分布式入侵检测系统及其认知能力*

陈 硕，安常青，李学农

(清华大学 信息网络工程研究中心，北京 100084)

E-mail: shuochen@crhc.uinc.edu; acq@tsinghua.edu.cn

http://www.tsinghua.edu.cn

摘要：DIDAPPER(distributed intrusion detector with apperception)系统是一种具有认知能力的分布式入侵检测系统.分布式结构、认知能力和知识的共享是该系统的重要特点.重点讨论了DIDAPPER系统的认知能力.流量标本和IP陷阱是DIDAPPER系统所提出的新概念.它们可以获取和识别异常的流量数据,而且适合于检测大规模网络攻击行为.DIDAPPER系统的认知能力的另一个方面是神经网络的模式识别方法.将具有自学习能力的BP网络应用于流量分析,很好地解决了流量模式的识别问题.

关键词：入侵检测系统(IDS);大规模自动攻击;流量标本;IP陷阱;模式识别;神经网络;BP网络

中图法分类号：TP393 **文献标识码**：A

网络安全在Internet中的重要性越来越明显,因此,作为网络安全措施的一个环节的入侵检测系统(简称IDS)也越来越受到关注.智能化、分布式和监视大规模网络是当前国际上许多入侵检测系统所强调的.例如,自治型入侵检测代理(AAFID2)[1,2]是Purdue University的COAST研究小组所从事的一个入侵检测课题.该项目从一个新的角度——分布式体系结构来研究入侵检测问题.这种结构的优势在于它的规模、高效、容错性和易配置性.该系统在多Agent之间的协作方面比较成功.又如,University of California at Davis的课题基于图的入侵检测系统(GrIDS)[3]的设计目标是检测对网络系统的大规模自动攻击,所提出的机制是建立"行为图".行为图描述了各主机之间的网络行为,并通过"聚合",与已知的入侵或敌对行为作比较,如果类似,则报警或采取相应的措施.再如,Bonifacio[4]介绍的IDS是神经网络在入侵检测领域的一个应用实例,其关键技术是将各种对网络所采取的行为编成二进制串.通过众多样本(二进制流)对系统的训练,使神经网络产生对某些串组合的敏感性.

DIDAPPER(distributed intrusion detector with apperception),即具有认知能力的分布式入侵检测系统,是清华大学信息网络工程研究中心的"园区网络安全监视系统"的核心部分,其结构如图1所示.DIDAPPER的设计目标是分析大型TCP/IP网络中的网络行为.DIDAPPER的认知能力是系统的特色之一.IP陷阱和流量标本是DIDAPPER系统所提出的新概念.IP陷阱是受保护子网中的一些专门用于捕捉异常流量的IP地址.当攻击行为涉及到IP陷阱时,系统记录下进出这些IP陷阱的数据,并将数据包头进行抽象,处理后得到流量标本.如果多个IP陷阱同时发生流量,则可以检测出网络的大规模攻击.流量标本还可以在主机和监视站之间共享,使网络内的其他站点也能够学习到这种攻击行为的特征.因此,利用IP陷阱和流量标本不仅能够识别已知的异常行为,

* 收稿日期：1999-09-08；修改日期：1999-11-23

基金项目：国家863高科技发展计划资助项目(863-317-01-99)

作者简介：陈硕(1975－),男,福建福州人,博士生,主要研究领域为计算机网络;安常青(1970－),女,江苏丰县人,工程师,主要研究领域为计算机网络;李学农(1945－),男,安徽桐城人,教授,主要研究领域为计算机网络.

还能够不断地学习和积累.这是系统具有认知能力的一个方面.另一方面的认知能力是系统采取神经网络的算法对网络的流量进行模式识别.我们采用的BP网络是一种具有前馈自学习功能的神经网络模型,其特点是能够不断调整模型的内部参数,使得模型不断逼近实际的模式.对样本进行"交叠分段",由多个BP网络共同对一个样本进行评估,这是DIDAPPER系统的独特之处.

