集结果并传给 Sink.由于在聚集过程中聚集节点是实时确定,且与网络拓扑结构无关,因此节省了网络拓扑结构维护能耗.聚集节点的部分聚集结果是由多个节点的感知数据构成,所以下一个聚集节点只能获得该部分聚集结果,而不能推导出任何节点的数据.同时,为了防止聚集节点获取数据节点感知数据,采用类似 He 等人[10]提出的切分-重组技术对感知数据进行切分操作,即,将数据分成 J 片,自身保留 1 片,其余的 J–1 片传输给 J–1 个安全链接邻居节点,保证感知数据的隐私性.SESDA 只对数据节点进行切分,且在聚集过程中无任何加/解密操作,因此与 SMART 相比,SESDA 不仅能够降低通信量,而且能够节省更多的能耗.同时,SESDA 降低了数据传输发生冲突的几率,且不存在 Sink 减去失效节点的随机数情况,所以 SESDA 聚集结果的精确度较高.另外,SESDA 与网络拓扑结构无关,节点之间不需要提前部署共有信息,使得网络具有良好的扩展性.理论分析和实验结果显示,该方案在安全性、能耗、精确度和扩展性方面都取得了较好的结果.

本文第 1 节介绍相关工作.第 2 节给出攻击模式、目标等预备知识.第 3 节详细描述本文提出的 SESDA 算法,分析其安全性、通信量和能耗等性能.第 4 节对路线失效和网络扩展性进行分析.第 5 节对 SESDA 算法进行模拟实验及分析.第 6 节对全文进行总结.

1 相关工作

数据聚集的思想是聚集不同节点的感知数据,消除数据冗余,减少通信量,从而节省能耗延长网络生命周期.现有隐私保护的数据聚集算法主要有基于树或簇的网络拓扑结构.

基于树的隐私保护数据聚集算法是指将网络中的节点构造成一棵以 Sink 为根节点的树,节点将数据加密或扰乱后传输给其父节点,父节点对数据进行聚集,并将聚集结果传输给其父节点.如此继续,直至 Sink,得到最终的聚集结果.文献[11]提出的 SDAP 算法采用分而治之的思想实现安全的数据聚集,即 SDAP 将拓扑树动态地划分成多个尺寸类似的子树(逻辑群),每个子树内执行逐跳的数据聚集.EEHA[12]算法与 SMART 算法类似,但 EEHA 只对叶子节点进行切分处理,使得 EEHA 算法具有更高的效率和精确度.

基于簇的隐私保护数据聚集算法是将网络分成若干个簇,节点将感知数据传给簇头节点,簇头对簇内数据

进行聚集,再将聚集结果传给 Sink.文献[10]提出的 CPDA 算法通过在数据中添加随机种子和随机数来隐藏真实数据,簇头节点利用多项式的代数性质求解出加聚集结果.文献[13]提出的 IPHCDA 算法采用基于椭圆曲线的同态加密模式实现隐私保护的数据聚集,将网络分成若干个区域,不同区域使用不同的公钥对数据进行加密,聚集节点对密文进行聚集,并将聚集结果传至基站,基站对数据进行解密.

由于 WSNs 结构变化频繁,为了保证聚集结果的正确性,基于树或簇的聚集算法需要维护网络的拓扑结构,因而产生大量的能耗.文献[8]提出了一种与网络拓扑结构无关的基于路线的数据聚集算法 IWQE.该算法沿 1 条或多条动态生成的聚集路线聚集区域内节点的感知数据.如图 1 所示,IWQE 包括 3 个步骤:

(1) 利用位置路由协议[14],Sink 将聚集请求传到聚集区域内的某个节点(起始聚集节点 A_1).

(2) 从该聚集节点开始,利用基于路线的聚集算法聚集区域内节点的感知数据,然后沿着理想路线(ideal itinerary)确定下一个聚集节点,并将聚集结果传输给该聚集节点.如此继续,直到聚集完区域内所有节点.

(3) 利用位置路由协议将聚集结果传回给 Sink.文献[8]证明:当路线的宽度不超过节点通信半径的 $\sqrt{3}/2$ 倍时,能够保证聚集到区域内所有节点的感知数据.

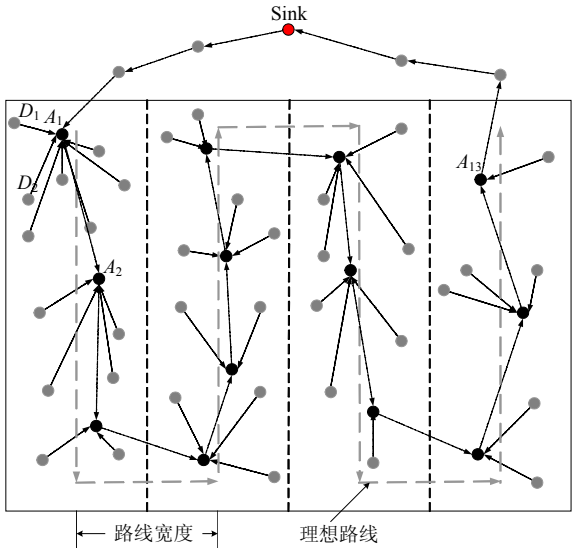


Fig.1 Itinerary route

图 1 路线路由

2 预备知识

WSNs 在数据聚集过程中,沿着理想路线动态地确定聚集节点,其余节点为数据节点.典型的聚集函数包括加、平均值、计数、最大/小值等.本文只讨论加聚集,因为其他聚集函数都可以转化为加聚集函数[9].

2.1 攻击模式

攻击者有以下攻击方式:

(1) 窃听攻击.由于WSNs采用无线通信,攻击者通过链路层窃听获取隐私数据.窃听攻击是WSNs最常见和容易发动的攻击,是本文研究的重点,本文假设攻击者能够窃听整个网络通信.

(2) 捕获传感节点.攻击者能够捕获 1 个或多个节点,获取节点中所有数据和密钥:一方面试图用获得的密钥对窃听到的数据进行解密以获取其他节点的感知数据,破坏数据的隐私性;另一方面,多个被捕获的节点串谋推测其相邻节点的感知数据.

2.2 设计目标

隐私保护数据聚集算法的主要目标是保证节点感知数据的私有性,此外,算法还必须考虑能耗、聚集结果的精确性和网络的扩展性等特性.因此,好的隐私保护数据聚集算法应满足下列标准:

(1) 隐私性:保证节点感知数据的隐私性是很多 WSNs 应用领域的关键问题.算法应能保证数据的隐私性,使得节点只知自身感知数据.因此,一种好的隐私保护数据聚集算法能够防窃听攻击和串谋攻击.

(2) 能耗:为了保证数据的隐私性,数据聚集算法额外增加了通信和能量开销.因此,一个好的隐私保护数据聚集算法在保证数据隐私性的情况下,其额外增加的开销应尽可能地小.

