Hash差分攻击算法研究

周 林 韩文报 王 政
(解放军信息工程大学信息研究系 郑州 450002)

摘 要 Hash函数广泛应用于商业、军事等领域,因此对Hash算法的攻击在理论上和实际应用上都有重要的意义。自王小云教授提出差分攻击算法并攻破SHA-1,MD5,RIPEMD,MD4以来,对该算法的研究日益受到关注。然而王教授没有给出如何寻找差分和差分路径的方法。国内外专家都猜测她是靠非凡的直觉手工完成的,如何寻找差分和差分路径的方法成为关注的热点。构造差分路径涉及到如何处理差分循环移位和选择高概率的充分条件。业已证明,一般情况下,差分位移后有4种情况,并给出了4种情况的概率,最后比较了4种情况的概率。

关键词 MD5,Hash函数,差分攻击,隧道技术,多消息修正方法
中图法分类号 TP309 **文献标识码** A

Research of Differential Attack Algorithms to Hash

ZHOU Lin HAN Wen-bao WANG Zheng
(Department of Information Research, PLA Information Engineering University, Zhengzhou 450002, China)

Abstract Hash functions are widely used in business, military field etc. Therefore, the attack to Hash functions has important meaning in theory and in practical application. Since professor Wang proposed differential attack algorithm and succeeded to break SHA-1, MD5, RIPEMD, MD4, this algorithm has been paid more and more attention. However, Pro Wang do not supply the method to get difference and differential path. Experts at home and abroad guessed that she made it by hand with her outstanding intuition. Therefore, finding the method to get difference and differential path becomes hotspot. We must tackle the circle shift difference and select the high probability sufficient conditions when constructing the differential path. This paper verified there are four conditions and gave their probability and compared them with each other.

Keywords MD5, Hash functions, Differential attack, Tunnel technique, Multi-message modification method

Hash函数是密码学的重要分支,以SHA-1,MD5为代表的MDx系列Hash算法是最为典型的Hash函数,其应用也最为广泛。例如Hash算法在密码协议中具有重要作用。在密码协议设计中一般都使用随机预言模型,即假设所使用的Hash算法是安全的。Hash算法的安全性直接关系到密码协议的安全性。因此对Hash函数的安全性分析一直是密码界的热点。

自王小云教授给出第一组差分和差分路径并成功找到SHA-0,MD5,RIPEMD,MD4算法的碰撞[1,3,4,7]以来,如何寻找差分和差分路径的方法成为了国内外密码学家关注的焦点。在构造差分路径时,处理差分移位和选择高概率充分条件是一个重要的问题。Yu Sasaki于2006年利用穷举的方法证明了差分移位后有4种情况[8],Tao Xie对特殊情形证明了差分移位后有4种情况[9]。本文从理论上证明了差分移位后有4种情况,并给出了4种情况的概率,并在差分重量为1时,对4种概率进行了比较。

本文第1节概括了目前对MDx系列Hash算法的攻击算法并提出问题;第2节对问题进行了论证并得到了主要结果;最后总结了全文。

1 Hash差分攻击算法

Hash函数攻击算法大体可分为两类:通用算法(例如:生日攻击、中途相遇攻击和穷举攻击)和特定算法(例如:王小云的差分攻击、Dobbertin的代数攻击)。通用算法一般适用于对所有Hash算法进行攻击,特定算法只能针对某一个或某一类Hash算法进行攻击。通用算法攻击的复杂度一般都很大,例如假设Hash函数输出的消息摘要长为n,则利用生日攻击所需的运算量是$O(2^{\frac{n}{2}})$。MD5的消息摘要长是128,所以利用生日攻击所需的运算量是$O(2^{64})$,而使用差分攻击算法,目前最好的结果是只需$O(2^{10})$。

特定攻击算法是利用Hash函数的内在结构缺陷,找到Hash函数的弱点有针对性地进行攻击。例如H Dobbertin根据MD5中活动状态的高位bit不能尽快充分混淆,通过构造两个不同的512消息分组和选择初始IV值得到半自由初

