一种基于图重写的计算机安全风险分析系统*)

李 娜[1] 谢冬青[1,2]
(湖南大学计算机与通信学院 长沙 410082)[1]
(中国科学院软件所计算机科学开放实验室 北京 100080)[2]

摘 要 基于项重写的安全风险分析的抽象规约模型在代数签名的基础上直接得到结果,没有提供相关攻击步骤明确描述,没有提供决策和攻击之间关系的统一视图,容易导致威胁的传播。为此,本文首先将图重写方案引入模型中,证明了引入图重写规则以后的风险分析系统仍然是终止的。然后利用图重写规则,提出了一种可以获得更优决策集合的方法,在改进的求带权二分图最小覆盖的方法的基础上,获得了一种具有相同时间复杂度和更高代价利益比的方法。整个模型高效、易于管理。

关键词 风险分析,图重写,终止,最小覆盖

A Computer Security Risk Analysis Model Based on Graph Rewriting System

LI Na[1] XIE Dong-Qing[1,2]
(College of Computer and Communication, Hunan University, Changsha 410082)[1]
(Laboratory of Computer Science, Institute of Software, The Chinese Academic of Sciences, Beijing 100080)[2]

Abstract The computer security risk analysis model bases on term rewriting comes out with the result immediately form algebra signature, ignoring the reduction procedure of related attack, providing no unified view of decisions and attacks, making it easy to propagation threat. This paper introduces graph rewriting into this model, and proves the new risk analysis system to be terminating. Also a new decision selection method is put forward with the help of the graph rewriting rule. Basing on the algorithm of the weighted vertex cover algorithm, this paper presents a new method of decision selection with the same time complexity and more benefit.

Keywords Risk analysis, Graph rewriting, Termination, Vertex cover

1 引言

由于通讯设施和协议的内在特点使得计算机网络环境不可避免地具有大量风险,如何评估和规避这些风险具有重要的意义。安全事件很大部分归因于技术管理的缺乏带来的弱点。因为系统结构过于复杂并且频繁,动态地变化,管理者很难做出决策,而且服务之间互相依赖,管理操作可能潜在的控制网络中的所有组件,攻击之间的交互,管理的不足可能出现大量的潜在弱点的传播,导致更多潜在威胁[1]。近来,风险分析成为研究的热点。风险作为威胁,弱点和资产价值的函数,反映了系统当前所处的安全状态。安全风险分析已经进入了以表达问题和方法空间的高度抽象为特征的第三个阶段。文[2]提出了一种安全模型,其中分成了三组安全信息:信息系统环境,信息系统和信息系统资产。模型指出了系统的当前安全状态。通过对信息系统潜在影响识别系统环境的威胁。文[3]提出了一种采用目录结构记录资产实体以及之间的关系,采用模型数据库来表示风险分析环境的方法,其中采用了自动化方式建立系统中关于威胁的网络结构。Mohamed 等人提出了一种自动化的风险管理方法[4],在定义的代数系统中将安全决策为攻击的逆元,在不涉及实现细节的情况下提出了在网络安全风险管理活动的代数规范。该规范包含签名和一组等式。并且证明了其决策选择过程的理论依据,即其中的决策集合是序关系。但是该方法仅仅建立了一个代数规范,其决策选择过程仍然无法自动化实现。于是 Mohamed 等人改进了这个方法引进了代数签名和代数重写系统[5]。该重写系统包含代数签名和一组代数重写规则。代数签名是由现实中抽象出来的数据对象的种类,和表示这些种类之间关系的谓词构成。该系统被证明是中止的并且会产生一个称为风险析等式的范式。该方法模拟了代价/利益比,提出了一个分步的代数解决方案。但是项重写的分析方法忽略了中间的推理过程。没有提供相关攻击步骤的明确描述,没有提供决策和攻击之间关系的统一视图,容易使决策者忽略攻击项和决策项之间的对应关系,导致威胁的传播。而这些问题都是项重写所不可避免的,所以我们考虑其他的方法。

图重写系统是项重写的衍生[6]。图提供了具有表现力的数据表示方法,其具有的一个明显优点是易读性,易于维护和修改[7]。由于其直观性和避免重复,结构化的图重写提供了更高的效率,更小的开销和广泛的应用[8]。本文引入图重写的方法,给整个分析过程提供了整体的视图和更方便的管理。并且在图重写的基础上找到一种更优的决策选择算法,证实了这种方法可以在相同的时间复杂度下产生更优的决策集。