(3) 精确性:聚集结果可能是做决策的关键因素,因此,保证聚集结果的精确非常重要.所以,聚集结果的精确性是隐私保护数据聚集算法的评价标准之一.

(4) 扩展性:传感节点低廉、易失效等特点,使得 WSNs 拓扑具有动态性.当网络产生失效节点、部署新节点或节点移动时,隐私保护的数据聚集算法应仍能继续正确执行,即算法应具有良好的扩展性.

2.3 密钥分配

邻居节点之间安全通道的建立需要通过数据加密实现,密钥管理采用文献[15]中提出的随机密钥分配方法.该方法主要包括密钥预分配和邻居节点共享密钥链路建立.若两节点共享的密钥到期则进行密钥更新,则两节点移除该到期密钥,并重新建立邻居节点共享密钥链路.在建立过程中,节点不需要向其他节点广播任何信息,因此,密钥更新简单,对其他节点没有影响.

采用随机密钥分配方法,任意两邻居节点至少有 1 个相同密钥的概率为 $p_{connect}$.当两个邻居节点通过相同的密钥进行通信时,第三方节点拥有该密钥的概率为 $p_{overhear}$.具体为[15]

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

3 安全、高效的空间数据聚集算法

3.1 假设与符号

类似于文献[8,16]的假设,所有节点维护其安全链接邻居节点(secure link neighbor,简称 SLN)的位置信息,其中,安全链接指的是节点之间至少共享 1 个密钥.所有节点传输半径均为 R,每个节点的 SLN 节点列表的平均大小为 N_S.节点传输和接收 1bit 的能耗分别为 e_T 和 e_R.网络建立安全通道的能耗为 E_{sc},聚集查询用 $AWQ(a_w)$表示,其中,a_w 表示矩形聚集区域,聚集区域内的节点数为 N,处理聚集查询的总能耗为 $E_{total}=E_s+E_a+E_b$,其中,E_s 表示将聚集请求发送到聚集区域内某个节点能耗,E_a 表示在聚集区域内发送聚集请求、切片传输和聚集数据的能耗,E_b 表示将最终的聚集结果返回给 Sink 的能耗.节点 S_1 和 S_2 之间的距离为 $f_{dist}(S_1,S_2)$,感知数据范围为$[0,...,R_d]$.本文假设在聚集时间周期 T 内进行快照聚集,同时假设网络是动态的,即可能存在添加新节点、节点遗失或移动,每个节点通过周期性交换信息来维护 SLN 列表.

3.2 算法思想

为了避免现有算法所存在的问题,本文提出一种与网络拓扑结构无关的安全高效数据聚集算法 SESDA.SESDA 分为 5 个阶段:路线设计阶段、初始化阶段、聚集请求阶段、数据聚集阶段和聚集结果返回阶段.

- 路线设计阶段:根据聚集区域大小、位置和节点传输半径确定理想线路.
- 初始化阶段:在对已预设密钥的邻居节点之间建立安全通道;
- 聚集请求阶段:利用位置路由协议将聚集请求发送至聚集区域内的某个节点(起始聚集节点),如图 1 中的节点 A_1.
- 数据聚集阶段:数据节点将感知数据传给聚集节点.聚集节点对收到的数据进行聚集并将聚集结果传给下一个聚集节点,直至遍历整个聚集区域.
- 聚集结果返回阶段:区域内最后一个聚集节点利用位置路由协议将最终的聚集结果通过加密传输返

回至 Sink.

3.2.1 路线设计阶段

根据聚集区域大小(不失一般性,区域为矩形),节点通信半径 R,设置路线宽度 W_I,为了保证能够聚集区域内所有节点的感知数据,路线宽度满足 $W_I \leqslant \sqrt{3}R/2$.在此基础上设置理想路线,从起始聚集节点开始,沿着理想路线确定下一个聚集节点.如此继续,直到最后一个聚集节点为止,形成聚集节点序列,即实际路线(real itinerary).如图 1 所示,3 条黑色虚线将聚集区域分成 4 个子区域,灰色虚线表示理想路线,沿着理想路线的黑色圆点(聚集节点)形成实际路线;灰色圆点表示数据节点,每个聚集节点只聚集本子区域的数据节点.

3.2.2 初始化阶段

根据前面介绍的密钥分配方案,每个节点从有 K 个密钥的密钥池中随机选取 k 个密钥,并通过共享密钥与邻居节点建立安全通道(共享随机数).例如,节点 D_i 与邻居节点 D_j 拥有相同的密钥 k_{ij},两节点建立安全通道的过程是:不失一般性,D_i 选择一个随机数 d_{ij},并用密钥 k_{ij} 加密,再将密文传输给 D_j,D_j 通过密钥 k_{ij} 解密得到随机数 d_{ij},d_{ij}(d_{ij}=d_{ji})即为 D_i 和 D_j 的安全通道.节点之间通过安全通道进行数据传输能够防窃听攻击.本文将拥有安全通道的邻居节点称为 SLN 节点,每个节点维护自身的 SLN 节点列表.

3.2.3 数据聚集阶段

从起始聚集节点(aggregator node,简称 A-节点)开始,A-节点接收数据节点的感知数据,对所有数据(包括自身数据)进行聚集,并将聚集结果传输到下一个 A-节点.如此继续,直至遍历整个聚集区域.最后一个 A-节点得到最终的聚集结果.为了保证数据的隐私性,所有数据都通过安全通道进行传输,使得数据能够抗窃听攻击.同时,为使数据节点数据不泄露给 A-节点,数据节点在传输给 A-节点之前对数据进行切分,并将这些切片发送给 SLN 节点.该阶段具体操作如下:

Step 1. 聚集节点选择和聚集请求广播.

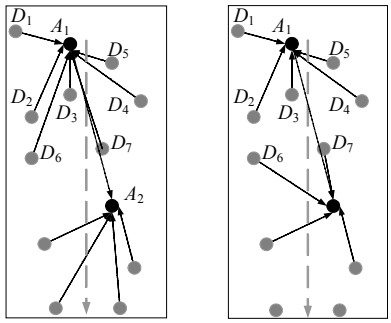
起始 A-节点 A_1 作为当前节点,根据 SLN 节点列表,选择在聚集路线方向上与理想线路尽可能贴近、前进距离尽量远的节点 A_2 作为下一个 A-节点.为了进一步量化选择标准,可设置公式 $S_i^{Agg}(j)=\gamma\times f_{ij}^{dist}+\delta\times f_j^{distII}$,其中,$\gamma$和$\delta$是系统参数.A-节点 A_i 选择 $S_i^{Agg}(j)$ 值最大的节点 A_j 作为下一个 A-节点.同时,A_i 向邻居节点广播聚集请求信息,包括聚集标识、当前 A-节点 ID 和下一个 A-节点 ID 等.A_i 完成聚集后,将当前聚集结果等信息传输给下一聚集节点,包括聚集标识、部分聚集结果等.