到稿日期:2009-10-12 返修日期:2009-12-30 本文受863国家重点基金项目(2009AA012417),国家自然科学基金(2007B74)资助。
周 林(1986-),男,硕士,主要研究方向为网络密码分析、Hash函数分析、GPGPU、FPGA在密码学中的应用,E-mail:zhoulinpx@163.com;韩文报(1963-),男,教授,博士生导师,主要研究方向为密码学和信息安全;王 政(1975-),男,副教授,主要研究方向为网络密码分析、Hash函数分析、网络协议分析。

始碰撞。王小云的差分攻击算法也是根据 MSB(最高比特位)不能尽快充分混淆,找到有效的差分和差分路径成功攻击了 MD5,MD4 等算法[1]。

差分攻击算法一般分为 3 个步骤:

1)构造可以产生高概率碰撞的差分 ΔM;

2)推导出 ΔM 的差分路径 DP 和实现差分路径需要满足的充分条件 SC;

3)利用单消息修正方法、多消息修正方法、隧道技术、"分而治之"技术设计和优化搜索满足充分条件的碰撞消息对。

步骤 1)中,将 $\Delta M\neq 0$ 加上一个消息 M 可得到 M',为了使得 $h(M)=h(M')$,差分 ΔM 在压缩函数 f 中的扩散和混淆必须按照预先设定的路径进行并最后消失。步骤 2)就是要构造这样的差分路径 DP,并推出在什么充分条件下能得到这样的 DP,充分条件数决定整个攻击算法的运算复杂度。步骤 3)利用消息中的自由比特位,使用单消息修正方法[1]、多消息修正方法[6,7]、隧道技术[2]、"分而治之"技术来提高所构造的消息满足所有充分条件的概率。

由上面分析可知:差分算法的关键是对链变量差分的良好控制。以 MD5 为例,设 MD5 轮步骤为:

$$Q_{t+1}=Q_t+(f_t(Q_t,Q_{t-1},Q_{t-2})+Q_{t-3}+K_t+W_t)<<<S_t \tag{1}$$

$$Q'_{t+1}=Q'_t+(f_t(Q'_t,Q'_{t-1},Q'_{t-2})+Q'_{t-3}+K_t+W'_t)<<<S_t \tag{2}$$

式中,f_t,K_t,S_t 分别为第 t 步的轮函数、轮常数、移位数,Q_{t+1} 为当消息输入为 W_t 时的链变量,Q'_{t+1} 为当消息输入为 W_t' 时的链变量,为考察差分,将式(2)-式(1)得到:

$$(Q'_{t+1}-Q_{t+1})-(Q'_t-Q_t)=(f(Q'_t,Q'_{t-1},Q'_{t-2})+Q'_{t-3}+K_t+W'_t)<<<S_t-(f(Q'_t,Q'_{t-1},Q'_{t-2})+Q'_{t-3}+K_t+W'_t)<<<S_t$$

我们需要根据已知量:

$\delta f_t=f(Q'_t,Q'_{t-1},Q'_{t-2})-f(Q,Q_{t-1},Q_{t-2})$,$\delta Q'_{t-3}=Q'_{t-3}-Q_{t-3}$,$\delta W_t'=W_t'-W_t$,$\delta Q_t=Q'_t-Q_t$ 推出$(Q'_{t+1}-Q_{t+1})$的值。

2 循环移位差分及其概率计算

本节将第 1 节的问题归纳为定理 1 和推论 1。

定理 1 设 $m_1,m_2\in Z_{2^{32}}$,$0\leqslant s\leqslant 31$,$y=(m_1<<<s)-(m_2<<<s)$,$x=m_1-m_2 \bmod 2^{32}$,则:

$$y=\begin{cases} x<<<s \bmod 2^{32} & x+m_2<2^{32}\text{且}(m_2 \bmod 2^{32-s})+(x \bmod 2^{32-s})<2^{32-s};\\ (x<<<s)+1 \bmod 2^{32} & x+m_2<2^{32}\text{且}(m_2 \bmod 2^{32-s})+(x \bmod 2^{32-s})\geqslant 2^{32-s};\\ (x<<<s)-2^s \bmod 2^{32} & x+m_2\geqslant 2^{32}\text{且}(m_2 \bmod 2^{32-s})+(x \bmod 2^{32-s})<2^{32-s};\\ (x<<<s)-2^s+1 \bmod 2^{32} & x+m_2\geqslant 2^{32}\text{且}(m_2 \bmod 2^{32-s})+(x \bmod 2^{32-s})\geqslant 2^{32-s}; \end{cases}$$