2 图重写的风险分析系统

这里首先介绍了基于代数重写规则的风险分析系统,然后引入了图重写,以图重写的形式给出了重写规则,构造出基于图重写的风险分析系统。

2.1 基于代数重写规则的风险分析系统

该重写系统包含代数签名和一组代数重写规则。代数签名是由现实中抽象出来的数据对象的种类,和表示这些种类之间关系操作和谓词项构成。

*)基金项目:国家自然科学基金资助项目(No. 60373085)。李 娜 硕士生,主要研究领域为信息安全;谢冬青 教授,博士生导师,主要研究领域为信息安全。

一个多种类签名 $\Sigma=(S,\Omega,\Pi)$，S 表示种类名称的集合，Ω 表示形如 $S^* * S$ 的操作名集合，也就是各个客体具有的性质，Π 表示谓词项，以 S^* 形式表示客体之间的关系。该风险分析系统提供了 asset，vuln，attack，decision，sysenv，action 的种类名称[5]，ispresent，exploits，mitigates，$\subseteq$，$*$，Θ，$\oplus$，$\otimes$，$\Diamond$，$\circ$ 等操作名，还有 $\leqslant_{act}$。其中 ispresent 表示资产具有的弱点，exploits 表示攻击揭漏了哪些弱点，mitigates 表示决策可以移除攻击带来的危害，$\subseteq$ 表示攻击属于某一攻击场景，$*$ 表示两个攻击之间的组成关系，Θ，$\oplus$，$\otimes$ 是构成整个系统的连接符。

一个代数重写系统 $\rho=\langle T(\Sigma,x),\rightarrow\rangle$，$\rightarrow$ 是 $T(\Sigma,x)$ 上的二进制关系。代数重写规则部分如下：

$(\rho 1)ispresent(as,v)\Theta Exploits(at,v)\rightarrow at\Diamond as$
$(\rho 2)mitigates(d,at)\oplus at\Diamond as\rightarrow at\Diamond as\otimes d\circ as$
$(\rho 3)(at_1\Diamond as)\otimes(at_2\Diamond as)\rightarrow(at_1 * at_2)\Diamond as$
$(\rho 4)at_1\subseteq at_2\oplus(at_1\Diamond as\otimes at_2\Diamond as)\rightarrow at_1\Diamond as$
$(\rho 5)at * la\rightarrow at$
$(\rho 6)la * at\rightarrow at$
$(\rho 7)act\otimes act\rightarrow act$

2.2 利用图重写方法表示的风险分析规则

我们首先引入图重写系统。图重写作为项重写的一个衍生，将重写系统中的项作为有向图处理，相对普通的项表示法，图表示可以明确地表示出其共同拥有的相，而且因为不用将公共项多份复制，可以提高重写的速度，并且降低空间利用率[5]。

在项图中，我们用节点表示谓词和元素项，边表示与对应谓词相连的节点项。

现在对原系统中的部分规则实行图重写。

定义 1[8] 图重写步骤 $G\Rightarrow_{v,l\rightarrow r}H$ 是一个三步的执行过程。其中 $l\rightarrow r$ 是重写规则，v 是起始结点。$G=G-\{e\}$，e 是以 v 作为终点的边；把 v 标志 r 的根结点，在 G 中找到 l 的根结点，然后将其代换为 r；最后将无效结点删除得到图 G 的过程就是由项重写规则 $l\rightarrow r$ 转化为图重写规则的步骤。简记为 $\Rightarrow$。

按照重写规则[8]我们定义的新的决策分析等式中的关于识别攻击和攻击场景的部分可以重写为如图所示。

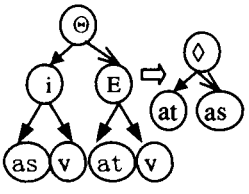

图 1 $i(as,v)\Theta E(at,v)\rightarrow at\Diamond as$

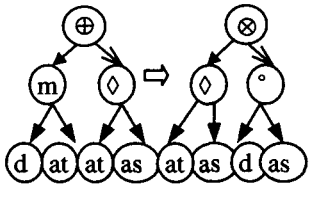

图 2 $m(d,at)\oplus at\Diamond as\rightarrow at\Diamond as\otimes d\circ a$

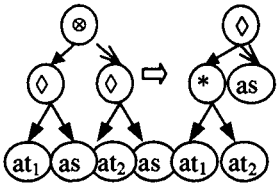

图 3 $(at_1\Diamond as)\otimes(at_2\Diamond as)\rightarrow(at_1 * at_2)\Diamond as$

