基于秘密共享协议的移动数据存储研究

冉 娟 李晓宇

(郑州大学信息工程学院 郑州 450001)

摘 要 针对移动数据库各方面的资源和能力均受到限制的问题,提出了基于秘密共享协议的移动数据存储方案。在移动客户端的应用程序上采用轻量级内存数据库仅存储少量数据,将大部分移动客户端所需数据存储在数据库服务器上。对存储在数据加密服务器上的敏感数据利用AES加密,对密钥利用秘密共享技术进行拆分后存储在不同的数据存储服务器上,使除了移动客户端的任何一方都不能同时拥有密钥和密文,减轻了移动客户端的存储压力,实现了数据控制权限的分离,保证了移动客户端对数据的访问具有最高权限,提高了数据的安全性。测试实验结果表明,该方案是可行的,具有较好的性能和应用前景。

关键词 移动计算,数据存储,数据安全,秘密共享协议,AES

中图法分类号 TP309.2 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.4.029

Mobile Data Storage Solution Based on Secret Sharing Protocol

RAN Juan LI Xiao-yu

(School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract Taking into account the limited resource and capability for mobile database, a mobile data storage solution based on secret sharing protocol was proposed. Lightweight main memory database is used in application to store a small amount of data. Then, the most data of the mobile client are stored in the database server. Sensitive data are stored on the data encryption server by using AES encrypting, and secret key is split by secret sharing technology and stored in different data storage servers, which guarantees that only the mobile client can get both the secret key and the cipher text, reducing the storage pressure of mobile client. The solution achieves the separation of data control permissions, ensuring the mobile client access to data with the hightest authority, improving the security of the data. The experiment results show that the solution is feasible with good performance and has good application prospects.

Keywords Mobile computing, Data storage, Data security, Secret sharing protocol, AES

1 引言

无线通信技术、移动计算技术的提高以及移动互联网的迅速发展和智能移动客户端的普及,使得人们随时随地可以获得互联网上的丰富信息。人们越来越依赖移动客户端来方便自己的生活。2014年7月发布的中国互联网络发展状况统计报告指出,截止2014年6月我国网民使用的上网设备中手机的使用率达83.4%,首次超过传统PC(Personal Computer)的使用率(80.9%)。网民通过移动客户端在电子商务类、休闲娱乐类、信息获取类等应用的使用率都在快速增长[1]。然而,网络安全一直令人担忧,近年,互联网金融蓬勃发展,但常有媒体报道多家P2P平台遭黑客攻击造成系统瘫痪、数据恶意篡改等。移动数据库的数据安全面临着严峻挑战。所谓移动数据库[2,3],是指支持在移动计算环境中工作的分布式数据库,具有分布式数据库的诸多优点和特性。移动数据库经常应用在车载设备、个人数字助理、掌上电脑、手机等移动智能设备中,所以移动数据库又通常可以称为嵌入式移动数据库[4]。本文针对移动计算环境中移动设备的资源有限、系统的安全性和可靠性较差等一系列问题,提出了一种基于秘密共享协议的移动存储方案,用于解决移动客户端的应用程序的数据安全存储问题。该方案采用基于MD5(Message Digest Algorithm 5)的算法来提供消息的完整性保护;对所有服务器和移动客户端都加入一个公开密钥系统,它们彼此的通信都是加密的,黑客即使监听到了也无法解密;使用AES对存储在服务器上的敏感数据进行加密[5];为了使移动数据库中的数据能灵活地被移动客户端使用,对移动数据库基于最小加密粒度即数据项进行加密,同时允许移动客户端对加密后的数据以不同的粒度访问;利用Shamir(k,n)门限秘密共享体制[6]对密钥进行拆分存储,根据负载均衡算法确定参与计算的服务器。该方案实现了最小特权机制,使除了移动客户端的任何一方都不能访问敏感数据,提高了移动数据的安全性。