且

$$P(y=x<<<s)=\frac{2^{32-s}-(x \bmod 2^{32-s})}{2^{32}}\cdot(2^s-\left\lfloor\frac{x}{2^{32-s}}\right\rfloor) \tag{3}$$

$$P(y=(x<<<s)+1)=\frac{(x \bmod 2^{32-s})}{2^{32}}\cdot(2^s-\left\lfloor\frac{x}{2^{32-s}}\right\rfloor-1) \tag{4}$$

$$P(y=(x<<<s)-2^s)=\frac{2^{32-s}-(x \bmod 2^{32-s})}{2^{32}}\cdot\left\lfloor\frac{x}{2^{32-s}}\right\rfloor \tag{5}$$

$$P(y=(x<<<s)-2^s+1)=\frac{(x \bmod 2^{32-s})}{2^{32}}\cdot(\left\lfloor\frac{x}{2^{32-s}}\right\rfloor+1) \tag{6}$$

证明:如果 $x+m_2<2^{32}$,即 $m_1\geqslant m_2$,则:$m_1=m_2+x$

$$\begin{aligned} y&=(m_1<<<s)-(m_2<<<s)\\ &=\left\{(2^sm_1 \bmod 2^{32})+\left\lfloor\frac{m_1}{2^{32-s}}\right\rfloor\right\}-\left\{(2^sm_2 \bmod 2^{32})+\left\lfloor\frac{m_2}{2^{32-s}}\right\rfloor\right\}\\ &=\left\{(2^s(m_2+x) \bmod 2^{32})+\left\lfloor\frac{m_2+x}{2^{32-s}}\right\rfloor\right\}-\left\{(2^sm_2 \bmod 2^{32})+\left\lfloor\frac{m_2}{2^{32-s}}\right\rfloor\right\}\\ &=2^sx \bmod 2^{32}+\left\lfloor\frac{m_2+x}{2^{32-s}}\right\rfloor-\left\lfloor\frac{m_2}{2^{32-s}}\right\rfloor \end{aligned}$$

若 $x \bmod 2^{32-s}+m_2 \bmod 2^{32-s}<2^{32-s}$,则:

$$\left\lfloor\frac{m_2+x}{2^{32-s}}\right\rfloor=\left\lfloor\frac{m_2}{2^{32-s}}\right\rfloor+\left\lfloor\frac{x}{2^{32-s}}\right\rfloor$$

$$y=2^sx \bmod 2^{32}+\left\lfloor\frac{x}{2^{32-s}}\right\rfloor=x<<<s$$

若 $x \bmod 2^{32-s}+m_2 \bmod 2^{32-s}\geqslant 2^{32-s}$,则:

$$\left\lfloor\frac{m_2+x}{2^{32-s}}\right\rfloor=\left\lfloor\frac{m_2}{2^{32-s}}\right\rfloor+\left\lfloor\frac{x}{2^{32-s}}\right\rfloor+1$$

$$y=2^sx \bmod 2^{32}+\left\lfloor\frac{x}{2^{32-s}}\right\rfloor+1=(x<<<s)+1$$

如果 $x+m_2\geqslant 2^{32}$,即 $m_1<m_2$,则:$m_1=m_2+x-2^{32}$

$$\begin{aligned} y&=(m_1<<<s)-(m_2<<<s)\\ &=\left\{(2^sm_1 \bmod 2^{32})+\left\lfloor\frac{m_1}{2^{32-s}}\right\rfloor\right\}-\left\{(2^sm_2 \bmod 2^{32})+\left\lfloor\frac{m_2}{2^{32-s}}\right\rfloor\right\}\\ &=\left\{(2^s(m_2+x-2^{32}) \bmod 2^{32})+\left\lfloor\frac{m_2+x-2^{32}}{2^{32-s}}\right\rfloor\right\}-\left\{(2^sm_2 \bmod 2^{32})+\left\lfloor\frac{m_2}{2^{32-s}}\right\rfloor\right\}\\ &=-2^s+2^sx \bmod 2^{32}+\left\lfloor\frac{m_2+x}{2^{32-s}}\right\rfloor-\left\lfloor\frac{m_2}{2^{32-s}}\right\rfloor \end{aligned}$$

