一种新的混沌伪随机序列生成方法 *

李孟婷, 赵泽茂
(杭州电子科技大学 通信工程学院, 杭州 310018)

摘 要: 针对单混沌系统因计算机有限精度效应产生的混沌退化问题,提出了一种多级混沌映射交替变参数的伪随机序列产生方法。该方法基于一维 Logistic 映射和二维 Henon 映射,用交错变参的 Logistic 映射的混沌迭代值的汉明重量来控制 Henon 映射输出的混沌迭代分量。生成序列通过仿真表明,符合 Golomb 三个随机性公设要求及局部随机性统计检验要求,可作为密钥流序列应用到加密体制中。

关键词: 有限精度效应; 混沌序列; 汉明重量; 随机性测试
中图分类号: TP918 **文献标志码**: A **文章编号**: 1001-3695(2011)01-0341-04
doi:10.3969/j.issn.1001-3695.2011.01.096

New method to generate chaotic pseudo-random sequence

LI Meng-ting, ZHAO Ze-mao
(*College of Communication Engineering, Hangzhou Dianzi University, Hangzhou* 310018, *China*)

Abstract: Due to chaos degeneration question caused by computer limited precision in one chaos system, this paper proposed a method of pseudo-random sequence generation with alternating parameter of multistage chaos mapping. Based on one-dimensional Logistic mapping and two-dimensional Henon map, the system output was one component of Henon chaotic iterative values, which was controlled by the Hamming weight of Logistic chaotic iteration value with alternating parameter. Computer simulation results show that, the sequences generated by the chaos system can pass the three randomness testing of Golomb and partial randomness testing, and can be used as key stream in the encryption system.

Key words: limited precision effect; chaos sequences; Hamming weight; randomness testing

近年来,混沌序列的研究越来越受到关注,被广泛应用于密码学、保密通信等领域[1~4]。混沌用于保密方面的工作主要有以下方面[5]:利用混沌产生伪随机序列并利用伪随机序列加密文本文件、图像文件;利用混沌同步理论进行同步保密通信。

本文主要研究的是用混沌来产生伪随机序列。利用混沌产生伪随机序列,主要有以下几个方面的方法:直接使用单个混沌系统产生伪随机序列;将两个或两个以上的混沌系统构成复合混沌系统;在常见的混沌系统的基础上重新构造混沌映射的迭代关系式变成新的混沌系统;将混沌系统与基于 LFSR 的生成器相结合,对混沌序列或 m 序列加入扰动。1989 年,Matthews[6] 最先提出将混沌理论应用于流密码。由于大部分基于混沌伪随机数发生器的流密码体制都是只使用单个混沌系统,这在计算机的有限数字精度下,其混沌特性存在明显的退化,从而使得生成的混沌序列退化为周期序列,而且实际生成的序列周期和密码学特征难以度量,导致实际结果与理论结果大相径庭。因此,有限精度效应是混沌序列从理论走向应用的主要障碍,单个混沌系统也几乎不再用来直接产生伪随机序列。文献[7,8]将多个混沌模型混合,该算法密钥空间大、对明文和密钥敏感,可以抵抗利用差分特性、统计特性和相空间重构对系统进行的攻击。但该算法选用多个混沌模型后,也同样导致计算量大增,仅适合于对安全性较高的场合。文献[9~11]在三维自治混沌系统的基础上构造了新的混沌系统。文献[12,13]对常见的 Logistic 映射进行改进构造了新的映射函数。文献[14]利用构造的分段非线性 Hybrid 映射,通过周期性地改变混沌迭代初值的办法来产生混沌序列,克服了序列有限精度效应的影响。这种通过改变常用混沌映射来构造新的混沌映射方法,常常需要对原有的映射函数进行升维或升级,这无疑大大增加了混沌映射的计算复杂度,并且使得混沌序列的理论分析更加困难。文献[15~18]用 m 序列与产生的混沌序列"异或"来克服有限精度的影响,通过伪随机序列加入扰动,使得混沌加密序列的周期更长、复杂度更高。但微扰是随机的,不易产生,而且系统分布以及相关性能取决于附加的 m 序列而不是混沌系统本身,参数的选择和判定目前也还存在一定的困难。文献[19,20]在构造复合混沌系统的基础上进一步通过变初值或变参数来克服有限精度的影响,是一种比较好的混沌伪随机序列产生方法。本文针对单混沌系统因计算机有限精度效应产生的混沌退化问题,从构造复合混沌系统的角度出发,提出了一种新的多级混沌映射交替变参数的伪随机序列产生方法。计算机仿真结果表明,该混沌系统生成的混沌序列具有良好的平衡性及自相关和互相关特性,并且产生的方法简单,具有较好的保密性。

