一种轻量级动态密钥建立算法研究

姜丽芬[1],赵 新[2],李章林[2]
JIANG Li-fen[1],ZHAO Xin[2],LI Zhang-lin[2]

1.天津师范大学 计算机与信息工程学院,天津 300387
2.南开大学 机器人与信息自动化研究所,天津 300071
1.College of Computer and Information Engineering,Tianjin Normal University,Tianjin 300387,China
2.Institute of Robotics and Information Automatic System,Nankai University,Tianjin 300071,China

JIANG Li-fen,ZHAO Xin,LI Zhang-lin.Research on kind of light-weight dynamic cryptographic key establishment algorithm.Computer Engineering and Applications,2009,45(15):139-143.

Abstract: The ideal way to solve security in RFID and low-computing-capability devices is realizing a dynamic key establishment algorithm.But all the classical dynamic key establishment algorithms are unsuitable for RFID.According to limited computational resources of RFID tags and low-computing-capability devices,this paper aimed to designs a kind of light-weight dynamic cryptographic key establishment algorithm.Recently,a dynamic key establishment algorithm based on mutual learning between TPM neural networks,KKK algorithm,has given a light to light-weight dynamic key establishment algorithm.This study has covered the theory and development of KKK algorithm,and established its simulation environment. And base on these,the most of KKK-like algorithms are realized,and the experiment shows that this attacking algorithm is more effective than others.

Key words: Radio Frequency Identification(RFID);genetic attacking algorithm;Tree Parity Machine(TPM);dynamic cryptographic key;lightweight

摘 要: 解决射频识别(RFID)和低运算能力设备安全的理想方法就是实现一种动态密钥建立算法,但是经典的动态密钥建立算法都不适用于RFID。旨在研究一种为RFID标签和低运算能力设备提供动态密钥建立的算法。基于TPM的密钥建立算法为轻量级的动态密钥建立提供了方法,KKK算法就是其中一种算法。研究了KKK算法的原理以及KKK算法的发展现状,建立了KKK算法仿真环境,并且实现了已经提出的大部分KKK类算法;提出了一种具有更强攻击效果的攻击算法——改进的遗传攻击算法,实验结果表明该算法优于目前提出的其他攻击算法。

关键词: 射频识别;遗传攻击算法;TPM;动态密钥;轻量级
DOI: 10.3778/j.issn.1002-8331.2009.15.040 **文章编号:** 1002-8331(2009)15-0139-05 **文献标识码:** A **中图分类号:** TP393

射频识别(Radio Frequency Identification,RFID)技术是一种非接触式自动识别技术。RFID体积小、成本低,其运算能力有限,难以实现复杂的密码学算法。研究一种轻量级且具有较强安全性的动态密钥建立算法将可以有效地解决RFID安全问题。所谓动态是指,标签和读写器在每次会话开始前都首先建立一个会话密钥。采用动态会话密钥可以方便地同时解决RFID安全中的隐私和认证问题。动态建立会话密钥的另外一个好处是密钥管理变得简单, 这是由于RFID标签数量巨大,若采用每个标签一个静态密钥的方法,难以管理密钥。

密钥建立协议分为密钥传输协议和密钥协商协议[1]。密钥传输协议,使得一个参与方先获得(或建立)一个密钥,然后安全地传输给另一方。密钥协商协议中,双方共同提供信息,推导出一个共享密钥,任何一方不能够预先确定结果的值。基于对称加密的密钥传输协议一般需要参与方预先共享长期密钥,该方法对于RFID密钥建立不合适。Shamir的无密钥算法能够使得参与方在不需要预先共享秘密值的方式下将一方的密钥安全地传输到另一方,但是它需要模指数运算,对于RFID芯片来说运算量太大。基于对称密钥的密钥协商协议,例如Blom的对称密钥预分发系统也需要可信服务器和共享长期密钥。著名的Deffie-Hellman密钥协商是基于公钥的密钥协商协议,但公钥加密方案都难以在标签上实现。可见经典的密钥建立协议都不能够为RFID系统提供有效的密钥建立方法。