Step 2. 数据切分与重组.

当节点收到聚集请求信息后,符合响应请求的节点,称为数据节点(data node,简称 D-节点)响应聚集请求.D-节点在将感知数据传输给 A-节点之前对数据进行切分,即,将数据 v_i 随机分成 J_i 片,$v_i=\sum_{j=1}^{J_i}v_{ij}$,并将 J_i–1 片数据通过安全通道传输给 SLN 节点.

由于节点间的距离越大,其链路质量的期望越小[17],所以当 D-节点接收到聚集请求后,可能有两个 A-节点可供选择,如图 2(a)所示,D_6 和 D_7 可选择 A_1 或 A_2 作为目的 A-节点.为了降低因较低的链路质量而多次重传造成的能耗,D-节点选择距离较近 $\min(f_{dist}(D_i,A_i),f_{dist}(D_i,A_j))$的 A-节点作为目的 A-节点.例如,未考虑链路质量.D_6 和 D_7 选择 A_1 作为目的 A-节点(如图 2(a)所示);当考虑链路质量后,则选择 A_2 作为目的 A-节点(如图 2(b)所示).

由于多个 D-节点可能同时传输数据,为了避免信道冲突,算法设定在每个确定时间内只有 1 个 D-节点传输数据.主要有基于 TDMA 和基于环形的虚拟令牌两种方案.这两种方案需要 D-节点之间或 D-节点与 A-节点之间进行通信.为了减少通信量,简化处理进程,本文采用类似基于环形的方案,具体如下:A-节点广播聚集请求信息中包括参考线信息,D-节点根据参考线信息,通过简单运算得出其传输切片数据的时间为 *timer_slice*=*max_delay*×(θ/4π),其中,θ是参考线与连接 D-节点和 A-节点的连线之间的夹角(不失一般性,按顺时针方向),如图 3 所示.其中,*max_delay* 指的是 A-节点完成数据聚集的最大时间.由于每个 D-节点需要进行切分操作并将切片传输给 SLN 节点和重组切片再将重组结果传输给 A-节点,因此 D-节点需要进行两轮传输,其中,*timer_slice* 为第 1 轮 D-节点切片传输时间.



(a) 未考虑链路质量 (b) 考虑链路质量

Fig.2 D-Nodes select the destination A-nodes

图 2 D-节点选择目的 A-节点

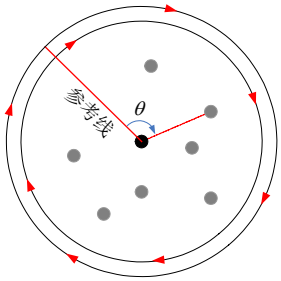


Fig.3 Time assignation

图 3 时间分配

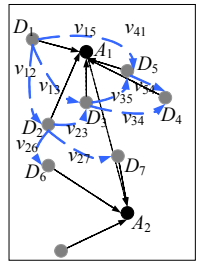


Fig.4 Illustrative example of slicing

图 4 切分实例

不同于 SMART 和 EEHA 算法将感知数据分成固定的片数,SESDA 将 D-节点感知数据分成 J 片,其中,J 的值是变化的.由于感知数据的隐私性与节点数据的切片数和收到的切片数相关联,因此,SESDA 中每个 D-节点感知数据的切片数不是随机确定,而是根据已收到的切片数动态确定切片数,优点是在切片总数一定的情况下,使数据的平均隐私性尽可能地高.显然,切片数 J 越小,通信量就越少,能耗就越低,数据隐私性也就越低.为了保证数据隐私性的等级,D-节点数据切片数必须符合下面两个条件:

$$\begin{cases} J_i \geqslant 1 \\ J_i + J_i^{rec} \geqslant J_{Secu} \end{cases},$$

其中,J_i 和 J_i^{rec} 分别表示 D-节点感知数据的切片数和收到其他 D-节点的切片数,J_{Secu} 是系统参数.由条件可知:D-节点的 θ 值越大,执行切片并传输的时间越晚,所以可能收到的切片数越多,需要对自身感知数据的切片数就越小.因此,为了尽可能地均衡各节点的能耗,A-节点发送的参考线位置是随机产生的.后面安全性能分析小节,我们将详细阐述数据的隐私性,以及在切片总数(通信量)一定的情况下,如何总体提高数据的隐私性.

图 4 具体描述了切分过程,D-节点 D_i 将感知数据随机分成 J_i 片,自己保留 1 片,其余的 J_i–1 片通过安全通道随机发送给 D_i 的 SLN 节点.例如,D_1 将数据切成 4 片,D_1 保留 v_{11},将其余 3 片发送给 SLN 节点 D_2,D_3 和 D_5,即 $D_1 \rightarrow D_2$:$v_{12}+d_{12} \bmod r$,$D_1 \rightarrow D_3$:$v_{13}+d_{13} \bmod r$ 和 $D_1 \rightarrow D_5$:$v_{15}+d_{15} \bmod r$.在保证所有切片都被接收后,D-节点对切片进行重组(聚集),并得到新的结果 v_i''.图 4 中,虽然 A_1 聚集结果不包含切片 v_{26} 和 v_{27},但这两片数据将包含在 A_2 聚集结果上.显然,只要保证 D-节点不要将切片传输给上一个 A-节点聚集范围内的 D-节点,聚集结果就是准确的.

Step 3. 数据聚集.

当节点接收到其他 D-节点切片后,对所有切片进行重组,再将重组结果传输给目的 A-节点.为了避免传输

冲突,每个 D-节点传输时间为 *timer_Mix*=*max_delay*×((*θ*+2π)/4π),即 *timer_Mix* 为第 2 轮 D-节点将重组结果传输给 A-节点时间.A-节点接收到 D-节点数据后,对所有数据(包括自身感知数据)进行聚集操作,再将聚集结果传输给下一个 A-节点.例如,图 5 显示图 4 中节点 A_1 的接收、聚集和传输过程:

1. 接收:
   D-节点: $v_i^d = v_i^n + d_{iA_1} \bmod r$, i=1,…,5
2. 聚集:
   $v_{A_1}^{agg} = \sum_{i=1}^{5}(v_i^d - d_{iA_1}) + v_{A_1} \bmod r$
3. 传输:
   $A_1 \to A_2$: $v_{A_1}^d = v_{A_1}^{agg} + d_{A_1A_2} \bmod r$

Fig.5 Illustration of the three steps of A-nodes

图 5 A-节点 3 步过程实例

当 A_2 收到 A_1 聚集结果后,A_2 作为当前 A-节点,根据前面的规则选择下一个 A-节点.如此继续,直到遍历完聚集区域内的所有节点,得到最终的聚集结果.