1 预备知识

1.1 一维非线性 Logistic 混沌映射

Logistic 映射是典型的一维非线性离散混沌动力系统,由生

收稿日期: 2010-08-12; **修回日期**: 2010-09-18 **基金项目**: 国家自然科学基金委员会与中国工程物理研究院联合基金资助课题(10776007)

作者简介:李孟婷(1985-),女,湖北武穴人,硕士研究生,主要研究方向为通信网络与信息安全技术(limt1202@163.com);赵泽茂(1965-),男,教授,博士,主要研究方向为信息安全技术.

物学家 May 于 1976 年提出。其定义如下[21]：

$$x_{k+1} = \mu x_k (1 - x_k) \tag{1}$$

其中：$x_k \in (0,1)$，控制参数 $\mu \in (0,4]$。当 $3.5699456 < \mu \leqslant 4$ 时，由该映射产生的序列呈现出混沌态。

1.2　二维非线性 Henon 混沌映射

由于高维混沌系统的应用尚处于不成熟阶段，一维 Logistic 映射和二维 Henon 混沌系统是目前应用最广泛的两种混沌系统。Henon 映射二维非线性离散混沌系统，由天文学家 Henon 在 1976 年提出。其定义如下[22]：

$$\begin{cases} x_{k+1} = 1 + y_k - a x_k^2 \\ y_{k+1} = b x_k \end{cases} \tag{2}$$

其中：当 $1.05 < a < 1.8$，$b = 0.3$ 时，系统产生混沌现象。

2　混沌系统模型

由于单个混沌系统在计算机的有限数字精度下存在明显的退化，本文考虑用一维 Logistic 映射和二维 Henon 映射这两种迭代方程简单易实现的混沌系统来克服有限精度的影响，提出一种多级混沌映射交替变参数的伪随机序列产生方法。该方法并不需要两个或两个以上的 Logistic 方程联立进行升维，只需交替地改变 Logistic 映射的控制参数。Henon 映射直接产生的序列仍不是很理想的伪随机序列，并不适合直接作为密钥流序列对明文进行加密，因此用交错变参的 Logistic 映射的混沌迭代值的汉明重量来控制 Henon 映射输出的混沌迭代分量，改进 Henon 混沌序列的伪随机性能，使其满足均匀分布特性、随机统计特性和相关特性。

