

文章编号:1001-9081(2012)06-1609-04

doi:10.3724/SP.J.1087.2012.01609

改进的 RSA 算法在无线传感器网络中的应用

杜治国*, 胡大辉

(西南大学 信息管理系, 重庆 402460)

(*通信作者电子邮箱 du_zhiguo@hotmail.com)

摘要:针对公钥密码体制在无线传感器网络密钥管理中存在计算速度慢、能量消耗大等问题,提出将一种改进的公钥算法应用其中。新算法利用蒙哥马利算法把大数的幂模运算转换成模幂运算,并使用中国剩余定理把模幂运算转换成求解同余方程组。算法安全性分析与实验结果表明,新算法能减少 55% 的运算开销,减少 67% 的存储空间占用,并增加 21% 的节点生命周期。新算法在保证密钥安全性的同时减少了运算量和存储空间,更加适合节点运算能力较低且能量有限的无线传感器网络。

关键词:无线传感器网络; 公钥密码; 中国剩余定理; 蒙哥马利算法

中图分类号: TP393.08 **文献标志码:**A

Application of improved RSA algorithm in wireless sensor network

DU Zhi-guo*, HU Da-hui

(Department of Information Management, Southwest University, Chongqing 402460, China)

Abstract: In order to solve the problems such as slow calculation and great energy consumption caused by the public-key-cryptosystem-based key management in wireless sensor network, an improved RSA public-key algorithm was suggested in this paper. In the new algorithm, Montgomery algorithm had been applied to transform large number's modular exponentiation to exponentiation modular. At the same time, the Chinese Remainder Theorem (CRT) was also employed to change modular exponentiation to congruence equations. The security analysis and experimental results show that the computation expenditure has been reduced by 55 percent, the storage space reduced by 67 percent and the life cycle of nodes increased by 21 percent in the new algorithm. The new algorithm provides better safety of the key as well as less computation and smaller storage space, which is more suitable for the wireless sensor network with low computation ability and limited energy.

Key words: Wireless Sensor Network (WSN); Public Key Cryptosystem (PKC); Chinese Remainder Theorem (CRT); Montgomery algorithm

0 引言

随着传感器技术、通信技术、微电机技术和计算机技术的发展,无线传感器网络(Wireless Sensor Network, WSN)的应用范围越来越广,通过人为的随机布置,数量巨大的传感器节点集中在需要监控的区域中,利用自带的数据处理和数据通信功能把节点连接成一个自组织网络。通过一些其他的网络设备(例如网关),无线传感器网络还可以连接在现有的局域网(Local Area Network, LAN)甚至 Internet 中,方便远程终端用户实时监测环境数据^[1]。

无线传感器网络主要应用在军事和商业等领域,对采集的数据有较高的安全要求^[2],数据传输过程和节点的分布都不能被未授权的用户轻易获取,因此无线传感器网络的安全性是重要的研究内容。

在无线传感器网络中,由于节点的计算能力较弱、电源能力有限、存储空间较小、通信能力较低以及网络的拓扑结构动态变化等特点,使之与传统的计算机网络有较大的差异。传统网络终端的处理器功能较强且有持续电源供应,可以使用比较复杂的加密算法来保证数据和通信的安全性,公钥算法是典型的代表。但传统的公钥算法运算量大,不适合在传感

器节点中应用,本文使用改进的公钥算法,减少运算量,降低处理器的时间复杂度和空间复杂度,使之能在无线传感器节点中使用。

1 应用现状

1.1 理想的 WSN 密钥加密算法

从无线传感器网络的自身特性出发,一个好的密钥算法必须符合下列几个原则^[3]:

