一种新颖的智能网络图像内容监测系统模型*

许 强, 赵 宏, 江 早

(东北大学 软件中心,辽宁 沈阳 110006)
E-mail: hsuqiang@hotmail.com
http://www.neu.edu.cn

摘要: 针对目前网络安全系统对于图像信息监测能力不足的问题,提出了一种基于图像内容的智能网络安全监测系统模型.该模型采用了信息反馈与知识辅助机制,以基于轮廓特征抽取与多智能体技术的图像检索算法作为图像内容监测与分析模型的核心,采用基于遗传算法的安全性审计机制实现对于历史监测数据及规则的智能挖掘与审计,从而能够准确、实时地监测网络中的图像信息,提高了网络系统的运行可靠性和安全性.此外,还给出了该模型的原型描述及实现.

关 键 词: 网络安全;图像内容监测;安全性审计;遗传算法;Daubechies 小波
中图法分类号: TP393 文献标识码: A

Internet 开放性带来巨大的安全风险,网络安全成为关系到国家与社会安全的一项重要问题.多媒体技术的飞速发展与广泛应用,对传统基于文本信息截取与过滤的网络安全技术提出了新的挑战.针对网络中越来越多的图像信息,虽然已经开发出了像 CyberPatrol,NetNanny,CyberSitter 等一些过滤软件包,但是所有这些软件包不是基于 IP 地址过滤,就是基于网页中文本内容的判断,具有较大局限性,滞后性强,准确性不高.因此,只有针对图像内容监测,才能从根本上解决目前网络安全技术对图像信息过滤与监控能力不足的问题.

当前,国外一些研究机构在这方面进行了探索性的研究,比较典型的是英国 Forsyth 研究小组[1].他们设计了一种针对人体的过滤算法,其基本思想是将人体看作按照一定规则的若干柱状区域组合,以基于颜色与纹理的特征抽取技术标识图像中的人体区域.研究表明,该系统仅能够处理单一类型图像,缺乏适应性和通用性;处理速度较慢,不适于网络条件下大规模的事务处理;图像识别率较低,准确性和智能性不高.

因此,为了能够在不影响网络正常使用条件下智能地监测并分析图像信息,本文提出了一种具有一定自适应性基于图像内容的智能网络监测系统模型.该模型具有信息反馈与知识辅助功能,以基于 Daubechies 小波与正则中心矩相结合的特征抽取技术与多智能体技术的图像检索算法作为图像内容监测数据分析核心,采用基于遗传算法的安全性审计机制实现对历史监测数据及规则的智能挖掘与审计,从而能够准确、实时地监测网络中的图像信息,克服了 Forsyth 系统准确性不高、实时性不强的缺点,提高了网络系统的运行可靠性和安全性.

1 系统模型

我们认为,系统模型应该具有功能模块化、结构构件化的特点.

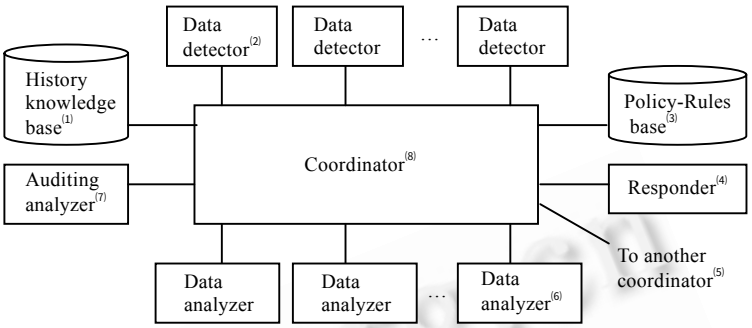
(1) 功能模块化.网络中媒体流监测的基本单元是相对固定的.随着各种媒体监测技术研究的深入,功能模块化满足多媒体监测技术的发展要求.

* 收稿日期: 2000-03-30; 修改日期: 2000-08-21
基金项目: 国家 863 高科技发展计划资助项目(863-306-ZT05-05-5)
作者简介: 许强(1973－),男,天津人,博士,主要研究领域为网络安全,图像识别;赵宏(1954－),男,辽宁沈阳人,博士,教授,博士生导师,主要研究领域为分布式多媒体信息处理技术,网络安全技术;江早(1965－),男,辽宁沈阳人,博士,副教授,主要研究领域为图像识别与理解.

(2) 结构构件化.媒体流监测技术千差万别,但处理过程均为媒体内容的监测、分析、审计和响应.以构件形式通过一定的连接与协调机制能够较好地构成具有可扩展性的基本系统结构.

