Journal of Computer Applications
计算机应用,2013,33(4):1081 - 1084
ISSN 1001-9081
CODEN JYIIDU
2013-04-01
http://www.joca.cn

文章编号:1001 - 9081(2013)04 - 1081 - 04
doi:10.3724/SP.J.1087.2013.01081

基于混沌 S 盒的无线传感器网络分组加密算法

何　远[1*]，田四梅[2]
(1.大理学院 数学与计算机学院,云南 大理 671003；2.中国移动江西景德镇分公司,江西 景德镇 333000)
(*通信作者电子邮箱 hy2050@163.com)

摘　要:针对无线传感器网络中现有的分组加密算法的优缺点,根据无线传感器网络安全需求提出了一种基于混沌 S 盒的分组加密算法。主要利用了混沌的非周期性、不可预测性等相关特性生成随机数,利用随机数设计对应的 S 盒,通过统计性检测对其安全性进行分析,并通过能耗仿真对其可用性进行分析,与 RC5、RC6 加密算法进行比较,结果表明该算法在无线传感器网络加密算法中有一定优势。

关键词:混沌;Logistics 映射;分组加密;降维;S 盒
中图分类号:TP309　　**文献标志码**:A

Block encryption algorithm based on chaotic S-box for wireless sensor network

HE Yuan[1*], TIAN Simei[2]
(1. *School of Mathematics and Computer Science, Dali University, Dali Yunnan* 671003, *China*;
2. *China Mobile Jiangxi Jingdezhen Branch, Jingdezhen Jiangxi* 333000, *China*)

Abstract: The pros and cons of the existing encryption algorithm for Wireless Sensor Network (WSN) were analyzed. A chaotic block cipher based on chaos box was proposed for WSN in accordance with its security request. Random number was generated by mainly using the chaotic aperiodicity, unpredictability and other related characteristics, and corresponding S box was designed by using random number. Finally, conclusion was made by comparing RC5 and RC6 at statistical performance and energy consumption. The results show this encryption scheme has better performance for WSN.

Key words: chaos; Logistics map; block encryption; dimension reduction; S-box

0　引言

无线传感器网络(Wireless Sensor Network, WSN)采用无线介质进行信息传输,其信息很容易被截获;节点无人看守,很容易被攻击者俘虏。因此信息安全是 WSN 研究领域中极其重要的内容,目前对 WSN 的安全研究主要有以下几个方面:密钥管理、认证协议、加密算法、安全路由、入侵检测、拒绝服务(Denial of Service, DoS)攻击以及访问控制[1],其中,加密技术是信息安全、可靠传输的基本要求,近年来被广大学者广泛研究。

WSN 中普遍使用的 TinySec(Security for TinyOS)、SPINS 等安全协议推荐使用的主要是 RC5、RC6 分组加密算法。RC5 由于其简单性,被广泛应用于 WSN 中,但近几年研究发现,RC5 存在一定的安全隐患。Biryukov 利用 2^{44} 的明文破译了 RC5-32/12/16,利用 2^{61} 的明文破译了 RC5-32/16/16,Miyaji 利用 $2^{63.67}$ 明文以 90% 的概率破译 RC5-32/10/16[2]。由于 RC5 在安全性上的隐患,提出了 RC6 算法。RC6 继承了 RC5 的优点,还使用了 4 个寄存器,加入 32 bit 的整数乘法,增强了扩散性。但乘法运算的引入增加了加密算法的能耗,文献[3]在 Tinyos 1.1.6 版本上对 SkipJack、RC5、RC6 等加密算法进行了仿真比较,数据显示 RC6 算法的能耗远远高出 RC5,乘法运算导致其算法难抵抗定时和能量攻击[4],同时硬件实现代价高,不利于在 WSN 的广泛应用。

1　WSN 中的混沌加密

混沌现象是指在确定系统中出现的一种类似随机的现象,常见的混沌映射有 Logistic 映射、Baker 映射、Lorenz 系统、Cellular neural network 超混沌系统等[5]。混沌系统产生的序列具有非周期性、不可预测、对初始条件和参数极端敏感性等特点,与传统密码学有许多相同之处。