2 预备知识

2.1 AES简介

AES[7,8]在2001年正式成为高级加密标准,又叫Rijndael

到稿日期:2015-03-20 返修日期:2015-06-20 本文受国家自然科学基金资助项目(61472412),河南省教育厅自然科学基金(14A520012)资助。

冉 娟(1989-),女,硕士生,主要研究方向为移动计算,E-mail:ieranjuan@163.com;李晓宇(1974-),男,博士,副教授,主要研究方向为移动计算、量子计算与量子信息。

加密法，是一种对称分组密码算法，代替了已经不安全的 DES (Data Encryption Standard)和慢速的 3DES(Triple-DES)，已经被多方分析且广为全世界所使用。AES 是一个迭代的、对称密钥分组的密码，它可以使用 128、192 和 256 位密钥，并且用 128 位(16 字节)分组加密和解密数据。与公共密钥密码使用密钥对不同，对称密钥密码使用相同的密钥加密和解密数据。通过分组密码返回的加密数据的位数与输入数据相同。迭代加密使用一个循环结构，在该循环中重复置换和替换输入数据。

2.2 秘密共享协议简介

秘密共享协议是一种把秘密分割存储的密码技术，可以达到阻止秘密过于集中、分散风险和容忍入侵的目的，是保证信息安全和数据保密的重要方法[9]。Shamir(k,n)门限方案是由密码学家 Shamir 提出的一种基于拉格朗日插值公式法的(k,n)门限秘密共享方案，它是最具代表性和被广泛应用的秘密共享方案。所谓(k,n)门限秘密共享协议，就是秘密 S 通过秘密共享协议被 n 个参与者所共同持有，每一个参与者只获得一个秘密份额且满足两个条件：第一，任意不少于 k 个的参与者通过自己所持有的秘密份额合作可以重构出秘密；第二，任意少于 k 个的参与者合作都无法重构出秘密。

最早的最小特权原则由 Saltzer 提出，它要求系统中每个用户或进程仅拥有执行其授权任务所必需的最小特权集而不是拥有所有特权。秘密共享协议把秘密进行分割存储，使持有者具有必不可少的特权以能够将秘密进行恢复，同时也限制了每个持有者能进行的操作。

2.3 AES 和 Shamir(k,n)秘密共享协议的结合

AES 虽然从众多加密算法中脱颖而出，但其安全性是相对的，并不是绝对的。AES 算法的有效性是通过密钥和明文的变换来保证的，其加密过程与解密过程使用一样的密钥并且是互逆的，这就给密钥的管理带来了挑战[10,11]。因此该算法中一个非常关键的问题就是如何来保证密钥的安全性和完整性，而这恰是 Shamir(k,n)门限秘密共享体制所要研究的问题。从前面的介绍可以看出，二者的结合一方面能保持 AES 加密算法良好的保密性，另一方面也能发挥了 Shamir (k,n)秘密共享协议共享秘密的优势。

3 基本思想

由于移动客户端的用户一般持有手机、Pad、笔记本等智能微终端设备，它们的电池容量在连续使用的情况下一般只能支持 3 到 5 个小时，对于计算密集型的程序其耗能会更大，并且其计算能力也是有限的[12,13]。因此，大量的计算、存储等工作将交由服务器处理，而像手机这类的移动客户端主要是提供操作窗口，并在移动客户端内置一个轻量级的内存数据库[14]。目前，轻量级内存数据库还是一个比较新的研究领域，没有权威公认的定义。事实上，这个轻量级内存数据库就相当于分布式数据库中的局部数据库。在本方案中，移动终端的这个轻量级内存数据库主要是用来存储少量基本信息，而大部分信息尤其是需要加密保护的敏感信息将存储在数据库服务器上。比如在一个用户提交个人信息的页面中，像籍贯对应的省份这些常用数据可直接从轻量级内存数据库读取；而像图片之类占内存较大、帐号密码较敏感的信息可以存储在数据库服务器上；对于比较流行的即时通讯软件，双方的交流信息大部分将存储在数据库服务器上，而移动终端仅保存最近的一些通信记录，将旧的聊天记录在一定时限后进行删除，并转移存储在服务器端。因此，基于秘密共享协议的移动存储方案比较适合应用在移动客户端的应用程序需要保存大量移动用户数据的情况。