从构件化角度来讲,基于图像内容的智能网络安全监测系统模型是一个以分布性、协同性和智能性为目标,建立在图像内容监测基础上,具有信息反馈与知识辅助功能的智能网络安全系统,如图 1 所示.

本模型主要由数据监测器、数据分析器、审计分析器、响应器、历史知识库、策略规则库和协作员这些构件组成.协作员是系统模型的核心.



(1)历史知识库,(2)数据监测器,(3)策略规则库,(4)响应器,(5)至另一个协作员,(6)数据分析器,(7)审计分析器,(8)协作员.

Fig.1 An intelligent network detecting system component model

图 1 智能网络监测系统构件模型

数据监测器是位于安全域或自治域边界上的执行监测与信息还原的网络监测器,采用一种上下文无关的高效分析机制,具有一定的采集密度与粒度控制功能,并支持不同监测器之间的协同处理.

数据分析器主要完成针对媒体内容的智能分析与检测功能.根据媒体对象的不同,以确定不同的内容分析算法进行事后离线检测.此外,分析器能够支持不同分析器之间的协同处理.

审计分析器在规则库和策略库的指导下,对历史知识库中大量历史知识进行搜索与模式匹配,以挖掘出新的规则和策略.

响应器主要针对当前安全状态采取实时反应行为,具备一定的网络监测配置协议的支持能力,能够根据需要调整网络监测器的监测粒度.

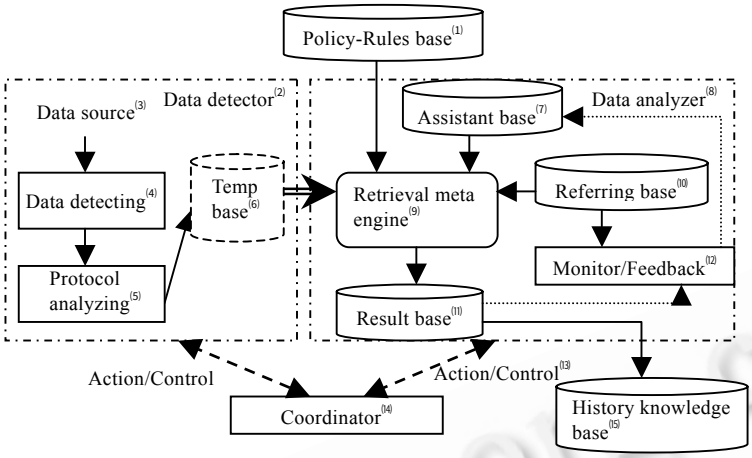
协作员是模型的中枢,执行协同、调度与管理功能,主要表现为:向外发起协同请求,通过安全传输获取域外信息;响应其他域的协同请求,将本域的相应信息通过安全传输提供给合作系统.

从功能模块化角度来讲,基于图像内容的智能网络监测系统是图像内容监测与分析模块和安全性审计模块的组合.

2 图像内容监测与分析模型

图像内容监测与分析模型由数据监测器、数据分析器、历史知识库、策略规则库、协作员等构件组成,具体包括数据监测模块、检索元引擎、参照库、辅助知识库和结果库,其数据控制流图如图 2 所示.本模型的核心算法具有一定的适应性,能够根据不同类型参照库监测不同种类对象;并且具有监督与反馈机制,能够以一定的概率对检索结果进行比较,对不收敛结果进行权值修正,并以上下文无关知识规则形式记入辅助知识库,作为运行时辅助决策的经验权值.该监督过程一直持续到系统运行稳定且收敛为止.

图像内容实质上就是图像中所包含对象的特征.基于内容检索就是基于图像对象特征的抽取与检索.对于特征抽取,目前典型方法有颜色直方图法、形状特征法、纹理特征法和轮廓特征法.其中,只有轮廓特征法比较适于描述图像中某一对象的略图,通用性强.但是,传统轮廓特征法对于图像中高频信息处理能力较弱.为此,本文在轮廓特征抽取法中采用了能够较好地描述高频信息的多尺度 Daubechies 小波技术.对于图像检索,关键是高效的特征多维索引技术,诸如吊桶算法、k-d 树、优先级 k-d 树[2]、R 树[3]及 R*树[4]等多维索引算法.但是,上述算法在大规模图像集合中存在着不同程度的检索效率低下问题.因此,本模型将分布式计算领域中的多智能体技术引入图像特征检索中,以基于 Daubechies 小波与正则中心矩的轮廓特征抽取与基于多智能体特征检索的图像内容检索算法作为检索元引擎的核心算法.该算法将特征检索看作一个分布式求解问题,把整个特征检索空间划分给不同的智能体,以并行方式检索图像特征,提高了处理速度,增强了灵活性与控制力.