混沌和密码学之间具有的天然联系和结构上的某种相似性,启示着人们把混沌应用于密码学领域。文献[6 - 7]利用混沌设计出了具有良好性能的混沌加密算法,但是这些研究都是针对混沌加密算法的安全性进行研究,并未结合具体的网络进行考虑。同样文献[8 - 9] 设计了混沌图像加密算法,但也没考虑具体的网络应用。分析了各种对称加密算法,指出 AES 标准的 Rijindael 算法虽然安全性比较好,但基本的 Rijindael 算法需要存储 20 个正向 S 盒、16 个逆向 S 盒,会占用芯片的大部分存储空间。典型的传感器节点包含 4 KB RAM、128 KB ROM[11],这对于存储能力有限的传感器节点是不合适的。当将混沌映射应用于 WSN 时,不得不考虑 WSN 节点的运算能力和有限的计算精度,难以直接处理浮点数运算等问题。

在 WSN 中为了保证均衡消耗各节点的能源,因此在设计路由时,往往使用多条路由完成一次数据传输。如果采用流密码的方式,就可能发生在某条路由上传输延迟或者丢失,而严重影响接收端的解密。所以把一次传输的数据分成相对独立的单元,分别对其进行加密和传输,则能把这种影响降到最低,因此在设计混沌密码时采用分组加密的方式。

对 WSN 已有加密算法的研究后,提出一种基于混沌 S 盒的分组加密算法,简称 BCC(Block Cipher based on Chaos)算法。BCC 算法采用可变长度加密,记为 BCC($w/r/b$),其中 w 表示字的长度(位),r 表示迭代次数,b 表示密钥长度(字节),

收稿日期:2012-10-19;**修回日期**:2012-11-24。

作者简介:何远(1977 -),男,云南大理人,助教,硕士研究生,主要研究方向:无线网络安全;　田四梅(1987 -),女,江西九江人,工程师,硕士研究生,主要研究方向:混沌密码学。

在本论文中采用 $w = 64, b = 64$ 进行讨论。

2 BCC 算法

2.1 算法结构

设计分组密码主要包括两大设计原则:混淆与扩散,主要由 S 盒和 P 置换来实现,其中 S 盒为密码算法提供了必要的混淆作用,P 置换为密码算法提供了扩散作用[12]。$n \times m$ 的 S 盒本质上可看作 n 比特输入对应 m 比特输出的映射。类似于 RC5 算法结构,BCC 采用交叉运算方式,加密框图如图 1 所示。

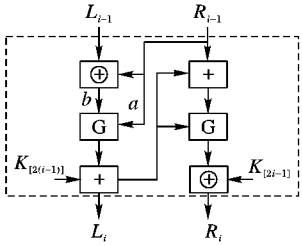

图 1 BCC 加密算法流程

其中 G 是基于混沌的 SP 网络,K 为 64 bit 的子密钥,将 128 bit 明文分为 L_{i-1} 和 R_{i-1} 左右各 64 bit 的数据块,每轮变换的整个过程可用式(1)表示:

$$\begin{cases} L_i = G(L_{i-1} \oplus R_{i-1}, R_{i-1}) + K[2(i-1)] \\ R_i = G(R_{i-1} + L_i, L_i) \oplus K[2i-1] \end{cases} \tag{1}$$

其中:"⊕"为二进制异或运算,"+"为二进制加法运算。

2.2 G 函数

在图 1 所示的 BCC 加密框图中,G 函数是由混沌构成的两层 S-P-S 网络,是算法混淆性、扩散性的关键所在,其结构如图 2 所示。

其中 a 为输入的 64 bit 数据块的其中 16 bit 数据,首先经过由混沌映射生成的 S 盒进行替换。64 bit 数据经过 S 盒替换后,再对其进行 P 置换,再进行 S 盒替换。算法中采用 8 bit(输入)×8 bit(输出)的 S 盒,对应着 0 ~ 255 的 16 × 16 的表格。S 盒的混沌算法设计如下:

1)选择 Logistic 映射和 Baker 映射作为产生 S 盒的混沌方程,算法流程如图 3 所示。

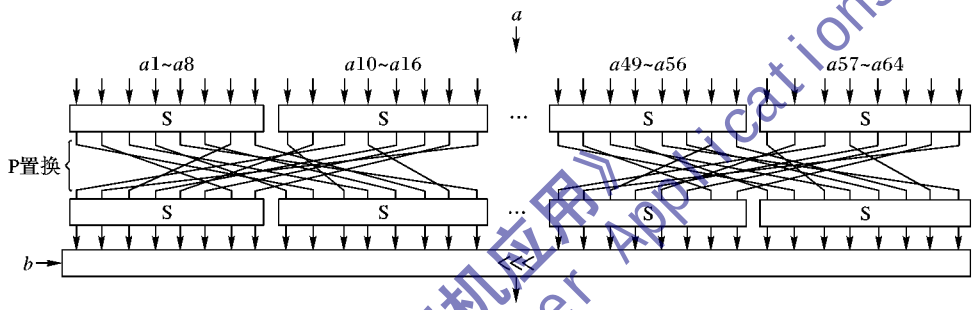

图 2 BCC 算法中的 G 函数

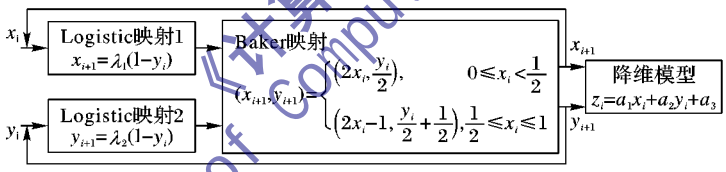

图 3 S 盒混沌算法流程

2 个 Logistic 映射的初始值参数如下所示:

$$x_{i+1} = \lambda_1(1 - x_i): \begin{cases} \lambda_1 = 3.9999 \\ x_0 = 0.3579 \end{cases}$$

$$y_{i+1} = \lambda_2(1 - y_i): \begin{cases} \lambda_2 = 3.6579 \\ y_0 = 0.0354 \end{cases}$$

由 2 个 Logistic 映射产生的输出 x_{i+1} 和 y_{i+1},分别作为 Baker 映射的输入 x_i 和 y_i,Baker 映射的方程式如下所示:

$$B(x_{i+1}, y_{i+1}) = \begin{cases} (2x_i,\ y_i/2), & 0 \leqslant x_i < 1/2 \\ (2x_i - 1,\ y_i/2 + 1/2), & 1/2 \leqslant x_i \leqslant 1 \end{cases} \tag{2}$$

由 Baker 映射得到输出 $B(x_{i+1}, y_{i+1})$,再分别作为 Logistic 映射 1 和 Logistic 映射 2 的初始值 x_i 和 y_i。

Baker 映射有 2 个输出值 x_{i+1} 和 y_{i+1},而 8 × 8 的 S 盒对应的是一维数据,因此,这里需要对输出采用采用如下模型对产生的序列进行降维:

$$Z(i) = a_1x(i) + a_2y(i) + a_3 \tag{3}$$

根据文献[13]的方法通过大量的仿真实验进行尝试,得出采用参数 $a_1 = 0.89, a_2 = 0.1, a_3 = 0.01$,可以使得产生的随机序列在[0,1]范围内能够得到均匀的分配。

2)由 2 个 Logistic 映射与 Baker 映射及降维模型产生的随机序列的取值范围在[-0.5,1.5],这里将[0,1]区间的取值平均分为 256 等份,即 $T_i = [t_i, t_{i+1})$,其中 $t_i = i/N(i = 0, 1, \cdots, 255)$。

3)Logistic 映射、Baker 映射进行交替运算 $d = 1000$ 次,得到的结果为 x_d、y_d,再将 x_d、y_d 作为初始值,经过 Logistic 映射、Baker 映射及降维模型的运算后,得到状态值 Z_{d+1},判断它在 $[t_i, t_{i+1})$ 的取值区间,并将该区间的标识符 T_i 作为输出。若 T_i 不在序列 *out* 中,则将添加到输出序列 *out* 中,若已存在,则继续进行迭代。

4)重复步骤 3),直到输出序列 *out* 的元素个数为 $N = 256$ 为止。

5)将输出序列 *out* 中的元素进行重新组合,转化为 $2^{n/2} \times 2^{n/2}$ 的表格,如表 1 所示。

表 1 S 盒(局部)

x	y							
	0	1	2	3	4	5	6	7
0	79	32	1F	54	08	00	34	CD
1	3F	9F	1E	64	C1	1D	01	52
2	CF	26	AB	FE	04	6F	E9	37
3	B8	4F	92	DA	20	73	4A	7F
4	85	E3	13	F2	9A	9D	C5	43
5	AC	B7	99	1C	50	47	5F	40
6	9B	12	A8	C4	D8	68	A3	42
7	6D	39	87	33	44	3A	2C	FF

S 盒的替换过程如下:假设输入 S 盒的数据是 8 bit 数据 a,用十六进制表示为 xy,对其进行 S 盒替换,xy 对应 S 盒的 x 行 y 列的数据,如 a = '00110100',xy = '34',对应表 1 的 3 行 4 列,经过 S 盒替换后变为"20",输出"00010100"。