若 $x \bmod 2^{32-s}+m_2 \bmod 2^{32-s}<2^{32-s}$,则:

$$\left\lfloor\frac{m_2+x}{2^{32-s}}\right\rfloor=\left\lfloor\frac{m_2}{2^{32-s}}\right\rfloor+\left\lfloor\frac{x}{2^{32-s}}\right\rfloor$$

$$y=2^sx \bmod 2^{32}+\left\lfloor\frac{x}{2^{32-s}}\right\rfloor-2^s=x<<<s-2^s$$

若 $x \bmod 2^{32-s}+m_2 \bmod 2^{32-s}\geqslant 2^{32-s}$,则:

$$\left\lfloor\frac{m_2+x}{2^{32-s}}\right\rfloor=\left\lfloor\frac{m_2}{2^{32-s}}\right\rfloor+\left\lfloor\frac{x}{2^{32-s}}\right\rfloor+1$$

$$y=2^sx \bmod 2^{32}+\left\lfloor\frac{x}{2^{32-s}}\right\rfloor+1-2^s=(x<<<s)+1-2^s$$

综上可知：

$$y=\begin{cases} x<<<s & \bmod 2^{32} & x+m_2<2^{32}\text{且}(m_2 \bmod 2^{32-s})+(x \bmod 2^{32-s})<2^{32-s}; \\ (x<<<s)+1 & \bmod 2^{32} & x+m_2<2^{32}\text{且}(m_2 \bmod 2^{32-s})+(x \bmod 2^{32-s})\geqslant 2^{32-s}; \\ (x<<<s)-2^s & \bmod 2^{32} & x+m_2\geqslant 2^{32}\text{且}(m_2 \bmod 2^{32-s})+(x \bmod 2^{32-s})<2^{32-s}; \\ (x<<<s)-2^s+1 & \bmod 2^{32} & x+m_2\geqslant 2^{32}\text{且}(m_2 \bmod 2^{32-s})+(x \bmod 2^{32-s})\geqslant 2^{32-s}; \end{cases}$$

设 A 表示事件“$x+m_2<2^{32}$”，B 表示事件“$(m_2 \bmod 2^{32-s})+(x \bmod 2^{32-s})<2^{32-s}$”，

$\Rightarrow$

$$P(y=x<<<s)=P(AB)=P(B)\cdot P(A|B)$$

$$=\frac{2^{32-s}-(x \bmod 2^{32-s})}{2^{32-s}}\cdot\frac{2^{32}-2^{32-s}\left\lfloor\frac{x}{2^{32-s}}\right\rfloor}{2^{32-s}\cdot 2^s}$$

$$=\frac{2^{32-s}-(x \bmod 2^{32-s})}{2^{32}}\cdot\left(2^s-\left\lfloor\frac{x}{2^{32-s}}\right\rfloor\right)$$

$\Rightarrow$

$$P(y=x<<<s+1)=P(A\overline{B})=P(\overline{B})\cdot P(A|\overline{B})$$

$$=\frac{(x \bmod 2^{32-s})}{2^{32-s}}\cdot\frac{2^{32}-2^{32-s}\left(1+\left\lfloor\frac{x}{2^{32-s}}\right\rfloor\right)}{2^{32-s}\cdot 2^s}$$

$$=\frac{(x \bmod 2^{32-s})}{2^{32}}\cdot\left(2^s-\left\lfloor\frac{x}{2^{32-s}}\right\rfloor-1\right)$$