3.3 性能分析

3.3.1 安全性分析

SESDA 通过安全通道确保其他节点或攻击者不能获得传输的实际值,同时采用切分技术,使得 A-节点不能获得任何 D-节点感知数据.由于 A-节点聚集多个 D-节点重组数据或切片数据,保证 A-节点原始数据没有泄漏给其他 A-节点.在 SESDA 中,D-节点和 A-节点隐私保护的策略不同.本文在分析安全通道安全性的基础上,分别分析 D-节点和 A-节点感知数据的隐私性能.

1) 安全通道

邻居节点 D_i 和 D_j 的安全通道是两节点共享随机数 d_{ij},可以通过解密或猜测来获取随机数 d_{ij}:(1) 对于其他节点来说,通过自身密钥解密获取随机数的概率为 $p=k/K$[15];(2) 猜测随机数,由于随机数 d_{ij} 在范围[0,…,r]中是均匀分布,其中,$r=R_d \times N$,因此,正确猜测的概率是 1/r.当节点 D_i 向 D_j 传输数据时,由于 d_{ij} 在范围[0,…,r]中是均匀分布的,因此 $v_i+d_{ij} \bmod r$ 在范围[0,…,r]中也是均匀分布,即,窃听到该数据后是不能推导出 v_i.因此,随机数泄漏的概率为 $P_r=\min((\sigma \times p \times n_{nei}),r)$,其中,$n_{nei}$ 为邻居节点数,σ是安全通道重建频率对安全性影响的系数.

2) D-节点

D-节点 D_i 将数据 v_i 切割成 J_i 片,并将 J_i−1 片通过安全通道发送(出度)给 SLN 节点,所以泄漏每片数据 v_{ij} 的概率为 P_r.要获取 v_i 值,必须得到 J_i−1 片数据和 v_i^n 值,由安全通道隐私性能分析可知:获得 J_i−1 片数据的概率为 $P_r^{J_i-1}$,v_i^n 的值由第 J_i 片数据和接收到的切片数据重组得到.因此,获取 v_i^n 值的概率为 $P_r^{J_i^{rec}+1}$,其中, J_i^{rec} 表示节点 D_i 接收(入度)的切片数.所以,D-节点数据 v_i 值泄漏的概率为

$$P_i^D = P_r^{J_i-1} \times P_r^{J_i^{rec}+1} = P_r^{J_i+J_i^{rec}} \tag{2}$$

3) A-节点

A-节点 A_i 聚集 D-节点聚集值、可能有的 D-节点切片和自身感知数据,并将聚集结果传输给下一个 A-节点.因此,获取 A_i 的 v_i 值必须得到所有 D-节点重组值和切片数据值.所以,v_i 泄漏的概率为

$$P_i^A = P_r^{n_i^{D_{num}}} \times P_r^{J_{A_i}^{rec}+1} = P_r^{n_i^{D_{num}}+J_{A_i}^{rec}+1} \tag{3}$$

其中,$n_i^{D_{num}}$ 表示向 A_i 节点传输数据的 D-节点个数.

对于节点密度较大的网络,A-节点收集到的 D-节点数据个数较多,因此 A-节点数据隐私性较高.由公式(2)可知:D-节点感知数据隐私性由切片数 J_i 和 J_i^{rec} 确定,其平均被泄漏的概率为 $P_{avg}^D = 1/D_{num} \sum_{i=1}^{D_{num}} P_i^D$;切片总数为 $J_{total} = \sum_{i=1}^{D_{num}} J_i$. 因此,切片总数越大,通信量就越大,数据的隐私性可能也就越高.由于 D-节点的切片数是变化

的,在总的通信量一定的情况下,如何使数据平均被泄漏的概率最低?由此得出定理 1.

定理 1(数据泄漏率). 在节点切片总数(通信量)一定的情况下,当所有 D-节点出入度之和相等时,数据平均被泄漏的概率最低,隐私性最高.

证明:即证明当 J_{total} 一定时,当 $J_1^T = J_2^T = ... = J_{D_{num}}^T$ 时 P_{avg}^D 最小,其中, $J_i^T = J_i + J_i^{rec}$.

由于只有极少部分切片传输给 A-节点,可忽略不计,因此可知 $\sum_{i=1}^{D_{num}} J_i = \sum_{i=1}^{D_{num}} J_i^{rec}$;

所以, $\prod_{i=1}^{D_{num}} P_i^D = P_r^{\sum_{i=1}^{D_{num}} J_i + J_i^{rec}} = P_r^{2\times\sum_{i=1}^{D_{num}} J_i} = P_r^{2\times J_{total}}$;

由于 J_{total} 是定值,所以 $G = \sqrt[D_{num}]{P_r^{2\times J_{total}}}$ 也是定值(P_r 是定值);

由于算术平均数大于等于几何平均数,

即, $\frac{1}{D_{num}} \sum_{i=1}^{D_{num}} P_i^D \geqslant \sqrt[D_{num}]{\prod_{i=1}^{D_{num}} P_i^D} = \sqrt[D_{num}]{P_r^{2\times J_{total}}}$ 当且仅当 $P_1^D = P_2^D = ... = P_{D_{num}}^D$ 成立时等号成立,

即, $J_1^T = J_2^T = ... = J_{D_{num}}^T$ 时, $P_{avg}^D = \sqrt[D_{num}]{P_r^{2\times J_{total}}}$ 为最小,隐私性最高.证毕. □

由定理 1 可知:当切片总数为定值时,每个 D-节点的出入度之和与平均值越接近,感知数据平均泄漏的概率就越低.因此,在实际执行过程中虽然很难使所有 D-节点出入度之和相等,但每个 D-节点根据接收到的切片数来动态地确定 J 值,在不增加通信量的情况下,可最大程度地提高数据的平均隐私性.同样地,在设置系统参数 J_{Secu}(隐私性)后,算法可动态地确定 J 值,在数据满足一定隐私性要求的前提下,可最大程度地降低通信量.另外,让所有 D-节点的出、入度之和相近,使所有节点能耗($e_T \approx e_R$)相近,有利于延长网络的生命周期.