2.3　密钥生成

子密钥 K 的生成过程如图 4 所示,P、Q 为 64 bit 的常量数据。这里 P 定义为 0xb7151628aed2a6b, Q 定义为 0x9e3779b97f4a7c15, key 为自己随意设定的 64 bit 的密钥,采用加法与数据依赖循环构成一个反馈式框架生成种子密钥。

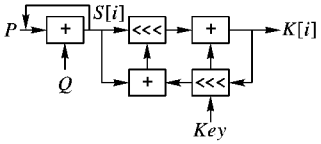

图 4　密钥扩展

子密钥生成过程可用式(3)表示:

$$S[0] = K[0] = P + Q \tag{3}$$

$$K[i+1] = ROL((S[i+1] + ROL(K[i],Key)), S[i+1]) + ROL(K[i],Key) \tag{4}$$

其中:$ROL(x,y) = \{x << (y \& (w-1))\} \mid \{x >> (w-(y \& (w-1)))\}$ 为 RC5 中采用的数据依赖循环,"&、|"分别为二进制按位与、或运算。

2.4　加解密过程

输入明文:128 bit 的 $M(m_1m_2\cdots m_{128})$,输出密文:128 bit 的 $C(c_1c_2\cdots c_{128})$,密钥 Key: 64 bit,循环次数 r 为定值。

算法加密:

1)密钥生成:按照 2.3 节式(3)~(4)得到 $2r$ 个子密钥 $K[0],K[1],\cdots,K[2r]$,其中 r 表示加密循环次数,记为 nub;

2)分块:将 128 bit 明文 $M(m_1m_2\cdots m_{128})$ 分为 64 bit 的 $L_0(m_1m_2\cdots m_{64})$ 和 $R_0(m_{65}m_{66}\cdots m_{128})$;

3)循环加密:在 1 到 nub 循环次数内,不断按照式(1)得到 $L_1L_2\cdots L_{nub}$、$R_1R_2\cdots R_{nub}$,将最后循环得到的 L_{nub}、R_{nub} 相互交换作为密文输出,即 $C = \{R_{nub}L_{nub}\}$。

算法解密:

BCC 算法的解密与加密框架类似,将加密过程逆变换。不同之处主要有将加法改成减法,P 置换改成 P 逆置换,数据依赖左循环改成数据依赖右循环。

3　性能分析

文献[14]指出目前对分组加密算法的性能分析,主要是通过局部抽样进行统计性分析。一般来说,对一个分组加密算法进行统计性检测主要包括数据变换的有效性、对明文的敏感性和对密钥的敏感性。

3.1　数据变换有效性测试

数据变换有效性测试主要考虑数据的随机性测试,随机性测试是对生成的若干密文分组进行统计性测试,若产生的密文分组是随机的,则应该具有较好的"0"、"1"平衡性。对 RC5、RC6、BCC 三种分组加密算法输出的密文进行统计性分析得到的 0/1 比接近 1(>0.998),可知 RC5、RC6、BCC 三种加密算法在随机性测试上都能满足随机性要求。

3.2　明文的敏感性测试

明文的敏感性测试主要有扩散性分析,即改变 1 bit 明文时密文改变的比特数、完全性、雪崩效应以及严格雪崩准则。

通过实验仿真发现,三种加密算法的完全性都具有很好的完全性和雪崩效应,但在严格雪崩准则方面表现各有不同。雪崩准则的理想值是 1,越接近 1,则说明算法对明文的严格雪崩性能越好,3 种算法的严格雪崩准则结果如图 5。

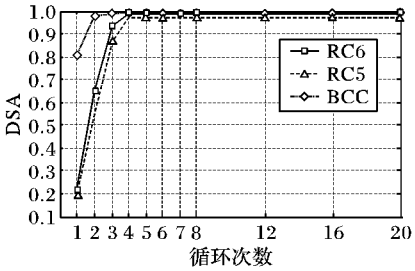

图 5　严格雪崩准则测试

由图 5 可见,RC5 在严格雪崩准则的统计性分析上,性能并不是很理想,略逊于其他 2 种算法。RC6 从第 4 轮开始可以满足雪崩准则的基本要求,BCC 从第 4 轮开始满足雪崩准则的基本要求,BCC、RC6 从第 4 轮开始性能相差不多,但在前 3 轮 BCC 扩散性优于 RC6。

3.3　密钥更换的有效性测试

从密钥更换的有效性考虑,一个分组密码算法对密钥的变化应是敏感的,即密钥的雪崩效应。根据分组密码测度中的严格雪崩准则,改变密钥中任一比特,应导致密文分组中大约一半比特的变化。RC5、RC6、BCC 三种加密算法的对比如图 6 所示。