(1)策略规则库,(2)数据监测器,(3)数据源,(4)数据监测,(5)协议分析,(6)临时库,(7)辅助知识库,(8)数据分析器,(9)检索元引擎,(10)参照库,(11)结果库,(12)监督/反馈,(13)事件/控制,(14)协作员,(15)历史知识库.

Fig.2 Image content detecting and analyzing model

图 2 图像内容监测与分析模型

2.1 Daubechies小波

根据文献[5],给出 Daubechies 正交小波基的定义.

定义 **1.** 对于 $\forall r \in Z$,$L^2(R)$上的 Daubechies 正交小波基为

$$\psi_{r,j,k}(x) = 2^{j/2}\psi_r(2^j x - k), \quad j,k \in Z .$$

其中,$L^2(R)$上函数 $\psi_r(x)$ 具有使 $\{\psi_r(x-k) \mid k \in Z\}$ 在 $L^2(R)$上成为正交序列的性质.

Daubechies 正交基具有如下属性:

- ψ_r 具有紧支区间[0,2*r*+1];
- ψ_r 具有 *r*/5 阶连续导数;
- $\int_{-\infty}^{\infty}\psi_r(x)\mathrm{d}x = \ldots = \int_{-\infty}^{\infty}x^r\psi_r(x)\mathrm{d}x = 0$.

Daubechies 小波的上述属性十分适于图像分析.首先,具有紧支集的小波函数可以很容易地由有限长度过滤器来实现.其次,具有连续导数的函数能够有效地分析连续的图像信号函数,从而避免了虚假边界的产生.因此,以 Daubechies 小波表示的图像信号函数可以看作是小波函数元素的线性组合.

在基于轮廓的特征抽取中,通常以特征向量的系数部分来准确地表示图像中的对象轮廓.而传统轮廓抽取法和其他小波函数都不可避免地在高通带宽部分产生噪声,只有 Daubechies 小波基能够在期望的高频带中获得确切的波动次数表示对象的轮廓,即 Daubechies 小波具有比其他小波更强的噪声分离能力和边界检测能力.

2.2 矩

为了能够识别从不同角度拍摄的相同对象图像,这里采用了正则中心矩辅助边缘检测.根据文献[6],矩主要用于形状和区域编码.

定义 **2.** 对于二维坐标平面 *xy* 中的任一离散函数 *f*(*x*,*y*),它的(*p*+*q*)阶矩为

$$m_{pq} = \sum_x\sum_y x^p y^q f(x,y), \quad p,q \in Z.$$

定义 **3.** 对于二维坐标平面 *xy* 中的任一离散函数 *f*(*x*,*y*),它的中心矩为

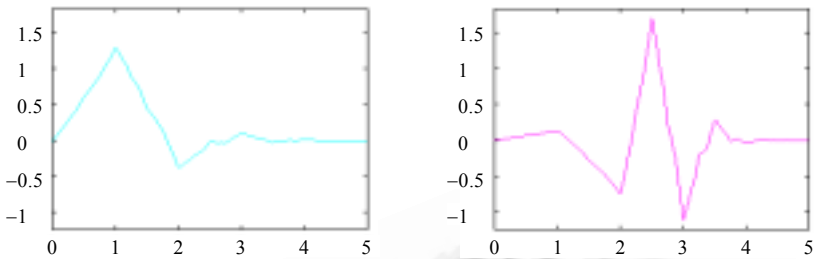
$$\mu_{pq} = \sum_x\sum_y (x-\frac{m_{10}}{m_{00}})^p (y-\frac{m_{01}}{m_{00}})^q f(x,y) .$$

定义 **4.** 对于二维坐标平面 *xy* 中的任一离散函数 *f*(*x*,*y*),它的正则中心矩为

$$\eta_{pq}=\frac{\mu_{pq}}{\mu_{00}^{\chi}},\quad \text{其中 } \chi=\frac{p+q+2}{2},\quad \text{对于 } p+q=2,3,4,...$$

2.3 核心算法

根据网络安全系统的特点,作为核心的特征抽取算法要求具有较高的处理速度,但对所抽取对象轮廓信息质量要求不高,仅需抽取出对象的主要轮廓即可.因此,本特征抽取算法采用 Daubechies-3 正交小波基,其尺度函数波形及小波函数波形如图 3 所示.