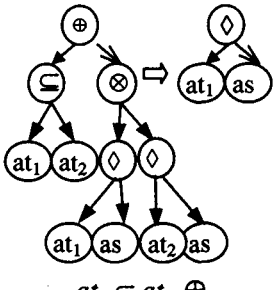

图 4 $at_1\subseteq at_2\oplus(at_1\Diamond as\otimes at_2\Diamond as)\rightarrow at_1\Diamond as$

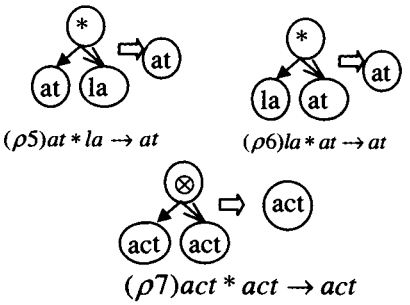

图 5 $\rho 5$，$\rho 6$，$\rho 7$ 对应的重写规则

这样就得到了图重写的风险分析系统，我们称之为 GRS-RA。

现在，分析一下引入了图重写之后，整个风险分析系统的性质。

首先是终止性。并不是所有的原本终止的项重写系统转化为图重写系统以后仍然是终止的。这里我们来证明本文所用的图重写系统是终止的。

定义 2[8] 回归路径序关系：设 $\supseteq$ 序关系，那么项图 TG 上的回归路径序关系定义如下：$G>_{rpo}H$ 如果：(1) $S>_{rpo}H$，或者 $S=H$，S 是 G 的直接子图，或者(2) 并且对于每个 H 中的直接子图 T 都有 $G>_{rpo}T$，或者(3) $top_G=top_H$ 并且 $sub_G>^{mul}_{rpo}sub_H$。其中 $M>^{mul}N$ 定义为如果 $x\subseteq M$，$N=(M-x)\cup y$，都有 $x>y$ 成立。

图重写系统如果不存在形如 $a_1\rightarrow a_2\rightarrow a_3\rightarrow\cdots$ 的无限序列，那么称其终止。$\rightarrow^*$ 表示 $\rightarrow$ 的传递闭包。如果对任意的 $b\leftarrow^* a\rightarrow^* c$，都存在 $b\rightarrow^* d\leftarrow^* c$，那么称之为合流的。

引理 1 如果 $>_{rpo}$ 是由一个严格序列关系引导的，对于规则集中的每一个规则 $l\rightarrow r$，都有 $L\Rightarrow_{root_L,l\rightarrow r}R$ 可以推导出 $L>_{rpo}R$ 那么 $\Rightarrow$ 是终止的。其中严格序列关系是指重写规则最顶端的运算满足反自反和传递性。

该引理在文[8]中已经得到证明。

定理 1 图重写系统 GRS-RA 是终止的。

证明：风险分析项重写系统 $\rho=\langle T(\Sigma,x),\rightarrow_p\rangle$ 是具有下面任一种形式的重写规则。

1. $t\varphi.t'\rightarrow t''\varphi.t'''$，$t,t',t'',t'''\in T(\Sigma,x)$，并且 $\varphi,\varphi'\in\{\otimes,\oplus,\Theta\}$。

2. $t\rightarrow t'$，t' 中没有变量。

3. $t\rightarrow t'$，都是 $t,t'\in T(\Sigma,x)$，并且 t' 是 t 的子项。

$\rho 1$，$\rho 2$，$\rho 3$ 属于第 1 类。$\rho 4$ 属于第 2 类，$\rho 5$，$\rho 6$，$\rho 7$ 属于第 3 类。先考察第 1 类情况。

对于 $t_1,t_2,t_3,t_4\in T(\Sigma,x)$，$\varphi,\varphi'\in\{\otimes,\oplus,\Theta\}$。$t_1\varphi.t_3\rightarrow t_2\varphi.t_4\in\rho$，定义 $\triangleright$ 关系为 $t_1\triangleright t_2$。