1) 占用较小的存储空间。传感器节点计算能量有限,存储容量较小,常用的加密算法因算法的空间复杂度较高而不能直接使用。

2) 较少的运算量。传感器节点的电源能量有限,不能随时更换电源,少量的运算可以减少处理器的耗能时间,节约电源能量。

3) 较小的通信开销。无线传感器网络因为节点电源能量有限,其通信是低速、低功耗的传输,不能持续传输大量数据。

4) 算法易于实现。传感器节点要完成数据采集、处理机传输等多项功能,由于节点计算能力的限制、寄存器位数的影响等,要求加密算法必须能在硬件功能较弱的情况下实现。

收稿日期:2012-01-10;修回日期:2012-02-29。

基金项目:国家自然科学基金资助项目(21007051);西南大学青年基金资助项目(2010RCQ003)。

作者简介:杜治国(1977-),男,四川仪陇人,讲师,硕士,CCF 会员,主要研究方向:计算机网络安全、无线传感器网络;胡大辉(1977-),女,重庆人,讲师,硕士,主要研究方向:信息安全、密码学。

5) 算法安全性必须保证。传感器节点可能存在“被俘”的情况,因此要求算法不仅能保证数据的安全,还要求其中某个节点的“被俘”不影响整个网络的正常工作。

1.2 常见加密算法

1) RC5/RC6 分组加密算法^[4]。该算法是一种对称的快速加密算法,在 1994 年由马萨诸塞技术研究所的 Rivest 教授提出,算法使用异或、加和循环三种初等运算来完成加解密过程,具有运算速度快、存储空间占用较少等优点,但在工作时需要传输的数据量较大,节点的通信开销较高。

2) 公钥加密算法^[5]。Rivest、Shamir 和 Adleman 在 1976 年创建了公钥加密算法——RSA 算法。RSA 算法是密码学中的一个重要里程碑,从基本原理上改变了加密和解密的过程。RSA 算法的安全性主要依赖于大数分解的难度,模数的位数越长,破解的可能性就越小。目前的实际应用过程中,模数的长度一般大于 1024 位。

3) 椭圆曲线加密^[6]。该算法是基于椭圆曲线数学的一种公钥密码的方法,于 1985 年由 Neal Koblitz 和 Victor Miller 分别独立提出。算法的安全性依赖于解决椭圆曲线离散对数问题的困难性,其优势在于能够使用更小的密钥和定义群之间的双线性映射,但其加解密运算的实现比其他算法耗时更多。

2 RSA 算法及其改进

2.1 RSA 算法^[7]

Rivest、Shamir 和 Adleman 在 RSA 算法中提出了使用乘方运算,明文以分组为单位进行加密,每个分组的二进制值均小于 n 。在实际的应用中,分组的大小是 i 位,其中 $2^i < n \leq 2^{i+1}$ 。

RSA 算法中密钥产生的具体步骤如下:

- 1) 选择两个素数 p 和 q , p 和 q 等长但 p 不等于 q ;
 - 2) 计算 $n = p \times q$;
 - 3) 计算 $\Phi(n) = (p - 1) \times (q - 1)$;
 - 4) 选择整数 e , 使得 $0 < e < \Phi(n)$ 且 $\gcd(e, \Phi(n)) = 1$;
 - 5) 计算 $d, d \equiv e^{-1} \pmod{\Phi(n)}$;
 - 6) 得到公共密钥 P_u 和私有密钥 $P_r, P_u = \{e, n\}, P_r = \{d, n\}$;
 - 7) 加密时计算密文 $C: C = M^e \pmod{n}$
 - 8) 解密时计算明文 M :
- $$M = C^d \pmod{n} = (M^e)^d \pmod{n} = M^{ed} \pmod{n}$$

RSA 算法虽然安全可靠,但是运算量巨大,需要处理器具有较强的运算能力、较大的存储器空间以及持续稳定的电源能量。无线传感器网络节点处理器的运算能力较弱、节点能量有限且存储空间较小,不能直接使用 RSA 算法,必须做一定的改进。本文提出把中国剩余定理和蒙哥马利算法运用于加解密运算过程中,加快运算速度,减少运算量,使之能适应无线传感器网络的具体使用环境。