在RFID密钥建立方面,Claude Castelluccia[2]也提出了一个轻量级的方案,该方案将Noisy标签置于标签和读写器通信范围内,Noisy标签发出干扰信号,该信号加密了标签发送给读写器的密钥,这样敌手无法通过监听获知密钥。但是该方案要求Noisy标签和读写器共享长期密钥,这就降低了系统的安全性,且该系统使用起来也不够灵活。最近M.Volkmer等将一种

基金项目: 国家自然科学基金(the National Natural Science Foundation of China under Grant No.60674068);国家高技术研究发展计划(863)(the National High-Tech Research and Development Plan of China under Grant No.2006AA04Z304)。
作者简介: 姜丽芬,女,副教授;赵新,男,教授,博士生导师;李章林,男,博士。
收稿日期: 2009-02-12 **修回日期:** 2009-04-13

基于 TPM(Tree Parity Machine)神经网络互学习的密钥建立算法应用于 RFID 中[3]。该算法只需要使用简单(例如 10 以内的数)的加和乘运算,且不需要可信服务器和长期密钥,满足RFID密钥建立要求。它有可能为 RFID 等低运算能力设备的密钥建立提供解决方法。

1 TPM 的密钥建立算法及其发展现状

1.1 KKK 算法

最近 Ido Kanter 等提出了一种新的密钥建立算法[4],该算法基于一个新的现象:两个 TPM 神经网络经过互学习能够达到同步,互学习比敌手通过监听的单方学习要更容易同步。在神经网络互学习中,双方皆为老师和学生,没有固定的学习目标。该现象可以应用于密钥协商,双方随机选择初始秘密值,且互不知道秘密值,双方通过 TPM 的互学习使得秘密值达到同步,然后立即停止互学习,敌手难以也达到同步,此时秘密值可以作为密钥。该算法被称为 KKK 算法。

1.2 TPM 结构

如图 1 所示为一个 TPM 结构的神经网络,该神经网络是树状结构,各个树枝之间互不相关。设在 KKK 算法密钥协商系统中,参与方各使用一个 TPM 用于协商密钥,分别称这两个 TPM 为 A 和 B。敌手的 TPM 用 E 表示。不失一般性,规定 A、B 开始协商时,A 首先发送信息给 B。一个 TPM 包含 K 个隐藏单元($K\geqslant 1$),而隐藏单元又由输入端 X_k、权重 W_k、隐藏单元输出 Y_k 构成($1\leqslant k\leqslant K$),如图 1 所示(图中 K=3)。其中:

$$X_k=(x_{k,1},x_{k,2},\cdots,x_{k,N}),1\leqslant k\leqslant K \tag{1}$$

$$W_k=(w_{k,1},w_{k,2},\cdots,w_{k,N}),1\leqslant k\leqslant K \tag{2}$$

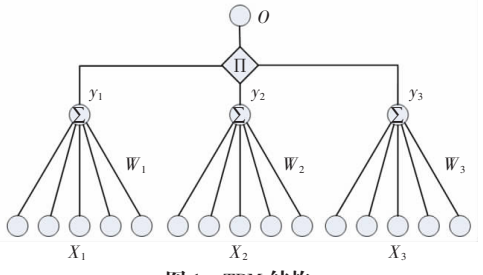

图 1 TPM 结构

N 为矢量长度($N\geqslant 1$)(图 1 中 N=5)。其中:

$$x_{k,j}\in\{1,-1\} \tag{3}$$

$$w_{k,j}\in\{-L,-L+1,\cdots,L\} \tag{4}$$

$$y_{k,j}\in\{1,-1\} \tag{5}$$

其中 L 为正整数。这样 K、N、L 共同构成了 TPM 的参数。另外设矢量:

$$\boldsymbol{X}=(X_1,X_2,\cdots,X_K) \tag{6}$$

$$\boldsymbol{W}=(W_1,W_2,\cdots,W_K) \tag{7}$$

$$\boldsymbol{Y}=(y_1,y_2,\cdots,y_K) \tag{8}$$

设第 k 个隐藏单元局部场(Local Field)为:

$$h_k=W_k\cdot X_k=\sum_{i=1}^{N}(x_{k,i}w_{k,i}) \tag{9}$$

则隐藏单元输出定义为:

$$y_k=sign(h_k)=sign\left(\sum_{j=1}^{N}(x_{k,j}w_{k,j})\right) \tag{10}$$

TPM 互学习有平行模式和反平行模式之分,设变量 τ=1 表示平行模式,τ=−1 表示反平行模式,当 h_k=0 时[4]:

$$y_k^A=1 \tag{11}$$

$$y_k^B=\tau \tag{12}$$

由于根据协商发起方,可确定了 A、B 的角色,所以 TPM 自身可确定采用式(11)还是式(12)。定义 TPM 的输出 O 为隐藏单元输出之积:

$$O=\prod_{k=1}^{K}y_k \tag{13}$$

1.3 算法过程

KKK 算法的执行过程是:开始时,A、B 各自以平均分布随机产生初始权重 W^A、W^B,双方互不知道初始权重。接着 A、B 进行多次互学习,互学习使得 W^A、W^B 趋于同步。一次互学习的步骤如下:

每次互学习 A、B 使用相同的输入矢量 $\boldsymbol{X}$,且每次互学习的 $\boldsymbol{X}$ 不同,$\boldsymbol{X}$ 以平均分布随机产生。$\boldsymbol{X}$ 是公开的,例如 $\boldsymbol{X}$ 可以通过卫星广播或者由一方产生并通过公开信道发送给另一方。此后 A/B 根据 $\boldsymbol{X}$、$W^{A/B}$ 计算 $O^{A/B}$,并将 $O^{A/B}$ 发送给对方。之后 A、B 根据 O^A、O^B 更新各自隐藏单元的权重 $W_k(1\leqslant k\leqslant K)$。当:

$$O^A=\tau\cdot O^B \tag{14}$$

$$O^{A/B}=y_k^{A/B} \tag{15}$$

同时成立时则进行更新。式(14)是所有隐藏单元更新的条件,式(15)是某个隐藏单元更新的条件。权重有三种更新方法[5]:

(1)Hebbian 学习

$$w_{k,j}\leftarrow w_{k,j}+O\cdot x_{k,j} \tag{16}$$

(2)Anti-Hebbian 学习

$$w_{k,j}\leftarrow w_{k,j}-O\cdot x_{k,j} \tag{17}$$

(3)随机游动(random walk)

$$w_{k,j}\leftarrow w_{k,j}+x_{k,j} \tag{18}$$

不管采用何种更新法,权重被限幅在[−L,L]内,即:如果 $w_{k,j}>L$,$w_{k,j}$ 被重置为 L;如果 $w_{k,j}<-L$,$w_{k,j}$ 被重置为−L。平行模式(τ=1)在 A、B 同步时有 $W^A=W^B$,而反平行模式(τ=−1)有 $W^A=-W^B$。

经过多次互学习以后 A、B 达到同步,A/B 可以通过式(14)连续成立的次数判断是否已达到同步。设同步时互学习次数为 t_{sync}。同步以后继续互学习将继续保持同步,但 W^A、W^B 动态变化。

1.4 基于 TPM 的密钥建立算法发展现状

自 KKK 算法提出以后,对该算法的攻击和完善一直没有停止,其安全性还未得到广泛地接受。Ido Kanter 等在提出 KKK 算法的同时也指出一种可能的攻击[4],敌手通过单方学习模仿参与者中的一方,期望在参与方同步时,敌手也能够同步,该攻击方法后来被称之为朴素(Naïve)攻击[6]或者简单(Simple)攻击[7],但是仿真结果表明朴素攻击不能有效地攻击 KKK 算法。Alexander Klimov 等[8]针对 KKK 算法提出了另外三种更有效的攻击方法:遗传(Genetic)攻击、几何(Geometric)攻击和概率(Probabilistic)攻击。遗传攻击指多个敌手同时进行单方学习,并对学习较成功的敌手进行遗传,对较不成功的敌手进行淘汰,仿真结果表明遗传攻击对参数 L 较小的 KKK 算法可以进行有效攻击。几何攻击又称为翻转(flipping)攻击,它只采用单个敌手但是改进了单方学习的更新方法,它对于 L 较小的 KKK 算法也可以进行有效攻击[5]。概率攻击通过 X 和 $O^{A/B}$ 来估计 $W^{A/B}$ 的概率分布,该攻击方法在后续文献中没有得到进一步研究。几何(Geometric)攻击的成功率随着 L 的增加呈指数下降,所以通过增加 L 可达到任意的安全要求。但是 L.N.Shacham