首先看第一部分规则：$\rho 1$ $\rho 2$ $\rho 3$ $\rho 5$ $\rho 7$。

看第 1 类规则。对于每个出现在第 1 类规则中的项 t_0 $[t_0]=\sum_{(t|t_0\triangleright t)}[t]$，可知：如果 $t_1\triangleright t_2$，那么 $\{t_2\mid t_2\triangleright t\}\subset\{t_1\mid t_1\triangleright t\}$，即 $[t_1]\geqslant[t_2]$。对 $\triangleright$ 运算采用多项式解释 $[\varphi](X_1,X_2)=X_1+X_2$，对任意规则 $t_1\varphi.t_3\rightarrow t_2\varphi.t_4\in\rho$，并且 $t_1\triangleright t_2$。在第 1 类规则中，每个项如果出现在规则右边，都没有出现在其他规则的左边。这样可以得到 $[t_1]>[t_2]$ 对于第 1 类规则中的每个规则都成立。

如果 $[t_1]>[t_2]$，$[t_2]>[t_3]$ 可以得到 $[t_1]>[t_3]$。这说明 $\triangleright$ 满足传递性。同时，由于 $[t_1]>[t_2]$，就有 $[t_1]<[t_2]$ 不成立。可以知道 $\triangleright$ 满足反对称性。由 $\triangleright$ 的定义可以知道其满足反自反性。所以 $\triangleright$ 运算满足反自反性，反对称性和传递性。

然后看第 2 类规则 $\rho 4$ 和第 3 类规则中的 $\rho 7$，作为 $t_1\varphi.t_3\rightarrow t_2\varphi.t_4\in\rho$ 的特殊情况，即 t_4 为空的情况，$t_1\triangleright t_2$。所以包括

了 $\rho1$ $\rho2$ $\rho3$ $\rho5$ $\rho7$ 的 5 个规则的图重写系统同样满足反自反性，反对称性和传递性。

然后考虑本项图重写系统。$\rho5$，$\rho6$，$\rho7$ 显然是满足回归路径序列的第 1 种情况。对 $\rho4$，令 $S=at_1 \diamond as \otimes at_2 \diamond as$，满足第 1 种情况。$\rho1$ 满足第 3 种情况，$\rho2$，$\rho3$ 满足第 2 种情况。所以本系统是回归路径序关系。

由引理 1 可知 $\triangleright$ 是良序关系，$>_{rp_0}$ 是由本规则集引导的。又根据上面的分析得知，每一个规则都满足 $L>_{rp_0}R$，那么由此，包含 $\rho1$ $\rho2$ $\rho3$ $\rho5$ $\rho7$ 的图重写系统满足引理 2，是终止的。

再看第二部分规则。对于，$\rho5$，$\rho6$，la 是幺元。因为包含 $\rho5$，$\rho6$ 的规则显然终止[9]，所以整个图重写系统是终止的。定理 1 得证。

对于合流性，如果⇒是由唯一范式的，那么当且仅当项重写系统是合流(confluent)的，其对应的项图重写是合流的。

这样，我们用图重写表示了代数重写系统，不仅避免了由项重写产生的视图分裂，带来了统一的视图，更会使决策者明了资产存在哪些对应攻击，以及攻击对应哪些资产。这种方法同样更有效地分析和解决了风险分析问题，同时也避免了由于忽略决策和攻击之间的对应关系带来的威胁传播。同时，二叉树结构的重写图可能给系统带来很多良好的性质。本文提出一种基于图的决策选择算法，提高了系统性能。

3 决策选择算法分析及改进

原有的决策选择系统的算法思想是在一个候选决策集合中按照决策出现的先后顺序，不断将可以使系统优化的决策，即开销小于收益的决策加入最后集合中。这样符合使系统效益最大化的原则，最后得到的结果也必然是可以使得系统获得效益的决策集。但是这种做法在各个决策解决的问题之间没有交集的时候，很好地解决了决策选择问题，但是当交集存在的时候，原有的算法根据决策在系统中出现的先后顺序，采纳先出现的决策，忽略了其中的差别，假如最后出现的决策是可以被选入决策集合最优决策，由于其解决的问题已经被前面出现的决策项解决，很可能被否定。

