GIS 中偏向性数据加密和保护方法研究

崔阿军 王晓明
(兰州理工大学电气工程与信息工程学院 兰州 730050)

摘 要 针对 GIS 系统中数据庞大、分类繁多和复杂多变的特点,提出一种偏向性数据加密和保护方法,阐述了数据偏向性保护的必要性和可行性,该方法对不同的应用,按照重点和倾向性保护的原则对数据进行分类,对不同的类别执行不同的数据保护方法,同时在分析传统加密算法的基础上,描述了一种通用性的加密方法。试验结果表明,该方法有效提高了 GIS 中数据加解密的效率。

关键词 GIS 系统,偏向性,加密,保护,柔性
中图法分类号 TP309 **文献标识码** A

Research of Bias Data Encryption and Protection Methods for GIS

CUI A-jun WANG Xiao-ming
(College of Electronical and Information Engineering, Lanzhou University of Technology, Lanzhou 730050, China)

Abstract Aiming at the problems that there has large, diverse and complex data in the GIS system, a bias data encryption and protection method for GIS was researched, proving it is necessary and feasible to protect data bias. The data are classified according to key and bias data protection, and different data are protected in different way. Meanwhile, a universal encryption method was discussed based on traditional method. Experiment shows that, to some extent, this solution reduces the spend of encryption and decryption.

Keywords GIS system, Bias, Encryption, Protection, Flexible

1 前言

随着信息技术的高速发展,要求信息系统全方位支撑企业发展的思想已经贯彻到了每个企业的理念中,地理信息系统(Geographic Information System,GIS)作为实时监控、动态传输、管理、分析地理及需求信息的服务软件,在能源、国防、规划等方面得到了广泛的应用,并逐步向大众化普及。

数据作为软件服务的核心内容,是软件存在的根本原因,通信技术的高速发展为数据的传输创造了条件,也对数据的安全性要求提出了更高的挑战。GIS 中的数据包括影像数据、矢量数据、元数据和各种应用数据,数据分类繁多,复杂多变,个性化要求多,如果使用单一的加密算法对所有的数据进行加解密,会极大地降低数据的保护效率,影响 GIS 的可用性,如何在保证安全性的基础上,优化数据的加密和保护方法是目前急需解决的问题。

传统的对称加密算法和非对称加密算法用于 GIS 数据的加密是普遍使用的加密手段,为了改进这种加密方法,文献[1]提出了一种地图数据网络分发的混合加密算法,该算法在一定程度上提高了数据的加密效率,但是没有对数据进行针对性的分类,使得数据保护失去了重点,该方法对于数据量比较小的应用是有效的,对于大型的应用效果不是很明显。文献[2]提出了在 GIS 空间数据中影藏标识数据生产单位版权以及用户使用权属的数字水印,但并没有对 GIS 庞大的数据加密和保护提出解决方法。针对这种缺陷,提出了一种 GIS 数据的偏向性加密和保护方法,在论述数据偏向性保护的同时,说明了一种柔性的加密算法,在保证数据安全性的基础上,提高数据的加密和保护效率。

2 基本概念和加密模型

一个加密系统的完整模型如图 1 所示[3]。

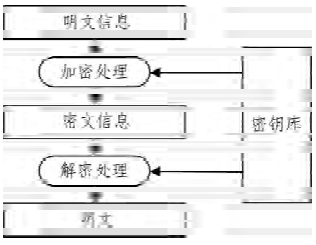

图 1 数据加密模型

加密是对数据的一种最基本的保护方式,也是确保主体安全的最低要求,让授权的人读懂承载信息的数据,是一般意义上的加密,严格的加解密定义是按照一定的算法规则,利用加密密钥,把明文(plain text)的信息或者数据转化为看似无规则的密文(cipher text),由接收方再利用解密密钥把密文还原成明文的过程。一个完整的加密系统 M 可以用数学符号

本文受甘肃省科技支撑计划(2009GS03448)资助。
崔阿军(1979-),男,博士生,主要研究方向为计算机技术、系统工程等,E-mail:3060074560@qq.com;王晓明(1954-),男,教授,主要研究方向为自动化控制、系统工程、计算机技术。