表 1　伪随机函数备选方案

伪随机函数	说明	rand( )	RAND_FLOAT( )	rand( )的 0/1 的个数(共 10^6 次)
VC rand 随机函数	VC 的 stdlib 的库函数 rand( )。它能够返回[0,32 767]的伪随机数	采用三个 rand( )函数的低 15 bit 拼接而成	采用 rand( )/32 768.0	16 000 138/15 999 862
Lehmer 随机函数[14]	Random( )产生周期为 $m-1$ 的平均分布随机浮点数,范围[1/m,1−1/m],其中 m=2 147 483 647	采用两个 Random( )×2^{16} 拼接而成	采用提供的 Random( )函数	16 005 896/5 994 104
Mersenne Twister 随机函数[15]	具有 $2^{19\,937}-1$ 的周期和 623-维度的均匀分布性。	采用提供的 BRandom( )函数	采用提供的 Random( )函数	15 995 393/16 004 607

等[9]提出了多数(Majority)攻击,该攻击法将几何攻击的单个敌手增加为多个敌手,且敌手间通过"投票"方式决定如何进行权重更新,仿真表明多数攻击的成功率不会随着 L 增加呈指数下降,这样 KKK 算法的安全性无法得到保障。A.Ruttor 等[10]提出改进的 KKK 算法——KKK-询问(KKK-Query)算法,KKK-询问算法选择能够产生绝对值为固定值的局部场 h_k 的 $\boldsymbol{X}$,该算法能够抵抗几何攻击和多数攻击,攻击成功率随着 L 增加呈指数下降。R.Mislovaty 等[11]提出 KKK-混沌(KKK-Chaotic)算法,KKK-混沌算法将混沌单元连接到隐藏单元输出,从而干扰敌手的学习,但是它不能够抵抗多数攻击[12]。于是 JianTao Zhou[12]等提出了 KKK-双混沌(KKK-Double-Chaotic)算法,相当于在隐藏单元输出链接两级混沌,从而能够达到同步所需步数小,抵抗多数攻击能力强的效果。

2　仿真环境的搭建和算法实现

计算机仿真是研究基于 TPM 的密钥建立算法的重要手段。在搭建仿真环境的基础上实现了各类算法,并验证各类算法实现的正确性,为后续改进算法的仿真正确性和可比性提供基础。

2.1　仿真环境搭建

由于考虑到仿真需要大量的计算,不采用 Matlab 作为仿真环境,而直接使用 C 程序进行仿真,使用 Microsoft Visual Studio 6.0(VC)编译环境。

仿真程序需要用到平均分布的伪随机函数,伪随机函数的特性好坏将会影响实验的结果。对此采用多个伪随机函数,如果多个伪随机函数得到相同的仿真结果,则可表明任意选择其中之一都是可以的。采用的伪随机函数备选方案如表 1 所示。

实验采用表 1 中不同的伪随机函数测试 KKK 算法的同步步数,结果如表 2 所示(<t_{sync}>表示 t_{sync} 的平均值)。由表 2 可知本文采用表 1 的伪随机函数得到基本相同的同步步数,且和文献[4]结果相同。这初步表明本文构建的仿真环境是正确的,KKK 算法的实现是正确的,且选择表 1 的任意伪随机函数都是可以的。由于 Mersenne Twister 伪随机函数具有较长的周期,后续实验采用 Mersenne Twister 伪随机函数。

表 2　采用不同伪随机函数时<t_{sync}>的比较

(K=3、L=3、平行模式、Hebbian 更新方法,10^5 次实验平均)