3.3.2 通信量

SESDA 通信量包括两部分:建立安全通道和执行数据聚集.节点 D_i 和 D_j 建立安全通道的过程是 D_i 加密随机数 d_{ij} 并将密文输出给 D_j,D_j 解密 d_{ij} 并返回确认信息,加密数据的位长为 $\overline{e}$, 节点 D_i 需要和 n_i^{SLN} 个节点建立安全通道,每对节点之间只需建立 1 条安全通道.因此,安全通道通信量为

$$T_{sc} = \frac{1}{2}\sum_{i=1}^{N}(\overline{e}+1)\times n_i^{SLN} \tag{4}$$

所有数据通过安全通道进行传输,数据位数均为 $\overline{d} = \lceil \log(R_d \times N) \rceil$.因此,感知数据、切片数据、部分聚集结果和最终聚集结果大小相等且均为 $\overline{d}$.此外,A-节点和 D-节点数据传输的机制不同,具体如下:

1) A-节点

广播聚集请求给所有一跳的 D-节点,位长为 $\overline{b_A}$, 并将所有接收到的重组数据和可能的切片数据进行聚集,最后将聚集结果传输给下一个 A-节点,具体为公式(5),其中,A_{num} 表示 A-节点个数, $n_i^{D_{num}}$ 表示 A-节点 A_i 接收到 D-节点个数:

$$T_{A-node} = \sum_{i=1}^{A_{num}} (\overline{b_A} + (n_i^{D_{num}} + 1 + J_{A_i}^{rec}) \times \overline{d}) \tag{5}$$

2) D-节点

D_i 需要将感知数据分成 J_i 片,并将 J_i–1 片传输给 SLN 节点,接收其他 D-节点 J_i^{rec} 片数据,并将重组结果传输给 A-节点,其通信量为公式(6),其中,D_{num} 表示 D-节点个数:

$$T_{D-node} = \sum_{i=1}^{D_{num}} ((J_i + J_i^{rec}) \times \overline{d} + \overline{b_A}) \tag{6}$$

由于节点总数为 N,可知 N=D_{num}+A_{num},且每个 D-节点接收聚集请求消息,所有节点接收到的切片总数与 A-节点接收到的重组数据(D-节点个数)之和与 D-节点的切片总数相等.因此,总通信量可简化为

$$T_{All-node} = N \times \overline{b_A} + \overline{d} \times \left(2 \times \sum_{i=1}^{D_{num}} J_i + A_{num}\right) \tag{7}$$

通过公式(7)可知:通信量与 D-节点和 A-节点所占比例有关,并与 D-节点的切片总数有关.由于 A-节点不需要进行切分操作,因此总体来说,D-节点数所占比例越高,通信量就越大.同时,为了提高安全性,每隔一个周期重建一次安全通道,假设每个周期进行 β 轮数据聚集,则每轮数据聚集的平均通信量为

$$T=\frac{1}{\beta}(T_{sc}+\beta\times T_{All\text{-}node}) \tag{8}$$

3.3.3 能 耗

能耗主要由通信和运算组成,其中,运算主要有加/解密运算和加模运算.与加/解密运算能耗相比,加模运算能耗可忽略不计,因此,本文只考虑加/解密运算的能耗.在SESDA中,所有加/解密操作只发生在安全通道建立阶段,每条安全通道需执行加密和解密操作各1次,因此,加/解密次数为

$$N_{dec}=N_{enc}=\frac{1}{2}\sum_{i=1}^{N}n_i^{SLN} \tag{9}$$

根据上面通信量的分析,$E_{D\text{-}node}$,$E_{A\text{-}node}$ 分别表示 D-节点和 A-节点通信量能耗,数据聚集能耗为 $E_a=E_{D\text{-}node}+E_{A\text{-}node}$,具体为

$$E_{D\text{-}node}=\sum_{i=1}^{D_{num}}(J_i\times\bar{d}\times e_T+(J_i^{rec}\times\bar{d}+\overline{b_A})\times e_R) \tag{10}$$

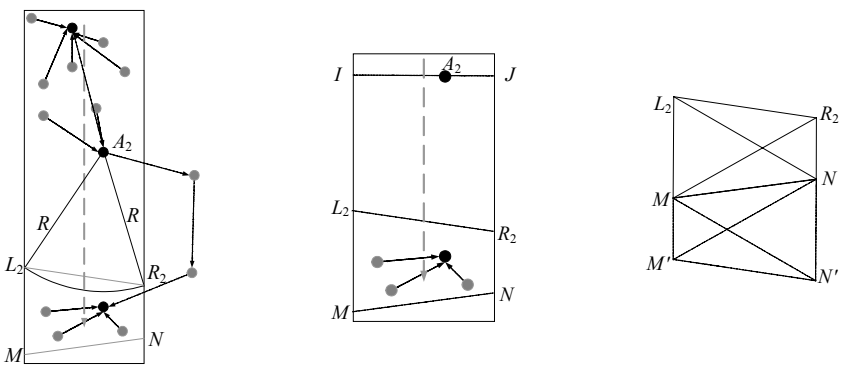
$$T_{A\text{-}node}=\sum_{i=1}^{A_{num}}(\overline{b_A}\times e_T+(n_i^{D_{num}}+1+J_{A_i}^{rec})\times\bar{d}\times e_R) \tag{11}$$

4 路线失效和网络扩展性

当WSNs是密集型网络时,A-节点能够找到下一个A-节点;但当网络节点分布是非均匀或节点密度较小时,则可能出现 A-节点在当前区域找不到下一个 A-节点.同时,由于传感节点易失效的特点,网络可能出现节点失效或部署新节点.下面具体阐述如何处理上述情况.

4.1 路线失效

假设网络节点分布不均匀或节点密度较小,当聚集区域中的某个 A-节点根据上述规则找不到下一个 A-节点时,即出现路线失效,如图 6(a)所示,SESDA 利用位置路由协议绕过该子区域继续执行.例如,图 6(b)中,A_2 在通信范围内找不到下一个 A-节点,出现路线失效,聚集操作无法继续执行.为了避免该问题,本文采用如下处理方法:A_2 找不到下一个A-节点时,继续广播聚集请求,并将下一个聚集节点ID设为–1;通信范围内所有D-节点收到聚集请求后,将 A_2 作为目标节点,并进行切分聚集操作.A_2 聚集完该范围内所有 D-节点数据后,以区域 L_2R_2NM 为目的位置(其中,$f_{dist}(L_2,N)=f_{dist}(R_2,M)=R$),利用位置路由协议将部分聚集结果和聚集消息发送至区域 L_2R_2NM 中的节点(即下一个A-节点)以保证路线失效时能继续完成聚集任务.当区域 L_2R_2NM 中没有节点时,A_2 将以区域 $MNM'N'$ 为目的位置(其中,$f_{dist}(M,N')=f_{dist}(N,M')=R$),如果区域 $MNM'N'$ 仍然没有任何节点,则以此类推,直到找到下一个 A-节点,如图 6(c)所示.



(a) 绕过失效区域 (b) 下一聚集节点不存在 (c) 确定目标区域

Fig.6 Illustrative example of itinerary void

图 6 路线失效示意图

定理 2(节点完全覆盖). 当路线失效时,SESDA 能够覆盖聚集区域内所有节点.

证明:

(1) 区域 IJL_2R_2 内没有传感节点,否则,聚集节点 A_2 将能够找到一下聚集节点,如图 6(c)所示,与假设矛盾.

(2) 如果区域 L_2R_2NM 内有节点,则 A_2 根据路由协议选择该区域内某个节点 A_3 作为下一个聚集节点(聚集节点选择规则与前面相同),于是,A_3 能够保证聚集区域 L_2R_2NM 内所有 D-节点;如果区域 L_2R_2NM 内没有节点,则考虑区域 $MNM'N'$ 并做同样处理,即可保证聚集区域 $MNM'N'$ 内所有节点数据.

