DOI:10.16180/j.cnki.issn1007-7820.2006.12.013

ART-2 神经网络及其在入侵检测中的应用

崔　远，杨　波，葛　宁
（西安电子科技大学 通信工程学院，陕西 西安 710071）

摘　要　在分别对 ART-2 神经网络和入侵检测原理进行介绍的基础上，指出用 ART-2 神经网络作为入侵检测系统检测算法的可行性。利用 KDD CUP-99 数据集对算法进行了 Matlab 仿真。实验表明，该入侵检测算法可实现较高的检测率和较低的误检率。

关键词　自适应共振理论；神经网络；入侵检测
中图分类号　TP183

ART-2 Neural Network and Its Application in IDS

Cui Yuan, Yang Bo, Ge Ning
(School of Telecommunications Engineering, Xidian University, Xi′ an 710071, China)

Abstract　On the basis of the introduction to the ART-2 neural network and intrusion detection, this paper points out the feasibility of applying ART-2 model in intrusion detection. Using the KDD CUP-99 dataset, a simulation is given with Matlab. The simulation shows that IDS with this algorism will achieve high detection rate and low false positive rate.

Keywords　ART; neural network; intrusion detection

1　入侵检测基本概念

作为一种积极主动的安全防护技术，IDS（Intrusion Detection System)，即入侵检测系统可以提供对内部攻击、外部攻击和误操作的实时防护，在网络系统受到危害之前拦截和响应入侵。IDS 的两大功能是实时检测和安全审计。一方面实时地监听、分析网络中所有的数据报文，并有选择地处理所捕获的数据报文；另一方面，记录网络事件，并对其进行统计分析，发现异常，提供给安全管理员作进一步分析或作为入侵活动的证据。

就检测方法而言，可分为异常检测（anomaly detection）和误用检测（misuse detection)。异常检测是指根据使用者的行为或资源使用状况的正常程度来判断是否入侵，而不依赖具体行为是否出现来检测；误用检测则是指将已知攻击方法定义为入侵模式，通过判断这些入侵模式是否出现来检测。本文主要讨论 ART-2 神经网络在异常检测中的应用。

收稿日期：2006-03-13
作者简介：崔　远（1982—），男，硕士研究生。研究方向：网络安全。

2　ART-2 神经网络原理

ART-2神经网络是一种无监督的矢量分类器，它能依照已存储的最相似的模式对输入矢量进行分类，还允许自适应地扩充神经元的输出层直至达到一个足够大的规模。ART-2网络由注意子系统、取向子系统和重置机构组成，其中注意子系统又包括比较层F_1、识别层F_2这两个短期记忆层（STM）和处于F_1、F_2之间的长期记忆层（LTM)。其原理如图1所示。

F_1采用了一种3层结构，有N个处理单元，以接受N维的观察向量$X(x_1, x_2, \ldots, x_N)$。每个处理单元都包含上、中、下3层，在每一层中又包括两种功能不同的节点。其中，空心圆点可以接受兴奋性输入或抑制性输入；实心圆点的功能是求输入向量的模。