随机函数	VC rand 随机函数	Lehmer 随机函数	Mersenne Twister 随机函数	文献[4]结果
<t_{sync}>	463	463	464	466±4

图 2 说明<t_{sync}>和 N 成反比,而当 N 趋向无穷大时,<t_{sync}>趋向 410 左右。该现象表明 KKK 算法只需要密钥建立双方交换大约 410 bit 的数据,即可实现超长密钥建立。由图 2 知 N 越大 t_{sync} 的方差越小。

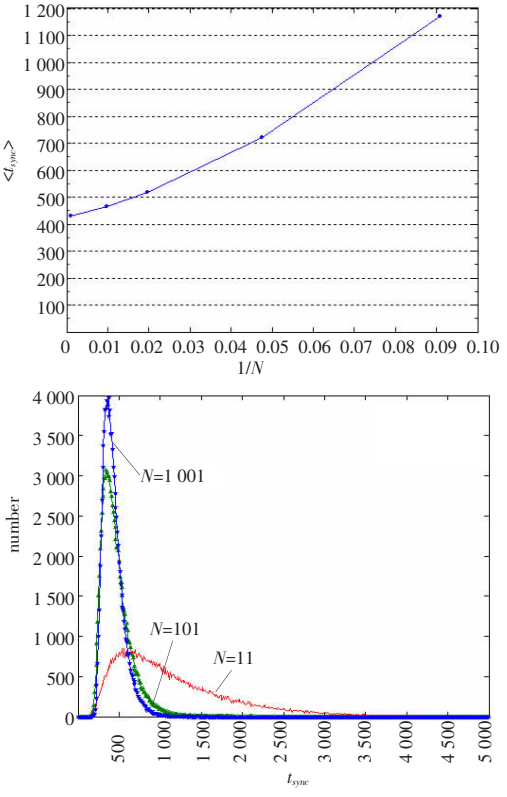

图 2　t_{sync} 和 N 的关系及 t_{sync} 分布直方图

(K=3、L=3、平行模式、Hebbian 更新方法,10^5 次实验平均,右图中曲线上的点(x,y)表示t_{sync} 落入[x,x+10)的实验次数为 y)

2.2　各类攻击算法的实现和比较

KKK 算法的攻击算法是指敌手通过监听 A、B 每次互学习的 $O^{A/B}$ 和 X,在 A、B 停止互学习时估计权重 $W^{A/B}$,如果估计正确则认为攻击成功。为了防止实验数据的波动,实验中常常认为:A、B 停止互学习时,当敌手有大于等于 98%的权重分量估计正确则认为攻击成功[13]。

将各类攻击算法按参与攻击的敌手的个数不同分为:单独攻击和联合攻击。单独攻击算法中只有一个敌手,该类算法包括朴素攻击和几何攻击;联合攻击是指多个敌手同时进行攻击从而提高攻击成功率,该类算法包括简单联合攻击、多数攻击、遗传攻击。由于篇幅有限,只详细论述遗传攻击算法。

遗传攻击算法简要描述[5]如下:设 M 为敌手数量的最大

值,初始时,敌手数量为1,接着在每步单方学习时进行遗传和淘汰:

(1)如果敌手数量小于等于 $M/2^{K-1}$,根据 O^A 得到 Y^A 的 2^{K-1} 种可能取值,将 $E_i(0\leqslant i\leqslant M)$复制$(2^{K-1}-1)$份,这样加上其自身每个敌手扩展为 2^{K-1} 个,这 2^{K-1} 个敌手的隐藏单元输出被设置为 Y^A 的 2^{K-1} 种可能值中的一个。然后每个敌手进行通常的权重更新。

(2)否则,进行淘汰。设 $N_{correct}^{E_i}$ 表示 $E_i(0\leqslant i\leqslant M)$在最近的 V 步(只包含 O^A、O^B 满足更新条件式(14)的步)单方学习中 $O^{E_i}=O^A$ 的次数。则 $N_{correct}^{E_i}$ 可以作为衡量 E_i 模仿成功与否的衡量标准-适应度函数。淘汰时,删除所有 $N_{correct}^{E_i}<U$ 的敌手。对于未淘汰节点进行一次单方学习。

