第 36 卷 第 1 期 计 算 机 工 程 2010 年 1 月
Vol.36 No.1 Computer Engineering January 2010
·安全技术· 文章编号：1000—3428(2010)01—0177—04 文献标识码：A 中图分类号：TN918.1

冗余方程对基于 Minisat 的代数攻击影响

卜 凡
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：分析基于 Minisat 软件的代数攻击方法，发现由该代数攻击方法对某些密码算法所建立的方程组中存在冗余方程，研究去除所有冗余方程的预处理方法，基于该方法提出先去除冗余方程，再利用 Minisat 软件求解无冗余方程组的代数攻击方法。实验结果表明，对 CTC 算法，新的攻击方法的攻击时间平均缩短了 1/2，冗余方程的存在降低了基于 Minisat 软件的代数攻击的效率。

关键词：代数攻击；非线性方程组；冗余方程；CTC 算法

Affection of Redundant Equations to Algebraic Attack Based on Minisat

BU Fan
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 This paper analyzes the method of algebraic attacks based on Minisat. It finds that the functions which are built from this method are redundant for some ciphers, gives a pretreatment method to throw off these redundancy functions and a method of algebraic attack based on this pretreatment and using Minisat to solve functions. Using this improved method, experimental results show that the method can cut down half time of one attack on average on CTC algorithm. These redundant functions make the algebraic attack based on Minisat becomes inefficient.

【Key words】 algebraic attack; non-linear system of equations; redundant equation; CTC algorithm

1 概述

代数攻击是采用基于代数思想的方法与技巧，将一个密码算法的输入输出及其各中间状态变量的关系归结为一个超定的多元高次方程组(即方程个数远大于未知量个数)，使得该密码算法的安全性完全依赖于求解多元高次方程组的困难性。

代数攻击首先是建立关于算法输入输出及各中间状态变量之间关系的方程组，而后解出方程组中所有变量的值从而恢复密钥。在建立关于算法的方程组的方法中，既有利用以算法中变换环节输入输出的各比特位为未知量来建立方程的方法[1-2]，也有利用以算法中变换环节输入输出比特块为未知量来建立方程的方法[3]；既有建立算法中变换环节的输出未知量关于输入未知量关系的显示表示的方法[4]，也有建立关于算法中变换环节的输入输出未知量关系的隐式表示的方法[1-2]。求解方程组的方法主要有线性化方法(包括直接线性化[5]、扩展线性化[6]等)、求 Gröbner 基(F4[7]、F5[8-9]算法等)的方法和转化为可满足性问题(SAT 问题)利用 SAT Solver 软件求解 SAT 问题从而求解方程组的方法[1, 10]。

目前，利用以算法中变换环节输入输出的各比特位为未变量来建立方程组，再将求解方程组的问题转化为 SAT 问题，进而利用 Minisat 软件求解 SAT 问题从而解得方程组的代数攻击方法已经实现对低圈的 DES[1]和 KeeLoq[11]算法的攻击。

本文介绍基于 Minisat 软件的代数攻击方法，分析该代数攻击方法所建立的方程组中存在的冗余方程的问题，给出去除方程组中所有冗余方程的方法，提出对基于 Minisat 软件的代数攻击的新方法，并通过实验说明该新方法的效果及冗余方程对基于 Minisat 软件的代数攻击方法的影响。

2 基于Minisat软件的代数攻击方法

2.1 方法介绍

文献[1]提出利用 Minisat 软件求解方程组的代数攻击方法，具体过程如下：

(1)建立以算法中变换环节输入输出的各比特位为未知量的方程组，其中算法的线性变换环节可直接建立以输入输出的各比特位为未知量的线性方程，非线性变换环节仅建立以输入输出的各比特位为未知量的低次非线性方程。

(2)将求解方程组的问题转化为 SAT 问题，进而利用 Minisat 软件求解 SAT 问题从而解得方程组。

该方法已经对 6 圈 DES[1]、KeeLoq[11]、CTC[2]和 CTC2[12]等算法进行了攻击实验。由于这些攻击实验建立的非线性方程均是低次非线性方程并且方法类似，因此本文仅以 CTC 算法为例分析基于 Minisat 软件的代数攻击方法所建立的非线性方程中存在的冗余方程问题。