F_1的底层和中层构成一闭合的正反馈回路，各节点运算方程为：

$$z_i = x_i + au_i ; \quad q_i = \frac{z_i}{\|Z\|} ;$$

$$v_i = f(q_i) + bf(s_i) ; \quad u_i = \frac{v_i}{\|V\|} .$$

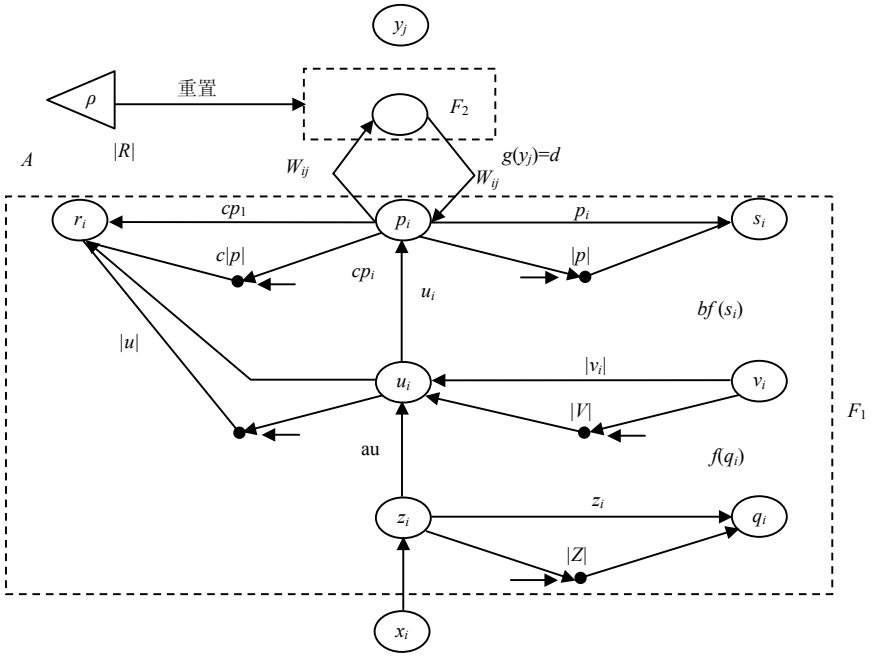

图1　ART-2原理示意图

其中$f(\cdot)$是用来对噪声进行抑制的非线性变换：

$$f(x)=\begin{cases}\dfrac{2\theta x^2}{(x^2+\theta^2)}, 0\le x<\theta; \\ x, \theta\le x;\end{cases}\qquad (\theta\text{是阈值})$$

F_1的中层和上层构成另一个闭合正反馈回路，各节点运算方程为：

$$s_i=\frac{p_i}{\|P\|};\qquad p_i=u_i+\sum_j g(y_j)w_{ij}'.$$

上式中w_{ij}'是自顶向下的LTM系数，y_j是F_1中第j个节点的STM变量。

由F_1送往F_2中第k个节点的输入成分为$T_k=\sum p_i\cdot w_{ki}$.

假定F_2中第j个节点被最大激活，即

$T_j=\max\{T_k\}$，则有：$g(y_j)=\begin{cases}d, T_j=\max\{T_k\};\\ 0，\text{其他}。\end{cases}$

(其中d为自下而上的反馈参量)

当$F_2\to F_1$的自顶向下向量和输入向量的相似度足够高，或开辟了一个新的输出端时，ART-2则进入LTM权值的学习阶段：

$$\frac{dw_{ij}}{dt}=d(1-d)\left(\frac{u_i}{1-d}-w_{ij}'\right).\text{和}\frac{dw_{ij}'}{dt}=d(1-d)\left(\frac{u_i}{1-d}-w_{ij}\right).$$

ART-2的定位子系统由图1的左边部分表示。其中$r_i=\dfrac{u_i+cp_i}{\|U\|+\|cP\|}$代表了$F_1$的STM信号与激活后的LTM信号之间的匹配度，且有$\|R\|=(\sum_i (r_i)^2)^{\frac{1}{2}}$.

设定警戒参数ρ (0<ρ<1)，并规定：当$\|R\|>\rho$时，无需对F_2重置，否则需要进行重置。

3　ART-2 应用于 IDS 的可行性

由以上对ART-2网络结构和工作原理的分析可以看出，它有以下几个特点：

(1) 自学习和自适应。

只要提供入侵检测系统的审计数据，ART-2 网络便可以通过自学习从中提取用户或系统活动的特征模式，而不需要获取描述用户行为特征的特征集以及用户行为特征测度的统计分布，避开了选择统计特征这一难题。

(2) 稳定性和可塑性的统一。

ART-2 网络的记忆容量可随样本自动增加，并且可以在保持旧信息相对稳定的情况下不断学习新信息。ART-2 网络能对输入数据无导师地进行分类，并为新出现的入侵类型自动建立新类。而一般的神经网络（如 BP 网），在新的入侵类型出现时，必须用新、旧数据重新训练网络，且存储在网络结构中的经验知识将被抹掉。随着入侵手段的不断更新，训练数据量将越来越大，训练时间和响应时间也将越来越长。