(3)A、B 同步时,如果有任何敌手的权重和 W^A 有大于等于98%相同,则认为攻击成功。

这里选择 $V=20$,$U=10$[5]。实验中,初始时 $N_{correct}^{E_i}$ 为一个在[1,V]内平均分布的随机数。文献[5]并没有指定未淘汰节点单方学习方法,而文献[8]采用朴素攻击,分别对采用朴素攻击、几何攻击、多数攻击(多数攻击的"投票"只有未淘汰节点参与)进行实验,结果如表3所示。

表3　遗传攻击中的未淘汰节点单方学习方法比较

($K=3$,$N=1\ 000$,$M=100$,反平行模式,hebbian学习,10^3 次实验平均)

单方学习方法	攻击成功率($L=3$)	攻击成功率($L=12$)	攻击成功率($L=16$)
朴素攻击	0.004	/	/
几何攻击	0.884	0.315	0.054
多数攻击	0.779	0.164	0.032

表3说明采用几何攻击优于朴素攻击,这是因为采用几何攻击每个敌手能够进行更准确的模仿。多数攻击本身优于几何攻击,但在未淘汰节点单方学习中采用多数攻击反而成功率下降,并且随着 L 的增加并没有发生改变。这可能是因为遗传攻击需要染色体具有一定的多样性,而多数攻击减少了多样性。

将本文遗传攻击算法对KKK-询问算法进行攻击,攻击效果和文献[5]进行比较,如图3所示。本文实验结果和文献[5]的曲线形状基本相符,若将本文曲线向左平移0.1个单位则和文献[5]曲线吻合,误差可能由于KKK-询问算法实现时对 H 的精度取舍不同造成的。说明本文的遗传攻击算法实现是基本正确的。

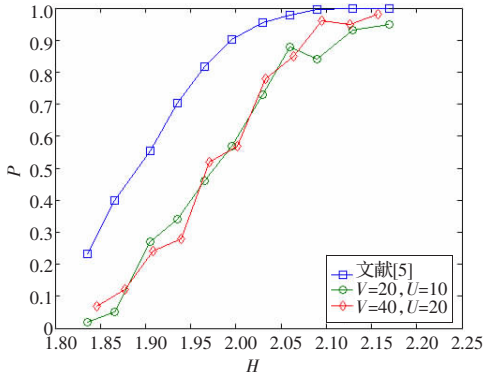

图3　遗传算法对KKK-询问算法攻击的成功率和 H 的关系

($L=6$,$K=3$,$N=1\ 000$,$M=4\ 096$,随机游动学习规则,100次试验。参考曲线为文献[5]的结果。实验结果的两条曲线分别采用 $V=20$,$U=10$ 和 $V=40$,$U=20$)

3　一种改进的遗传攻击算法

对于KKK算法的攻击成功性取决于能够在多大得程度上正确的模仿 A 的更新。所谓模仿 A 的更新是指在每一步与 A 更新相同的隐藏单元,这就需要 E 能够猜测 A 的隐藏单元。遗传算法的优胜劣汰的思想正和提高模仿程度的思路相符。关键是针对KKK类算法设计出高效的遗传算法适应度函数。对此,本文提出改进的遗传攻击算法。

3.1　算法描述

改进的遗传攻击算法描述如下:初始时,随机产生 M 个敌手,接着在每步单方学习进行以下步骤:

(1)如果更新第一条件式(14)不满足,不做任何操作。

(2)否则。如果步数小于 $t_{genetic}$ 或者是奇数步采用简单联合攻击,否则进行淘汰和遗传。

①淘汰:设 t 时刻敌手数量为 m,计算 t 时刻的适应度的均值和方差为:

$$N_{correct}^{mean}=\frac{1}{m}\sum_{i=1}^{m}N_{correct}^{E_i} \tag{19}$$

$$N_{correct}^{delta}=\sqrt{\frac{1}{m}\sum_{i=1}^{m}(N_{correct}^{E_i}-N_{correct}^{mean})^2} \tag{20}$$