2.2 方法分析

CTC 算法是 Courtois 为了验证所提出的代数攻击方法的正确性和有效性而提出的一个玩具分组密码算法。该算法采用 SPN 结构，分组长度 $3B$ ($1 \leqslant B \leqslant 128$)、密钥长度 $3B$ 和迭代圈数 N_r 均是可变的，圈函数包括圈密钥加、混乱变换和扩散变换，其中圈密钥加是将圈函数的输入与圈密钥逐比特“异或”，混乱变换是由 B 个 3 比特 S 盒并置构成，扩散变换是 $\{0,1\}^{3B}$ 到 $\{0,1\}^{3B}$ 上的线性变换。圈密钥仅是通过算法密钥循环移动若干比特位得到。

作者简介：卜 凡(1982－)，男，硕士研究生，主研方向：密码学
收稿日期：2009-06-08 **E-mail**：bufan1982@yahoo.cn

在 CTC 算法的圈函数中，圈密钥加变换和扩散变换都是线性变换，因此可以很容易得出这些变换的以输入输出比特位为未知量的线性方程；而混乱变换是由 B 个 3 比特 S 盒并置构成的非线性变换，其中代替表 S 盒为 $\{7,6,0,4,2,5,1,3\}$，即若 S 盒输入的 3 比特为 $x_3x_2x_1$，输出的 3 比特为 $y_3y_2y_1$，则 $y_3y_2y_1$ 是 S 盒中第 $4x_3+2x_2+x_1$ 个值对应的二进制数，文献[2]中基于 Minisat 软件的代数攻击方法建立了 14 个以 x_3,x_2,x_1,y_3,y_2,y_1 为未知量的二元域上的二次非线性方程，并基于这些方程利用Minisat软件对CTC进行了代数攻击实验。这些方程具体为

$$\begin{cases}
0=x_1x_2\oplus y_1\oplus x_3\oplus x_2\oplus x_1\oplus 1\\
0=x_1x_3\oplus y_2\oplus x_2\oplus 1\\
0=x_1y_1\oplus y_2\oplus x_2\oplus 1\\
0=x_1y_2\oplus y_2\oplus y_1\oplus x_3\\
0=x_2x_3\oplus y_3\oplus y_2\oplus y_1\oplus x_2\oplus x_1\oplus 1\\
0=x_2y_1\oplus y_3\oplus y_2\oplus y_1\oplus x_2\oplus x_1\oplus 1\\
0=x_2y_2\oplus x_1y_3\oplus x_1\\
0=x_2y_3\oplus x_1y_3\oplus y_1\oplus x_3\oplus x_2\oplus 1\\
0=x_3y_1\oplus x_1y_3\oplus y_3\oplus y_1\\
0=x_3y_2\oplus y_3\oplus y_1\oplus x_3\oplus x_1\\
0=x_3y_3\oplus x_1y_3\oplus y_2\oplus x_2\oplus x_1\oplus 1\\
0=y_1y_2\oplus y_3\oplus x_1\\
0=y_1y_3\oplus y_3\oplus y_2\oplus x_2\oplus x_1\oplus 1\\
0=y_2y_3\oplus y_3\oplus y_2\oplus y_1\oplus x_3\oplus x_1
\end{cases}\tag{1}$$

容易验证，方程组(1)的解为

$$\{(x_3,x_2,x_1,y_3,y_2,y_1):4y_3+2y_2+y_1=S(4x_3+2x_2+x_1),x_1,x_2,x_3\in\{0,1\}\}$$

如果将方程组(1)的 14 个方程从上到下依次编号为(1.1)~(1.14)，则发现(1.2)~(1.14)构成的方程组的解与方程组(1)的解相同，这说明方程(1.1)对于求解方程组(1)没有提供任何信息量，即(1.1)是冗余方程。事实上，我们发现仅由(1.2), (1.4)和(1.12)构成的方程组的解与方程组(1)的解相同，这说明方程组(1)中除了(1.2), (1.4)和(1.12)外的 11 个方程相对于(1.2)、(1.4)和(1.12)这 3 个方程来说都是冗余方程。