2.1　交替变参的多级混沌系统

基于一维 Logistic 映射和二维 Henon 映射，本文设计了一个参数交替变化的多级混沌系统如图 1 所示。

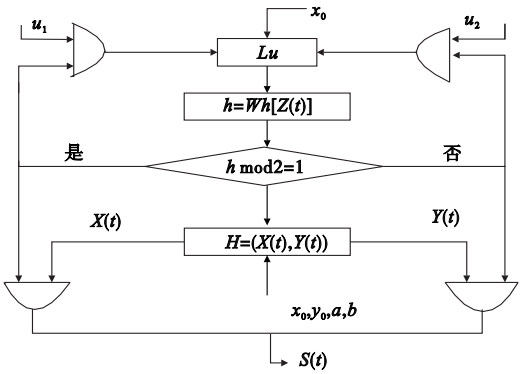


图1　基于参数交替变化的多级混沌系统

图 1 中，x_0、u_1、u_2 是 Logistic 映射的初值和参数；x_0、y_0、a、b 是 Henon 映射的初值和参数。一维 Logistic 映射 $x(i+1) = L^k(x(i), u)$，其中，k 是迭代级数，参数 u 在 u_1 和 u_2 之间交替变化。将 Logistic 映射的混沌序列 $x(t)$ 转换为二进制伪随机序列 $Z(t)$，如将实数 $|x(i)|$ 转换为 l 位二进制数 $w_{l-1}w_{l-2}\cdots w_1 w_0$，$w_i$ $(i = 0,1,\cdots,l-1)$ 的取值为 0 或 1。l 越大，表示数据的精度越高。$h = W_H[Z(i)] = W_H\{w_{l-1}, w_{l-2}, \cdots, w_1, w_0\}$，表示实数 $|x(i)|$ 的二进制序列 $\{w_i\}$ 的汉明重量。

L_u 中的参数 u 是这样控制在 u_1 和 u_2 之间来回切换的：当 $h \bmod 2 = 1$ 时，L_u 中使用参数 u_1；当 $h \bmod 2 = 0$ 时，L_u 中使用参数 u_2。同时，当 h 为奇数时，将 Henon 映射 $H(x(t), y(t))$ 中的 $x(t)$ 分量作为输出序列 $S(t)$；当 h 为偶数时，将 Henon 映射 $H(x(t), y(t))$ 中的 $y(t)$ 分量作为输出序列 $S(t)$。

这里，主要思想是用 Logistic 映射混沌值的二进制序列的汉明重量来控制 L_u 中参数的交替变换和 Henon 映射的输出分量，相当于用 Logistic 映射的输出来反馈控制 Logistic 映射的输入和 Henon 映射的输出。所以对于 Logistic 映射的二进制序列 $Z(t)$ 来说，即使当 Logistic 映射的某次迭代产生的 $x(t_2)$ 与之前的某次 $x(t_1)$ 相等时（其中 $t_2 > t_1$），与 $x(t_2)$ 对应的参数 $u(t_2)$ 也以 50% 的概率与 $x(t_1)$ 对应的参数 $u(t_1)$ 不相等。因此混沌序列要出现循环，当且只当某次的迭代状态与之前的相同而且要使其对应的参数也与之前的相同。对于 Henon 映射的输出序列 $S(t)$ 来说，每一时刻 h 的奇偶性都是不定的，所以 $H(x(t), y(t))$ 的输出分量也是无法预测的。用该变参的多级混沌系统产生的序列周期明显比单个 Logistic 映射和 Henon 映射产生的序列具有更高的安全性，且产生方法也比较简单。

2.2　混沌序列的二进制转换

将生成的实值混沌序列 $\{x(t)\}$ 转换为二进制伪随机序列 $\{S(t)\}$，方法如下：

a）将实数 $x(t)$ 的绝对值 $|x(t)|$ 用 l 位无符号定点小数来表示，即 $|x(t)| = w_{l-1}w_{l-2}\cdots w_i w_{i-1}\cdots w_1 w_0$。在实值量化的时候，用一位二进制数 w_k 表示 $x(t)$，这里 $k = 0,1,\cdots,l-2,l-1$，w_k 的取值为 0 或 1。l 越大，表示的数据精度越高。

b）对于实值混沌序列 $\{x(t)\}$，统一将其实值量化后的第 k 位二进制数 w_k（0 或 1）作为二进制量化序列 $\{w(k)\}$。

c）为了避免混沌序列产生自相关性，进一步增加算法的随机性，提高序列的抗破译能力，使得对初始条件的攻击无效，在使用量化二进制序列作加密运算的时候截掉序列的初始段和结尾段部分。假设序列 $\{w(k)\}$ 的长度为 L，任意取两个整数 N_1 和 N_2（$1 < N_1, N_2 < L$），截取这两个截点之间的二进制伪随机序列 $\{W(k)\}$ 为加密密钥序列，序列的长度为 $N_2 - N_1 + 1$。这样增加了混沌密钥序列的复杂性，提高了加密密文的安全性。该算法的保密性不但依赖于混沌系统的参数 u_1、u_2、a、b 和初始值 x_0、y_0，而且还依赖于两个截点 N_1、N_2 和特定量化位置 k。这样加密密钥为 $\{u_1, u_2, a, b, x_0, y_0, N_1, N_2, k\}$，密码分析就更加困难。