描述为：$M=\{L,A,J,S,N\}$。其中 L 表示明文空间，是由明文组成的集合；A 表示密文空间，是由密文组成的集合；J 表示密钥空间，是由加密规则中的参数组成的集合；S 表示加密算法，是由规则和公式组成的集合；N 表示解密算法，是由与 S 有关系的规则组成的集合。

3 数据加密算法

3.1 对称加密体制

对称加密是传统的密码算法，这种算法应用较早，技术相对成熟，如果用 K_j 表示加密密钥，用 K_n 表示解密密钥，在对称加密算法中 $K_j=K_n$，加密过程中，数据发送方将加密密钥和明文结合在一起经过加密算法计算后，将其变换为看似混乱的密文，接受者必须使用加密时使用的密钥和加密的相逆算法对其解密得到明文。该算法应用效率高、运算速度快，但由于数据发送方和接收方都知道密钥，而且密钥和数据一起传输，安全性保障不足。

如果有 n 对主体之间需要独立数据传输，使用对称加密算法时就需要 n 个不相同的密钥，当主体的通信量增加时，通信双方所管理的密钥数量就会呈几何级数增长，密钥的管理将会花费巨大开销。代表性的对称加密算法有 DES[4] 和 3DES 等。

3.2 非对称加密体制

非对称加密算法中 $K_j\neq K_n$，该算法需要公开密钥和私有密钥两个密钥来完成加解密过程，所以也称公开私钥加密算法，如果数据发送方用公开密钥加密，则接收方必须用对应的私有密钥才能解密，而如果用私有密钥加密的话，则必须用对应的公开密钥才能解密。假设 A 是数据发送方，B 是数据接收方，非对称加密算法工作过程如下：

①B 生成一对密钥 K_g 和 K_p，其中 K_g 是公开密钥，对外界公开，K_p 是私有密钥，不对外公开。

②A 使用 K_g 对所要传输的数据 D_t 进行加密，生成密文 D_p。$D_t\xrightarrow{Asy(RSA)}D_p$。

③B 使用 K_p 对密文 D_p 进行解密，生成明文 D_t。

$D_p\xrightarrow{Asy(RSA)}D_t$。

非对称加密算法本身复杂，所以导致加密速度没有对称加密算法速度快，安全性依赖于算法。对称加密算法中只有一种非公开的密钥，如果要解密就得让对方知道密钥，而非对称性加密算法有两种密钥，解密只需要知道一种密钥，就没必要传输密钥，安全性得到了保障。非对称加密算法适合加密小规模数据，一般在数字签名等应用中较多。其代表算法有 RSA[5] 和 Elgamal。

4 GIS 中偏向性数据加密

4.1 偏向性数据加密和保护

当 GIS 空间系统为大型企业服务时，势必会有巨大的数据需要传输，这些数据不仅包括地图元数据和数据库数据，而且包括各种各样的应用数据，这些应用数据是 GIS 空间软件存在的核心，也是提供服务的必要元素。对于这些庞大的数据，GIS 不仅要提取、存储、分析、处理、传输，还要对这些重要的数据进行加密，如果对所有的数据使用相同的加密方法，无疑会失去重点，降低了整个应用的效率，甚至失去了 GIS 服务的目的。

GIS 中的数据一般分为两类，用集合描述为 $S=\{u,v\}$，其中 u 表示需要加密的数据，v 表示一般数据，即不需要加密的数据，则 $S\sim B(n,p)$ [6]。

$$P\{X=k\}=C_n^k p^k(1-p)^{n-k} \tag{1}$$

性质 1 $S\sim B(n,p)$，则当 $k=[(n+1)p]$ 时（$[\cdots]$ 取整数），p_k 取得最大值；若 $(n+1)p$ 为整数，则 $p_k=p_{k-1}$ 同为最大值。

故必存在 k_0。

(1) $(n+1)p-1<k_0(n+1)p$，即 $k_0=[(n+1)p]$，当 $k<k_0$ 时，$p_{k-1}<p_k$，当 $k>k_0$ 时，$p_k>p_{k+1}$，所以 p_{k_0} 为极大值。