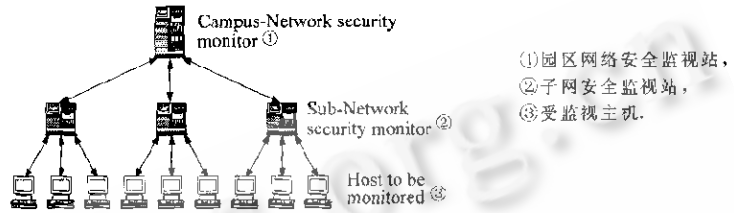


Fig.1 3-Hierarchy architecture of DIDAPPER

图1 DIDAPPER的三级层次结构

1 DIDAPPER的系统结构及主要功能

DIDAPPER系统采用分布式的三级结构."分布式"是该系统的一个重要特征.DIDAPPER系统的设计目标是应用于大规模网络中,在这种环境中,由于操作系统的不同和网络结构的差异,加上网络的庞大规模,使得集中式结构难以胜任.DIDAPPER借鉴了AAFID2所强调的自治性,在功能模块的分布上,主机安全的监视基本由安装在主机上的模块来完成;子网安全监视站负责监视对子网的入侵或子网的异常;园区网络安全监视站负责监视整个网络的异常和实现整个网络间信息的共享.

DIDAPPER的主要功能包括:(1)检测大规模网络攻击;(2)记录和识别异常的网络行为;(3)利用神经网络进行网络流量分析;(4)通过对受监视主机的口令询问进行IP真实性验证;(5)追踪发起入侵行为的源头[5].

2 IP陷阱与流量标本

2.1 IP陷阱

检测网络大规模自动攻击是入侵检测的一个具有挑战性的课题.这类攻击往往是由许许多多分散的行为构成的.这些行为有一定的时间跨度和空间范围,而孤立地来看,每一个行为都是合法的,只有从整个网络范围的一定时间跨度上看,才能发现问题.由于攻击者和被攻击者之间的通信量可能很小,很不明显,因此,如何区分正常的网络访问和可疑的访问成为检测大规模自动攻击的关键.

IP陷阱是DIDAPPER系统的一项重要措施.通常情况下,一台主机设置一个IP地址.攻击者的攻击行为和正常用户的访问都使用同一个IP地址,很难区分.IP陷阱技术则为一台主机设置多个IP地址,其中有且仅有一个地址为"主IP",其他地址为"陷阱IP"(一般将陷阱IP设置成与主IP相邻).该主机对网络的主动访问全部由主IP负责,如果该主机对外提供服务,则所使用的服务器地址也是主IP地址.在正常使用时,陷阱IP不会有任何流量(除了与路由器之间的少量通信以外).如果发现某个陷阱IP产生了流量,那么一定有异常的情况,或者是正常用户访问了错误的地址,或者是攻击者将其选定为目标,或者是发生了大规模的自动攻击.如果在一个较短的时间间隔内,若干个陷阱IP同时发现异常流量,则可以断定是大规模的自动攻击.我们可以看看扫描和蠕虫

的例子,如图 2 所示.

(a) Network scanning
(a) 网络的扫描

(b) Worm spread
(b) 蠕虫的传播

Fig. 2
图 2

当攻击者发起扫描时,网络中的一个连续 IP 地址区间都会遭到扫描,其中必然包含了陷阱 IP. 如果发现多个陷阱 IP 同时与一个 IP 地址通信,则可以检测出这种网络扫描行为.

如果在某段时间内,多个陷阱 IP 同时产生流量,并且这些流量并不是来自于同一个 IP 地址,而是来自于本网络内部的不同的 IP 地址,这时可能会检测到出现了蠕虫.

比起 GrIDS 的基于行为图的方法,IP 陷阱方法十分简单、有效. 因为行为图的方法有一定的难度,比如它必须对网络中发生的所有通信都进行上述的处理和分析,而且当网络通信量较大时,弧在行为图中存在的时限不能太长,否则误报率会增加. 如 Staniford-Chen[3] 指出:"子图被合并起来..... 仅当节点的 time 属性在 30 秒之内". 也就是说,如果蠕虫每 60 秒才有一次活动,系统则无法将蠕虫的一系列活动合并到一起,因而无法得到表现蠕虫活动特征的"树状(tree-like)图". 另外,该系统中判断子图是否类似也有一些难度. IP 陷阱方法则不同由于进入其中的流量数量少,因此,系统分析流量的工作量极大地减轻了;又由于捕捉的流量都是非正常的,因此,监视的时限可以很大,而不必担心会因此增加误报率.

2.2 流量标本

从以上的介绍可以看出,IP 陷阱的设置有助于检测网络大规模攻击. IP 陷阱的另一个用处是捕捉流量标本.