另一方面，基于 Minisat 软件的代数攻击方法在得到关于算法的方程组后，将求解方程组的问题转化为 SAT 问题，进而利用 Minisat 软件求解 SAT 问题从而解得方程组。在这个过程中，方程组中的方程数量越多，转化为 SAT 问题的规模就越大(包括变量个数、语句个数、语句总长度)，即 Minisat 软件运行时的输入规模就越大。由于冗余方程对于求解方程组不提供任何信息量并且去除冗余方程使得 Minisat 软件运行时的输入规模减小，因此笔者期望在得到关于算法的方程组后，通过去除方程组的冗余方程的方法来提高基于 Minisat 软件的代数攻击的速度。

3 冗余方程对基于Minisat代数攻击的影响

本文首先给出去除冗余方程的压缩查表法，基于压缩查表法给出基于 Minisat 软件的无冗余方程的代数攻击方法，最后通过对 CTC 算法的实验说明新的代数攻击方法的性能，进而分析冗余方程对代数攻击的影响。

3.1 去除冗余方程的压缩查表法

首先引入下面的概念:

定义 设 $f_1,f_2,\cdots,f_r$ 是二元域上的 n 多元多项式，则称使得 $f_1=f_2=\cdots=f_r=0$ 成立的未知量 $x_1,x_2,\cdots,x_n$ 的所有可能值构成的集合为 $f_1,f_2,\cdots,f_r$ 构成的方程组的解集，记为 $V(f_1,f_2,\cdots,f_r)$。若存在多项式 f_i，使 $V(f_1,f_2,\cdots,f_{i-1},f_{i+1},\cdots,f_r)=V(f_1,f_2,\cdots,f_r)$，则称 $f_i=0$ 是方程组 $f_1=f_2=\cdots=f_r=0$ 的冗余方程。

根据上述定义可直接得出判定方程组 $1\leqslant i\leqslant r, f_i=0$ 中 $f_t=0$ 是否为冗余方程的方法：穷举 $x_1,x_2,\cdots,x_n$ 得到方程组 $1\leqslant i\leqslant r, f_i=0$ 的解集 $V(f_1,f_2,\cdots,f_r)$；穷举 $x_1,x_2,\cdots,x_n$ 得到方程组 $1\leqslant i\leqslant r, i\neq t, f_i=0$ 的解集 $V(f_1,f_2,\cdots,f_{t-1},f_{t+1},\cdots,f_r)$，如果 $V(f_1,f_2,\cdots,f_r)\neq V(f_1,f_2,\cdots,f_{t-1},f_{t+1},\cdots,f_r)$，则 $f_t=0$ 不是冗余方程，否则 $f_t=0$ 是冗余方程。该方法每判定方程组中的 1 个方程就需要对 $x_1,x_2,\cdots,x_n$ 穷举一次，下面给出仅需对 $x_1,x_2,\cdots,x_n$ 穷举一次就能判定并去除方程组中所有冗余方程的方法。

定理 1 设 $f_1,f_2,\cdots,f_r$ 是二元域上的 n 多元多项式，则有

(1) $V(f_1,f_2,\cdots,f_r)=\bigcap_{i=1}^{r}V(f_i)$；

(2)如果 $\{g_1,g_2,\cdots,g_t\}\subseteq\{f_1,f_2,\cdots,f_r\}$，则 $V(f_1,f_2,\cdots,f_r)\subseteq V(g_1,g_2,\cdots,g_t)$。

定理 1 中的(1)说明方程组的解集可以通过先分别求出方程组中各方程的解集，再求它们的交集得到。具体地，对于方程 $f_i=0$，开辟 2^n 个存储单元 $tag[2^n]$，依次穷举 $x_1,x_2,\cdots,x_n$，如果 $x_1,x_2,\cdots,x_n$ 是 $f_i=0$ 的解，令 $tag[\sum_{i=1}^{n}2^{i-1}x_i]=1$；否则令 $tag[\sum_{i=1}^{n}2^{i-1}x_i]=0$。对于由 r 个方程构成的方程组，则需要开辟 $r\times 2^n$ 个存储单元 $tag[r][2^n]$ 来标记 r 个方程各自的解集。显然，方程组的解集就是 $\{(x_1,x_2,\cdots,x_n):\bigwedge_{t=1}^{n}tag[t][\sum_{i=1}^{n}2^{i-1}x_i]=1\}$。