$\Rightarrow$

$$P(y=(x<<<s)-2^s)=P(\overline{A}B)=P(B)\cdot P(\overline{A}|B)=$$

$$\frac{2^{32-s}-(x \bmod 2^{32-s})}{2^{32-s}}\cdot\frac{2^{32-s}\left\lfloor\frac{x}{2^{32-s}}\right\rfloor}{2^{32-s}\cdot 2^s}$$

$$=\frac{2^{32-s}-(x \bmod 2^{32-s})}{2^{32}}\cdot\left\lfloor\frac{x}{2^{32-s}}\right\rfloor$$

$\Rightarrow$

$$P(y=(x<<<s)-2^s+1)=P(\overline{A}\overline{B})=P(\overline{B})\cdot P(\overline{A}|\overline{B})$$

$$=\frac{(x \bmod 2^{32-s})}{2^{32-s}}\cdot\frac{2^{32-s}\left(\left\lfloor\frac{x}{2^{32-s}}\right\rfloor+1\right)}{2^{32-s}\cdot 2^s}$$

$$=\frac{(x \bmod 2^{32-s})}{2^{32}}\cdot\left(\left\lfloor\frac{x}{2^{32-s}}\right\rfloor+1\right)$$

推论 1 假设如定理，令 $x=2^k$，$0\leqslant k\leqslant 31$，则 $P(y=x<<<s)=\max(P(y=x<<<s),P(y=(x<<<s)+1),P(y=(x<<<s)-2^s),P(y=(x<<<s)+1-2^s))$

证明：若 $0\leqslant k<32-s$，则：

$$\left\lfloor\frac{x}{2^{32-s}}\right\rfloor=\left\lfloor\frac{2^k}{2^{32-s}}\right\rfloor=\left\lfloor 2^{k-(32-s)}\right\rfloor=0,$$

$$P(y=x<<<s)$$

$$=\frac{2^{32-s}-(x \bmod 2^{32-s})}{2^{32}}\cdot\left(2^s-\left\lfloor\frac{x}{2^{32-s}}\right\rfloor\right)$$

$$=\frac{2^{32-s}-2^k}{2^{32-s}}$$

$$P(y=(x<<<s)+1)$$

$$=\frac{(x \bmod 2^{32-s})}{2^{32}}\cdot\left(2^s-\left\lfloor\frac{x}{2^{32-s}}\right\rfloor-1\right)$$

$$=\frac{2^k}{2^{32}}\cdot(2^s-1)$$

$$P(y=(x<<<s)-2^s)$$

$$=\frac{2^{32-s}-(x \bmod 2^{32-s})}{2^{32}}\cdot\left\lfloor\frac{x}{2^{32-s}}\right\rfloor=0$$

$$P(y=(x<<<s)-2^s+1)=\frac{(x \bmod 2^{32-s})}{2^{32}}\cdot\left(\left\lfloor\frac{x}{2^{32-s}}\right\rfloor+1\right)=\frac{2^k}{2^{32}}$$

$\Rightarrow$

$$P(y=x<<<s)-P(y=(x<<<s)+1)$$

$$=\frac{2^{32-s}-2^k}{2^{32-s}}-\frac{2^k}{2^{32}}(2^s-1)$$

$$=\frac{2^{32}-2^{s+1+k}+2^k}{2^{32}}$$

因为 $0\leqslant k<32-s$ 所以 $k\leqslant 31-s$，则有：

$$P(y=x<<<s)-P(y=(x<<<s)+1)\geqslant\frac{2^k}{2^{32}}>0$$

$$P(y=x<<<s)-P(y=(x<<<s)-2^s+1)$$

$$=\frac{2^{32-s}-2^k}{2^{32-s}}-\frac{2^k}{2^{32}}$$

$$=\frac{2^{32}-2^{s+k}-2^k}{2^{32}}\geqslant\frac{2^{32}-2^{31}-2^k}{2^{32}}=\frac{2^{31}-2^k}{2^{32}}>0$$

