

一种基于复数域的数据融合完整性保护算法

赵丹, 杨庚

(南京邮电大学 计算机学院, 江苏 南京 210003)

摘要:随着无线传感器网络技术的快速发展,传感器网络开始承载越来越多的应用服务,很多应用都需要保证信息或数据的隐私性和完整性,这对网络数据融合提出了更高的要求。因此,设计一种能够实现隐私保护兼完整性保护的数据融合方案显得尤为重要。文中提出了一种基于复数域的新无线传感器网络数据融合完整性保护算法,通过对实部真实数据增添私有种子进行隐私保护,并利用复数的虚实部关联特性进行数据的完整性保护。此外,算法依靠数据融合树型结构本身的特性,减少了数据通信开销,计算复杂度低。理论分析表明,在恶意节点的各种攻击情况下,算法具有良好的完整性保护性能。仿真结果显示,算法可以在有效保护数据隐私性和完整性的前提下,花费与TAG相同的时间,得到精确的数据融合结果。

关键词:物联网;无线传感器网络;数据融合;完整性保护;隐私保护

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2012)08-0150-05

A Complex Field-based Integrity-protecting Data Aggregation Algorithm

ZHAO Dan, YANG Geng

(College of Computer Science & Technology, Nanjing University
of Post & Telecommunications, Nanjing 210003, China)

Abstract: With the rapid development of network communication technology, the internet begins to carry more and more application services, it brings forward very high demands for network data aggregation. So, designing a data aggregation scheme which can protect both data privacy and integrity seems very important. It presents a complex field-based new WSN data aggregation algorithm for integrity protecting. It adds privacy seed to the real sampling data in order to preserve privacy and protect data integrity by using the associated characteristics between the real part and imaginary part of complex numbers. Moreover, depending on its own characteristics of data aggregation tree structure, the algorithm decreases data communication overhead and computation overhead. Theoretical analysis shows that, in all attacking cases, the algorithm achieves good integrity protection performance. The simulation results show that under the premise of privacy preserving and integrity protecting, the algorithm can get accurate data aggregation result, just spending the same time of TAG.

Key words: internet of things; wireless sensor network; data aggregation; integrity protecting; privacy preserving

0 引言

无线传感器网络作为物联网的重要组成部分,它主要依靠网络中随机分布的大量节点收集并返回其所在区域的监测信息,供查询用户进行分析和处理,这也是传感器网络的基本功能。由于传感器网络的资源和能量都很有限,在收集信息的过程中采用各个节点单

独传送数据到QS的方法是不合适的。这不仅会浪费通信带宽和能量,也会降低信息收集的效率。因此,设计并研发出一种对原始数据进行高效处理的方案显得尤为重要。数据融合是传感器网络中一种高效的数据查询处理方案,它将多份数据或信息进行处理,组合出更有效、更符合用户需求的数据。数据融合的方法普遍应用于人们的日常生活中,例如在森林防火的应用中,需要对多个温度传感器探测到的环境温度数据进行融合;在目标自动识别应用中,需要对图像监测传感器采集的图像数据进行融合处理。在传感器应用中,大多数时候只关心监测结果,并不需要收到大量原始数据,数据融合是实现此目的的重要手段。

传感器网络中采集到的信息作为物联网应用的基础,是物联网的重要资源之一,也是需要保护的敏感信

收稿日期:2012-01-10; **修回日期:**2012-04-13

基金项目:国家自然科学基金资助项目(60873231, 60977069);江苏省自然科学基金(BK2009426);江苏省高校自然科学研究重大项目(11KJA520002)

作者简介:赵丹(1988-),女,江苏淮安人,硕士研究生,主要研究方向为无线传感器网络数据融合、完整性保护;杨庚,教授,博士生导师,主要研究方向为无线传感器网络、计算机通信与网络、并行与分布式计算、信息安全。

息,其安全性是需要着重考虑的一个方面。安全性问题不仅局限于隐私保护方面,还包括信息的完整性鉴别、点到点的消息认证问题、新鲜性问题、认证组播/广播问题等。尤其是信息的完整性鉴别可有效地识别接收方获取的信息是否与最初发送方传来的消息一样,是否被恶意节点篡改或传输中出错。经过数据融合后的信息是用来供用户分析与处理,或制定相应的解决方案的,信息的正确与否直接影响着决策者的判断。如果信息的完整性被破坏,那么融合后的信息将与原始信息不一致,用户依赖此信息进行的分析等一系列措施将会有偏差。所以,完整性鉴别在数据融合中占据极其重要的地位。

目前,现有的研究^[1~11]已经提出了一些完整性保护方案。例如,He等人提出的iPDA^[1]利用数据的冗余达到完整性的鉴别,但也恰恰是冗余造成了信息传输的通信量、计算量都约翻倍,能量消耗相应增大,时延也相应增长。He等人提出的iCPDA^[2]的计算复杂度和工作量都相当大,而且它仅适合簇状结构的传感器网络,适用范围不具备普遍性。