去除方程组中所有冗余方程的思想为：对于 $1\leqslant i\leqslant r$，穷举计算方程 $f_i=0$ 的解并标记在数组 $tag[i][\,]$ 中；对于 $0\leqslant j\leqslant 2^n-1$，令 $V[j]=\bigwedge_{t=1}^{r}tag[t][j]$，则 $V[j]$ 标记出方程组 $1\leqslant i\leqslant r, f_i=0$ 的解集；记集合 $I=\{1,2,\cdots,r\}$，将去除 I 中 1 个元素后的集合记为 I'，对于 $0\leqslant j\leqslant 2^n-1$，计算 $U[j]=\bigwedge_{t\in I'}tag[t][j]$，则 $U[j]$标记出方程组 $i\in I', f_i=0$ 的解集；如果对于 $0\leqslant j\leqslant 2^n-1$，$U[j]$=$V[j]$均成立，则令 $I=I'$，继续去除 I 中 1 个元素得到 I' 后按同样的方法检验；只要 $U[j]$=$V[j]$对于 $0\leqslant j\leqslant 2^n-1$中的一个 j 不成立，则继续去除 I 中未曾检验过的 1 个元素得到 I' 后按同样的方法检验；最终，如果 I 中元素经检验均不能去除，则说明以 I 中元素为下标的方程构成的方程组为无冗余方程组。

在具体实现时，由于标记方程解集的数组 $tag[r][2^n]$, $V[2^n]$和 $U[2^n]$中各存储单元的取值仅为 0 或 1，因此可以将它们进行压缩存储，即利用 32 比特整型变量数组 $tagI[r][2^{n-5}]$ 来存储 $2^{n-5}\times 32=2^n$ 个比特，其中 $tag[t][j]=(tagI[t][u]>>v)\bmod 2$，“$x>>y$”表示 x 右移 y 比特位，$u=floor(j/32)$，$floor(x)$ 为下取整函数，$v=31-(j\bmod 32)$。这种方法不仅降低了算法所需的存储空间，还大大降低了算法的计算量。

综上所述，去除冗余方程的压缩查表算法如下:

输入 r 个方程 $f_1=f_2=\cdots=f_r=0$，其中 $f_1,f_2,\cdots,f_r$ 是二元域上的 n 元多项式

输出 方程组 $1\leqslant i\leqslant r, f_i=0$ 的无冗余方程组

(1)开辟 $r\times 2^{n-5}$ 的 32 比特无符号整型变量存储空间 $tagI[r][2^{n-5}]$，2^{n-5} 的32比特无符号整型变量存储空间 $VI[2^{n-5}]$ 和 $UI[2^{n-5}]$，并将 $tagI[r][2^n]$、$VI[2^{n-5}]$ 和 $UI[2^{n-5}]$ 均初始化为 0，令集合 $I=\{1,2,\cdots,r\}$。

(2)计算方程组中每个方程的解集。对于 $1\leqslant i\leqslant r$，依次执行：穷举 $x_1,x_2,\cdots,x_n$ 的所有可能取值，记 $u=\sum_{i=6}^{n}2^{i-1}x_i$，$v=\sum_{i=1}^{5}2^{i-1}x_i$，如果 $x_1,x_2,\cdots,x_n$ 是 $f_i=0$ 的解，则令 $tagI[i][u]:=tagI[i][u]+2^{31-v}$。

(3)计算方程组的解集。对于 $0\leqslant i\leqslant 2^{n-5}-1$，计算 $VI[i]=\bigwedge_{t=1}^{r}tagI[t][i]$。

(4)检测并去除冗余方程。令 $k=1$，$I'=\{1\leqslant i\leqslant r: i\neq k\}$。对于 $0\leqslant i\leqslant 2^{n-5}-1$，计算 $UI[i]=\bigwedge_{t\in I'}tagI[t][i]$。当 $UI[i]=VI[i]$ 对 $0\leqslant i\leqslant 2^{n-5}-1$ 均成立时，说明 $f_k=0$ 是冗余方程，此时令 $I=I'$，并将 k 增 1。如果 $k\leqslant r$，则返回步骤 4 检测下个方程 $f_k=0$ 是否为冗余方程，否则输出以 I 中元素为下标的方程构成的方程组，算法终止；