2.2 预备定理

费马小定理^[8] 若 p 是素数, a 是正整数且不能被 p 整除, 则 $a^{p-1} \equiv 1 \pmod{p}$, 或写作: $a^p \equiv a \pmod{p}$, 其中 p 是素数且 a 是任意正整数。

欧拉定理^[9] 对于任意互素的 a 和 n , 有 $a^{\varphi(n)} \equiv 1 \pmod{n}$ 。其中, $\varphi(n)$ 称为欧拉函数, 表示小于 n 且与 n 互素的正整数个数, 本定理也可写作: $a^{\varphi(n)+1} \equiv a \pmod{n}$ 。

中国剩余定理^[10] 令 r 个整数 m_1, m_2, \dots, m_r 两两互素, a_1, a_2, \dots, a_r 是任意 r 个整数, 则 r 个同余方程组 $x \equiv a_i \pmod{m_i}$ ($1 \leq i \leq r$) 的模 $M = m_1 m_2 \cdots m_r$ 有唯一解, 且该解的表达式为:

$$x = \sum_{i=1}^r a_i M_i y_i \pmod{m}$$

其中: $M_i = M/m_i$, $y_i = M_i^{-1} \pmod{m_i}$, $1 \leq i \leq r$ 。

蒙哥马利算法^[11] 令 $2^{n-1} \leq N \leq 2^n, R = 2^n$ 且 N 与 R 互素, $A < N, B < N$ 。

A 关于 R 的剩余为 $\bar{A} = A \cdot R \pmod{N}$

B 关于 R 的剩余为 $\bar{B} = B \cdot R \pmod{N}$

用 $MMJ(\bar{A}, \bar{B})$ 表示定义在 R 剩余系中 \bar{A}, \bar{B} 的蒙哥马利乘积, 则:

$$MMJ(\bar{A}, \bar{B}) \equiv \bar{A} \cdot \bar{B} \cdot \bar{R}^{-1} \pmod{N}$$

2.3 算法的改进

已知 RSA 算法中私钥为 (d, n) , 公钥为 (e, n) , p, q 是生成 RSA 密钥对的一对大素数, C 是密文, M 是对应的明文。

RSA 算法加密过程: $C = M^e \pmod{n}$ 。

改进的加密运算过程中, 应用这个剩余定理和蒙哥马利算法来求解模幂运算。在计算 $x = ab \pmod{n}$ 时, 可以把大数变换到 n 的剩余系中, 用 $\begin{cases} \bar{a} = aR \pmod{n} \\ \bar{b} = bR \pmod{n} \end{cases}$ 来替代 a 和 b , 接着计算 $\bar{x} = \bar{a}\bar{b}R^{-1} \pmod{n} = xR \pmod{n}$, 最后计算出 x 。显而易见, 指数越大, 效率越高。

RSA 算法的解密过程:

$$M = C^d \pmod{n} = C^d \pmod{(pq)}$$

利用中国剩余定理, 上式可以分解为:

$$M_1 = C^d \pmod{q}$$

$$M_2 = C^d \pmod{p}$$

利用费马小定理可知, $a^{m-1} \equiv 1 \pmod{m}$ 。其中, m 为素数, 且 a 不是 m 的倍数。

因此简化为:

$$M^1 = C^{d1} \pmod{q}$$

$$M^2 = C^{d2} \pmod{p}$$

其中:

$$d1 = d \pmod{q-1}$$

$$d2 = d \pmod{p-1}$$

据中国剩余定理可知:

$$M = \left(M_1 c_1 \frac{pq}{q} + M_2 c_2 \frac{pq}{q} \right) \pmod{n} =$$

$$(M_1 c_1 p + M_2 c_2 q) \pmod{n}$$

因为

$$c_1 = p^{-1} \pmod{q}; c_2 = q^{-1} \pmod{p}$$

所以

$$M = ((M_1(p^{-1} \pmod{q})p) + (M_2(q^{-1} \pmod{p})q)) \pmod{n}$$

上述算法中, 设 n 的长度为 k , 那么 p, q 的长度约为 $k/2$ 。假设 $d1, d2, p^{-1} \pmod{q}, q^{-1} \pmod{p}$ 都已知, 则整个计算过程约需要 $3k^3/8$ 次位运算, 而没有使用改进算法之前, 则约需要 $3k^3/2$ 次位运算, 所以本方法可以减少约 55% 的运算量。