3　混沌伪随机序列的特性分析

3.1　保密性分析

对于单一的混沌映射来说，系统初始值可以利用非线性逆推方法来估计，某些系统参数可以利用混沌序列的统计特性来估计。再加上混沌序列实现时的有限精度效应的影响，单一映射的混沌序列存在着安全隐患。本文提出的组合映射模型有效地克服了一维映射的这一不足，同时作为控制序列输出的 Logistic 映射的参数是在两个给定的参数之间随机切换的。参数的切换原则又是根据 Logistic 映射输出实值的二进制序列的汉明重量来确定的，而单一的混沌序列本身就有比较理想的平衡性和相关性。因此，可以通过参数间的随机切换来提高保密性。

在实际通信过程中，窃听者要对截获的信息进行解密，必须掌握密钥序列的生成结构和变化规律。密钥序列的产生依赖的参数越多，系统的保密性就越好。组合映射要比单一映射复杂得多，控制密钥为 $\{u_1, u_2, a, b, x_0, y_0, N_1, N_2, k\}$，窃听者在解密过程中必须分析这多个参数及其切换信息，这使得密码分析就更加困难。同时对于单个的 Logistic 映射和 Henon 映射而言，其混

沌序列本身就具有初值敏感性,初值和参数的细微变化都会引起整个序列的巨大改变,攻击者很难通过对序列的分析找出序列产生的结构模型。因此,组合映射混沌序列的最大特点是增强了混沌序列的保密性,适合用于保密通信。

3.2　平衡性

取迭代初值 $x_0 = y_0 = 0.2, u_1 = 3.65, u_2 = 4, a = 1.4, b = 0.3$。通过计算机对大量混沌序列进行统计后发现其 0、1 个数确实不具规律性,但个数相差较少。统计结果如表 1 所示。

表 1　0、1 的个数

	40000	50000	60000	70000	80000
0	20172	25212	30182	35103	40106
1	19828	24788	29818	34897	39894

理论上,二进制伪随机序列 0-1 比计算公式如下:

$$r_{01} = \min_{L\to\infty}\frac{N_0(J)}{N_1(J)} = \frac{1-\iint_{00}^{LL} T_n(x,y)P(x,y)\,\mathrm{d}x\mathrm{d}y}{\iint_{00}^{LL} T_n(x,y)P(x,y)\,\mathrm{d}x\mathrm{d}y} = 1 \tag{3}$$

其中:$N_0(J)$ 和 $N_1(J)$ 分别表示二进制伪随机序列中 0 和 1 的个数,由此可以看出该序列有均衡的 0-1 比。

3.3　游程特性

对该二进制混沌序列进行游程统计,结果如表 2 所示。

表 2　输出序列的游程统计

	0	1	0/1	测试值	理论值
游程长为 1	10002	10087	0.991573	0.501423	0.500000
游程长为 2	5008	4993	1.003004	0.249626	0.250000
游程长为 3	2483	2421	1.025609	0.122404	0.125000
游程长为 4	1305	1296	1.006944	0.064921	0.062500
游程长为 5	610	623	0.979133	0.030776	0.031250
游程长为 6	305	315	0.968254	0.015475	0.015625
游程长为 7	168	154	1.090909	0.008037	0.007813
游程长为 8	65	69	0.942029	0.003345	0.003906

从表 2 中可以看出,不同长度的游程中,游程 0 和 1 的个数大致相等,且长度为 l 的游程总数大致占所有不同长度游程总数的 $1/2^l$。

3.4　相关特性

序列自相关函数的定义如下:

$$R(m) = \lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}(S_i - S_{\mathrm{mean}})(S_{i+m} - S_{\mathrm{mean}}) \tag{4}$$

互相关函数:

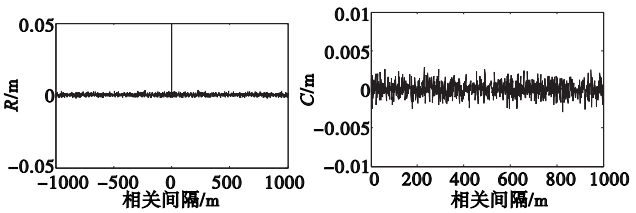
$$C(m) = \lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}(S_i - S_{\mathrm{mean}})(S_{i+m} - S_{\mathrm{mean}}) \tag{5}$$

其中:$\{s_i\}$ 和 $\{s_t'\}$ 为不同初值的两个二进制混沌序列,s_{mean} 为序列的均值。二进制混沌序列的自相关和互相关特性如图 2 所示。

在图 2 中,横坐标 m 是步长参数。图 2(a)中,当步长变化时,若自相关系数变化越小,说明对应的序列随机性越好。图 2(b)中,若互相关函数取值越接近 0,说明两个序列越互不相关,差异程度越大。从图中可以看出,该混沌二进制序列有尖锐的自相关和良好的互相关特性,具有类似 δ-like 的性质。

3.5　局部随机性统计检验

密钥序列如果要在加密体制中用于加密,除了要通过 Golomb 的三点随机性公设外,还要进一步作局部随机性检验,对序列的各个段落进行统计性检验。



(a)混沌序列的自相关特性　　(b)混沌序列的互相关特性

图2　混沌序列的自相关和互相关特性

设待测序列 $\{s_i\}$ 的长度为 L,其中 0 和 1 的个数分别为 L_0 和 L_1。定义检验的显著性水平 $\alpha = 0.01$。

1)单比特频数检验

单比特频数检验是检验一个比特序列中 0 和 1 的个数是否相等,相当于前面的 0-1 分布特性测试,只是这里采用的是数理统计的方法。利用统计量 $S = |2L_1 - L|/\sqrt{L}$,可算得 $S = 0.749\,533$,所对应的标准正态分布的接受水平 $P = 2\Phi(-S) = 0.453\,2$,大于显著性水平 0.01。说明待测序列中 0 和 1 的个数大致相同,通过测试。

2)单比特连续检验

单比特连续检验是检验序列产生算法的输出在 0 和 1 之间摆动的次数。首先从 $i = 1,2,\cdots,n-1$,计算摆动次数 $r(i)$。如果 $s_i = s_{i+1}$,则 $r(i) = 0$,否则 $r(i) = 1$。利用统计量

$$S = \sqrt{L}\left|\frac{L[1+\sum_{i=1}^{n-1} r(i)]}{2L_1[L-L_1]} - 1\right| \tag{6}$$

算得 $S = 0.454\,538$,所对应的标准正态分布的接受水平 $P = 2\Phi(-S) = 0.652\,8$,大于显著性水平 0.01,通过测试。

3)频谱检验

频谱检验是检验序列产生算法输出的离散傅里叶变换的峰值高度。首先将待测序列中的 0 和 1 分别转换成 −1 和 1,用 $\{x_i\}$ 表示新序列,其中 $x_i = 2s_i - 1$。对新序列进行离散傅里叶变换 $F = \mathrm{DFT}[\{x_i\}]$,计算 F 的前一半子序列 Z 的模值 $|Z|$ 和 95% 的峰值高度门限值 $T = \sqrt{3L}$,再计算小于 T 的期望峰值数 $N_0 = 0.475L$,最后统计 $|Z|$ 中小于 T 的实际峰值数 N_1。利用统计量 $S = |N_1 - N_0|/\sqrt{0.05N_0}$,算得 $S = 0.022\,942$,所对应的标准正态分布的接受水平 $P = 2\Phi(-S) = 0.984$,大于显著性水平 0.01,通过测试。