文中提出了一种基于复数域的数据融合完整性保护算法CBIPDA,它对由Bista等人提出的新型敏感数据融合完整性保护方案^[3~5]做了相应的改进,使用逐跳的(hop-by-hop)数据融合方式,具有计算复杂度与数据传输量小的优点,且数据融合时间效率高。CBIPDA算法建立在TAG^[12]融合算法之上,采用依靠数据融合树型结构本身特性的办法,将节点信息的实数域扩展到复数域,并利用虚数部与实数部真实数据相关联的特性,有效地实现了信息完整性的鉴别。同时,通过对实数部真实数据添加伪数据的方法,保证了信息的隐私保护。文中着重介绍数据融合完整性方面的保护,在新型敏感数据融合完整性保护方案的基础上,改进了其存在的缺陷,并在消耗同等通信开销、相近计算开销的基础上,达到了更为可靠的完整性鉴别效果。

1 相关工作

数据融合完整性保护方面比较典型的方案分别是由He等人提出的iPDA^[1]、iCPDA^[2]方案和由Bista等人提出的一组新型数据融合安全性保护方案^[3~5],其中iPDA和文献[3]方案与文中研究有一定联系。

iPDA算法是SMART^[13]算法的延伸,在其基础上增加了完整性保护的功能。它通过构造不相交融合树,利用冗余性来实现完整性保护,由冗余引起的数据通信开销、计算开销也相应增加,这导致了能量消耗翻倍、时间延迟,网络生命周期缩减。

文献[3]算法的基本思想是将数据从实数域扩展到复数域,使用逐跳(hop-by-hop)的数据融合方式和

点到点(node-to-node)的加解密模式,在能够达到数据融合精确度要求的情况下,阻止外部入侵者和内部可信节点对信息进行截获和篡改。它有效地保证了信息的隐私性,然而完整性保护还不够完善,在特定情况下恶意节点仍有可趁之机。

文献[3]的算法步骤分为三步,构造复数算法、融合算法和完整性鉴别算法。

1) 构造复数算法。

各传感器节点在采样到的数据 a 上加上一个伪数据 a' 共同构成自定义数据的实部 s ,再在实部上加一个伪数据 bi (自定义数据的虚部),构成复数 $s + bi$ 。

2) 融合算法。

各节点加密自身数据 $s + bi$,沿数据融合树向上传给父节点,父节点利用共享密钥将解密后的子节点数据与自身数据进行融合并向上传送,重复此过程直到最终在QS处得到融合结果: $SUM^2 = \langle SUM^{2r}, SUM^{2im} \rangle$ 。

3) 完整性鉴别算法。

单独计算出各节点的伪数据 a' 之和 SUM^{1r} ,得到节点采集数据的融合结果为 $SUM = SUM^{2r} - SUM^{1r}$ 。计算各节点的虚部伪数据 b 之和, SUM^{1im} ,并比较 SUM^{1im} 是否等于 SUM^{2im} ,若相等则完整性未被破坏。如果在融合过程中,某恶意节点对中间的数据篡改或数据在传输过程中出错,那么 SUM^{1im} 就不等于 SUM^{2im} ,完整性被破坏。

这种完整性鉴别方法在对实虚部都篡改时是成立的,当恶意节点只篡改数据的实数部分,即只篡改 s 时, SUM^{1im} 仍然等于 SUM^{2im} ,系统断定完整性未被破坏,鉴别出错,给恶意节点带来了可趁之机。

为克服文献[3]中算法存在的缺陷,文中提出了一种高效节能且通用的数据融合完整性保护算法CBIPDA。与现有算法比较分析表明,其数据通信开销和计算开销都小,可以支持各种无线传感器网络的拓扑结构。

2 系统模型与算法实现

2.1 网络模型

在文中,无线传感器网络由一个连通图 $G(V, E)$ 来表示,其中的顶点 $v(v \in V)$ 表示无线传感器网络中的节点,边 $e(e \in E)$ 表示节点间的通信链路。记无线传感器网络中节点的数量为 $N = |V|$ 。在无线传感器网络中,包含了三种类型的节点:QS(Query Server)节点、中间融合节点和叶子节点。QS节点应答查询请求,同时也是数据融合结果的最终汇聚处。在文中,只考虑网络中只有一个QS节点的情况。中间融合节点负责向下传递查询请求,并在融合过程中融合从子节点接收的数据和自身采集的数据,再向上传递给其父

节点。叶子节点只负责采集数据并传递给其父节点。

2.2 数据融合

定义数据融合函数为 $y(t) = f(d_1(t), d_2(t), d_3(t), \dots, d_N(t))$, $d_i(t)$ 表示节点 i 在 t 时刻采集到的数据, 数据融合示意如图 1 所示。