(a) Daubechies-3 wavelet scale function
(a) Daubechies-3 尺度函数

(b) Daubechies-3 wavelet
(b) Daubechies-3 小波函数

Fig.3
图 3

定义 **5.** 对于任意一幅图像 I,运用 Daubechies-3 小波基对其处理,称其中所有在行和列方向上均为低频信息的部分为 LL(low-low)频带;称所有在行方向上为低频信息且在列方向上为高频信息的部分为 LH(low-high)频带;称所有在行方向上为高频信息且在列方向上为低频信息的部分为 HL(high-low)频带;称所有在行和列方向上均为高频信息的部分为 HH(high-high)频带,如图 4 所示.

LL	HL
LH	HH

(a) 1-level wavelet transform
(a) 一阶小波变化

0	0
LH	0

(b) Matrix used for inverse wavelet transform
(b) 反向小波变化矩阵

Fig.4
图 4

进一步来讲,LH 频带对水平方向上的边界比较敏感,HL 频带对于垂直方向上的边界比较敏感,而 HH 频带对于对角线方向上的边界比较敏感.

算法 **1.** 基于轮廓的特征抽取算法

Procedure Edge-Detect ($I[m,n]$) // 设 $I[m,n]$为大小为 $m\times n$ 的图像.

Begin

// Phase 1: 边界检测

$\Phi_{LH}=\Pi_{LH}f_{Daubechies\text{-}3}(I)$; // 对 I 进行 LH,HL,HH 划分

$\Phi_{HL}=\Pi_{HL}f_{Daubechies\text{-}3}(I)$;

$\Phi_{HH}=\Pi_{HH}f_{Daubechies\text{-}3}(I)$;

if ($\Phi_{LH}\neq$NULL) then // 找出 I 中所要识别对象的水平边界;

$Edge_h[m,n]=f^{-1}_{Daubechies\text{-}3}(\Phi_{LH})\cdot Detector_{z\text{-}c}(\Phi_{LH})_v$;

// $Detector_{z\text{-}c}(\Phi_{LH})_v$ 为水平零交叉检测器[7];

if ($\Phi_{HL}\neq$NULL) then //找出 I 中所要识别对象的垂直边界;

$Edge_v[m,n]=f^{-1}_{Daubechies\text{-}3}(\Phi_{HL})\cdot Detector_{z\text{-}c}(\Phi_{HL})_h$;

// $Detector_{z\text{-}c}(\Phi_{HL})_h$ 为垂直零交叉检测器;

if ($\Phi_{HH}\neq$NULL) then // 找出 I 中所要识别对象对角线方向边界;

$Edge_d[m,n]=f^{-1}_{Daubechies\text{-}3}(\Phi_{HH})\cdot Detector_{z\text{-}c}(\Phi_{HH})_d$;

// $\text{Detector}_{z\text{-}c}(\Phi_{HH})_d$ 为对角线零交叉检测器;

//Phase 2: 边界合并

for i=1, j=1 to i=m, j=n do

$\text{Edge}[i,j]=(\text{Edge}_h[i,j]^2+\text{Edge}_v[i,j]^2+\text{Edge}_d[i,j]^2)^{1/2}$;

$I_{new}=\text{Edge}[m,n]$;

//Phase 3: 计算 I_{new} 的正则中心矩

if ($I_{new}\neq$NULL) then

$$\eta_{pq}(I_{new})=\frac{\mu_{pq}}{\mu_{00}^{\chi}}$$

end // end of Procedure

算法 **2**. 基于多智能体技术的特征检索算法

由于对轮廓特征的认知和选择在一定范围内存在模糊性和随机性,因此需要将检索结果扩展到一定的分布空间才能准确地反映出客观的匹配结果.所以,本文采用现实世界中所有非均匀分布中可能性最大的一种分布——正态分布拟合法来扩展满足检索条件的图像特征范围.

假设待检索图像特征值为η_{pq},若未经拟合,则只能检索出与η_{pq}匹配的参照库中的一幅图像,方差趋于 0;假设给定模糊度为σ,则经正态分布拟合以后,图像特征$f(\eta_{pq})$为

$$f(\eta)=\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{(\eta-\eta_{pq})^2}{2\pi\sigma^2}}.$$

可以证明,η在区间$((\eta_{pq}-\sqrt{3}\sigma),(\eta_{pq}-\sqrt{3}\sigma))$范围内基本上包含了所有的图像特征分布.