若 $32-s\leqslant k\leqslant 31$，则 $x \bmod 2^{32-s}=0$，

$$P(y=x<<<s)=\frac{2^{32-s}-(x \bmod 2^{32-s})}{2^{32}}\cdot\left(2^s-\left\lfloor\frac{x}{2^{32-s}}\right\rfloor\right)$$

$$=2^{-s}(2^s-2^{k+s-32})=1-2^{k-32}$$

$$P(y=(x<<<s)+1)=\frac{(x \bmod 2^{32-s})}{2^{32}}\cdot\left(2^s-\left\lfloor\frac{x}{2^{32-s}}\right\rfloor-1\right)$$

$$=0$$

$$P(y=(x<<<s)-2^s)=\frac{2^{32-s}-(x \bmod 2^{32-s})}{2^{32}}\cdot\left\lfloor\frac{x}{2^{32-s}}\right\rfloor$$

$$=2^{-s}\cdot 2^{k+s-32}=2^{k-32}$$

$$P(y=(x<<<s)-2^s+1)=\frac{(x \bmod 2^{32-s})}{2^{32}}\cdot\left(\left\lfloor\frac{x}{2^{32-s}}\right\rfloor+1\right)$$

$$=0$$

则有：

$$P(y=x<<<s)-P(y=(x<<<s)-2^s)=1-2^{k-31}\geqslant 0$$

综上可知，结论成立。

推论 1 表明当输入差分重量为 1 时，选择式(3)能达到最大概率，且式(3)产生的差分重量最小，因此一般情况下式(3)是最佳选择。

结束语 王小云教授提出的差分攻击算法是目前 Hash 攻击算法中最为有效的方法。本文考察了差分攻击算法的基本思想，分析了循环移位差分及其概率，给出了当输入差分重量为 1 时循环移位差分概率之间的关系，为研究差分攻击算法提供了理论依据。

参 考 文 献

[1] Wang Xiaoyun, Yu Hongbo. How to Break MD 5 and Other Hash Functions[C]//Eurocrypt2005

[2] Klima V. Tunnels in Hash Functions: MD5 Collisions Within a Minute. Cryptology ePrint[R]. Archive 2006/105. 2006. http://eprint.iacr.org/

[3] Wang Xiaoyun, Feng Dengguo, Lai Xuejia, et al. Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. Cryptology ePrint Archive[R]. 2004/199. 2004. http://eprint.iacr.org/

[4] Wang Xiaoyun, Yu Hongbo. How to Break MD 5 and Other Hash Functions[C]//Ronald Cramer, ed. Advances in Cryptology-EUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science. Springer, 2005: 19-35

[5] McDonald C, Hawkes P, Pieprzyk J. Differential Path for SHA-1 with complexity O(2^{52}). Cryptology ePrint Archive[R]. 2009/328. March 2009. http://eprint.iacr.org/

[6] Zhang Meng, Sasaki Y, Naito Y, et al. Improved Collision Attack on MD5. Cryptology ePrint Archive[R]. 2005/400. November 2005. http://eprint.iacr.org/

[7] Wang Xiaoyun, Yin Y L, Yu H. Finding Collisions in the Full SHA-1. 2008

[8] Sasaki Y, Naito Y, Yajima J, et al. How to Construct Sufficient Condition in Searching Collisions of MD5[C]//Phong Q Nguyen, ed. VIETCRYPT, volume 4341 of Lecture Notes in Computer Science. Springer, 2006

[9] Xie Tao, Liu Fanbao, Feng Dengguo. Could The 1-MSB Input Difference Be The Fastest Collision Attack For MD5? Cryptology ePrint[OL]. http://eprint.iacr.org/

(上接第 76 页)

(1)染色体编码:采用二进制编码方式,将隐含层节点个数设定在 1～4,学习速率的范围在 0.2～0.8,动量因子的范围在 0.5～0.9。

(2)适应度函数选择:按下式计算各个体的适应度:

$$f=\frac{1}{F} \tag{7}$$

式中,$F=\sum_{i=1}^{l}e(i)^2$,$e(i)=y(i)-y_m(i)$,l 为样本数,$y(i)$为网络的输出值,$y_m(i)$为期望输出值,$e(i)$为两者之间的误差。