在基于秘密共享协议的移动数据存储方案中，我们要实现的整个过程由四方参与，即移动客户端(Mobile Client)、数据加密服务器(Data Encryption Server)、数据存储服务器(Data Storage Server)以及数据恢复服务器(Data Recover Server)。在基于秘密共享协议的移动数据存储方案中，移动客户端访问服务器的示意图如图 1 所示。

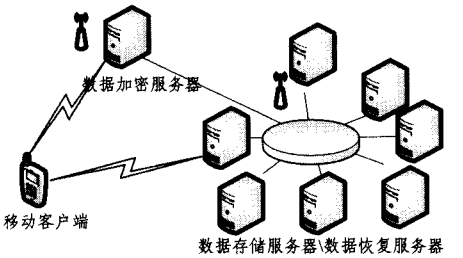

图 1 方案中移动客户端访问数据的示意图

在数据加密服务器上对合法的移动客户端提交入库的敏感数据进行 AES 加密，将密钥利用 Shamir(k,n)门限共享方案进行拆分，并把拆分后的影子密钥和加密后的密文通过安全高速的固定网络分别传送给 n 个数据存储服务器。

移动客户端访问数据时，向数据加密服务器发送请求，数据加密服务器确认是合法的移动客户端发送的请求后从数据存储服务器的 n 个服务器中随机选取 k 个参与成员，在这 k 个成员中利用负载均衡算法选择一台服务器作为数据恢复服务器，然后将 $k-1$ 份影子密钥都传送给这个数据恢复服务器，数据恢复服务器可能为 n 个数据存储服务器中的任意一台。

在数据恢复服务器上，k 份影子密钥利用 Shamir(k,n)门限共享方案进行重组，即可恢复密钥，解密经 AES 加密的移动数据库的数据，然后发送给移动客户端。移动客户端对发送方的身份进行认证后接收信息。

在整个移动客户端访问基于秘密共享协议的移动数据库中，数据加密服务器不参与文件本身的操作，主要是加密数据并处理产生的密钥。数据恢复服务器不是固定的某台服务器，而是根据负载均衡算法确定的。数据存储服务器只对数据进行物理意义上的存放。这样就实现了最小特权机制，数据的控制权限将由传统的移动客户端和数据存储服务器共享转为数据单方面对移动客户端透明。

4 基于秘密共享协议的移动数据存储方案

4.1 数据存储

实现移动数据库的数据存储的过程中，首先要选用 n 个服务器来作为数据存储服务器，所选的 n 个服务器上都有加密后的数据库的副本，这 n 个服务器是相互独立的。加密数据的服务器相当于秘密共享协议里分发秘密的角色，在这里假设它是诚实可信的，并负责把产生的密文和 n 个影子密钥分别传送到 n 个数据存储服务器上。

在 Shamir(k,n)门限秘密共享方案的秘密分发阶段，设 D 是秘密分发者并且持有要分享的主密钥 s，n 是参与者的数目，k 是门限值，q 是一个大素数($q>n$ 且 $q>s$)，$P=\{P_1,P_2,\cdots,P_n\}$是 n 个共享密钥的参与者的集合，秘密空间和秘密份额空间均为有限域 Z_p。

密钥的分发者 D 给 n 个参与者 $P_i(1\leqslant i\leqslant n)$分配份额的过程即方案的分配算法如下[6,9]：

(1)D 随机选择一个 F_p 上的 $k-1$ 次多项式：$f(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1}\in Z_p[x]$，使得 $a_0=f(0)=s$ 为要在 n 个参与者中分享的秘密，且 D 对 $f(x)$保密。