综合情形(1)和情形(2)可知,算法能够保证聚集任意两个聚集节点之间的所有 D-节点.证毕. □

4.2 扩展性

由于传感器网路的动态性及传感节点的易失效性,网络运行过程中可能存在节点失效或部署新节点的情况.在已有的聚集查询算法中,当部署新节点时,需要对该节点与 Sink/其父节点/子树根节点提前部署一些必要的信息,如密钥、随机数等,网路扩展比较困难.本文提出的算法具有很好的扩展性,当需要部署新节点时,只要提前将密钥池加载到该节点即可,具体是:

(1) 添加新节点:当节点 D_i 部署到网络中时,确定其 SLN 节点列表并与列表中的节点建立安全通道;同时,SLN 节点列表中的节点将 D_i 添加到自身的 SLN 节点列表中,完成新节点的部署.

(2) 遗失节点:当 D_i 的 SLN 节点列表中的某节点超过一定时间没有响应后,D_i 认为该节点失效,并将该节点从 SLN 节点列表中删除,防止 D_i 将切片传输给该失效节点,保证网络正常工作.

5 仿真实验及分析

为了对算法的通信量、能耗、精确度和隐私性等性能进行比较,本节在文献[18]的 WSNs 模拟器基础上,仿真实现 SESDA,SMART 和 IWQE 算法.为了更好地比较各算法的性能,3 种算法采用同样的实验数据集 Intel Lab Data[19].实验环境为 Core i3-3220CPU,4G 内存;软件环境为 Win7 操作系统,VS.NET 2010 和 Matlab.采用文献[20]给出的 TelosB 参数,传输和接收 1bit 的能耗分别为 e_T=0.72μJ 和 e_R=0.81μJ.利用 RC4 对数据进行加/解密,10bit 数据能耗为 8.92μJ.实验结果是执行 20 轮的平均值,每轮随机产生一个 WSNs 拓扑.其他参数见表 1.

Table 1 Experimental paramaters

表 1 实验参数

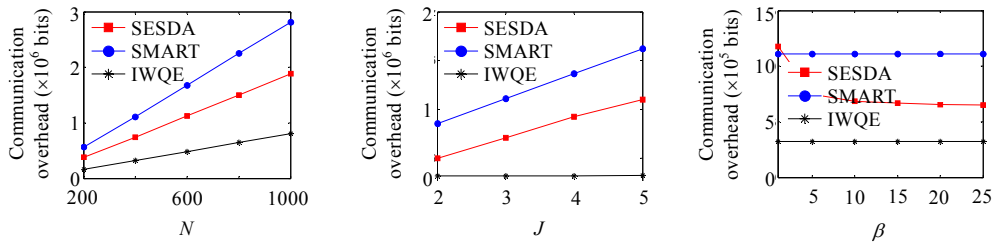
参数名	参数值
网络覆盖区域	100m×100m
网络节点分布	随机均匀分布
节点通信半径	10m
节点数	400
感知数据消息大小	40bytes
聚集区域占网络覆盖区域的百分比	20bytes
聚集请求消息大小	100%
网络宽度占通信半径的比率	$\sqrt{3}/2$

5.1 通信量及能耗

测试 SESDA,SMART 和 IWQE 这 3 种算法在不同的节点数、不同的平均切片数和每周期不同数据聚集轮数情况下,算法总的通信量和能耗.

1) 通信量

图 7 显示 3 种算法在不同参数下通信量的变化.因为 SMART 需要将所有节点感知数据切割成 J 片,并将 J–1 片加密传输给其邻居节点,因此,SMART 算法数据传输的通信量为 $N\times J\times \bar{e}$.从图 7 可以看出,IWQE 的通信量最小,但 IWQE 没有考虑数据隐私性.除了每次聚集前都重新建立安全通道(β=1)的情况下,SESDA 的通信量比 SMART 稍高以外,SESDA 通信量比 SMART 要少;而且随着 N 和 J 的增大,SESDA 通信量减少的幅度更大.当β值较大时,SESDA 需要的通信量比 SMART 小很多,最多达到 42%.



(a) N 的影响 (b) J 的影响 (c) β的影响

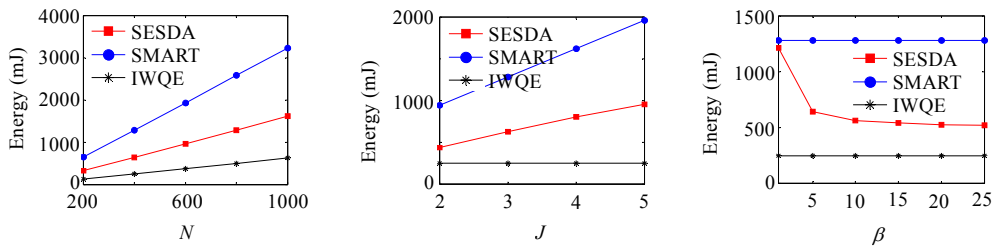
Fig.7 Communication cost

图 7 通信量

2) 能耗

由于 SESDA 只在安全通道建立阶段需要进行加/解密计算,而在数据聚集阶段没有任何加/解密计算,极大降低了计算能耗.因此,即使在不考虑网络拓扑结构维护开销的情况下,SESDA 比 SMART 能耗减少幅度更大.

- 如图 8(a)所示,随着 N 的增大,降低幅度也随之增大,达到 50%.
- 同时,随着 J 的变大,SMART 由于切片数的增加,其加/解密次数随之增加,而 SESDA 的加/解密次数与切片数无关,所以 SESDA 比 SMART 节省更多能耗,如图 8(b)所示.
- 从图 8(c)可知,β值越大,SESDA 的能耗越接近 IWQE 算法.



(a) N 的影响 (b) J 的影响 (c) β的影响

Fig.8 Energy consumption

图 8 能量消耗

5.2 隐私保护

图 9 显示 SESDA,SMART 和 SESDA-NonOpt 感知数据泄漏的概率(隐私性),其中,SESDA-NonOpt 表示没有应用本文提出的切片数优化确定机制,即,D-节点切片数完全随机,不考虑节点出入度之和的均衡性.

实验结果显示:在破解链路安全的概率 P_{LP} 较低时,SESDA 和 SMART 感知数据泄漏的概率近似,都具有较高的隐私性;但随着 P_{LP} 的增大,SESDA 的感知数据具有更好的隐私性,特别是当 P_{LP} 大于等于 0.8 时,SESDA 感知数据的隐私性比 SMART 具有明显的优势.同时,从图 9 还可以看出,SESDA-NonOpt 数据的隐私性没有 SESDA 和 SMART 高.主要原因是 SESDA-NonOpt 没有综合考虑节点的出度和入度,使得节点间隐私度相差较大,造成感知数据平均隐私性较低.因此,在没有增加通信量和能耗的情况下,综合考虑节点的出入度,动态确定节点的切片数,对提高感知数据的隐私性具有重要的影响.