定理 2 去除冗余方程的压缩查表算法的存储复杂性为 $(r+2)\times 2^{n-5}$。

证明：去除冗余方程的压缩查表算法需要的存储空间为 $tagI[r][2^{n-5}]$，$VI[2^{n-5}]$ 和 $UI[2^{n-5}]$，故算法的存储复杂性为 $(r+2)\times 2^{n-5}$。

说明：如果直接利用冗余方程的定义去除冗余方程，则在检验方程 $f_k=0$ 是否为冗余方程时，需要穷举 $x_1,x_2,\cdots,x_n$，并检测 $x_1,x_2,\cdots,x_n$ 是方程组的解是否等价于它是去掉方程 $f_k=0$ 后的方程组的解，此时最大的穷举量是 2^n。但是，如果采用本文提出的压缩查表算法，只需穷举 $u=(x_6,x_7,\cdots,x_n)$，并检测 $UI[u]=VI[u]$ 是否对所有 u 成立即可，此时最大的穷举量是 2^{n-5}。因此，压缩查表算法也将计算复杂性降低为原来的 1/32。

3.2 基于Minisat软件的无冗余方程的代数攻击方法

在去除荣誉方程的压缩查表法基础上，基于 Minisat 软件的无冗余方程的代数攻击方法如下：

(1)建立以算法中各变换环节的输入输出的各比特位为未知量的方程组，其中算法的线性变换环节可直接建立以输入输出的各比特位为未知量的线性方程，非线性变换环节仅建立以输入输出的各比特位为未知量的低次非线性方程；

(2)对于算法中每个非线性变换环节对应的低次非线性方程构成的方程组，调用去除冗余方程的压缩查表法来去掉其中的冗余方程，其中去除冗余方程的压缩查表法尽量去除项数多的冗余方程，保留项数少的方程构成无冗余方程组，以进一步降低后续转化为 SAT 问题时产生的语句个数；

(3)将排除冗余后的方程组的求解问题转化为 SAT 问题，进而利用 Minisat 软件求解 SAT 问题从而解得方程组。

说明：对密码算法进行实际的代数攻击时，上述新方法的前两步均可作为整个代数攻击的预处理过程提前进行，再将无冗余方程组转化为 SAT 问题，这样就可以在得到 1 个或若干个明密对时，仅需将涉及到明密文的方程转化为 SAT 问题从而大大提高攻击效率。

3.3 性能评测

本文分别利用已有的基于 Minisat 软件的代数攻击方法和本文所提出的新方法对 CTC 算法做了大量实验。已有的基于 Minisat 软件的代数攻击方法[1-2, 10]是指建立了关于算法的方程组后直接转化为 SAT 问题，利用 Minisat 软件求解的方法，而新方法是指建立了关于算法的方程组后先去除冗余方程再将无冗余方程组转化为 SAT 问题，利用 Minisat 软件求解的方法。

实验环境为 Pentium 4 PC，主频 2.5 GHz、内存 256 MB, Minisat 2.0。实验情况总结如下：

(1)迭代圈数 $N_r=4$、每轮含 $B=40$ 个 S 盒的 CTC 算法，则密钥长度和分组长度均为 120 bit。在已知 1 个明密对和 85 个密钥比特的条件下，对剩余 35 bit 进行攻击。选取 50 个密钥及各密钥对应的 1 个明密对，分别利用已有方法和新方法进行攻击实验：使用已有方法时 Minisat 的平均求解时间为 99.44 s；使用新方法时 Minisat 的平均求解时间为 39.47 s；但是，其中 2 组实验中，使用已有方法时 Minisat 的求解时间小于使用新方法时 Minisat 的求解时间。新方法将攻击时间缩短了 1/2。