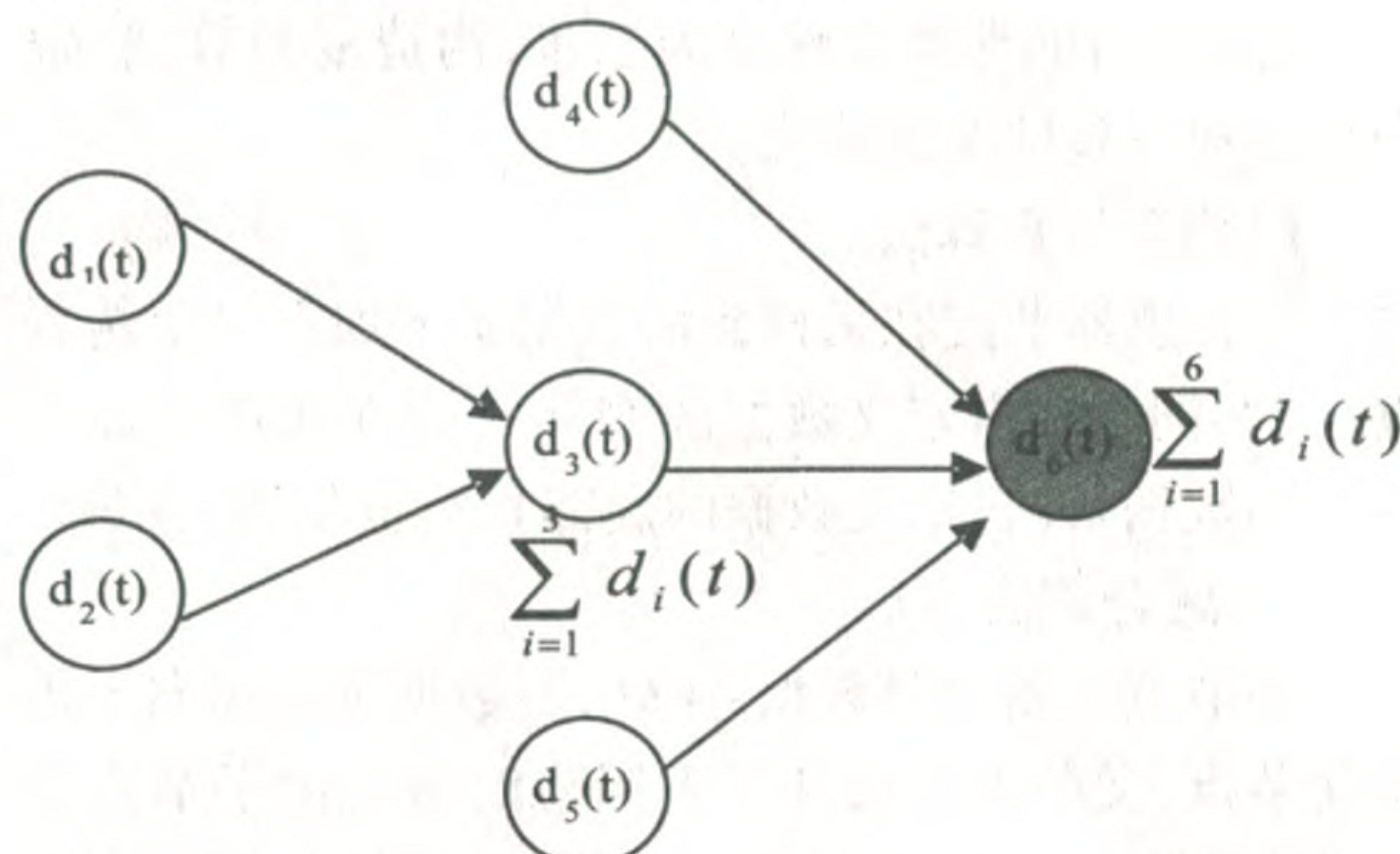


图 1 数据融合 SUM 函数示意图

由于许多典型的数据融合函数, 如 count、average、max、min 等都可以化简为 sum 函数, 因此文中以 sum 函数为研究对象, 记 $y(t) = \sum_{i=1}^N d_i(t)$ 。