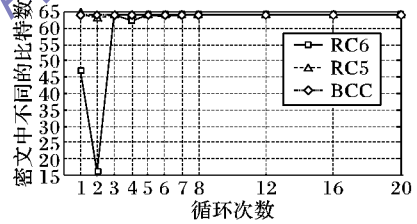

图 6　密钥扩散性统计

通过对密钥的雪崩效应性能进行测试可看出,RC6 在第 1,2,4 轮循环时,波动幅度大,RC5 在第 2 轮循环时,性能有所下降,BCC 性能比较稳定,RC5、BCC 在密钥的雪崩性上要好于 RC6 算法。

4　能耗测试分析

文献[15]的研究结果表明,对于 WSN 传输能耗远远大于节点的处理能耗。通过网络仿真软件 NS2 建立相同的网络场景对 3 种算法进行仿真的结果如图 7 所示。

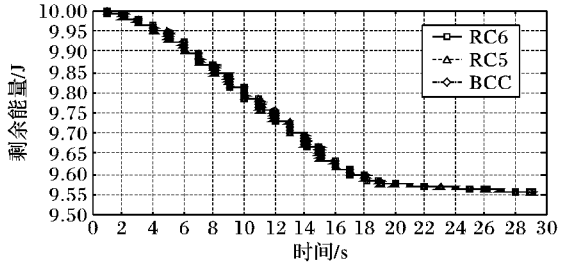

图 7　NS2 三种算法的能耗仿真

从图 7 可看出,RC5、RC6、BCC 三种加密算法在发送、传输、接收状态的能耗基本相同,说明加密算法的复杂度对数据传输的能耗影响不大,这是因为三种加密算法基于类似的结构,加密后的数据量一样。

通过图 8 对空间占用对比的结果可看出,BCC 算法 ROM

的空间占用比 RC5 多 4198 字节、比 RC6 多 3596 字节。其主要原因是该算法需要存储 2 个的 S 盒,以及 2 个置换矩阵。

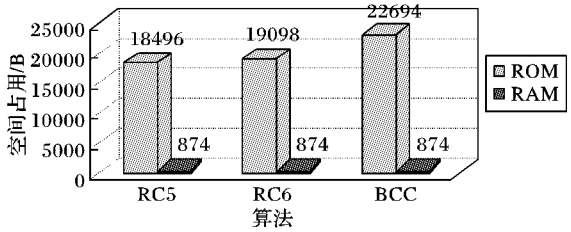

图 8 算法占用空间比较

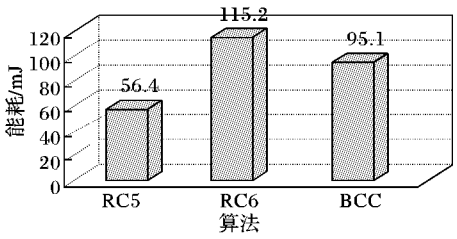

图 9 算法在 WSN 中的能耗仿真

由图 9 仿真结果,可看出 RC5 算法的能量消耗相比 RC6、BCC 算法具有明显优势。BCC 算法比 RC6 算法能耗稍低。

对于 WSN 在考虑加密算法时,需要从安全性、空间占用、耗能等进行考虑,安全性越高,算法越复杂,空间占用、能量消耗相应会增加。

5 结语

在实际应用中需要对各种参数进行综合考虑,寻找平衡点。BCC 算法正是基于这种观点,利用空间消耗来换取安全性的提高和能量消耗的降低。通过对 BCC 算法与 RC5、RC6 算法进行了对比分析,结果显示 BCC 算法除了占用空间多,其他的安全指标和性能指标具有一定的综合优势。随着存储器件容量不断提高,体积不断减小,价格不断下降,BCC 算法将会在 WSN 中得到较好的应用。

参考文献:

[1] 裴庆祺, 沈玉龙, 马建峰. 无线传感器网络安全技术综述[J]. 通信学报, 2007, 28(8): 113 - 122.

[2] LAW Y W, DOUMEN J, HARTEL P. Survey and benchmark of block ciphers for wireless sensor network [J]. ACM Transactions on Sensor Network, 2006, 2(1): 65 - 93.

[3] GUIMARAES G, SOUTO E, SADOK D, *et al*. Evaluation of security mechanisms in wireless sensor network[C]// Proceeding of the 2005 Systems Communications. Washington, DC: IEEE Computer Society, 2005: 428 - 433.