图 10 显示平均切片数 *Ave-J* 不同时,SESDA 感知数据的隐私性.从图中可知:*Ave-J* 值越大,感知数据的隐私性就越好,但其通信量和能耗也越高.因此,SESDA 可以通过设置不同 *Ave-J* 值,在私有保护和通信/能耗之间取得平衡.

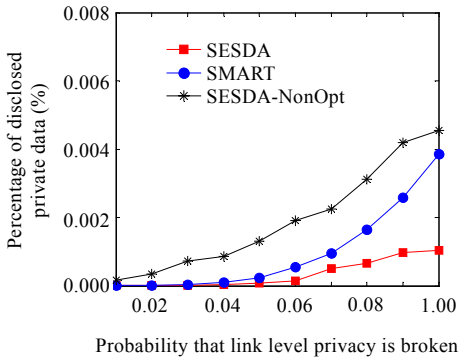


Fig.9 Privacy comparisons

图 9 私有性比较

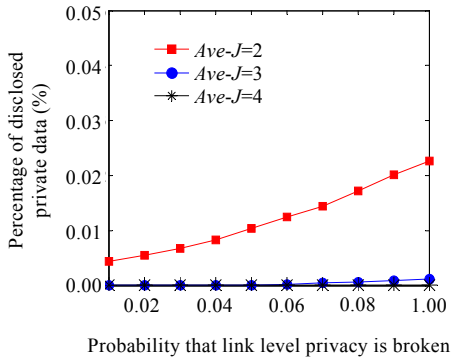


Fig.10 Privacy with respect to the average number of slices

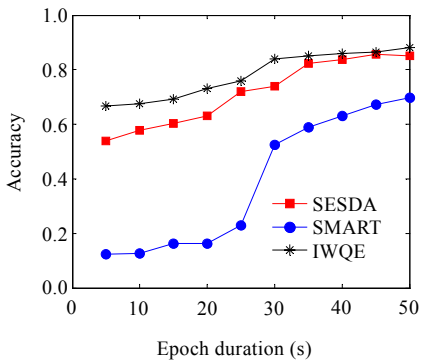
图 10 不同平均切片数私有性比较

5.3 聚集精确度

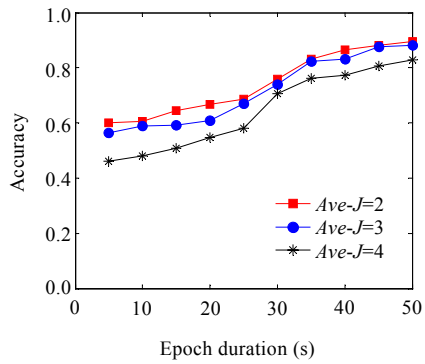
理想情况下,没有数据丢失,聚集结果精确性将是 100%;但由于网络无线通道的冲突性、数据处理的延迟性导致传输信息的丢失和节点的失效性,使得聚集结果的精确性受到影响.精确性为算法聚集结果与实际的感知数据和之间的比率.由于本文研究的是加聚集,因此,精确度定义为公式:

$$p_c = \frac{\text{聚集结果}}{\sum_{i=1}^{N} d_i} \tag{12}$$

图 11(a)显示了 3 种算法在不同时间周期下得到的聚集结果精确度,从图中可知:时间周期越长,聚集精确度越高,主要原因是:(1) 时间周期越长,使得在周期内传输的数据包之间发生碰撞的几率越小;(2) 时间周期越长,使得数据包有越大的概率在传输时间截止前完成传输.另外,因为 SMART 在聚集过程中需要对每片数据进行加/解密操作,而 SESDA 在聚集过程中没有加/解密操作,节省了大量的时间,减少了延迟.因此,SESDA 聚集结果的精确度比 SMART 更高(当时间周期相对较小时,精确度差距更大).由于 IWQE 不需要进行加/解密和切片操作,因此聚集精确度最高.从图 11(b)可知,不同的 *Ave-J* 值对 SESDA 精确度的影响不大.但更小的 *Ave-J* 值具有相对较高的精确度,主要原因是:随着 *Ave-J* 的增大,需要将更多的数据包传输给安全链接邻居节点,因此数据包有更大的概率发生碰撞,降低了聚集结果精确度.



(a) SESDA,SMART 和 IWQE



(b) 不同 *Ave-J* 值情况

Fig.11 Aggregation accuracy

图 11 聚集精确度

由实验结果可以看出:SESDA 在通信量、能耗和聚集精确度方面比 SMART 具有明显的优势;在链路安全

较低时,SESDA 感知数据的隐私性能更好.因此,与 SMART 相比,SESDA 需要更少的通信量和能耗,能够达到更高的聚集精确性和更好的数据隐私性.同时,SESDA 通过调节β和 *Ave-J* 值,更便于在私有保护、聚集精确度和通信/能耗之间取得平衡.

6 总 结

WSNs 中提供具有隐私保护的高效的数据聚集算法是一个挑战性的问题.我们提出了一种安全数据聚集算法 SESDA.SESDA 采用基于路线的聚集请求和数据聚集,使得算法的执行与 WSNs 的拓扑结构无关,节省了维护网络拓扑结构的消耗,当部分传感节点发生失效或移动时,数据聚集能够继续正确执行,且在网络中容易部署新节点,即算法具有良好的扩展性.同时,感知数据通过安全通道进行传输,所以在保证数据隐私性的情况下,聚集过程无需任何加/解密操作,使得计算能耗可以忽略不计,比较适合传感节点电池供电、难以维护的特点,且各节点能耗比较均衡,有利于延长整个网络生命周期.此外,SESDA 能够极大地缩短数据处理时间,降低处理延迟,提高聚集精确度.因此,SESDA 能够应用到部署在野外、网络结构动态变化、保证数据隐私和聚集结果精确度要求较高的网络场景.例如在军事领域,军队通过使用 WSNs 代替周边防务的哨兵,通过对潜在攻击的定位和识别来保证士兵的安全,并对打击敌人给予信息支持.这类 WSNs 部署在野外、网络难以维护、结构动态变化,且感知数据面临隐私泄露问题,SESDA 适应于这类网络场景要求.实验结果显示:SESDA 算法在增加少量通信量和能耗的情况下,保证了数据的隐私性.与已有的安全的数据聚集算法 SMART 相比,SESDA 需要更少的通信量/能耗、更高的聚集精确度和更好的扩展性.

致谢 在此,我们向对本文的工作给予支持和建议的同行表示感谢.