2.3 算法实现与阐述

CBIPDA 算法模型先以 TAG 算法建立融合树, 在收集信息过程中, 将节点数据由实数域扩展到复数域。设传感器节点采集到的真实数据为 a , 扩展得到的复数数据模型公式如下:

$$R = s + bi = a + a' + b * i;$$

其中, 实数部分 a' 由系统 MD 装置为每一节点分发, 用于数据隐私保护; 虚数部分 b 用于完整性验证, 且 $b = k * a$ 。 k 是某一特定查询任务中整棵融合树中节点共享的一个全局变量, 其数值在下一次查询中随机改变。CBIPDA 算法数据模型的特点是将虚数部分与实数部分相关联, 通过取节点采集到的真实数据的 k 倍构成虚部中的 b , 在 QS 节点的融合结果中进行算术运算, 比较采集数据的和是否与 b 的和依然成 k 倍关系。无论将数据模型中的虚实部都篡改, 还是只篡改其中一部分, 对于最终的融合结果而言, k 倍关系必然被破坏, 所以, 文中算法可以实现数据融合中完整性的鉴别。

文中方案的核心算法与阐述如下:

(1) 节点初始化。

Sense a // 节点 a

Mask(a, a') // a' 是 real seed, 用于隐藏真实数据

$s = a + a'$; // 实数域部分数据

GetCmpxNum(s, b) // 虚部 b

$R_i = s + bi = a + a' + b * i$; // 其中, $b = k * a$, k 是一次查询任务中整棵融合树共享的一个重要的全局变

量

$C_j = E_k(R_i)$; // 数据加密

Transmit(C_j);

(2) 数据融合。

Drc(C_j) // 解密数据

Add()

$R' = R_1 + R_2$;

$C_r = E_k(R')$; // 数据加密

Transmit(C_r);

(3) 计算 SUM 的值。

receive(C_n) // QS 处数据接收

for all C_n

drc($(K, (C_i))$)

add()

$SUM^2 = R_1 + R_2 + \dots + R_k$ // 复数域数据融合结果

果

(4) 计算真实数据融合结果及完整性鉴别。

disjoin(SUM^2) // 分离出

实数域结果

$SUM^2 = \langle SUM^{2r}, SUM^{2im} \rangle$

$SUM^{1r} = \text{Compute}(\text{sum of real seeds of all source nodes})$

$SUM = SUM^{2r} - SUM^{1r}$ // 得到实数中的真实数据和

$SUM^{1im} = SUM * k$ // 通过真实数据和, 计算虚数部分 b 和

if $SUM^{1im} \neq SUM^{2im}$ // 数据被篡改, 完整性被破坏

reject SUM;

else

return SUM;

当 QS 接收到一个基于数据融合查询请求, 将该请求向整个传感器网络传播。每个传感器节点接收到查询请求后采集数据得到 a , 并加上一个私有实部种子 a' 得到 $s = a + a'$ 。接着, 在 s 上再加上一个私有虚部 bi 构成一个复数 $R = s + b * i$ 。在无线传感器网络的部署中, MD (Master Device) 利用与各节点之间的共享密钥给每个节点分发实部和虚部的种子。由于 MD 是非在线装置, 它分发的数据仅对当前节点和 QS 透明, 即各节点的实部、虚部的种子对外部入侵者和网络中的其余非 QS 节点是保密的。随后, 源节点加密 s 并向上传递给其父节点。父节点解密从子节点接收到的数据, 将其和自身采集到的数据进行加法运算, 得到一个中间融合结果, 父节点对该结果加密并传递给自己的父节点。这个过程层层向上重复, 得到若干个中间融合结果, 直到最终所有的中间融合结果都传递到

QS处。QS节点接收来自所有子节点传送的中间融合数据,并对其解密,对解密后的数据按复数的加法特性计算最终的融合结果 SUM^2 。将 SUM^2 分离成实数域 SUM^{2r} 和虚数域 SUM^{2im} 两部分,计算出各私有实数部种子之和 SUM^{1r} ,则可得到各节点采集数据融合结果 $SUM = SUM^{2r} - SUM^{1r}$ 。由 SUM 可计算出虚部种子融合结果应为 $SUM^{1im} = SUM * k$,比较 SUM^{2im} 和 SUM^{1im} 是否相等进行完整性鉴别,若相等,则完整性未被破坏,否则相反。

3 性能分析

在本节中主要从数据通信开销及完整性鉴别两个方面分析CBIPDA的性能。在无线传感器网络数据融合完整性鉴别方案中,目前较典型的有iPDA和文献[3]算法,将这两种算法作为CBIPDA算法性能的分析对比项。使用TOSSIM^[14]进行仿真,具体的网络环境配置为:600个节点随机分布于400m×400m区域中,无线信道对称,标准室内环境,背景噪声为-105.0dBm,高斯白噪声为4dB,节点的数据传输速率为1Mbps,节点的灵敏度为-108.0dBm,节点的传输距离为50m。

3.1 通信开销

对于TAG算法的通信开销,衡量的是网络节点在一次建树和融合的过程中发送的数据包个数的总和。下述比较的各算法,其建树过程都基于TAG算法,对于同等规模和范围的无线传感器网络,各算法建树时数据通信开销相等。因此,下述数据通信开销的比较只讨论建树之后的过程。其中,TAG算法数据通信开销为 $O(N)$ (N 表示无线传感器网络中节点的数量)。下面对iPDA、文献[3]算法和文中算法分别进行理论和仿真分析。