2.4 改进算法的安全性分析

2.4.1 计时攻击分析

在使用蒙哥马利算法中, 需要额外的约简操作, 对于不同的初始数据, 这个操作的耗时是不同的。由于运算中要多次使用 MMJ 函数, 由此可能检测到不同输入数据运算后的时间差。有研究表明, 在一个模幂运算 $x^k \pmod{m}$ 中, 发生一个额外约简的概率与 x 同 m 之间的近似度成比例^[12]。某位为 1 时, 对其进行模幂运算的速度很慢, 若模幂运算很快则表明该位很

可能是0,这容易导致攻击者猜测出某位是1还是0。在实际的测试过程中发现,模幂运算的时间差异很小,一次执行的时间不会超过算法的平均时间。但是这种安全威胁是存在的,因此可以通过下列一些简单的方法进行解决:

1)每次运算时间保持不变。每次运算完成在返回结果时等待一段时间,使每次运算的总耗时相同,这种方法简单有效,但会降低算法的效率。

2)随机延时。在运算的过程中加入随机延时,攻击者就不能通过运算时间的长短来破获密钥。

3)随机位运算。在运算开始之前,密文乘以一个随机数,得到随机处理的位,使得攻击者不能得到正确的密文顺序。

本文提出的改进算法使用第3种方式来提高安全性,因为前两种方式需要额外的时间和电力能量消耗,不适合在无线传感器网络中使用。

2.4.2 出错攻击

在使用中国剩余定理时,如果系统出现软硬件错误(包括意外错误和人为故意攻击错误),可能导致攻击者从错误的消息中分析出大整数^[13]。

从改进算法可知:

$$C_p = m^{d1} \pmod{p}$$

$$C_q = m^{d2} \pmod{q}$$

$$(C^e - m \pmod{n}) \pmod{q} = ((C_q (q^{-1} \pmod{q})^e -$$

$$m \pmod{n}) \pmod{q} = (C^e - m) \pmod{q} = 0$$

假设 C_p 计算错误, C_q 计算正确, 经过中国剩余定理计算后会产生一个错误的 C' 。

系统在没有错误的情况下:

$$C = (C_p (m^{d1} \pmod{p}) + C_q (p^{-1} \pmod{q}) p) \pmod{n}$$

由于 C' 是错误的, 所以:

$$(C'^e - m \pmod{n}) \pmod{p} \neq 0$$

由此可知:

$$\gcd((C'^e - m \pmod{n}), n) = q$$

上述推论过程表明, 攻击者在知道错误的密文和一个明文的基础上可能计算出大数 q 。

针对这种攻击, 可以使用确认手段来避免。确认有两种方式:一是在系统运行之前, 把一组正确的初始数据放入, 运算的结果与事先设定的结果一致则说明整个系统没有出错, 否则系统发生错误应停止使用;二是把加密完成后的数据在原地完成解密过程, 通过明文的比对可以得知系统是否出错。本改进算法使用第一种方式来防止出错攻击。

3 实验验证与数据分析

3.1 实验平台

实验使用宁波中科集成电路设计中心开发的 GAINS 系列硬件平台。GAINS 是工作在 433 MHz 的无线网络传感器开发平台, 节点间的数据吞吐量为 76.8 Kbps, 微控制器使用 ATMEL 公司的 ATmega128L, 无线收发器使用的是 Chipcon 公司的 CC1000。GAINS 系统为提高平台的适应性, 其平台传感器接口是可扩展的, 扩展后可接入多种传感器, 例如光传感器、湿度传感器、温度传感器等。