（3）搜索与直达的统一。

ART-2 网络对于已学习过的模式具有稳定的快速识别能力。而当一个长期记忆中没有的新模式输入网络后，可以立即被当作新模式加以学习。只有那些与长期记忆中若干模式都有一定相似度的输入才需要经过匹配—警戒检验—重置—再匹配的搜索过程。因此可以提高入侵检测的速度。

4 系统仿真

我们在 Matlab6.5 环境下对 ART-2 算法进行编程，并用它来进行基于网络数据的入侵检测仿真实验。

4.1 实验数据

实验数据采用DARPA（Defense Advanced Research Projects Agency）为1999年KDD（Knowledge Discovery and Data Mining）竞赛所建立的数据集KDD CUP 99[1]，该数据集是专门用来评估入侵检测系统性能的。其中每条TCP/IP连接记录包含41个特征，分为4类：基本TCP特征，与有效载荷有关的特征，基于时间的流量特征和基于主机的流量特征。本实验选取基本TCP特征中的6项作为输入特征，详见表1。

表 1　实验中所用到的 TCP/IP 连接记录特征

特征名	描　述	类型
duration	连接持续时间/s	连续
protocol_type	协议类型	离散
service	目的端口的网络服务	离散
src_bytes	从源端口发到目的端口的字节数	连续
dst_bytes	从目的端口发到源端口的字节数	连续
flag	表示连接正常或出错的标志	离散

从数据集中抽取标记为’normal’,’ ipsweep’,’ buffer_overflow’, ‘guess_passwd’的数据各10 000条作为训练样本；重新抽取标记为’normal’,,’ ipsweep’,’ buffer_overflow’, ‘guess_passwd’,’ portsweep’,’ smurf’的数据各10 000条作为测试样本。其中’ portsweep’和’ smurf’两类攻击数据是训练样本中没有的。

ART-2神经网络只能处理数值型的输入，所以要对表1 中的三项离散特征进行编码，变为数值型数据。另外，表1中三项连续特征的取值范围很大，为了减小数值差异过大对网络学习产生的不良影响，需要预先对所有输入向量的各分量进行规一化预处理。

4.2 实验步骤

（1）从KDD CUP99数据集中抽取训练样本和测试样本并进行预处理。

（2）在Matlab环境下编程实现ART-2入侵检测系统，输入训练样本，进行多次训练，每次训练过程中调整警戒参数、输出层神经元数量、阈值等参数，直到网络聚类结果最接近训练样本的实际类别情况。ρ=0.990时，网络自动将输入模式分为2类；ρ=0.994时，网络将输入模式分为3类；ρ=0.997时，网络将输入模式分为4类，此时再对其他参数进行微调，使类内差异最小，同种攻击的数据尽量被分在同一类中，此时ART-2网络参数被调整到最佳状态。

（3）将测试样本输入调整好的ART-2网络，检验网络对已知和未知攻击的检测能力。表2 列出最终的检测结果。

表 2　ART-2 入侵检测系统实验结果

攻击类型	检测率/ %	误检率/ %
normal（正常访问）	89.5	2.9
ipsweep	70.3	9.7
buffer_overflow	83.9	5.2
guess_passwd	86.3	4.8
portsweep（新类型）	80.4	10.1
smurf（新类型）	76.5	9.6

4.3 结果分析

分析上述实验结果可以看出：

（1）ART-2 神经网络适用于入侵检测系统的分析模块，能够对网络连接数据自动分类，并对新的攻击类型建立新类，解决了预分类不完全的难题。同时实现了较高的检测率和较低的误检率。

（2）警戒参数 ρ 是决定 ART-2 网络分类效果的重要参数，可以用它来协调稳定性与可塑性的关系。ρ 越小，对模式之间的相似度要求越低，聚类越粗糙；ρ 越大则聚类越细致。实际上警戒参数是一个经验参数，需要通过大量的试验来确定。如何自适应地调整警戒参数将是我们未来研究的课题。

（3）实验中某些攻击的检测结果相对较差，这主要是因为 KDD CUP99 数据的 41 个特征中，部分特征能反映某种攻击的本质，对于发现这种攻击很有帮助，而其余特征却不那么重要。今后将结合其它方法，进一步探索如何选取最有效的输入特征。