1) iPDA。

根据文献[1],该算法为实现可靠的隐私保护,至少取分片数 $L=2$ 。又因为它构造了两棵不相交的融合树,其中每棵融合树中的每个节点需要传送 $L-1+L$ 个分片,即需要 $2L-1$ 个消息用于传送数据分片,另需一个消息用于传送重组后的数据,所以该算法的数据通信开销为 $O(2LN)$,因 $L=2$,数据通信开销为 $O(4N)$ 。

2) 文献[3]算法。

该算法对节点采集的数据分配伪数据,用以隐藏节点的真实数据,实现信息的隐私保护。节点无需对数据进行分片和串通,只需要在融合之前构造出自身复数形式的数据即可。在数据融合阶段,该算法基于TAG算法按照同样的机制进行融合,所以建树后数据通信开销与TAG算法相同,为 $O(N)$ 。

3) CBIPDA。

本算法通过增添私有种子对节点采集数据进行隐私保护,同时使虚部的实数与采集到的真实数据成 k 倍比例关系,实现对信息的完整性保护。在融合阶段之前,它同样无需对数据进行分片和串通,在数据融合阶段中,它基于TAG算法按照同样的机制进行融合,所以建树后数据通信开销与TAG算法相同,为 $O(N)$ 。

下面以图表的形式对上述3种算法的通信开销进行对比,见图2。

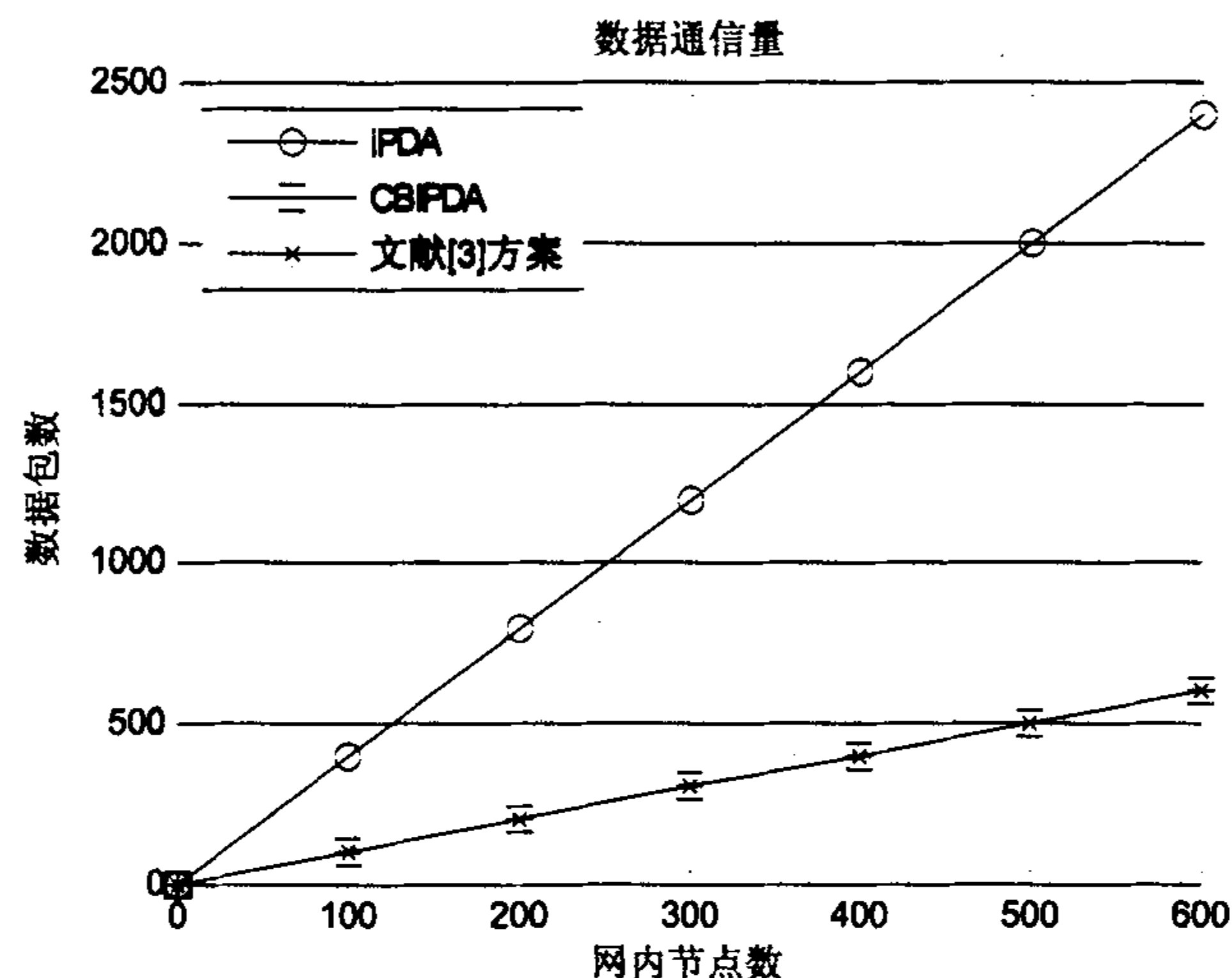


图2 iPDA、文献[5]方案及CBIPDA通信开销对比

图2说明了iPDA、文献[3]算法及CBIPDA算法的通信开销与无线传感器网络中节点数目之间的关系,三种算法的通信开销都随着节点的增加而增加,并且在节点数目相同时,iPDA的通信开销是其余两算法的四倍,与理论分析一致。

3.2 完整性比较

对于文献[3]中的算法,当恶意节点只篡改节点数据的实数部分时,虚部不受影响,那么在QS节点处比较各节点虚部总和 SUM^{1im} 与最终融合结果的虚部 SUM^{2im} ,两者仍然相等,无法鉴别出信息完整性已被破坏。

CBIPDA算法的核心思想是使虚部数据 b 与节点采集到的真实数据 a 成 k 倍比例关系,由于各节点采集到的真实数据 a 及比例值 k 是机密的,所以恶意节点无法做到对 a 和 b 同时按 k 倍关系篡改。恶意节点一旦篡改了 $s+bi$,在QS处必定能够鉴别出来,从而实现完整性保护。

为方便分析,随机取传感器网络中的6个节点,假设其拓扑结构如图1所示且节点6为QS节点,通过举例比较文献[3]算法与CBIPDA算法完整性鉴别的性能。

表1简明清楚地显示了文献[3]算法在特定情况下不能正确地进行完整性鉴别,指出了该算法的缺陷;

表 1 文献[3]算法的完整性鉴别

Node ID	Reading ds	Real seed sr	Masked value a=ds+sr	Imaginary seed bi	Complex number (a+bi)	Query Server(N6)		
						SUM ^{2im}	SUM ^{lim}	SUM ^{2im} ,SUM ^{lim} 是否相等
1	21	539	560	230i	560+230i	1814i	1814i	相等，完整性未被破坏
2	30	360	390	605i	390+605i			