下面简单列出几种局部随机性检验的接受水平,如表 3 所示。

表 3　局部随机性检验

测试名称	接受水平	结果
单比特频率测试	0.453 2	success
分块频率测试	$0.975 < p < 0.99$	success
字频率测试	$0.25 < p < 0.75$	success
单比特连续测试	0.652 8	success
分组连续测试	$0.10 < p < 0.25$	success
频谱测试	0.984	success
非重叠字匹配测试	$0.25 < p < 0.75$	success

理论分析与统计结果表明,生成序列能够通过局部随机性能检验,是一种优良的伪随机序列,并且更加随机和不可预测,能够用于保密通信等领域。与单一的混沌系统相比,系统复杂度更高,也比较容易实现,同时序列的分析测试也更加困难。

4　结束语

一维混沌映射迭代产生的序列虽然有比较理想的平衡性和

相关性,但是复杂度不高,保密性不理想,因此在实际应用中应合理使混沌映射复杂化,以增强产生的混沌序列的保密性。本文混沌序列的产生方法是将一维 Logistic 映射和二维 Henon 映射这两种迭代方程简单易实现的混沌映射组合起来,组合的映射模型克服了单一映射可能存在的一些安全隐患,比单一映射产生的混沌序列更复杂,增加了预测难度,提高了保密性。此序列不仅有理想的平衡性,而且有良好的相关性,满足伪随机序列的各项特性要求,可作为密钥流序列用在加密体制中,是一类很有实际应用前景的伪随机加密序列。下一步的工作重点将放在对 Logistic 和 Henon 混沌序列改进方法的理论推导和算法优化上面,使序列产生算法的效率更高并更能有效地抵抗密码算法的攻击。

参考文献:

[1] FREY D R. Chaotic digital encoding: an approach to secure communication[J]. IEEE Trans on Circuits and Systems, 1993, 40(10): 660-666.

[2] STOJANOVSKI T, KOCAREV L. Chaos-based random number generators-part I: analysis[J]. IEEE Trans on Circuits Systems, 2001, 48(3): 281-288.

[3] STOJANOVSKI T, PIHI J, KOCAREV L. Chaos-based random number generators-part Ⅱ: practical realization[J]. IEEE Trans on Circuits Systems, 2001, 48(3): 382-385.

[4] 王育民. 混沌密码序列实用化问题[J]. 西安电子科技大学学报, 1997, 24(4): 560-562.

[5] 王继志, 王英龙, 王美琴. 一类基于混沌映射构造 hash 函数方法的碰撞缺陷[J]. 物理学报, 2006, 55(10): 5048-5054.

[6] MATTHEWS R. On the derivation of a "chaotic" encryption algorithm [J]. Cryptologia, 1989, 13(1): 29-42.

[7] FEI Peng, QIU Shui-sheng, MIN Long. An image encryption algorithm based on mixed chaotic dynamic systems and external keys[J]. IEEE Trans on Circuits Systems, 2005, 46(5): 1135-1139.

[8] 彭军, 廖晓峰, 张伟. 基于复合混沌系统的图像加密[J]. 计算机工程, 2006, 32(7): 34-36.

[9] 唐良瑞, 李静, 樊冰, 等. 新三维混沌系统及其电路仿真[J]. 物理学报, 2009, 58(2): 785-793.

[10] 王光义, 丘水生, 陈辉, 等. 一个新的混沌系统及其电路设计与实现[J]. 电路与系统学报, 2008, 13(5): 58-65.

[11] 许 , 刘崇新, 杨韬. 一种新型混沌系统的分析及电路实现[J]. 物理学报, 2010, 59(1): 131-139.

[12] 柳平, 闫川, 黄显高. 改进的基于 Logistic 映射混沌扩频序列的产生方法[J]. 通信学报, 2007, 28(2): 134-140.

[13] 张雪峰, 范九伦. 一种新的分段非线性混沌映射及其性能分析[J]. 物理学报, 2010, 59(4): 2298-2304.

[14] 罗启彬, 张健. 一种新的混沌伪随机序列生成方式[J]. 电子与信息学报, 2006, 28(7): 1262-1265.

[15] 周红. 有限精度混沌系统的 m 序列扰动实现[J]. 电子学报, 1997, 25(7): 95-101.