(2)D 在 F_p 中选择 n 个互不相同的非零元素 $x_1,x_2,\cdots,x_n$，计算 $s_i=f(x_i)$，$1\leqslant i\leqslant n$。

(3)将$(x_i,s_i)(1\leqslant i\leqslant n)$通过秘密信道分配给参与者 $p_i(1\leqslant i\leqslant n)$，值 x_i 是公开的，s_i 作为 p_i 的秘密份额由 p_i 保密。

(4) 密钥的分发者 D 为了安全考虑，在各秘密份额(x_i,s_i)分发结束后将密钥 s 销毁。

4.2 确定 Data Recover Service 服务器

移动客户端要使用表中的数据时，必须找到密钥和相应的密文。由于移动客户端的电量、存储能力、计算能力等方面的限制，不能考虑在客户端对数据库进行恢复，而是由指定的性能较好的服务器来进行数据的恢复。移动客户端要想确定用来恢复数据的服务器，将根据服务器负载均衡状况来选用相应的对策。

服务器负载均衡[15]是指由多台服务器以对称的方式组成一个服务器集合，每台服务器都具有等价的地位，都可以单独对外提供服务而无须其他服务器的辅助。通过某种负载分担的算法，将外部发送来的请求均匀分配到对称结构中的某一台服务器上，而接收到请求的服务器独立地回应客户的请求。

常被使用的负载均衡算法有[15,16]：

(1)轮循均衡(Round Robin)。每一次来自网络的请求轮流分配给内部中的服务器。

(2)权重轮循均衡(Weighted Round Robin)。根据服务器的不同处理能力，给每个服务器分配不同的权值，使其能够接受相应权值数的服务请求。

(3)处理能力均衡(Processing Capacity)。把服务请求分配给内部中处理负荷(根据服务器 CPU 型号、CPU 数量、内存大小及当前连接数等换算而成)最轻的服务器。

除了以上列出的负载均衡算法，还有响应速度均衡(Response Time)、最少连接数均衡(Least Connection)、DNS 响应均衡(Flash DNS)等算法，可以根据服务器的实际情况而定。本文中的测试实验考虑到内部服务器的处理能力及当前网络运行状况，采用处理能力均衡算法。

4.3 数据恢复

数据加密服务器从 n 个数据存储服务器中随机确定 k 个服务器，并使这 k 个服务器所持有的 k 份影子密钥分别传送给确定的数据恢复服务器，即可在该服务器上恢复密钥解密密文，然后安全地传送给移动客户端以供使用。

由于 $f(x)$的次数至多为 $k-1$ 次的随机多项式，系数 $a_0,a_1,\cdots,a_{k-1}$是 $Z_p[x]$中的未知元素，$a_0=s$ 是秘密。因为 $s_i=f(x_i)$，$1\leqslant i\leqslant n$，从这 n 个参与者中可以得到 k 个以 $a_0,a_1,\cdots,a_{k-1}$为未知数的线性方程。根据 Lagrange 插值公式，如果这些方程式线性独立，则存在唯一解，解出的 a_0 值即为秘密 s。

因此，任意 k 个成员提供相应的 k 个点，即可利用 Lagrange 插值公式合作计算出[9,11]：

$$f(x)=\sum_{j=1}^{k}f(i_j)\prod_{\substack{t=1\\t\neq j}}^{k}\frac{(x-i_t)}{(i_j-i_t)}$$

设 $w_j(x)=\prod_{\substack{t=1\\t\neq j}}^{k}\frac{(x-i_t)}{(i_j-i_t)}$，从而有 $s=f(0)=\sum_{j=1}^{k}s_{i_j}w_j(0)$，其中 $s_{i_j}=f(i_j)$。