3	27	478	505	331i	505+331i			
4	32	708	740	450i	740+450i			
5	26	624	650	198i	650+198i			
	SUM=136	SUM ^{1r} =2709	SUM ^{2r} =2845	SUM ^{lim} =1814i	SUM ² =2845+1814i			
5'	节点 5 经恶意节点篡改后变为 5': 650+198i → 180+457i			SUM ^{lim} =1814i	SUM ² =2375+2073i	2073i	1814i	不等，完整性被破坏拒绝接收
5''	节点 5 经恶意节点篡改后变为 5'': 650+198i → 180+198i			SUM ^{lim} =1814i	SUM ² =2375+1814i	1814i	1814i	相等，完整性未被破坏
结论	i 当恶意节点对整个节点数据篡改，如 5'，完整性鉴别正确！							
	ii 当恶意节点只对实部数据篡改，如 5''，完整性鉴别出错！							

表 2 CBIPDA 算法的完整性鉴别

Node ID	Reading a	Real seed a'	Masked value s=a+a'	Imaginary seed bi (k=10,b=k*a)	Complex number (s+bi)	Query Server(N6)		
						SUM ^{2im}	SUM ^{lim} =SUM*k=(SUM ^{2r} SUM ^{1r})*k	SUM ^{2im} ,SUM ^{lim} 是否相等
1	21	539	560	210i	560+210i	1360i	(2845-2709) × 10=1360i	相等，完整性未被破坏
2	30	360	390	300i	390+300i			
3	27	478	505	270i	505+270i			
4	32	708	740	320i	740+320i			
5	26	624	650	260i	650+260i			
	SUM=136	SUM ^{1r} =2709	SUM ^{2r} =2845		SUM ² =2845+1360i			
5'	节点 5 经恶意节点篡改后变为 5': 650+260i → 730+457i				SUM ² =2925+1557i	1557i	(2925-2709) × 10=2160i	不等，完整性被破坏拒绝接收
5''	节点 5 经恶意节点篡改后变为 5'': 650+260i → 730+260i				SUM ² =2925+1360i	1360i	(2925-2709) × 10=2160i	不等，完整性被破坏拒绝接收
5'''	节点 5 经恶意节点篡改后变为 5''': 650+260i → 650+457i				SUM ² =2845+1557i	1557i	(2845-2709) × 10=1360i	不等，完整性被破坏拒绝接收
结论	i 当恶意节点对虚实部数据均篡改，如 5'，完整性鉴别正确！							
	ii 当恶意节点只对实部数据篡改，如 5''，完整性鉴别正确！							
	iii 当恶意节点只对虚部数据篡改，如 5'''，完整性鉴别正确！							