ATmega128L 是 8 位低功耗微控制器, 其最大优点是功耗低。ATmega128L 内部有 128 KB 闪存(Flash), 4 KB 静态存储器(Static Random Access Memory, SRAM) 和 4 KB 可擦除存储器(Electrically Erasable Programmable Read-Only Memory, EEPROM), 静态存储器还可扩展至 64 KB。无线收发器 CC1000 是低电压的单片特高频(Ultra High Frequency, UHF)收

发器, 其优点是工作电压低、能耗小、体积小、无外接滤波电路且可直连外部天线。GAINS 的硬件组成结构如图 1 所示^[14]。

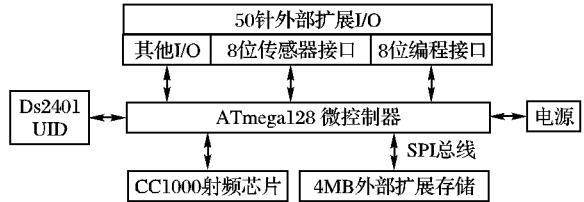


图 1 GAINS 硬件结构

测控软件是无线传感器网络系统的重要组成部分, 是获取和分析传感器网络数据的重要工具, 本实验使用传感器网络分析与管理平台(Sensor Network Analysis and Management Platform, SNAMP) 获取和分析数据。SNAMP 是一款无线传感器网络平台, 其显著特点是测控过程可视化, 能较直接地提供相关数据。SNAMP 主要功能模块有: Mac 层分析、串口监听、传感数据分析、网络层分析、数据库管理等。

3.2 实验数据分析

实验在一个 8 m × 9 m 的实验室中进行, 使用 8 个无线传感器节点, 节点人为随机放置在实验台上, 节点使用 300 mA 锂电池, 节点不使用外接天线, 不使用外接扩展口和外接数据存储器。实验主要分两次进行, 一次在节点上运行 RSA 算法, 另一次在节点上运行本文提出的改进算法。

3.2.1 运算时间分析

RSA 算法安全可靠, 但运算量巨大, 微控制器高负荷运行, 需要消耗大量的节点能量和时间。改进的 RSA 算法在保证安全性的前提下大大降低了运算量, 微控制器的运算时间明显减小, 表 1 是 8 个节点在两种算法下运算时间的比较。

表 1 处理器运算时间表 ms

节点	加密运算耗时		解密运算耗时	
	RSA 算法	本文算法	RSA 算法	本文算法
节点 1	3 824.31	2 489.63	4 023.58	2 674.39
节点 2	3 794.29	2 377.84	3 976.34	2 603.78
节点 3	3 787.46	2 398.56	3 954.33	2 702.93
节点 4	3 812.85	2 403.98	3 985.12	2 721.65
节点 5	3 890.42	2 496.35	4 012.57	2 693.17
节点 6	3 901.37	2 387.74	4 103.67	2 661.82
节点 7	3 765.09	2 432.73	4 078.38	2 598.53
节点 8	3 845.95	2 493.76	3 984.59	2 931.54
平均	3 827.72	2 435.07	4 014.82	2 698.48

3.2.2 存储空间分析

利用 SNAMP 软件, 可以实时监测节点中存储空间使用情况, 图 2 是两种不同算法情况下, 节点消耗存储空间的情况。

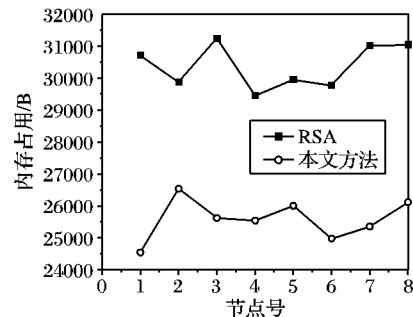


图 2 节点存储空间占用情况

从图 2 的数据可知, 本文算法大约只需占用原存储的 1/3, 即能节约 67% 的存储空间占用。

3.2.3 电源能量损耗分析

无线传感器网络中的传感器节点在不同状态时消耗的能量是不一样的,通常情况下,节点主要有发送耗能、接受耗能、监听耗能和休眠耗能。用 E_n 表示节点总能耗, E_s 表示节点发送耗能,用 E_r 表示节点接受耗能,用 E_l 表示节点监听耗能,用 E_e 表示节点休眠耗能,则节点的能耗可用下式^[15] 来表示:

$$E_n = E_s + E_r + E_l + E_e$$

影响 E_s 和 E_r 的主要因素是节点间的传输距离和单位时间内发送的比特数。假设单位时间数据发送率为 x , 节点间的传输距离为 m , 则节点的发送能耗计算公式^[16] 如下:

$$E_s = \begin{cases} xE_{use} + x\delta m^2, & m \leq m_0 \\ xE_{use} + x\delta m^4, & m > m_0 \end{cases}$$

其中: E_{use} 是节点发送 1 b 能耗; m_0 是临界距离, 经实验测试, m_0 大约为 86.4 m。

节点的休眠及侦听功率在节点制造时已被厂商确定, 而节点的接受能耗计算公式^[17] 如下:

$$E_r = xE_{use}$$

节点能量耗尽后, 无线传感器网络的生命周期也就结束了, 因此测试节点的能耗就能测试网络的生存时间。在全负荷运行的情况下, 测试 8 个节点在两种算法情况下能量耗尽的时间如表 2 所示。实验数据表明, 使用改进的方法大约能延长 1/5 的网络生存周期。

表 2 能量耗尽时间表

节点	能量耗尽时间		节点	能量耗尽时间	
	RSA 算法	本文算法		RSA 算法	本文算法
节点 1	65	82	节点 5	68	83
节点 2	57	81	节点 6	66	80
节点 3	69	82	节点 7	62	79
节点 4	71	84	节点 8	60	76

4 结语

物联网的高速发展, 将积极推动无线传感器网络的发展, 其在军事、环境保护、医疗卫生、家庭生活及工农业生产中都有广泛的应用。无线传感器网络节点通常都是一个嵌入式系统, 由于制造成本、节点体积及能量供给等因素的制约, 其运算能力、存储能力和通信距离等都有待提高。一方面可以通过改善节点制造技术来提高节点性能(例如提高电源单位体积存储电荷的能力); 另一方面可以改进现有算法或者管理模式, 以减少微控制器的运算量, 减小能量消耗, 延长节点的寿命。

本文提出把改进的公钥算法应用在无线传感器网络中,

(上接第 1604 页)

学有效的。但是由于颜色聚类参数受节点分配的影响^[10], 其伪图像的增强效果也会受到限制, 因此, 下一步需要对色彩渐进插值的矿井预警数据集三维可视化伪图像编码算法进行基于视觉特征量化的改进研究, 以进一步提高伪图像的处理效果。

参考文献:

- [1] 李今秀, 李均利, 魏平. 基于梯度的医学图像伪彩色编码[J]. 光学技术, 2008, 34(4): 576–582.
- [2] 魏志强, 高兴堂, 纪莜鹏. 基于 K 均值算法的彩色编码条纹分色研究[J]. 计算机应用, 2011, 31(12): 67–69.
- [3] 李志球, 梁双华. 改进的灰度级—彩色变换法在 B 超图像中的应用[J]. 工程图学学报, 2010, 31(4): 87–93.
- [4] 杨来侠, 池雄飞, 张宁芳. 三维打印快速成型技术的色彩渐变插

运算量明显降低, 能量消耗显著减少, 能在保证加解密效果的同时, 提升网络的生存周期, 实验结果验证了理论推导。

参考文献:

- [1] 党小超, 李小艳. 无线传感器网络节点定位加权校正模型[J]. 计算机应用, 2012, 32(2): 355–358.
- [2] 成奋华. 传感器网络中基于信誉模型的对偶密钥建立算法[J]. 计算机应用, 2011, 31(7): 1876–1879.
- [3] 王汝传, 孙力娟. 无线传感器网络技术及其应用[M]. 北京: 人民邮电出版社, 2011.
- [4] 何文才, 牛晓蕾, 刘陪鹤, 等. 密码算法 RC5 和 RC6 的分析和比较[J]. 网络安全技术与应用, 2007, 5(2): 2–3.
- [5] STALLINGS W. 密码编码学与网络安全——原理与实践[M]. 4 版. 北京: 电子工业出版社, 2006.
- [6] 阙喜戎, 孙悦, 龚向阳, 等. 信息安全原理及应用[M]. 北京: 清华大学出版社, 2005.
- [7] 鄢喜爱, 杨金民, 田华. RSA 公钥密码算法的分析[J]. 长春工业大学学报: 自然科学版, 2006, 27(2): 142–144.
- [8] 尹绪昆, 黄世中. RSA 算法硬件实现的几个关键技术[J]. 河北省科学院学报, 2011, 28(3): 10–15.
- [9] 唐勇, 许金玲. 快速 RSA 算法研究[J]. 燕山大学学报, 2007, 31(6): 481–484.
- [10] 王琴琴, 陈相宁. Montgomery 算法在 RSA 中的应用及其优化[J]. 计算机技术与发展, 2007, 17(6): 145–150.
- [11] 兰海兵, 程胜利. RSA 算法及其实现技术的改进研究[J]. 交通与计算机, 2006, 24(1): 95–97.
- [12] 冯登国. 密码工程实践指南[M]. 北京: 清华大学出版社, 2001.
- [13] 孙秀娟, 金民锁. 基于中国剩余定理的 RSA 系统中的出错攻击与防范[J]. 哈尔滨商业大学学报: 自然科学版, 2009, 25(4): 477–478.
- [14] 徐勇军, 安竹林, 蒋文丰, 等. 无线传感器网络实验教程[M]. 北京: 北京理工大学出版社, 2007.
- [15] SINHA A, CHANDRAKASAN A, MIT C. Dynamic power management in wireless sensor networks[J]. IEEE Design & Test of Computer, 2001, 18(2): 62–74.
- [16] PERING T, BURD T, BRODERSEN R. Dynamic voltage scaling and the design of a low-power microprocessor system [C]// ISCA1998: International Symposium on Computer Architecture. Piscataway: IEEE Press, 1998: 17–22.
- [17] HUI J, AIDA H. A cooperative game theoretic approach to clustering algorithm for wireless sensor networks[C]// PACRIM 2009: IEEE Pacific Rim Conference on Communications, Computers and Signal Processing. Piscataway: IEEE Press, 2009: 140–145.

值方法[J]. 西安科技大学学报, 2009, 3(2): 214–218.

- [5] 李占利, 胡德洲. 三维模型的直接分层软件研究与开发[J]. 西安科技大学学报, 2002, 22(2): 190–193.
- [6] McGAVIN D, BERNARD S. Color figures in BJ: RGB versus CMYK[J]. Biophysical Journal, 2005, 88(2): 761–762.
- [7] DAI J B, ZHOU S X. Computer aid pseudo-coloring coding of gray image-complementary coloring coding technique[J]. SPIE, 1996, 2896: 181–191.
- [8] 李长春, 王祝文, 孙刚. 基于克里格方法的相空间重构统计特征研究与应用[J]. 地球物理学进展, 2010, 2(4): 1474–1478.
- [9] 李勇, 王虎, 王树仁. 矿井主要含水层三维可视化模型构建及其应用[J]. 煤炭科学技术, 2011, 39(6): 102–114.
- [10] 施海滨, 周勇. 混合聚类彩色图像分割方法研究[J]. 计算机工程与应用, 2011, 47(9): 181–184.