(3)根据上一代群体的适应度,利用遗传算法的 3 种遗传算子[选择、交叉、变异]得到下一代群体。

(4)将新一代群体插入到种群 p 中,并计算新一代群体的适应度。

(5)计算网络的误差平方和,若达到预定值 ε_{GA},则转(6),遗传优化操作结束;否则转(3),继续进行遗传操作。

(6)经过遗传操作后,选出适应度最高的个体将对应的隐层节点数、学习速率和动量因子赋给 BP 网络作为初值,网络可直接仿真。也可以进一步设置 BP 网络的训练参数,再进行 BP 训练,然后仿真。为使网络对输入有一定的纠错能力,还可利用不含和含有噪声的输入样本反复训练网络后再次仿真。

4.2 GA-BP 识别网络的设计与训练

本文调制识别分类采用基于 GA 算法的 3 层 BP 神经网络,网络输入的个数即为调制信号特征参数的个数 2,输出神经元的个数即为目标矩阵的维数 3,网络的训练函数取 traingdx 函数,隐含层和输出层神经元的传递函数均取为 logsig 函数。仿真中对 3 种数字调制信号采用统一的载频 f_c=40kHz,采样频率 f_s=400kHz。训练样本集为分别在理想条件下采样得到的 100 个样本及 SNR 值为 10dB 和 15dB 条件下进行采样得到的 100 个样本;测试样本集为分别在 SNR 值为 5dB 和 10dB 下进行采样各得到的 100 个样本。再对 GA 参数进行设置:初始种群设为 30;遗传代数设为 100;选择函数为 normGeomSelect,交叉函数为 arithXover,变异函数为 nonUnifMutation,交叉概率为 0.95,变异概率为 0.08,训练目标为误差小于 0.001。利用上述 GA 参数优化 BP 网络,得到最优化的结构参数,学习速率为 0.2593,动量因子为0.8747,隐层节点数为 3,其后利用训练样本集对 GA-BP 网络进行训练。最后,用测试样本集对所设计的神经网络识别系统进行仿真,根据仿真结果计算正确识别率,从而检验网络的识别性能。

4.3 GA-BP 调制识别网络仿真结果

当网络训练结束之后,分别用各 SNR 值下的测试样本对所得到的网络性能进行测试。为了验证遗传 BP 算法的分类效果,本文采用附加动量法的改进 BP 算法与之相比较。测试的结果分别如表 2 和表 3 所列。

表 2 采用改进 BP 算法网络性能测试结果

调制类型 \ SNR	5dB	10dB
2ASK	94%	97%
2FSK	91%	96%
2PSK	96%	98%

表 3 采用 GA-BP 算法网络性能测试结果

调制类型 \ SNR	5dB	10dB
2ASK	97%	99%
2FSK	96%	97%
2PSK	99%	100%

结束语 本文设计了一种基于软件无线电的 RFID 调制信号识别分类器。其中采用了改进的自适应阈值小波算法对调制信号进行优化消噪处理,并利用 GA 算法优化 BP 网络拓扑结构设计了一个识别分类器。仿真结果表明,采用这种方法,使网络对信号识别效率有了很大的提高,在 SNR 为 5 时识别准确率达到了 96%以上。提取更好的特征参数,提高整个系统的识别速率,以满足测试平台对实时性的要求,以及如何实现低信噪比环境下的识别,有待进一步研究。

参 考 文 献

[1] 彭艺,周正中,姚绍文. 基于计算机网络的下一代软件无线电[J]. 计算机科学,2003,30(03):9-12

[2] 杨宇,谢胜曙,何怡刚. 基于小波分析的 RFID 信号调制识别[J]. 微计算机信息,2009,25(2-2):185-186

[3] 谭晓衡,刘娟,胡友强. 一种新的低信噪比下的数字调制识别方法[J]. 系统工程与电子技术,2009,31(6):1520-1524

[4] 陈华丽,李裕能. 基于小波变换的自适应阈值消噪法[J]. 电力科学与工程,2003,3:8-10

[5] Nandi A K, Azzouz E E. Automatic identification of digital modulation types[J]. Signal Processing, 1995(47): 55-69

[6] Nandi A K, Azzouz E E. Algorithms of automatic modulation recognition of communication signals[J]. IEEE Trans. on Communication, 1998, 46(4): 431-436

[7] 黄勤,颜海松,李腩. 改进的遗传 BP 网络在旋转机械故障诊断中的应用[J]. 计算机科学,2008,35(8)