[4] 吴文玲, 冯登国, 张文涛. 分组密码的设计与分析[M]. 北京: 清华大学出版社, 2009: 64 - 84.

[5] 廖晓峰, 肖迪, 陈勇, 等. 混沌密码学原理及其应用[M]. 北京: 科学出版社, 2009: 55.

[6] CHEN Z, ZHANG Z W, JIANG N. A session key generator based on chaotic sequence[C]// International Conference on Computer Science and Software Engineering. Washington, DC: IEEE Computer Society, 2008: 635 - 637.

[7] PENG J, JIN S Z, LIN H L, *et al*. A block cipher based on a hybrid of chaotic system and Feistel network[C]// 2009 Fifth International Conference on Natural Computation. Piscataway, NJ: IEEE Press, 2009: 17.

[8] 邓绍江, 黄桂超, 陈志建. 基于混沌映射的自适应图像加密算法[J]. 计算机应用, 2011, 31(6): 1502 - 1504.

[9] 肖迪, 赵秋乐. 一种基于 Logistic 混沌序列的图像置乱算法的安全分析[J]. 计算机应用, 2010, 30(7): 1815 - 1817.

[10] LIANG W, XU J B, TANG M D, *et al*. A new embedded encryption algorithm for wireless sensor networks[C]// IFITA'09: Proceedings of the 2009 International Forum on Information Technology and Applications. Washington, DC: IEEE Computer Society, 2009: 119 - 122.

[11] ULUAGAC A S, BEYAH R A, LI YINGSHU, *et al*. WEBEK: virtual energy-based encryption and keying for wireless sensor networks[J]. IEEE Transactions on Mobile Computing, 2010, 9(7): 994 - 1007.

[12] MASUDA N, JAKIMOSKI G, AIHARA K, *et al*. Chaotic block ciphers: from theory to practical algorithms[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2006, 53(6): 1341 - 1352.

[13] 陈帅. 网络混沌加密理论及其关键技术研究[D]. 重庆: 重庆大学, 2006.

[14] TANG G P, LIAO X F, CHEN Y. A novel method for designing S-boxes based on chaotic maps[J]. Chaos, Solitons & Fractals, 2005, 23(2): 413 - 419.

[15] 杨吉云. 混沌密码在无线传感器网络安全中的应用研究[D]. 重庆: 重庆大学, 2007.

(上接第 1080 页)

参考文献:

[1] 田俊峰, 刘永立. 一种新的蜜网模型——BRHNS[J]. 计算机工程与应用, 2007, 43(7): 139 - 143.

[2] 尚治宇. 蜜罐系统的研究与实现[D]. 北京: 北京交通大学, 2010.

[3] 曹付元. 面向分类数据的聚类算法研究[D]. 太原: 山西大学, 2010.

[4] KDD99. KDD99 cupdataset[EB/OL]. [2005 - 11 - 02]. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[5] Intrusion detection working group. Intrusion detection message exchange format data model and EXtensible Markup Language (XML) document type definition[R]. Internet-Draft, 2003: 21 - 26.

[6] 朱明. 数据挖掘[M]. 合肥: 中国科技大学出版社, 2002.

[7] 孙吉贵, 刘杰, 赵连宇. 聚类算法研究[J]. 软件学报, 2008, 19(1): 45 - 61.

[8] RALAMBONDRAINY H. A conceptual version of the k-means algorithm[J]. Pattern Recognition Letters, 1995, 16(11): 1147 - 1157.

[9] 肖宇, 于剑. 基于近邻传播算法的半监督聚类[J]. 软件学报, 2008, 19(11): 2803 - 2813.

[10] JIANG R, LIU Q, LIU Q, *et al*. A proposal for the morphological classification and nomenclature of neurons [J]. Neural Regeneration Research, 2011, 6(25): 1925 - 1930.

[11] XU R, WUNSCH D. Clustering[M]. Hoboken, New Jersey, USA: John Wiley & Sons, 2009.

[12] 杨博, 刘大有, LIU J M, 金弟, 等. 复杂网络聚类方法[J]. 软件学报, 2009, 20(1): 54 - 66.

[13] ZHANG S H, WANG R S, ZHANG X S. Identification of overlapping community structure in complex networks using fuzzy *c*-means clustering[J]. Physica A, 2007, 374(1): 483 - 490.

[14] 石立宪. 网络陷阱的研究与实现[D]. 大连: 大连海事大学, 2006.