(2) $k_0=(n+1)p$，为整数时，$p_{k_0}=p_{k_0-1}$ 同为极大值。

性质 2 当 n 足够大，分布的偏度就比较小，在此情况下，$B(n,p)$ 的近似是正态分布：$N(np,np(1-p))$。

性质 3 当试验的次数趋于无穷大，而乘积 np 固定时，二项分布收敛于泊松分布。

$$P(X=k)=\frac{e^{-\lambda}\lambda^k}{k!} \tag{2}$$

GIS 中的数据由 u 和 v 组成，v 是不需要加密的数据，这类数据一般是 GIS 系统中的元数据，元数据所占容量肯定不为零，对这些数据的加密是需要代价而且不必要的，偏向性加密是对 u 的加密，并且在加密过程中选择合适的加密算法，保证加密的性价比。

普通的数据保护方法没有抓住重点数据，偏向性的数据加密和保护方法旨在保证数据安全性和可用性的基础上，提高 GIS 服务的效率。

4.2 加密方法

在众多的加密算法中，选取合适的算法对 GIS 中的数据进行加密，既保证数据的安全性，又不影响服务效率，是必须考虑的问题。

DES、3DES、RC2、RC4、IDEA（International Data Encryption Algorithm）、RSA 等都是目前常用的加密算法，GIS 的数据包括地图数据、文本数据、元数据和应用数据等，要实现偏向性数据加密和保护，使用一种加密算法是不现实的，鉴于 GIS 中数据的这种特点，本文提出用通用性加密算法来完成对数据的加密。

针对对称加密算法适合处理庞大数据、效率高的特点，GIS 中的海量应用数据选用该算法进行加密，同时考虑到不同的数据需要不同的保护级别，对安全级别要求不同的数据配以密钥长度不同的加密方法。而对 GIS 中的认证数据、验证数据、授权数据和其他重要数据，采用非对称加密算法进行加密，充分发挥了其安全性高的优势，并且不会成为影响整个数据偏向性保护效率的瓶颈。

设 $A=\{M,N,I\}$ 表示要偏向性保护的数据集合，其中 M 和 N 分别表示要偏向性加密的数据，I 表示不需要加密的数据，工作流程如下：

$$\mathrm{Ch1}:M_p\xrightarrow{Asy(RSA),Sing(DSA)}M_t$$

$$\mathrm{Ch2}:N_p\xrightarrow{Sym(DES),Sym(3DES)}N_t$$

$$\mathrm{Mes}:F=\xi(M_t,N_t,I)$$

最后的数据经过了多次处理，对于不同的应用环境和要求，赋予不同的处理方法，可以在上面 Mes 中体现，这样就提高了偏向性加密方法的通用性。

5 GIS 中数据偏向性保护实例分析

电网 GIS 平台作为提供电网资源空间信息管理及电网空间信息服务的企业级公共信息服务平台，是 GIS 系统的具体应用之一，电网 GIS 涉及的地理范围广阔，功能强大，该平台提供图形浏览、查询定位、矢量图形、电网专题图、空间分析、电网拓扑分析、瓦片地图、电网基础等服务。对认证、发电、输电、变电、配电、用电数据采用偏向性数据加密方法来保护，分析方法的效率如表 1 所列。

表 1　偏向性数据加密效率分析

数据类型	加密算法	时间/s
认证	RSA	20
输电	DES	32
变电	DES	39
配电	3DES	76
用电	AES256	45
总体数据包	DES	251

从表 2 可以看出，GIS 中数据的偏向性加解密方法所用时间明显小于传统的加解密方法，偏向性数据加密方法分类对数据处理，细化了数据类型，在加密过程中可以做到有的放矢，提高效率，并且有利于过程控制。

表 2　数据解密效率分析

数据类型	解密算法	时间/s
认证	RSA	20
输电	DES	31
变电	DES	40
配电	3DES	76
用电	AES256	48
总体数据包	DES	254

结束语　安全和高效是 GIS 提供服务的前提，GIS 的数据复杂多变，要求分门别类，为了在保证安全性的基础上，尽量提高数据处理效率，本文研究了一种偏向性数据加密方法，针对不同的应用，划分数据的分类，细化数据的流程，选择不同的加密方法，可以柔性地满足不同的要求。经过实际的应用分析，证明该方法在加密效率方面存在优势。