设置了 IP 陷阱,就可以记录下每次落入陷阱的数据包的包头. 例如,记录下源 IP、源端口、目的 IP、目的端口、协议号、包的长度,并对其中的一些数据进行一些抽象. 我们称抽象后的包头为"抽象包头". 所谓流量标本,就是异常流量中具有代表性的抽象包头的序列. 当一个 IP 陷阱捕捉到了一种标本流量以后,该标本通过子网安全监视站或园区网络安全监视站在子网或整个网络内得到共享. 也就是说,通过标本的共享,网络中所有的主机都可以识别出某种行为的特征.

2.3 实用性

我们将一个局域网内的 12 个 IP 地址设置为陷阱 IP,对它们进行监听. 首先,模拟的攻击者和这些 IP 进行通信,此间的所有数据包的包头都被完整地记录在文件里. 对每个捕捉到的标本,安全管理员给出其名称、特征、捕捉到的日期等有关信息. 该文件可以在局域网内部共享. 之后,当模拟的攻击者采用大体相同的方法攻击局域网内的其他主机时,系统可以立即报告出现了可疑的通信,并给出有关的信息. 由于系统是实时分析的,因此,可以在模拟的攻击者的行为刚开始时立刻报警.

我们还用自己设计的简单的模拟"蠕虫"程序(一个在已知若干主机的口令后,在这些主机之间自我复制的小程序)对系统进行了测试. 我们将蠕虫传播速度降低到每 30 分钟一次,依然可以被系统检测出来.

除了上述的模拟攻击行为以外,我们每天都检测到数次网络扫描.其中有些扫描软件是我们的标本库中存在的,可以报告出扫描软件的名称,另一些扫描行为则是第一次捕捉到的.

我们认为,设置IP地址能够较好地检测出大规模网络攻击,而结合了流量标本以后,系统可以具有一定的认知能力.

3 神经网络的模式识别算法

与文献[4]的应用领域不同,DIDAPPER将神经网络应用于园区网络、子网和特定服务器的流量监测.

这种模式识别技术的采用是DIDAPPER系统具有认知能力的另一个因素.Teresa F. Lunt指出[6]:神经网络与传统的统计算法不同,它可以识别出十分抽象的模式,而传统的统计算法需要基于对数据分布的事先的假设(例如,某个变量服从正态分布),但这些假设可能不准确或不存在.

目前,我们利用该技术对清华大学校园网总流量进行了有效的分析,训练出了合适的神经网络模型.利用类似的算法,我们将进一步对若干子网和服务器进行流量分析.在本文中,我们将以清华大学校园网的总流量为例进行描述.

3.1 神经网络与BP模型

常见的神经网络模型有感知器(perceptron)、线性神经网络、BP网络、径向基函数网络等,其中BP网络是一种被广泛使用的模型[7].BP网络是一种多层前馈神经网络.各层神经元之间的关联强度(权值)的调整采用反向传播(back propagation)的学习算法,因此被称为BP网络.在确定了BP网络的结构后,利用输入、输出样本集对其进行训练,即对网络的权值进行学习和调整,以使网络实现给定的输入、输出映射关系.经过训练的BP网络,对于不是样本集中的输入也能给出合适的输出,这种性质称为泛化(generalization)功能.

3.2 数据源的选取

对流量的监测可以有几种可能的数据源.我们对清华大学校园网进行了33天的连续观察,得到了一些数据.我们随意选取了其中7个正常工作日的数据,将它们绘成折线图,如图3所示.我们认为,进出校园网的包数有较强的规律性,同时,包数的突增和突减也能反映网络的流量异常,因此适合作为神经网络的数据源.进出校园网的国内流量字节数和国际流量字节数变化较大,不适合进行模式识别,只能采取简单的设定阈值的方法进行报警.

3.3 BP网络的结构设计

最初,我们只使用一个BP网络进行曲线的模式识别,每个样本曲线由24个数据表示(对应于一天的24小时).我们将一组正常曲线输入BP网络进行训练,设定期望值为1.训练完毕后,将新的样本曲线输入BP网络,我们发现,虽然正常曲线的实际输出十分接近期望值1(一般在0.9~1.1之间),但还有相当数量的异常曲线的评估值也十分接近1(特别是当曲线只有个别点出现异常时),因而有时异常曲线被误认为正常.