例 1 决策 a，b，c，代价分别是 4，9，12，对应攻击 1，2，解决后带来的收益是 8，10。决策 a 解决攻击 1，决策 b 解决攻击 2，决策 c 都可以解决。用项重写方法选择决策。

我们知道最后应选择决策 c，但是计算得知 a，b，c 的代价利益比分别是 0.5，0.9 和 0.667。样我们就会首先选择 a，然后剩下两个里会选择 b。这样当然是我们不希望看到的。我们尝试通过其他方法获得更为符合系统的最优解。

可以看出，决策集合之间各项没有关系，攻击项目集合之间各项也没有边相连，所以可以将其抽象成二分图问题。问题描述为：两个集合，攻击集 A 和决策集 B，每一个决策可能解决一个或多个攻击带来的问题。要求是在保证决策集的开销小于攻击集的损失，也就是消除了该攻击带来的收益的情况下，选择最小权值的最小覆盖(如果最小覆盖存在)[10]。

现在重新定义这个问题，并且提出 NDC 决策选择算法。设置每项决策的开销为 C_i，每个攻击被消除后带来的收益是 B_j，每项决策可以消除的攻击列为 0-1 矩阵 T，其中项 t_{ij} 表示第 i 项攻击是否可以由第 j 项决策解决，是则值为 1，否则为 0。X_i 则为第 i 项是否出现在决策集中的 0/1 变量。因为我们要使系统的收益减去开销的值最大化，所以这里维持另外一个数组 $E_i=\sum B_j \times t_{ij} - C_i$，其意义是对于单独的每一个决策项可以带来的收益与开销之差，也就是为系统带来的增益。

定理 2 该系统中仅存在决策开销小于决策收益的项。

证明：反证法，如果存在决策开销大于决策收益的决策项，那么去掉该决策时，系统会获得更大的收益。即系统中不存在决策开销大于决策收益的项。

图 G 是关于包括了攻击集合 V_a 和决策集合的 V_d 组成的顶点集合 V，对应关系 T，还有各个顶点的权值 B_j，C_i。Chosen 集合表示已经被选中的决策。

NDC 决策选择的算法描述：

输入：$G((V,T)B,C)$，$V=V_a+V_d$，

起始值：Chosen 集合为空，

算法：while(max(E(v_i)))>0}

$V_d=V_d-\{v_i \mid E(v_i)<0\}$；

利用重写规则建立 V_d 的关联矩阵 F；

if(deg $ree(F(v_i)))==0$}

Chosen=Chosen+v_i；

$V_d=V_d-v_i$

按照图着色法将 V_d 分为几个具有相同颜色的节点集合 L_1，L_2，$L_3 \cdots L_k$；

$L_i=\min\{i \mid \sum B(v_j)/\sum C(v_j), v_j \in L_i\}$；

Chosen=Chosen+v_i，$v_i \in L_i$；

$V_d=V_d-v_i$；

$V_a=V_a-\{v_i \mid T(V_i,V_j)==1\}$；

结果：Chosen

1. 每个存在的决策项都满足条件：决策开销小于决策收益。即 E_i 值>0，但是一个决策的收益可能是因为解决了多个攻击带来的，所以，如果同时有两个决策可以解决同一个攻击，如果其中一个被选入决策集，那么如果另外一个决策带来的收益应该减去已经解决的那个攻击所带来的收益。所以，我们可以同时选择的决策是彼此解决的攻击之间没有交集的决策。这样我们先引入图着色问题。引入另外一个图重写规则[7]，这样将产生一个只有决策项的图，成为决策关系图。在系统中与同一个攻击相连的决策项都有一条无向边相连。利用图的着色算法，求出图的着色方案。

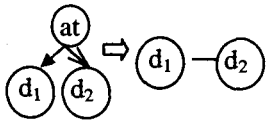

图 6 决策优化的图重写规则

2. 计算每种相同颜色的决策点的 E_i 之和。选出具有最大值的那一种颜色所对应的决策点。把这些决策点放入决策集合之中。

3. 对应这些决策点的邻接顶点，因为已选择决策点，其可以解决的攻击少了，其对应增益也肯定减少了。需要更改其 E_i 的值。即将已选决策顶点和对应解决的攻击从图中删除，将对应矩阵对应 t_{ij} 全部置 0，然后重新计算每个决策点的新 E_i 值。如果有决策点的 $E_i<0$，那么将该 E_i 对应的决策点删除。