Procedure Feature-Retrieval (η_{pq}) // 设η_{pq}为图像 I 的正则中心矩

Begin

// Phase 1: 初始化

(1) 系统初始化,生成一个 TaskAgent 和一个 ControlAgent;

(2) 参照库图像特征矢量化形成参照特征库 RefLib;

(3) 参照特征库树形分布化:

Begin

设定阈值 th_1,th_2,σ,W; // th_1为树节点数目阈值;th_2为中心向量方差阈值

StructTree=NULL; // σ为系统设定的模糊度;W 为权值

repeat

根据 Lloyd[8]算法, 将特征库 RefLib 分成两部分 SubLib[i](i=1,2)

$\Leftrightarrow\forall\text{SubLib}[i],\exists\text{CentralVec}\in\text{SubLib}[i]\cdot$

$$\forall\text{Vec}_j\in\text{SubLib}[i]\wedge\sum_{j=1}^{\infty}(\text{Vec}_j-\text{CentralVec})^2\,p_{\text{Vec}_j}<th_2,$$

其中, $p_{Vec_j}=\frac{1}{\sqrt{2\pi}\sigma}e^{-\frac{(\text{Vec}_j-\mu)^2}{2\sigma^2}}$;

StructTree=StructTree+AddNode(SubLib[i]);

RefLib=SubLib[i];

until $\text{Num}_{leaf}(\text{StructTree})\geq th_1$

将树节点间的关系存入 TaskAgent,同时为每个叶节点生成一个 RetrievalAgent_i;

end

// Phase 2: 向量检索

(4) 为检索η_{pq}选择合适 RetrievalAgent_i.

TaskAgent:

repeat

if $\exists$EuclideanDistance(CentralVec$_i$, η_{pq})$\in$($(\eta_{pq}-\sqrt{3}\sigma)$, $(\eta_{pq}+\sqrt{3}\sigma)$)

then 选定 RetrievalAgent$_i$;

until 遍历所有的 RetrievalAgent

(5) 生成局部解.

选定的 RetrievalAgent$_j$(j=1,2,…,k):

if $\exists$Vec$_i\in$RetrievalAgent$_j$·EuclideanDistance($W\times$Vec$_i$, η_{pq})$\in$($(\eta_{pq}-\sqrt{3}\sigma)$, $(\eta_{pq}+\sqrt{3}\sigma)$)

then 生成局部解;

else FALSE;

(6) ControlAgent 根据 RetrievalAgent$_i$ 的局部解生成一个全局解.

End // end of Procedure

2.4 算法复杂度分析

定理 1. 算法 Feature-Retrieval 是确定的,上界为$\Theta(n\log n)$.

证明:令 η_r 为所要检索的特征向量,σ为检索模糊度,Ver=$\{\eta_1,\eta_2,\ldots,\eta_k\}$为单一特征空间$\Gamma$中满足 EuclideanDistance($\eta_r$,$\eta_i$)$\in$($(\eta_r-\sqrt{3}\sigma)$, $(\eta_r+\sqrt{3}\sigma)$)(i=1,2,…,k)的结果特征集合.

因为 Feature-Retrieval 的参照特征库树形分布化过程是单一特征空间Γ的一个完全划分;

所以$\forall\eta_i\in$Ver,$\exists$RetrievalAgent$_i$·$\eta_i\in\Gamma$(RetrievalAgent$_i$);

算法 Feature-Retrieval 的确定性得证. □

令参照图像库具有 n 幅图像,每个 RetrievalAgent$_i$ 具有不多于 c 幅图像的子特征库,则将生成 n/c 个 RetrievalAgent$_i$.

执行一次 Feature-Retrieval(η_r)时,首先,η_r 与 $2\log(n/c)$个中心欧氏距离进行比较,以确定执行的 RetrievalAgent$_i$;然后,在该 RetrievalAgent$_i$ 的检索空间上,需要耗费 $T(c)$时间来确定局部解;因此,总共需要 $T(c+2\log(n/c))$时间,即$\Theta(\log n)$时间,小于$\Theta(n\log n)$时间.

令同时检索 k 个特征向量$\{\eta_j|\ j=1,2,\ldots,k,k\le(n/c)\}$,若 $k>(n/c)$,可以看作是 k mod (n/c)次同时检索 k 个特征向量.