5 安全性分析

基于秘密共享协议的移动数据存储方案具有以下安全性优势。

(1)数据存储位置

由于移动存储设备易丢失、易损坏，因此本方案的存储方式转移了移动存储设备的存储风险，而由抗击能力强的服务器来应对，保护了移动用户的隐私，防止移动设备丢失后数据被他人读取以及损坏后数据永久丢失。

(2)数据通信

该方案采用基于 MD5 算法的报文验签，保证了报文传输的完整性；对服务器和移动客户端之间的通信加入的公开密钥系统，避免了黑客截取报文中的敏感信息和对数据进行篡改。

(3)鲁棒性

在 n 台数据存储库服务器中，若有少数(不大于 k 台)几台服务器损坏，将不影响敏感数据的恢复，移动客户端可对数据进行正常的访问，这样就提高了存储设备的容灾性能。

(4)负载平衡性

当大量移动客户端并发访问数据时，数据的恢复与反馈工作可以分散在多台服务器上进行操作，不会因为大量移动终端同时访问一个服务器而造成服务器的性能瓶颈。

(5)数据控制权分离

实现了最小特权机制，这使得文件的控制权分离，数据恢复服务器只有在移动客户端的请求下才能获取其它数据存储服务器上存储的影子密钥，除此之外的任何一方都不能恢复原始密钥和明文。

6 实验结果与分析

该测试实验的处理器采用 Inte(R)Core(TM)i3-413@3.4GHz 3.4GHz，内存为 4GB，操作系统为 64 位 Windows7。开发平台为 Eclipse Juno，数据库服务器使用 MySQL 5.6。

该实验中，Shamir(k,n)门限方案的 k、n 均可取 0～20，AES 密钥长度采用 128 位，移动客户端个数可任意取值，负载均衡算法采用处理能力均衡策略。

图 2 的横轴为移动客户端并发访问量，纵轴为在实验中统计 500 次单个移动客户端在有多个移动客户端同时需要获取密钥时所花费的平均响应时间。图中共有 4 条曲线，分别是在 Shamir(k,n)门限共享方案(k,n)取值分别为(3,5)、(5,10)、(7,10)、(15,20)下的实验结果。从图 2 中可以看出，当移动客户端并发访问量一定时，移动客户端获取密钥的平均

访问时间会随着参与共享秘密的份额和门限值的同时增大而增加；当负责存储影子密钥的参与者一定时，移动客户端获取密钥的平均访问时间会随着门限值的增加而增加；当 Shamir (k,n) 门限共享方案值确定时，移动客户端获取密钥的平均访问时间会随着移动客户端并发访问量的增加而增加。

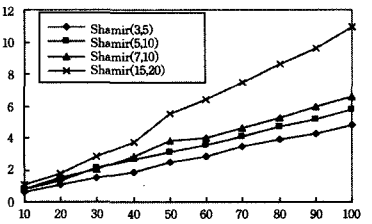

图 2　访问密钥的平均时间-移动客户端并发访问量

图 3 的横轴为移动客户端并发访问量，纵轴为在实验中获取密钥后统计的 500 次单个移动客户端在有多个移动客户端同时需要访问 AES 解密的数据所花费的平均响应时间。图 3 共有 3 条曲线，分别是在解密不同大小数据的情况下的实验结果。从图 3 中可以看出，当需要解密的数据大小相同时，AES 平均解密时间随移动客户端并发访问量的增加而增加；当访问数据的移动客户端并发量一定时，需要解密的数据越大，花费的 AES 平均解密时间越长。