例 2 决策 a，b，c，代价分别是 4，9，12，对应攻击 1，2，解决后带来的收益是 8，10。决策 a 解决攻击 1，决策 b 解决攻击 2，决策 c 都可以解决。用 GRS-RA 方法选择决策。

决策 a，b，c，代价分别是 3，8，12，对应攻击 1，2，解决后带来的收益是 8，10。决策 a 解决攻击 1，决策 b 解决攻击 2，决策 c 都可以解决。首先看图着色之后分 2 种颜色，决策点 a，b 是一种，决策点 c 是第二种。分别计算它们的增益和，为 5，6。这样显然选择的是后者，即第 3 个决策。

先看一下这个算法的时间复杂度：

假设原图中每个节点最大的度为 p，决策项有 m 个，攻击项有 n 个。计算的整体的时间复杂度 $O(m^2 \times n)$。原有算法的时间复杂度也是 $O(m^2 \times n)$。这样在同等的时间复杂度下就需要比较这两种方法的效果了。

4 实验结果分析

在matlab的环境下，对输入G中V_a和V_d的个数作为观察对象，对B_i和C_i在0～5内随即取浮点数值，分别用两种算法取每十次随机试验结果的平均值，得出数据绘图如图7、8所示。

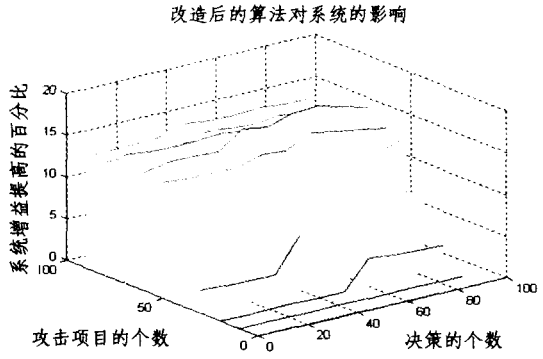

图7 决策和攻击项个数对新决策选择算法的影响

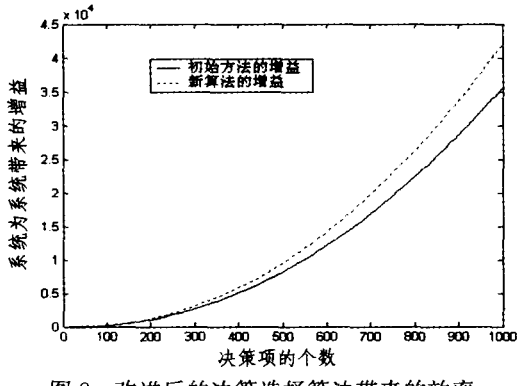

图8 改进后的决策选择算法带来的效率

图7中，取决策的个数从10到100，攻击的个数从10到100，由10次随机试验的结果平均得到，以NDC决策选择算法的比原有决策选择算法的增益提高的百分比考察本文算法对系统的增益，可以知道，

1. 随着攻击项和决策项个数的增加系统增益明显增加。

2. 决策项个数相同的条件下，攻击项目的增加对系统增益影响较大。攻击项目的个数一定时，决策个数的增加对系统效能的增加不会有很大影响。

3. 决策项目个数的增加在数量较少的情况下对系统影响增长较快。决策项个数大于攻击项个数的时候系统的增益有所提高。

4. 当系统中的攻击项和决策项的个数达到50以后，系统增益稳定在10%以上。

现实中可以使用的决策个数很多，再分析上述结果的基础上，图8选择考察本算法中决策项的个数增加对系统增益的影响，选择每5次随机试验的平均结果。纵坐标表示选择的决策集合对系统整体的增益。随着决策个数的增加，选择的决策集合能够更大地增加系统性能。可以看出，随着影响因素的增加，也就是决策集中决策的数目和攻击的数目的增加，系统的增益呈现上升趋势。并且维持比例不断增加。当系统中的影响因素达到500以上的时候，系统增益在15%左右。