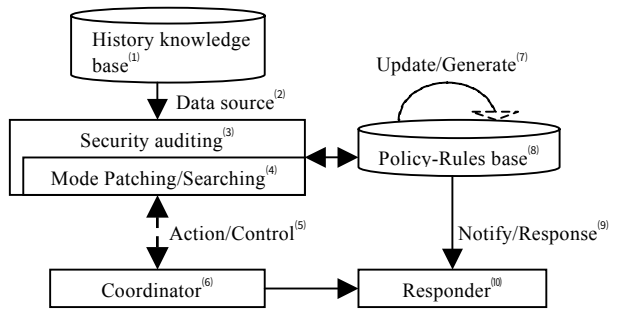
这样,确定执行的 RetrievalAgent$_i$ 总共需要 $2k\log(n/c)$次中心欧氏距离的比较运算;对于 RetrievalAgent$_i$ 的检索,最坏情况下,即所有检索都由某一特定的 RetrievalAgent$_m$ 来完成需要耗费 $kT(c)$时间来确定局部解;一般情况下需要{RetrievalAgent$_j$| j=1,2,…,t,$t\le k$}来完成,总共需要耗费 $\max\{T(c_j)|j=1,2,\ldots,t\}$时间.因此,当 $k\to n$ 时,总共需要时间 $T\in(\max\{T(c_j)\}+T(2k\log(n/c)),kT(c)+T(2k\log(n/c)))$,即$\Theta(n\log n)$时间.

所以,算法 Feature-Retrieval 的上界为$\Theta(n\log n)$. □

3 安全性审计模型

安全性审计模型由审计分析器、响应器、历史知识库、策略规则库、协作员等构件组成,负责从历史知识库中发掘出潜在的上下文相关规则为系统提供决策依据与策略,如图 5 所示为数据控制流图.针对历史知识库中大量的上下文无关知识规则,审计分析器在策略规则库指导下从中挖掘出一些上下文相关的监测规则,并对策略规则库进行更新.传统方法有两种:统计方法[9]和专家系统方法[10].其中,统计模型参数选择错综复杂;统计模型只对监测内容的显著变化产生警报流,入侵者可以通过缓慢地改变行为欺骗系统.专家系统需要将专家知识编码为规则集合,而本身并不完整,具有一定的局限性.为此,本文将安全性审计作为一个模式匹配问题,提出了一种基于遗传算法的启发式搜索匹配机制.

3.1 问题描述与分析



(1)历史知识库,(2)数据源,(3)安全性审计,(4)模式匹配/搜索,(5)事件/控制,(6)协作员,(7)更新/产生,(8)策略规则库,(9)通知/响应,(10)响应器.

Fig.5 Security auditing model

图 5 安全性审计模型

安全性审计问题可以看作是一个模式匹配问题:将历史知识库中审计规则集合看作一个字母表,每个规则作为一个字符,审计分析是在主串中搜索出潜在规则子串.因此,安全性审计问题可以描述为"已知一个正则表达式 r 组成的模式和一个输入字符串 s,判断 s 中是否包含一个与 r 匹配的子串".经证明,安全性审计问题是一个 NP 完全问题[11].为了缩短搜索空间和时间,提高搜索效率和性能,适宜采用基于启发式的遗传算法求解.

在安全性审计中,普遍存在着一定的假设关系[12].这里,引入了假设-推导机制,即在审计规则集合中选取一个定假设规则集,计算所有与其相关匹配的规则数;如果对于某一类型的假设规则,匹配规则数小于等于策略规则库中的相应值,则认为该假设是现实的;相应的推导过程通过适应度函数评估假设来实现.

因此,基于遗传算法安全性审计的数学描述如下:

问题实例: 假设

· N_r 为历史知识库中审计规则的数目,N_p 为潜在规则的数目.

· PR 为 $N_r \times N_p$ 规则矩阵,表示由每个潜在规则产生的审计规则集合.$PR_{ij}(PR_{ij} \geq 0)$为由事件 j 产生类型 i 的审计规则数目.

· W 为一个 N_p 维加权向量,W_i $(W_i>0)$表示与潜在规则 i 相关联的权值.

· O 为一个 N_r 维策略规则库审计向量.

· H 为一个 N_p 维假设向量;其中,$H_i=1 \Leftrightarrow$根据假设潜在规则 i 存在.

可行性解: 确定 H 向量,满足$(PR.H)_i \leq O_i (1 \leq i \leq N_r)$.

目标函数: $y=W \times H$.

优化目标: Max$(W \times H)$.

3.2 编码与适应度函数设计

为了与假设向量 H 对应,采用了二进制串编码.根据目标函数 $y=W \times H=F(H)$,令 I 为对应于自变量 H 的二进制串,长度为 N_p.