表 2 说明了文中算法在各种情况下都能够对信息的完整性进行正确地鉴别,可以提供更为可靠而优越的信息完整性鉴别方法。

4 结束语

文中提出了一种新的无线传感器网络数据融合完整性保护方案,它是对文献[3]方案的一种改进。相比于文献[3]算法,它可以在花费相等数据通信开销与相近计算开销的前提下,提供更有效更可靠的数据完整性保护,并能得到精确的数据融合结果。

表 3 显示了文中算法在隐私保护、完整性保护、通信开销等方面的性能分析结果,进一步研究可使虚部数据与采集数据之间的关系不再是单一的线性关系,可以采用非线性关系或随机模型进行数据的隐藏,增

强算法的安全性,同时,减低算法的通信与计算开销也是有意义的研究问题。

表 3 五种数据融合方案性能对比

融合算法	TAG	ESPART	文献[3]	iPDA	CBIPDA
隐私保护性	无	好	好	好	好
完整性保护	无	无	较好	好	好
通信开销	小	较大	小	非常大	小
精确性	好	好	好	较好	好
计算开销	小	较大	较小	非常大	较小
时间效率	快	慢	快	很慢	快

参考文献:

[1] He W, Nguyen H, Liu X, et al. iPDA: an integrity-protecting private data aggregation scheme for wireless sensor networks

(下转第 158 页)

这个方法是 Menezes、Okamoto 和 Vanstone 在 1991 年提出的将 ECDLP 归约到有限域上离散对数的有效解法,称为 MOV 归约。这一方法主要用于对超奇异椭圆曲线的攻击,对其它的椭圆曲线不适应。

(2)Smart 方法。

1997 年 Smart、Sato 和 Araki 同时分别独立地提出了对素域上某一类非正规椭圆曲线的攻击方法,即 SSAS 攻击或 Smart 方法。所谓非正规椭圆曲线为有限域 F_q 上的一条椭圆曲线的阶恰好是 q 的椭圆曲线。Smart 方法对于其它类型的椭圆曲线是无效的。

4 结束语

ECC 密码体制是建立在椭圆曲线密码理论基础上的先进公钥密码体制。该系统所具有的安全性已经被全世界所承认。基于其极强的安全性 ECC 加密技术将会广泛地被应用,因此文中基于 ECC 算法的注册码软件加密保护设计方案具有一定的理论参考价值和实际应用价值。

参考文献:

- [1] 于 彬,许占文. 椭圆曲线密码体制的研究[J]. 沈阳工业大学学报,2004(5):551-554.
- [2] 徐秋亮,李大兴. 椭圆曲线密码体制[J]. 计算机研究与发

展,1999(11):1282-1288.

- [3] 黄 俊,许 娟,左洪福. 基于 RSA 算法的注册码软件加密保护[J]. 计算机应用,2005(9):2080-2085.
- [4] 张晓丰,樊启华,程红斌. 密码算法研究[J]. 计算机技术与发展,2006,16(2):179-180.
- [5] 张 雁,林 英,郝 林. 构建安全椭圆曲线密码体制的关键问题[J]. 计算机应用,2004(12):82-84.
- [6] IEEE P1363/D6(Draft Version 6). Standard Specification for Public Key Cryptography [EB/OL]. 2004. <http://grouper.ieee.org/groups/1361/P1363/draft.html>.
- [7] Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) [S]. 1998.
- [8] 户军茹,韩益亮. 椭圆曲线密码体制相关问题[J]. 通信技术,2003(12):151-152.
- [9] 王张宜,杨寒涛,张焕国. 椭圆曲线密码的安全性分析[J]. 计算机工程,2002(5):161-163.
- [10] Saeki M. Elliptic curve cryptosystems [EB/OL]. 2003-09-03. <http://cnscenter.future.co.kr/crypto/algorithm/ecc.html>.
- [11] Pohlig S, Hellman M. An Improved Algorithm of Computing Logarithms Over $GF(p)$ and Its Cryptographic Significance [J]. IEEE Trans on Information Theory, 1978(1):106-110.
- [12] 于雪燕,胡金初,柴春轶. 椭圆曲线密码体制及其参数生成的研究[J]. 计算机技术与发展,2006,16(11):160-161.