淘汰:

$$N_{correct}^{E_i}<\lfloor N_{correct}^{mean}-Q_{genetic}N_{correct}^{delta}+0.5\rfloor \tag{21}$$

的所有敌手。并且保证淘汰以后敌手总数大于等于20个。

②遗传:更新 m 为淘汰以后的敌手数量,选择$\lfloor(M-m)/(2^{K-1}-1)\rfloor$个适应度最高的敌手进行遗传,且保证$\lfloor(M-m)/(2^{K-1}-1)\rfloor\leqslant m$。遗传方法和原遗传攻击算法相同。

③更新:对于没有淘汰和遗传的节点采用几何攻击更新权重。

(3)A、B 同步时,如果有任何敌手的权重和 W^A 有大于等于98%相同,则认为攻击成功。

实验时,取 $Q_{genetic}=1.85$(该值是通过实验求得的较佳值),取 $t_{genetic}=100$。适应度函数估计中 $V=40$。

改进遗传攻击算法主要在以下方面作了改进:

①初始敌手数量从1变为 M,这样增加了初始染色体的多样性。

②在 $t_{genetic}$ 步之前采用简单联合攻击,这样减小 t 较小时淘汰的盲目性。

③只有在偶数步才进行遗传和淘汰,使得每个敌手有一定的进化时间,从而有利于更加正确的判断适应度。

④采用更加准确的适应度函数。原算法采用 U 作为适应度衡量的阈值,显然随着 t 的增加,敌手整体性能提高,阈值应该随着 t 增加。本文根据当前敌手的整体水平采用动态阈值式(21),从而能够更加准确地进行淘汰。

⑤遗传和淘汰操作在每步都执行:原算法的遗传和淘汰操作分别在不同的步执行,且遗传占的步数比例较少,不利于快速进化。改进算法中,只要空间允许每步都进行遗传,加快了遗传。另外这也增加了内存空间的利用。

⑥将敌手分为三个等级:将每个敌手分为淘汰、几何攻击、遗传三个等级。

⑦增大 V。实验发现删除操作的准确性对算法性能影响很大,提高 V 有利于提高适应度函数的准确性。

3.2　实验结果

各类攻击算法的攻击效果如图4所示。从图4可以看出简单联合攻击、遗传攻击、几何攻击、朴素攻击的攻击性能依次减

弱。$1-(1-P_{flip})^M$ 代表对 M 次不同密钥建立的攻击,只做参考,不列入比较。

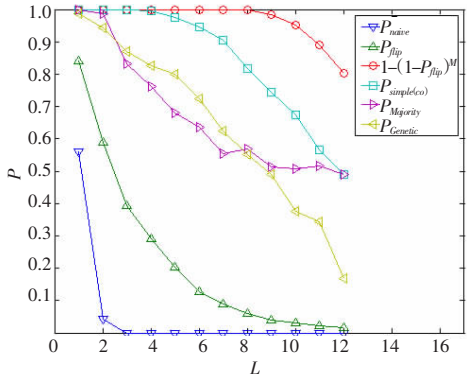

图 4　各类攻击成功率比较

(K=3,N=1 000,M=100,反平行模式,hebbian 学习,10^3 次实验平均次)

其中,多数攻击和其他攻击方法的显著不同点是多数攻击成功率随着 L 的增加并没有呈明显下降趋势。由于 KKK 算法通过 L 的增加提高安全性,这使得多数攻击成为目前对 KKK 算法最有威胁的攻击算法。

图 5 所示为改进的遗传攻击算法的攻击成功率和其他攻击算法的比较。实验结果表明改进遗传攻击算法优于图 4 中的所有攻击算法,且和多数攻击算法一样随着 L 的增加攻击成功率没有显著下降。