由于优化的目标是求函数最大值,并且目标函数 $y=W \times H$ 总取正值,所以个体适应度函数直接设定为目标函数:Fitness$=\sum_{i=1}^{N_p} W_i \cdot I_i$,I 为个体.但是,在上述适应度函数中存在某些类型规则满足$(PR.H)_i>O_i$ 的情况,这意味着在 2^{N_r} 种可能情况下某些假设规则是不现实的.因此,引进了罚函数作为目标函数的惩罚: $P=T_r^{\ p}$,式中 T_r 为满足 $(PR.H)_i>O_i$ 规则类型数.实验表明,一个二次罚函数(p=2)能够很好地区分上述个体.

定义 **6.** 安全性审计问题适应度函数为

$$F(I_i)=\begin{cases}\alpha+\left(\sum_{i=1}^{Nr} W_i \cdot I_i-\beta \cdot T_r^2\right) & \text{if } F(I_i)>0\\ 0 & \text{if } F(I_i)\leq 0\end{cases}.$$

其中,β为罚函数斜度的修正值;α为一个使 $F(I_i)$为正的阈值.如果存在 $F(I_i)<0$ 的情况,则 $F(I_i)=0$.这样使得相应个体不被选中,从而去除某些不现实的假设.

3.3 实验结果

根据安全性审计问题需要,经多次实验与统计分析,相应遗传算子选择如下:选择运算使用比例选择算子,交叉运算使用单点交叉算子,变异运算使用基本位变异.

根据安全性审计问题需要,经多次实验与统计分析,相应遗传算子选择如下:选择运算使用比例选择算子,交叉运算使用单点交叉算子,变异运算使用基本位变异.

以四元组(P_c,P_m,L,R)表示算法的运行参数,其中:P_c表示交叉概率,P_m表示变异概率,L表示种群大小,而 R 表示潜在规则数.实验中,四元组分别取值 P_c=0.6,P_m=0.002,L=500,R=2 时,运行 10 次,适应度最大、最小及平均值如图 6 所示.实验表明:在 24×28 维规则矩阵上,经过 20 代遗传,最大适应度值能够迅速收敛于最优化;经过 100 代遗传,平均适应度值能够达到最大适应度值的 99%.

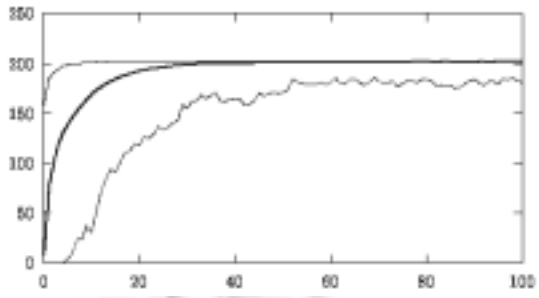


Fig.6 Simulation running result
图 6 仿真运行结果

4 原型实现

在网络安全系统中,性能是首要问题.为了平衡负载,适应大规模高速网络监测,原型系统采用了二级主机结构:前端主机和后端主机.前端主机以高性能为原则,以具有 2M 同步接口 Intel/Linux 平台实现针对广域 IP 网络的数据监测;同时,为了防止对后端主机产生过大数据压力,前端主机具有一定的处理和过滤功能,只传送给后端主机需要的数据.后端主机则实现数据分析、安全审计、管理协同等相对复杂、全面的功能,但在性能上要求不如前端主机,采用了诸如 Sybase 数据库等复杂系统.此外,根据前、后端主机通信内容的不同,原型系统采用了不同的传输机制:对于采集的大量图像数据以明文传输,保证了整个系统的高性能;对于管理/控制信息采用基于 IP Security 的安全传输,保证了整个系统的安全性.

我们在 Pentium II-450/Linux 平台上对原型系统进行了验证,对于 10 000 幅图像的参照库需要大约 3.5 小时来生成参照特征库,相应的图像识别率/错分率和单/双 CPU 上的检索速率比较结果分别如表 1 和表 2 所示.实验表明,原型系统比 Forsyth 系统具有较高的智能性、鲁棒性和高效性,能够基本上实现图像在线监测与事后分析功能.

Table1
表 1

	Correct rate[1](%)	Error rate[2](%)
Prototype system[3]	95.2	10.7
Forsyth system[4]	57	3.4

(1)识别率,(2)错分率,(3)原型系统,(4)Forsyth 系统.

Table 2
表 2

	Single CPU[1](s)	Double CPU[2](s)
Result in referring base[3]	0.02	0.014
Result not in referring base[4]	0.5	0.3

(1)单 CPU,(2)双 CPU,(3)结果在参照库,(4)结果不在参照库.