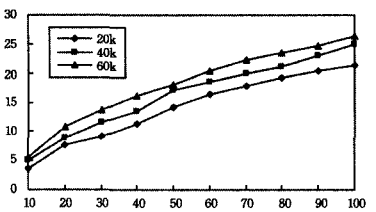

图 3　AES 平均解密时间-移动客户端并发访问量

图 4 的横轴为移动客户端并发访问量，纵轴为在实验中统计 500 次单个移动客户端在有多个移动客户端同时访问数据时所花费的平均响应时间。图 4 中有 4 条曲线，分别对应要取的数据大小为 20k 且 Shamir (k,n) 门限共享方案 (k,n) 取值分别为 $(3,5)$、$(5,10)$、$(7,10)$、$(15,20)$ 的情况。从图 4 可知，当移动客户端并发访问量一定时，移动客户端访问数据的平均时间随参与共享秘密的份额和门限值的同时增大而增加；当负责存储影子密钥的参与者一定时，移动客户端访问数据的平均时间会随着门限值的增大而增加；当 Shamir (k,n) 门限共享方案值确定时，移动客户端访问数据的平均时间会随着移动客户端的并发访问量的增加而增加，随着移动客户端并发访问量的增加，平均访问时间呈线性增长，并未出现大幅度指数上升，说明即使在移动客户端并发访问量很多的情况下该方案仍然适用，它具有较好的健壮性。

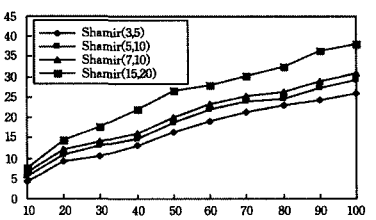

图 4　平均响应时间-移动客户端并发访问量

结束语　基于秘密共享协议的移动数据存储方案从多方面提高了移动数据的安全性。要想追求该方案更高的安全性和效率，可以再深入研究秘密共享协议、针对数据库数据的加密算法和针对服务器的负载均衡算法。另外，可以考虑利用秘密共享协议直接对移动数据库的数据进行拆分，这样，数据分散存储到各服务器中将可以减轻服务器的存储压力，更多细节问题还有待进一步研究。

参 考 文 献

[1] China internet network information center. Statistical report on the development of China Internet Network in the thirty-fourth time[R/OL]. 2014. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201407/P020140721507223212132.pdf(in Chinese)
中国互联网络信息中心. 第 34 次中国互联网络发展状况统计报告[R/OL]. 2014. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201407/P020140721507223212132.pdf

[2] Wu W W, Chen S Y. Research and Development Trend about Eembed Mobile Data Base[J]. Computer Science, 2005, 32(12): 88-90(in Chinese)
吴娓娓，陈蜀宇. 嵌入式移动数据库现状与发展趋势[J]. 计算机科学，2005，32(12)：88-90

[3] Amja A M, Obaid A, Seguin N. A Distributed Mobile Database Architecture[C]// 2011 IEEE Asia-Pacific Conference on Services Computing. 2011: 62-69

[4] Ying Y, Ren K. Research on mobile database key technologies and application[J]. Microcomputer Information, 2010, 10(2): 89-90(in Chinese)
应毅，任凯. 微终端移动数据库关键技术及其应用研究[J]. 微计算机信息，2010，10(2)：89-90

[5] Wang J D. Design and implementment of database encryption system based on advanced data encrytion standard AES[D]. Xi'an: Xidian University, 2011(in Chinese)
王劲东. 基于高级数据库加密标准 AES 的数据库加密技术研究与实现[D]. 西安：西安电子科技大学，2011

[6] Shamir A. How to Share a Secret [J]. Communication of the ACM, 1979, 22(11): 612-613

[7] Hu Z H, Tan Z P, Zhang Q. Novel Method for Impossible Differential Cryptanalysis of 9-Round AES_256 [J]. Computer Science, 2014, 41(8): 196-198(in Chinese)
胡志华，覃中平，张青. 一种新的 9 轮 AES_256 不可能差分分析[J]. 计算机科学，2014，41(8)：196-198