5 结束语

ART-2 神经网络实际上是一个模式分类器，当应用于入侵检测时，同样具有强大的攻击模式识别能力。ART-2 网络的引入，为 IDS 的研究开辟了崭新的空间。

参考文献

1 KDD-CUP-99 Task Description [EB/OL]. http://kdd.ics.uci.edu/ databases/ kddcup99/task.html, 1999-5-13.
2 唐正军. 入侵检测技术导论[M]. 北京: 机械工业出版社, 2004.
3 闻新等. MATLAB 神经网络仿真与应用[M]. 北京: 科学出版社, 2003.
4 戴英侠, 连一峰, 王 航. 系统安全与入侵检测[M]. 北京: 清华大学出版社, 2002.
5 危胜军等. 基于BP神经网络改进算法的入侵检测方法[J]. 计算机工程, 2005, 31(13): 154～158.
6 杨建刚. 人工神经网络实用教程[M]. 杭州: 浙江大学出版社, 2001.

（上接第 38 页）

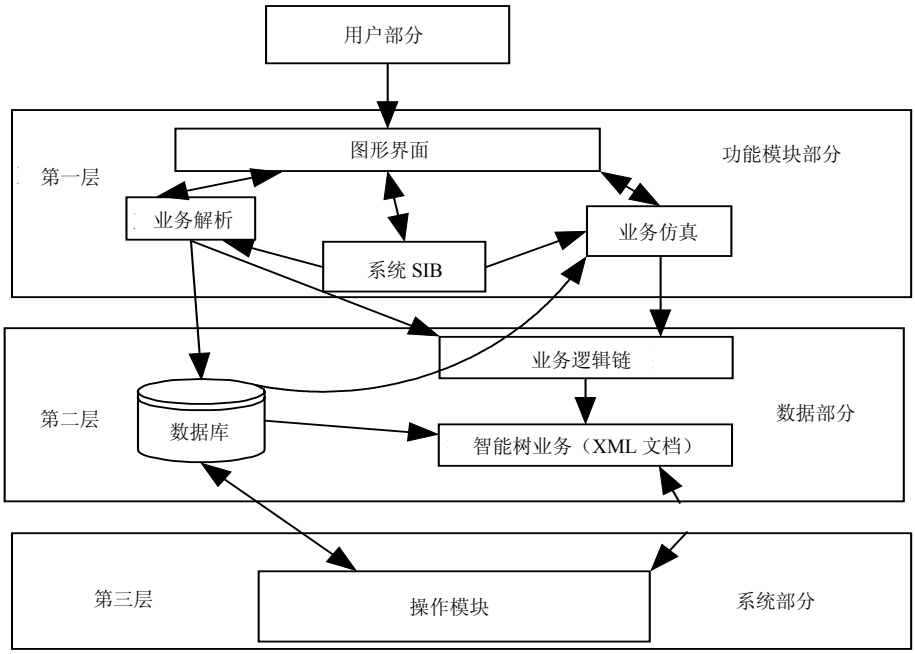

图 2 智能业务生成环境仿真平台设计示意图

利用 JAVA 和 XML 语言开发的仿真平台可以具有 SCE 的基本功能，可能在一些地方不是太理想，如对 SIB 的动态加入可能支持不太好，仿真功能简单。相信建立一个完善的功能完善平台，无疑会给智能网在铁路通信设计产生重大意义。

4 结束语

智能网作为一个能够快速灵活地提供、生成和管理新业务的体系，经过几十年的发展，智能网作为一种非常成熟的技术，必将在 GSM-R 的建设中发挥更为重要的意义。

参考文献

1 钟章队, 蒋文怡. 铁路综合数字移动通信系统[M]. 北京: 中国铁道出版社, 2003.
2 赵晓亮. 移动智能网在 GSM-R 铁路专网中的应用[J]. 电气化铁道, 2005(5): 46～48.
3 阎中印. 基于 GSM-R 智能网的接入矩阵业务, 铁道通信信号[J]. 2005, 41(12): 58～59.
4 石 波. 智能网技术在 GSM-R 网络中的应用与研究[J]. 铁路通信信号工程技术, 2006, 3(1): 18～19.