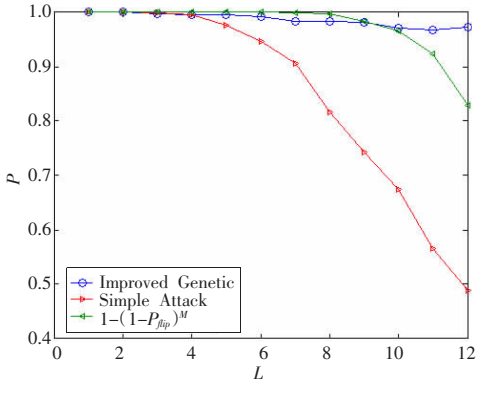

图 5　改进遗传攻击算法攻击成功率和其他攻击算法的比较

(K=3,N=1 000,M=100,反平行模式,hebbian 更新,实验次数为 10^3 次)

参考文献:

[1] Menezes A J,van Oorschot P C,Vanstone S A.应用密码学手册[M].北京:电子工业出版社,2005:437-483.

[2] Castelluccia C,Avoine G.Noisy tags:A pretty good key exchange protocol for RFID tags[C]//International Conference on Smart Card Research and Advanced Applications(CARDIS'06),2006:289-299.

[3] Volkmer M,Wallner S.Lightweight key exchange and stream cipher based solely on Tree parity machines[C]//ECRYPT(European Network of Excellence for Cryptology) Workshop on RFID and Lightweight Crypto,Graz University of Technology,Graz,2005:102-113.

[4] Kanter I,Kinzel W,Kanter E.Secure exchange of information by synchronization of neural networks[J].Europhys Lett,2002,57(1):141-147.

[5] Ruttor A,Kinzel W,Naeh R,et al.Genetic attack on neural cryptography[J].Phys Rev E,2006,73.

[6] Rosen-Zvi M,Klein E,Kanter I,et al.Mutual learning in a tree parity machine and its application to cryptography[J].Phys Rev E 66,2002,66.

[7] Ruttor A,Kinzel W,Kanter I.Dynamics of neural cryptography[EB/OL].(2006).http://arxiv.org/cond-mat/0612537.

[8] Klimov A,Mityaguine A,Shamir A.Analysis of neural cryptography[C]//Advances in Cryptology-ASIACRYPT'02,2002.

[9] Shacham L N,Klein E,Mislovaty R,et al.Cooperating attackers in neural cryptography[J].Phys Rev E,2004,69.

[10] Ruttor A,Kinzel W,Kanter I,et al.Neural cryptography with queries[EB/OL].(2005).http://arxiv.org/cond-mat/0411374.

[11] Mislovaty R,Klein E,Kanter I,et al.Public channel cryptography by synchronization of neural networks and chaotic maps[J].Phys Rev Lett,2003,91.

[12] Zhou Jian-tao,Xu Qin-zhen,Pei Wen-jiang,et al.Setp to improve neural cryptography against flipping attacks[J].International Journal of Neural Systems(IJNS),2004,14(6):393-405.

[13] Mislovaty R,Perchenok Y,Kanter I,et al.Secure key-exchange protocol with an absence of injective functions[J].Phys Rev E,2002,66.

[14] Park S,Miller K.Random number generators:Good ones are hard to find[J].Communications of the ACM,1988,31(10):1192-1201.

[15] Matsumoto M,Nishimura T.Mersenne twister:A 623-dimensionally equidistributed uniform pseudo-random number generator[J].ACM Transactions on Modeling and Computer Simulation,1998,8(1):3-30.

(上接 106 页)

[10] Padmanabhan V N,Subramanian L.An investigation of geographic mapping techniques for internet hosts[C]//Proc ACM SIGCOMM,San Diego,2001.

[11] Freedman M,Vutukuru M,Feamster N,et al.Geographic locality of ip prefixes[C]//Proceedings of ACM Internet Measurement Conference,Philadelphia,2005.

[12] Ren S,Guo L,Jiang S,et al.SAT-match:A self-adaptive topology matching method to achieve low lookup latency in structured P2P overlay networks[C]//Proc of the 18th Int'l Parallel and Distributed Processing Symposium(IPDPS 2004).New York:IEEE Press,2004.

[13] Zegura E W,Calvert K L,Bhattacharjee S.How to model an Internetwork[C]//Proc of the IEEE INFOCOM'96.New York:IEEE Press,1996:594-602.