[8] Zhang J H, Guo X B, Fu X. AES encryption algorithm and the application in information security[J]. The Security of Information Network, 2011(5): 32-33(in Chinese)
张金辉，郭晓彪，符鑫. AES 加密算法分析及其在信息安全中的应用[J]. 信息网络安全，2011(5)：32-33

[9] Jiang L L. Research of Rational Secret Sharing Technology[D]. Harbin: Harbin Normal University, 2011(in Chinese)
江林临. 理性秘密共享技术研究[D]. 哈尔滨：哈尔滨师范大学，2011

[10] Li S Y, Shi R H. A Dynamic Secret Key Sharing Scheme[J]. Journal of Anhui University (Natural Science Edition), 2010, 34(3): 38-42(in Chinese)
李素云，石润华. 一种动态的密钥分存方案[J]. 安徽大学学报(自然科学版)，2010，34(3)：38-42

[11] Zhou Z Y, Liu S J, Wang Z Y, et al. Implementation of a Threshold Encryption Scheme[J]. Modern Computer, 2009(11): 41-44(in Chinese)
周振宇,刘少军,王子燕,等. 一种门限加密方案的实现[J]. 现代计算机(专业版),2009(11):41-44

[12] Xu M, Cao J N, Peng W. Mobile computing technology[M]. Beijing: Tsinghua University Press, 2008: 12-13(in Chinese)
徐明,曹建农,彭伟. 移动计算技术[M]. 北京:清华大学出版社,2008:12-13

[13] Pu Y Y, Pei Q J, Li H Y. Exploiting the Performance-Energy Tradeoffs for Mobile Databa[J]. Journal of Universal Computer Science, 2014, 20(20): 1488-1498

[14] Lan Li-na, Mao Jing-li, Gou Xue-rong. A Novel Lightweight Main Memory Database for Telecom Network Performance Management System[J]. Journal of Networks, 2012, 7(4): 667-674

[15] Quan Y, He M. Application and implementation of servers load balance[J]. Microcomputer Applications, 2006, 27(4): 433-435 (in Chinese)
全宇,何苗. 服务器负载均衡的应用与实现[J]. 微计算机应用,2006,27(4):433-435

[16] Cheng B. Design and Implementation of Load Balancing Scheduling System[D]. Wuhan: Huazhong University of Science and Technology, 2011(in Chinese)
程斌. 负载均衡调度系统的设计与实现[D]. 武汉:华中科技大学,2011

(上接第 117 页)

动群智网机会中继电磁兼容复杂度模型并验证了该模型的可行性。然后,在移动机会中继上通过协作组建了集群 IIR、FIR 滤波器,设计了协作电磁兼容控制算法。最后,在此基础上,基于集群滤波器提出了优化协作电磁兼容控制复杂度算法。实验结果表明,所提算法在优化协作电磁兼容机会移动中继功耗和 CPU 占用率及复杂度等方面具有良好表现,具有降低资源消耗和提高通信可靠性的能力。

参 考 文 献

[1] Zhang Xiang-ming, Zhao Zhi-hua, Guo Fei, et al. Electromagnetic Interference Analysis and Its Suppression of EMC Testing System[J]. Transactions of China Electrotechnical Society, 2010, 25(10): 14-19(in Chinese)
张向明,赵治华,郭飞,等. 电磁兼容测试系统电磁干扰问题分析与解决[J]. 电工技术学报,2010,25(10):14-19

[2] Jiang Long, Xia Guang-qiong, Wu Jia-gui, et al. Optimization Analysis on Complex Degree of Optical Chaos in a Semiconductor Laser with Double Optical Feedback[J]. Chinese Journal of Lasers, 2012, 39(12): 1-5(in Chinese)
蒋龙,夏光琼,吴加贵,等. 双光反馈半导体激光混沌高复杂度优化分析[J]. 中国激光,2012,39(12):1-5

[3] Lallechere S, Bonnet P, Paladian F. Electrical stochastic modeling of cell for bio-electromagnetic compatibility applications [J]. Annals of Telecommunications-Annales Des Telecommunications, 2014, 69(5/6): 295-308