(2)迭代圈数 $N_r=6$、每轮含 $B=85$ 个 S 盒的 CTC 算法，则密钥长度和分组长度均为 255 bit。在已知 1 个明密对和 237 个密钥比特的条件下，对剩余 18 bit 进行攻击。选取 50 个密钥及各密钥对应的 1 个明密对，分别利用已有方法和新方法进行攻击实验：使用已有方法时 Minisat 的平均求解时间为 208.74 s；使用新方法时 Minisat 的平均求解时间为 147.1 s。新方法将攻击时间缩短了 1/3。

(3)迭代圈数 $N_r=6$、每轮含 $B=85$ 个 S 盒的 CTC 算法，则密钥长度和分组长度均为 255 bit。在已知 1 个明密对和 234 个密钥比特的条件下，对剩余 21 比特进行攻击。选取 20 个密钥及各密钥对应的 1 个明密对，分别利用已有方法和新方法进行攻击实验：使用已有方法时 Minisat 的平均求解时间为 1 601.43 s；使用新方法时 Minisat 的平均求解时间为 765.14 s。新方法将攻击时间缩短了 1/2。

(4)迭代圈数 $N_r=6$、每轮含 $B=85$ 个 S 盒的 CTC 算法，则密钥长度和分组长度均为 255 bit。在已知 1 个明密对和 233 个密钥比特的条件下，对剩余 22 bit 进行攻击。选取 20 个密钥及各密钥对应的 1 个明密对，分别利用已有方法和新方法进行攻击实验：使用已有方法时 Minisat 的平均求解时间为 3 209.76 s；使用新方法时 Minisat 的平均求解时间为 1 581.57s。新方法将攻击时间缩短了 1/2。

说明：新方法中去除冗余方程的时间在上述实验中都不超过 2 秒。在相同实验条件下，Minisat 的求解时间对不同的明密对差异很大，例如在实验(2)的 50 例实验中利用新算法时 Minisat 的求解时间最短为 20.6 s，最长为 292.7 s；同时虽然新方法在平均时间上比原有方法快，但针对个别明密对，使用新方法的求解时间比原方法求解时间长，如在实验(1)的 50 例中，有 2 例使用新方法的求解时间没有旧方法的快。实验(2)~实验(4)都未出现这种情况，即使用新方法的求解速度都比原有的方法快。

对 CTC 算法来说，本文所提出的新方法平均将攻击时间缩短了 1/2，这也说明新方法的合理性和有效性。因此，冗余方程的存在降低了基于 Minisat 软件的代数攻击方法的效率。

4 结束语

本文对基于 Minisat 软件的代数攻击方法进行分析时发现由该代数攻击方法对某些密码算法所建立的方程组中存在

冗余方程，提出了去除所有冗余方程的压缩查表法，基于该压缩查表法提出了先去除冗余方程再用 Minisat 软件求解无冗余方程组的代数攻击方法，利用新方法对 Courtois Toy Ciper(CTC)做了大量实验，实验结果表明对 CTC 算法来说，新方法的攻击时间平均缩短了 1/2，冗余方程的存在降低了基于 Minisat 软件的代数攻击方法的效率。

参考文献

[1] Courtois N T, Bard G V. Algebraic Cryptanalysis of the Date Encryption Standard[Z]. (2006-01-04). http://eprint.iacr.org/2006/402.

[2] Courtois N T. How Fast can be Algebraic Attacks on Block Ciphers?[Z]. (2006-05-20). http://eprint.iacr.org/2006/168.

[3] Courtois N T, Pieprzyk J. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations[Z]. (2002-11-12). http://eprint.iacr.org/2002/044.

[4] Courtois N T. Fast Algebraic Attacks on Stream Ciphers with Linear Feedback[C]//Proc. of Cryptology-Crypto’03. Santa Barbara, California, USA: Springer Verlag, 2003: 176-194.

[5] Courtois N T, Klimov A, Patarin J. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations[C]//Proc. of Cryptology-Crypto’00. New York, USA: Springer-Verlag, 2000: 392-407.

[6] Kipnis A, Shamir A. Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization[C]//Proc. of Cryptology-Crypto’99. Santa Barbara, California, USA: Springer-Verlag, 1999: 19-30.