所以整个改进的算法可以很大程度上提高决策集的效果，使得选择的决策集为系统带来更大的利益。

总结 针对风险分析纷繁复杂，难于掌握和控制，本文在改进已有的风险分析模型的基础上引入图重写系统，提供了攻击步骤以及决策和攻击之间关系的描述，潜在地避免了威胁的传播，使得其简单高效，便于观易于管理。提高了系统的整体性，提供了统一的视图。同样利用图重写系统，在改进二分图的最小覆盖算法的基础上，利用图着色法获得了更优决策集选择方法。随着系统决策个数增加能够增大算法带来的增益提高比例，并保证在系统中决策个数达到一定数目时有较大的增益提高。使得系统在相同的时间复杂度内大幅度的提高了可获得的利益。为风险分析提供了一个很好的方法，有效提高了系统的整体效能。

参 考 文 献

1 Rothmaier G, Pohl A, Krumm H. Analyzing Network Management Effects with SPIN and cTLA. IFIP world computer conference. Toulouse, France, 2004
2 Anderson A, Longley D, Kwok Lam-for. Security Modelling for Organisations. ACM Conference on Computer and Communications Security. Fairfax, Virginia, USA 1994
3 Kwok Lam-for. Longley Dennis. Security Modelling for Risk Analysis. IFIP world computer conference. Toulouse, France, 2004
4 Hamdi M, Bourdriga N. Algebraic Specification of Network Security Risk Management. First ACM Workshop on Formal Methods in Security Engineering, Washington D. C. 2003
5 Hamdi M, Bourdriga N. An Abstract reduction model for computer security risk. IFIP world computer conference. Toulouse, France, 2004
6 Corradini A, Gadducci F. Categorical rewriting of term-like structures. Electronic Notes in Theoretical Computer Science 51. Elsevier Science B. V. 2002. 3～6
7 Blostein D, Fahmy H, Grbavec A. Practical Use of Graph Rewriting: [technical report]. Kingston, Ontario, Canada: Queens University. 1995
8 Plump D. Term Graph Rewriting. In Handbook of Graph Grammars and Computing by Graph Transformation, World Scientific, 1999, 2(1): 3～61
9 Kruskal J B. Well-quasi-ordering, the Tree Theorem, and Vazsonyi's conjecture. Transactions of the American Mathematical Society, 95, May 1960. 210～225
10 杨继峰，孙永强. 项重写的图实现. 计算机工程，1998(4)：3～6
11 Bar-yehuda R, Even S. A Local-Ratio Theorem for approximating the weighted vertex cover problem. Annals of Discrete Mathematics, 1985. 27～46

(上接第262页)

发和维护两方面对事务工作流应用系统的关注、关注之间的实现以及关注实现编织过程进行描述。在采用基于面向方面开发的软件体系结构实现的软件系统中，当系统需求的任何一方面关注发生变化时(不论是流程定义、活动定义、事务定义，还是参与者)，只需要对该关注重新实现，然后与其他方面关注已有的实现再一次进行编织，就完成了系统的维护与更新，这种实现和编织都可以借助软件开发辅助工具来实现，不需要对系统的底层结构进行编程。该方法拟在协同工作流管理系统SynchroFLOW-T开发中采用，将极大地提高工作流软件开发的效率，增强工作流应用系统适应需求变化的敏捷度。

参 考 文 献

1 Laddad R. I Want My AOP (JavaWorld). http://www.javaworld.com/javaworld/jw-04-2002/aspect3/jw-0412-aspect3.zip, 2002
2 董云卫，郝克刚. 一种面向方面的软件体系结构. 微机发展，2004，14(6)
3 郝克刚，王斌君，安贵. WPDL中的JOIN语义问题和分区解决方案. 计算机科学，2003，30(7)
4 董云卫，郝克刚. 一种乐观嵌套工作流事务模型. 计算机科学，2005，32(8)
5 Hoffmann M, Mike D S. Ebbers, Image and Workflow Library: Advanced Work- flow Solutions using IBM FlowMark, IBM Workflow Solutions, Boeblingen, Germany, Jan. 199
6 BEA White Paper: Building A Fully Integrated, Extended Enterprise, San Jose, CA U. S. A., Http://www.bea.com, 2003
7 Khan R. Supporting BPM Teams. http://www.ultimus.com/ultwhite/BPM_Ultimus.pdf, 2004