5 结 论

针对多媒体内容的网络监测是现代网络安全研究的重要内容之一,也是一个新的挑战.本文针对目前网络安全系统在这方面的不足,提出了一种基于图像内容的智能网络安全监测系统模型.该模型具有一定的智能性,主要表现在:

(1) 以信息反馈与知识辅助机制实现了系统模型的自主性和自动性;
(2) 以协作员机制保证了系统模型的分布性和协同性;
(3) 以基于轮廓特征抽取与多智能体技术的图像检索算法保证了系统模型的自适应性;
(4) 以基于遗传算法的安全性审计机制保证了系统模型潜在的自学习性;
(5) 以功能模块化、结构构件化保证了系统模型的可扩展性,通过增加针对音频和视频的检索元引擎构件

可以实现基于多媒体信息的智能网络监测.

近年来,多媒体信息隐藏技术的出现,使得秘密资料和不安全信息可以通过图像、语音、视频等载体轻易地越过网络安全系统,起到泄密、攻击等破坏作用.如何有效地监测这种新型入侵手段,成为下一步要解决的问题之一.

References:

[1] Forsyth, D.A., Malik, J., Fleck, M.M., *et al*. Finding pictures of objects in large collections of images. In: Proceedings of the International Workshop on Object Recognition. Cambridge, 1996. http://www.cs.berkeley.edu/~daf/.

[2] White, D., Jain, R. Similarity indexing: algorithms and performance. In: Sethi, I.K., Jain, R.C., eds. Proceedings of the SPIE Storage and Retrieval for Still Image and Video Databases Ⅳ. San Jose, CA: SPIE Press, 1996. 62~73.

[3] Guttman, A. R-trees: A dynamic index structure for spatial searching. In: ACM SIGMOD, ed. Proceedings of the 1984 ACM SIGMOD International Conference on Management of Data. Boston, MA: ACM SIGMOD, 1984. 47~57.

[4] Sellis, T., Roussopoulos, N., Faloutsos, C. The R+ tree: a dynamic index for multi-dimensional objects. In: Stocker, P.M., Kent, W., Hammersley, P., eds. Proceedings of the 13th International Conference on Very Large Data Bases. Brighton: Morgan Kaufmann, 1987. 507~518.

[5] Daubechies, I. Orithonormal basis of compression and compactly/supported wavelets. Pure Applied Mathematics, 1988,41(9): 909~996.

[6] Gonzalez, R.C., Woods, R.E. Digital Image Processing. Reading, MA: Addison-Wesley, 1993.

[7] Aydin, T. Multidirectional and multiscale edge detection via M-band wavelet transform. IEEE Transactions on Image Processing, 1996,5(9):1370~1377.

[8] Lloyd, S.P. Least squares quantization in PCM. IEEE Transactions on Information Theory, 1982,28(2):127~135.

[9] Sebring, M.M., Shellhouse, E., Hanna, M.E., *et al*. Expert system in intrusion detection: a case study. In: SRI International, ed. Proceedings of the 11th National Computer Security Conference. Baltimore: NBS/NCSC, 1988. 74~81.

[10] Tsudik, G., Summers, R. Audes: an expert system for security auditing. Computer Security Journal, 1991,6(1):10~16.

[11] Aho, A.V. Algorithms for Finding Patterns in Strings. In: van Leeuwen, J., ed. Handbook of Theoretical Computer Science. Amsterdam: Elvesier Science Publishers BV, 1990. 256~300.

[12] Peng, Y., Reggia, J.E. A probabilistic causal model for diagnostic problem solving, Part 1: integrating symbolic causal inference with numeric probabilistic inference. IEEE Transactions on Systems, Man and Cybernetics, 1987,17(2):160~171.

A Novel Intelligent Network Image Content Detecting System Model*

XU Qiang, ZHAO Hong, JIANG Zao

(*Software Center*, *Northeastern University*, *Shenyang* 110006, *China*)

E-mail: hsuqiang@hotmail.com

http://www.neu.edu.cn

Abstract: In allusion to the deficiency of image detecting ability of current network security system, an intelligent network security system model is developed based on image content detecting. It adopts an information-feedback and knowledge-aid mechanism, brings forward an image content retrieval algorithm based on layout feature extraction and multi-agent technology as the kernel of image content detecting-analysis model, and realizes a security-auditing mechanism based on genetic algorithm to audit and mine the history knowledge base intelligently. Therefore, it can improve the security and reliability of the network system. Furthermore, a prototype of the system model is described.

Key words: network security; image content detecting; security audit; genetic algorithm; Daubechies wavelet

* Received March 30, 2000; accepted August 21, 2000

Supported by the National High Technology Development 863 Program of China under Grant No.863-306-ZT05-05-5