[16] ZHOU Liang-qiang, CHEN Fang-qi, CHEN Yu-shu. Chaotic behavior on reduction of perturbed KdV equation in form of parametric excitation [J]. Trans of Nanjing University of Aeronautics & Astronautics, 2007, 24(4): 283-287.

[17] 高洁, 袁家斌, 徐涛, 等. 一种基于混合反馈的混沌图像加密算法[J]. 计算机应用, 2008, 28(2): 434-436.

[18] 张雪峰, 范九伦. 基于线性反馈移位寄存器和混沌系统的伪随机序列生成方法[J]. 物理学报, 2010, 59(4): 2289-2297.

[19] 张巍, 李德华. 一种新的混沌序列生成方式[J]. 华中科技大学学报, 2001, 29(11): 64-66.

[20] 周志刚, 徐江峰, 李苏贵. 多级混沌映射变参数伪随机序列产生方法研究[J]. 数学的实践与认识, 2009, 39(3): 166-171.

[21] KOCAREV L, MAGGIO G M, OGORZALEK M, *et al*. Special issue on application of chaos in modern communication systems[J]. IEEE Trans on Circuits and Systems: Fundamental Theory and Applications, 2001, 48(12): 1394-1404.

[22] FRIDRICH J. Image encryption based on chaotic maps[C]//Proc of IEEE International Conference on Man and Cybernetic Computational. 1997: 1105-1100.

(上接第 337 页)

[3] AKYILDIZ I F, LEE W Y, CHOWDHURY K R. CRAHNs: cognitive radio Ad hoc networks[J]. Ad hoc Networks, 2009, 7(5): 810-836.

[4] VURAN M C, AKYILDIZ I F, LEE W Y, *et al*. Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey[J]. Computer Networks, 2006, 50(13): 2127-2159.

[5] ZHANG Xue-ying, LI Cheng. Constructing secured cognitive wireless networks: experiences and challenges[J]. Wireless Communications and Mobile Computing, 2010, 10(1): 50-69.

[6] MATHUR C N, SUBBALAKSHMI K P. Security issues in cognitive radio networks[M]//Cognitive Networks. 2007: 272-290.

[7] ARKOULIS S, KAZATZOPOULOS L, DELAKOURIDIS C, *et al*. Cognitive spectrum and its security issues[C]//Proc of the 2nd International Conference on Next Generation Mobile Applications, Services, and Technologies. 2008: 565-570.

[8] XUE Nan, ZHOU Xian-wei, ZHOU Jian. Self-behavior problems and security solutions in cognitive radio networks[J]. Journal of University of Science & Technology, 2009, 31(9): 1207-1212.

[9] CHEN Rui-liang, PARK J M, REED J H. Defense against primary user emulation attacks in cognitive radio networks[J]. IEEE Journal on Selected Areas in Communications, 2008, 26(1): 25-37.

[10] ZHU Li, ZHOU Huai-bei. Two types of attacks against cognitive radio network MAC protocols[C]//Proc of 2008 International Conference on Computer Science and Software Engineering. 2008: 1110-1113.

[11] KURODA M, NOMURA R, TRAPPE W. A radio-independent authentication protocol (EAP-CRP) for networks of cognitive radios[C]//Proc of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad hoc Communications and Networks. 2007: 70-79.

[12] XUE Nan, ZHOU Xian-wei, ZHOU Jian. A deception attack problem and its security solution in cognitive radio network[J]. Telecommunications Science, 2009, 25(5): 81-85.

[13] HU Fei, DONG De-Cun, XIAO Yang. Attacks and countermeasures in multi-hop cognitive radio networks[J]. International Journal of Security and Networks, 2009, 4(4): 263-271.

[14] BROWN T, SETHI A. Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: a multi-dimensional analysis and assessment[J]. Mobile Networks and Applications, 2008, 13(5): 516-532.

[15] STEINER M, TSUDIK G, WAIDNER M. Diffie-Hellman key distribution extended to group communication[C]//Proc of ACM CCS. [S. l.]: ACM Press, 1996: 31-37.