[7] Faugere J C. A New Efficient Algorithm for Computing Gröbner Basis(F4)[J]. Journal of Pure and Applied Algebra, 1999, 139(1): 61-88.

[8] Faugere J C. A New Efficient Algorithm for Computing Gröbner Basis Without Reduction to Zero(F5)[C]//Proc. of ISSAC’02. Lille, France: [s. n.], 2002: 75-83.

[9] Seger A J M. Algebraic Attacks from a Gröbner Basis Perspectives[Z]. (2004-07-06). http://www.win.tue.nl/~henkvt/images/Report- SegersGB2-11-04.

[10] Bard G V, Courtois N T, Gregory C J. Efficient Methods for Conversion and Solution of Sparse Systems of Low-degree Multivariate Polynomials over GF(2) via SAT-Solvers[Z]. (2007-11-12). http://eprint.iacr.org/2007/024.

[11] Courtois N T, Bard G V, Wagner D. Algebraic and Slide Attacks on KeeLoq[Z]. (2007-12-10). http://eprint.iacr.org/2007/055.

[12] Courtois N T. CTC2 and Fast Algebraic Attacks on Block Ciphers Revisited[Z]. (2007-09-02). http://www.eprint,iacr.org/2007/152.

编辑　金胡考

（上接第 173 页）

参考文献

[1] Eschenauer L, Gligor V D. A Key-management Scheme for Distributed Sensor Networks[C]//Proc. of the 9th ACM Conference on Computer and Communications Security. Washington D. C., USA: ACM Press, 2002: 41-47.

[2] Cha W, Wang G, Cho G. A Pair-wise Key Agreement Scheme in Ad Hoc Networks[C]//Proc. of ICCS’04, Alabama, USA: [s. n.], 2004.

[3] Wang G, Cho G, Bang S. A Pair-wise Key Establishment Scheme without Predistributing Keys for Ad-hoc Networks[C]//Proc. of ICC’05. Seoul, Korea: [s. n.], 2005.

[4] Lee J S, Chang C C. Secure Communications for Cluster-based Ad hoc Networks Using Node Identities[J]. Journal of Network and Computer Applications, 2007, 30(4): 1377-1396.

[5] Koblitz N, Menezes A J, Vanstone S A. The State of Elliptic Curve Cryptography[J]. Design, Codes and Cryptography, 2000, 19(2/3): 173-193.

[6] Schneier B. Applied Cryptography Protocols Algorithms and Source Code[M]. 2nd ed. [S. l.]: John Wiley and Sons Inc., 1996.

编辑　金胡考

（上接第 176 页）

(3)在推荐因子的计算中，融入了分类结果。当出现恶意推荐时，通过信任向量的更新来降低推荐节点的某些属性值(如可靠性、历史推荐信誉度)，从而在下次推荐分类时，该类节点会从可信度高的分组中剔除，从而避免了恶意节点的再次影响(通常情况下，节点不会轻易放弃通过大量交互积累起来的多方面的信誉值，否则有可能得不偿失)。限于篇幅，此问题将在后续的研究中展开。

4　结束语

本文基于社会网络人际交互的特征，提出了基于动态推荐的信任评估模型。在获取推荐信任前，较为全面地考察了推荐节点的可信度，并根据不同交互目的动态选择推荐节点，从而可有效地避免推荐选择的盲目性，提高推荐的可靠性。

参考文献

[1] 郭　成，李明楚，姚红岩，等. P2P 网络下基于推荐的信任模型[J]. 计算机工程, 2008, 34(24): 157-159.

[2] Teacy W T L, Patel J, Jennings N R. TRAVOS: Trust and Reputation in the Context of Inaccurate Information Sources[J]. Autonomous Agents and Multi-Agent Systems, 2006, 12(2): 183-198.

[3] 赵铁柱，杨秋鸿，梅登华. 基于模糊集和灰色关联的 P2P 信任模型[J]. 计算机工程, 2009, 35(6): 173-175.

[4] 唐　文，陈　钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报, 2003, 14(8): 1401-1408.

[5] 田慧蓉，邹仕洪，王文东，等. P2P 网络层次化信任模型[J]. 电子与信息学报, 2007, 29(11): 2560-2563.

编辑　张正兴