[4] Perumalraj R, Narayanan K S. Nano silver conductive composite material for electromagnetic compatibility[J]. Journal of Reinforced Plastics and Composites, 2014, 33(11): 1000-1016

[5] Miyata S, Yamaoka K, Kinoshita H. Optimal Threshold Configuration Methods for Flow Admission Control with Cooperative Users[J]. IEICE Transactions on Communications, 2014, 97(12): 2706-2719

[6] Giannini A, Pelorossi F, Pasian M, et al. The Sardinia Radio Telescope Upgrade to Telemetry, Tracking and Command: Beam Squint and Electromagnetic Compatibility Design[J]. IEEE Antennas and Propagation Magazine, 2015, 57(1): 177-191

[7] Barzegaran M R, Nejadpak A, Mohammed O A. Physics-Based Modeling of Power Converter Drive System for Evaluation of Electromagnetic Compatibility [J]. Applied Computational Electromagnetics Society Journal, 2015, 30(6): 660-669

[8] Tian Jin, Xie Yong-jun, Xin Hong-quan, et al. A Synthetical EMC Evaluation Method for a Complicated System Based on a Novel TOPSIS Approach[J]. Acta Electronica Sinica, 2013, 41(1): 105-109(in Chinese)
田锦,谢拥军,辛红全,等. 复杂系统电磁兼容评估的改进 TOPSIS 方法[J]. 电子学报,2013,41(1):105-109

[9] Xi He-xun, Tang Guang-fu, Cao Jun-zheng, et al. Research Progress of Electromagnetic Field and Electromagnetic Compatibility of UHVDC Converter Valves[J]. Proceedings of the CSEE, 2012, 32(22): 1-7(in Chinese)
习贺勋,汤广福,曹均正,等. 特高压直流换流阀电磁场与电磁兼容研究进展[J]. 中国电机工程学报,2012,32(22):1-7

[10] Wang W, Wang D, Peng Z H. Cooperative fuzzy adaptive output feedback control for synchronisation of nonlinear multi-agent systems under directed graphs[J]. International Journal of Systems Science, 2015, 46(16): 2982-2995

[11] Feng Wen-jiang, Jiang Wei-heng, Deng Yi-na, et al. Joint power control for untrusted relay cooperation-based confidential communication[J]. Journal on Communications, 2014, 35(11): 59-80(in Chinese)
冯文江,蒋卫恒,邓艺娜,等. 基于非信任中继协作的保密通信联合功率控制[J]. 通信学报,2014,35(11):59-80

[12] Ou Jing-lan, Wu Hao-wei, Zou Yu-tao, et al. Opportunistic Two-Way Relay Selection Scheme with Outdated Channel State Information[J]. Journal of Beijing University of Posts and Telecommunications, 2014, 37(6): 44-48(in Chinese)
欧静兰,吴皓威,邹玉涛,等. 过时信道状态下机会双向中继选择算法[J]. 北京邮电大学学报,2014,37(6):44-48

[13] Jia Jian-bin, Chen Ying-wen, Xu Ming. Prediction Based Relay Selection Method in Opportunistic Vehicular Networks [J]. Journal of Software, 2015, 26(7): 1730-1741(in Chinese)
贾建斌,陈颖文,徐明. 基于预测的机会车载网络中继选择策略研究[J]. 软件学报,2015,26(7):1730-1741

[14] Liao Dai-hui, Cheng Ai-guo, Zhong Zhi-hua. Study on Optimization for Automobile Safety and Lightweight Based on Variable Complexity Approximate Model [J]. China Mechanical Engineering, 2013, 24(15): 2118-2121(in Chinese)
廖代辉,成艾国,钟志华. 基于变复杂度近似模型的汽车安全性和轻量化优化[J]. 中国机械工程,2013,24(15):2118-2121