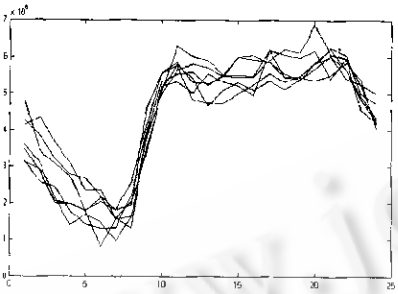
出现上述现象的原因,我们认为有以下两方面:

(1) 我们只能对BP网络进行"正例"的训练,而无法进行"反例"的训练.也就是说,只能告诉它什么是正确的,而不能告诉它什么是错误的.因为"正例"的样本才具有一定的规律,而"反例"则有太大的随意性,没有哪些可以作为"有代表性的反例",因此,在识别异常曲线时可能出现失误.我们曾经试图将一些随机性很强的曲线作为"反例"(期望值为0),结果BP网络不仅无法收敛,而且迅

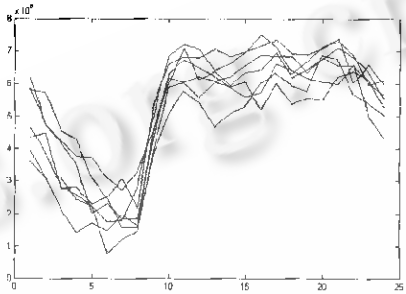
速发散.

(2) 个别异常的点,其异常特征在 24 点的曲线中被其他点的正常特征所掩盖,无法在实际评估值中反映出这些异常.

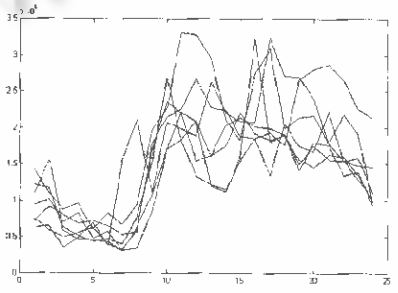
针对上面两个原因,我们对原算法进行了改进.新算法采用"交叠分段"的方法将整条 24 点的曲线分为等长的 5 段,每段是一条含有 8 个样本点的曲线,如图 4 所示.



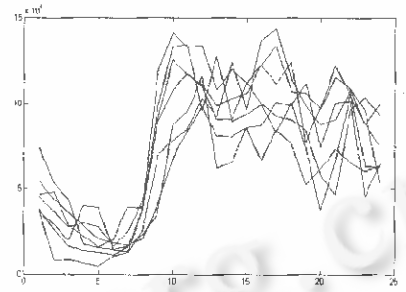
(a) Number of packets coming into the campus network
(a) 流入校园网的包数



(b) Number of packets going out of the campus network
(b) 流出校园网的包数

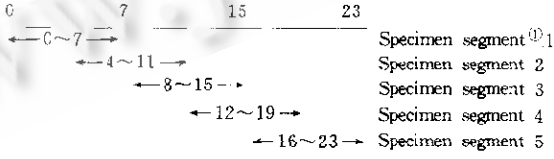


(c) Number of civil bytes coming into the campus network
(c) 流入校园网的国内字节数



(d) Number of international bytes coming into the campus network
(d) 流入校园网的国际字节数

Fig. 3 Some potential data sources
图 3 几种候选数据源



①样本片段.

Fig. 4 The overlapping segmentation of 24 hours
图4 一天24小时的"交叠分段"

每个样本片段对应于一个 BP 网络.在对网络进行训练时,所有 33 条输入曲线的 33 个样本片段 1对 BP 网络 1 进行训练,样本片段 2 对 BP 网络 2 进行训练,依此类推;在实际识别时,新样本的样本片段 1 由 BP 网络 1 进行评估,新样本的样本片段 2 由 BP 网络 2 进行评估,依此类推.这样,对于每个样本,我们得到了 5 个评估值.显然,正常的输入曲线应该使 5 个评估值都接近 1,而 5 个评估值中如果有任何一个偏差较大,都可以显示出曲线的异常性.

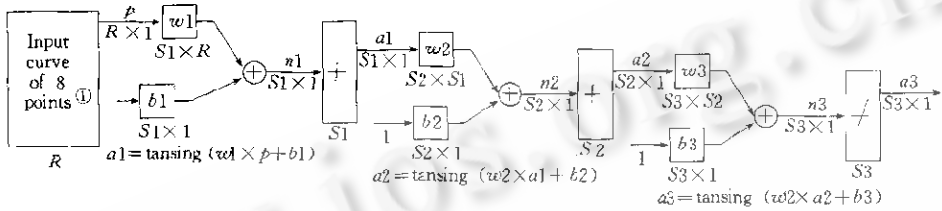
这种"交叠分段"的优点可以由如下几点看出:

(1) 曲线的连续性得到保持,避免了因分段所造成的两个端点的不连续性;

(2) 由于第 4～19 点都同时属于两个样本片段,因此异常性被检测出来的概率增加了;

(3) 8 个输入的样本片段比起 24 点的样本,对于个别异常点更为敏感.