随着信息技术的发展和应用，人们在强调信息技术的应用的同时，更多地开始关注稳定和安全的保障，所以对数据加密的研究一直很炙手，只要有足够的时间保证，像 DES 加密算法都可以破解[7,8]，其他加密算法也一样，偏向性数据加密和保护方法在研究加密算法的同时更多地关注数据保护的技巧和方法，倡导一种模块化的数据加密和保护思想，优化数据处理流程，减少无用的数据处理。对偏向性数据保护思想在其他系统中的扩展需要继续延伸。

参 考 文 献

[1] 刘爱龙，张东，陈涛，等. 地图数据网络分发的混合加密算法[J]. 计算机工程，2008，34(18)：186-188

[2] 贾培宏，马劲松，史照良，等. GIS 空间数据水印隐藏与加密技术方法研究[J]. 武汉大学学报：信息科学版，2004，29(8)：747-751

[3] 蔡乐才. 应用密码学[M]. 北京：中国电力出版社，2005

[4] 谈娴茹. 基于 DES 和 RSA 的网络数据安全系统[J]. 中国民航学院学报，2003，21(A02)：133-136

[5] 林柏刚. 网络与信息安全教程[M]. 北京：机械工业出版社，2004

[6] 杨德保. 工科概率统计(第 3 版)[M]. 北京：北京理工大学出版社，2007

[7] 王立胜，王磊，顾训穰. 数据加密标准 DES 分析及其攻击研究[J]. 计算机工程，2003，29(13)：130-132

[8] Zadeh J A. Review of a Mathenmatical Theory of Evidence [J]. Al Magazine，1984，5(3)：81-83

(上接第 412 页)

[23] Wikipedia. Heartbleed[EB/OL]. [2014-6-14]. http://en.wikipedia.org/wiki/Heartbleed

[24] Durumeric Z, Kasten J, Adrian D, et al. The matter of Heartbleed[C]// ACM Internet Measurement Conference(IMC). 2014

[25] Momani E M H, Hudaib A A Z. Comparative Analysis of OpenSSL Vulnerabilities & Heartbleed Exploit Detection[J]. International Journal of Computer Science and Security (IJCSS), 2014, 8(4): 159

[26] Mpofu T P, Elisa N, Gati N. The Heartbleed Bug: An Open Secure Sockets Layer Vulnerability[J]. International Journal of Science and Research(IJSR). 2012, 2319(7064): 1470-1473

[27] Ye E, Yuan Y, Smith S. Web spoofing revisited: SSL and beyond [J]. Dartmouth Computer Science Technical Report, 2002, 417 (36): 1-15

[28] Adelsbach A, Gajek S, Schwenk J. Visual spoofing of SSL protected web sites and effective countermeasures[M]// Information Security Practice and Experience. Springer Berlin Heidelberg, 2005: 204-216

[29] Herzberg A, Gbara A. Protecting (even) naive Web users, or: preventing spoofing and establishing credentials of Web sites [J]. Bar Ilan University, 2004, 7(18): 1-26

[30] Felten E W, Balfanz D, Dean D, et al. Web spoofing: An internet con game[J]. Software World, 1997, 28(2): 6-8

[31] Soghoian C, Stamm S. Certified lies: Detecting and defeating government interception attacks against ssl(short paper)[M]// Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2012: 250-259

[32] Ornaghi A, Valleri M. Man in the middle attacks Demos [EB/OL]. [2014-6-14]. http://www.smarttech.ie/wp-content/uploads/2013/12/bh-us-03-ornaghi-valleri.pdf

[33] Dacosta I, Ahamad M, Traynor P. Trust no one else: Detecting MITM attacks against SSL/TLS without third-parties[M]// Computer Security-ESORICS 2012. Springer Berlin Heidelberg, 2012: 199-216

[34] Holz R, Riedmaier T, Kammenhuber N, et al. X.509 Forensics: Detecting and Localising the SSL/TLS Men-in-the-middle[M]// Computer Security-ESORICS 2012. Springer Berlin Heidelberg, 2012: 217-234

[35] Alicherry M, Keromytis A D. Doublecheck: Multi-path verification against man-in-the-middle attacks[C]// IEEE Symposium on Computers and Communications(ISCC 2009). IEEE, 2009: 557-563