References:

[1] Culler D, Estrin D, Srivastava M. Overview of sensor networks. IEEE Computer, 2004,37(8):41−49. [doi: 10.1109/MC.2004.93]

[2] Xu N, Rangwala S, Chintalapudi KK, Ganesan D, Broad A, Govindan R, Estrin D. A wireless sensor network for structural monitoring. In: Stankovic JA, Arora A, Govindan R, eds. Proc. of the 2nd ACM Conf. on Embedded Networked Sensor Systems. Baltimore: ACM Press, 2004. 13−24. [doi: 10.1145/1031495.1031498]

[3] Zhang XW, Dai HP, Xu LJ, Chen GH. Mobility-Assisted data gathering strategies in WSNs. Ruan Jian Xue Bao/Journal of Software, 2013,24(2):198−214 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4349.htm [doi: 10.3724/SP.J.1001.2013.04349]

[4] He W, Nguyen H, Liu X, Nahrstedt K, Abdelzaher T. iPDA: An integrity-protecting private data aggregation scheme for wireless sensor networks. In: Proc. of the IEEE Military Communication Conf. San Diego: IEEE Press, 2008. 1−7. [doi: 10.1109/MILCOM.2008.4753645]

[5] Girao J, Westhoff D, Schneider M. CDA: Concealed data aggregation for reverse multicast traffic in wireless sensor networks. In: Proc. of the IEEE Int'l Conf. on Communications. Seoul: IEEE Press, 2005. 3044−3049. [doi: 10.1109/ICC.2005.1494953]

[6] Yu Y, Krishnamachari B, Prasanna VK. Energy-Latency tradeoffs for data gathering in wireless sensor networks. In: Proc. of the 23rd IEEE Int'l Conf. on Computer Communications. Hong Kong: IEEE Press, 2004. 244−255. [doi: 10.1109/INFCOM.2004.1354498]

[7] Madden S, Franklin MJ, Hellerstein JM, Hong W. TAG: A tiny aggregation service for ad-hoc sensor networks. In: Proc. of the ACM OSDI. Boston: ACM Press, 2002. 131−146. [doi: 10.1145/844128.844142]

[8] Xu Y, Lee WC, Xu J, Mitchell G. Processing window queries in wireless sensor networks. In: Liu L, Reuter A, Whang KY, Zhang JJ, eds. Proc. of the 22nd IEEE Conf. on Data Engineering. Atlanta: IEEE Press, 2006. 70−80. [doi: 10.1109/ICDE.2006.119]

[9] Castelluccia C, Mykletun E, Tsudik G. Efficient aggregation of encrypted data in wireless sensor networks. In: Proc. of the 2nd Annual Int'l Conf. on Mobile and Ubiquitous Systems. San Diego: IEEE Press, 2005. 109−117. [doi: 10.1109/MOBIQUITOUS.2005.25]

[10] He W, Liu X, Nguyen H, Nahrstedt K, Abdelzaher T. PDA: Privacy-Preserving data aggregation in wireless sensor networks. In: Proc. of the 26th IEEE Int'l Conf. on Computer Communications. Alaska: IEEE Press, 2007. 2045−2053. [doi: 10.1109/INFCOM.2007.237]

[11] Yang Y, Wang X, Zhu S, Cao G. SDAP: A secure hop-by-hop data aggregation protocol for sensor networks. ACM Trans. on Information and System Security, 2008,11(4):18. [doi: 10.1145/1380564.1380568]

[12] Li HJ, Lin K, Li KQ. Energy-Efficient and high-accuracy secure data aggregation in wireless sensor networks. Computer Communications, 2011,34(4):591−597. [doi: 10.1016/j.comcom.2010.02.026]

[13] Ozdemir S, Xiao Y. Integrity protecting hierarchical concealed data aggregation for wireless sensor networks. Computer Networks, 2011,55(8):1735−1746. [doi: 10.1016/j.comnet.2011.01.006]

[14] Karp B, Kung HT. GPSR: Greedy perimeter stateless routing for wireless networks. In: Pickholtz RL, Das SK, Cáceres R, *et al*., eds. Proc. of the 6th Annual ACM Int'l Conf. on Mobile Computing and Networking. Boston: ACM Press, 2000. 243−254. [doi: 10.1145/345910.345953]

[15] Eschenauer L, Gligor VD. A key-management scheme for distributed sensor networks. In: Vijayalakshmi A, ed. Proc. of the 9th ACM Conf. on Computer and Communications Security. Washington: ACM Press, 2002. 41−47. [doi: 10.1145/586110.586117]

[16] Fu TY, Peng WC, Lee WC. Parallelizing itinerary-based KNN query processing in wireless sensor networks. IEEE Trans. on Knowledge and Data Engineering, 2010,22(5):711−729. [doi: 10.1109/TKDE.2009.146]

[17] Zuniga M, Krishnamachari B. Analyzing the transitional region in low power wireless links. In: Proc. of the 1st Annual IEEE Communications Society Conf. on Sensor and Ad Hoc Communications and Networks. Washington: IEEE Press, 2004. 517−526. [doi: 10.1109/SAHCN.2004.1381954]

[18] Coman A, Nascimento MA, Sander J. A framework for spatio-temporal query processing over wireless sensor networks. In: Labrinidis A, Madden S, eds. Proc. of the 1st Workshop on Data Management for Sensor Networks, in Conjunction with VLDB. Toronto: ACM Press, 2004. 104−110. [doi: 10.1145/1052199.1052217]

[19] Samuel M. Intel lab data. 2004. http://db.csail.mit.edu/labdata/labdata.html

[20] Groat MM, He W, Forrest S. KIPDA: *k*-Indistinguishable privacy-preserving data aggregation in wireless sensor networks. In: Proc. of the 30th IEEE Int'l Conf. on Computer Communications. Shanghai, 2011. 2024−2032. [doi: 10.1109/INFCOM.2011.5935010]

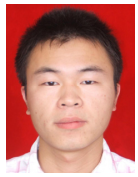
附中文参考文献:

[3] 张希伟,戴海鹏,徐力杰,陈贵海.无线传感器网络中移动协助的数据收集策略.软件学报,2013,24(2):198−214. http://www.jos.org.cn/1000-9825/4349.htm [doi: 10.3724/SP.J.1001.2013.04349]

王涛春(1979－),男,安徽无为人,博士生,副教授,主要研究领域为无线传感器网络,隐私保护.
E-mail: wangtc@nuaa.edu.cn

秦小麟(1953－),男,教授,博士生导师,CCF高级会员,主要研究领域为分布式数据管理与安全,时空数据管理.
E-mail: qinxcs@nuaa.edu.cn

刘亮(1985－),男,博士,讲师,主要研究领域为无线传感器网络,分布式数据管理.
E-mail: liangliu@nuaa.edu.cn



丁有伟(1987－),男,博士生,主要研究领域为能量高效数据管理,云计算.
E-mail: dingyouwei@nuaa.edu.cn