(上接第 154 页)

- [C]//Military Communications Conference. San Diego, CA: [s. n.], 2008:1-7.
- [2] He W, Liu X, Nguyen H, et al. A cluster-based protocol to enforce integrity and preserve privacy in data aggregation[C]//29th IEEE International Conference on Distributed Computing Systems Workshops. Montreal, QC: [s. n.], 2009:14-19.
- [3] Bista R, Yoo H K, Chang J W. A new sensitive data aggregation scheme for protecting integrity in wireless sensor networks [C]//10th IEEE International Conference on Computer and Information Technology. Bradford, UK: [s. n.], 2010:2463-2470.
- [4] Bista R, Jo K J, Chang J W. A new approach to secure aggregation of private data in wireless sensor networks[C]//Eighth IEEE International Conference on Dependable Autonomic and Secure Computing. Chengdu, China: [s. n.], 2009:394-399.
- [5] Bista R, Kim H D, Chang J W. A new private data aggregation scheme for wireless sensor networks[C]//10th IEEE International Conference on Computer and Information Technology. Bradford, UK: [s. n.], 2010:273-280.
- [6] 刘鑫芝. 无线传感器网络安全数据融合算法研究[J]. 计算机与现代化,2010(5):151-155.
- [7] 唐 慧,胡向东. 无线传感器网络安全数据融合算法研究[J]. 通信技术,2007(12):290-293.

- [8] 罗 蔚,胡向东. 无线传感器网络中一种高效的安全数据融合协议[J]. 重庆邮电大学学报(自然科学版),2009(1):110-114.
- [9] 覃志松,黄延磊. Zigbee 无线传感器网络安全研究及改进[J]. 微计算信息,2010(3):54-55.
- [10] 邓黎黎,刘才兴. 基于信任的无线传感器网络安全路由研究[J]. 计算机技术与发展,2010,20(6):159-162.
- [11] 魏琴芳,张双杰,胡向东,等. 基于同态 MAC 的无线传感器网络安全数据融合[J]. 传感技术学报,2011(12):1750-1755.
- [12] Madden S, Franklin M J, Hellerstein J M. TAG: a tiny aggregation service for ad-hoc sensor networks[C]//Proceedings of the 5th symposium on operating systems design and implementation. New York, USA: [s. n.], 2002:131-146.
- [13] He W, Liu X, Nguyen H, et al. PDA: privacy-preserving data aggregation in wireless sensor networks [C]//Proceedings of the 26th IEEE International Conference on Computer Communications. Anchorage, AK: [s. n.], 2007:2045-2053.
- [14] Levis P, Lee N, Welsh M, et al. TOSSIM: accurate and scalable simulation of entire TinyOS applications[C]//1st international conference on embedded networked sensor systems. Los Angeles, USA: [s. n.], 2003:126-137.

基于多项式基的非对称量子纠错码的构造

作者:

邓楠, 李雷, 赵生妹

作者单位:

邓楠,李雷(南京邮电大学理学院,江苏南京210003), 赵生妹(南京邮电大学通信与信息工程学院,江苏南京210003)

刊名:

计算机技术与发展

英文刊名:

Computer Technology and Development

年, 卷(期):

2012(8)

参考文献(14条)

1.He W:Nguyen H:Liu X iPDA:an integrity-protecting private data aggregation scheme for wireless sensor networks 2008

2.He W:Liu X:Nguyen H A cluster-based protocol to enforce integrity and preserve privacy in data aggregation 2009

3.Bista R:Yoo H K:Chang J W A new sensitive data aggregation scheme for protecting integrity in wireless sensor networks 2010

4.Bista R:Jo K J:Chang J W A new approach to secure aggregation of private data in wireless sensor networks 2009

5.Bista R:Kin H D:Chang J W A new private data aggregation scheme for wireless sensor networks 2010

6.刘鑫芝 无线传感器网络安全数据融合算法研究 2010(05)

7.唐慧;胡向东 无线传感器网络安全数据融合算法研究[期刊论文]-通信技术 2007(12)

8.罗蔚;胡向东 无线传感器网络中一种高效的安全数据融合协议[期刊论文]-重庆邮电大学学报(自然科学版) 2009(01)

9.覃志松;黄延磊 Zigbee无线传感器网络安全研究及改进 2010(03)

10.邓黎黎;刘才兴 基于信任的无线传感器网络安全路由研究[期刊论文]-计算机技术与发展 2010(06)

11.魏琴芳;张双杰;胡向东 基于同志MAC的无线传感器网络安全数据融合[期刊论文]-传感技术学报 2011(12)

12.Madden S:Franklin M J:Hellerstein J W TMG:a tiny aggregation service for ad-hoc sensor networks 2002

13.He W:Liu X:Nguyen H PDA:privacy-preserving data aggregation in wireless sensor networks 2007

14.Lewis P:Lee N:Welsh M TOSSIM:accurate and scalable simulation of entire TinyOS applications 2003

本文链接: http://d.g.wanfangdata.com.cn/Periodical_wjfx201208039.aspx