每一个神经网络都是一个三层 BP 网络,输入数据是 8 个,输出数据是 1 个.第一隐含层含有 30 个神经元,转换函数为 tansig(正切的 Sigmiod 函数);第二隐含层含有 8 个神经元,转换函数为 tansig;输出层含有 1 个神经元,转换函数为 purelin(纯线形函数),其结构如图 5 所示.



R(number of points to input ②)=8, S1(number of neurons in layer 1 ③)=30,
S2(number of neurons in layer 2)=8, S3(number of neurons in layer 3)=1,
w1,w2,w3: each matrix of weight ④, b1,b2,b3: each matrix of threshold ⑤,
a1,a2,a3: each output matrix ⑥.

①8点的输入曲线,②输入数,③神经元数,④各级权值矩阵,⑤各级阈值矩阵,⑥各级输出矩阵.

Fig. 5 3-Layer BP network
图5 三层BP网络的结构

3.4 BP 网络的训练算法

反向传播算法是 BP 网络的核心.它通过把输出层单元的误差逐层地向前一级反向传播以分摊给各层单元,从而获得各层单元的参考误差,以便调整相应的连接权.反向传播算法的详细描述参见文献[7].用 MATLAB[8] 语言将 BP 网络对分段样本的训练和评估算法描述如下:

```
/* Program 1:分段样本的训练算法 */
pp=[样本 1 的 24 小时数据;
    ...
    样本 n 的 24 小时数据
   ];                    /* 样本数据 */
p=pp'/10000000;   /* 转置并规范化 */
t=[n 个 1]; /* t 是期望值向量 */
w1=[];w2=[];w3=[]; /* 权值矩阵 */
b1=[];b2=[];b3=[]; /* 阈值向量 */
for i=1:4:17   /* i 是样本片段起点 */
    pp=p(i:(i+7),:); /* 取 8 个数据的样本片段 */
    S1=30;   /* 第 1 层神经元数 */
    S2=8;    /* 第 2 层神经元数 */
    [ww1,bb1,ww2,bb2,ww3,bb3]=initff(pp,S1,'tansig',S2,'tansig',t,'purelin');
    /* 初始化权值矩阵和阈值向量,前两层的转换函数都为 tansig,输出层转换函数为 purelin */
    eg=0.02;  /* 期望误差 0.02 */
    lr=0.01;
    tp=[df me eg lr];
    [ww1,bb1,ww2,bb2,ww3,bb3]=trainbp(ww1,bb1,'logsig',ww2,bb2,'tansig',ww3,bb3,'purelin',pp,t,tp);
    /* 用样本片段训练该神经网络 */
    w1=[w1 ww1];w2=[w2 ww2];w3=[w3; ww3];
    b1=[b1 bb1];b2=[b2 bb2];b3=[b3 bb3];
    /* 将训练成功后的矩阵合并入大的矩阵 */
end   /* for */
```

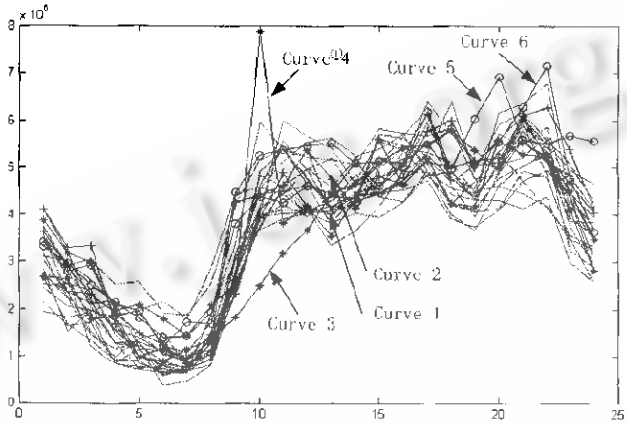
我们将期望误差设为 0.02,BP 网络经过 228 次训练,达到了期望的误差值.我们认为,"包数-时间"曲线可以在我们构造的三层 BP 网络中迅速而稳定地收敛.

3.5 实用性

图 6 和表 1 的数据和曲线是 1999 年 7 月实际观测得到的,其中 Curve 1 和 Curve 2 我们认为

是正常曲线,而评估结果与我们所期望的相符——5 个评估值都接近 1. Curve 3 在 9～12 一段出现异常,因此反映在对片段 2～4 的评估值偏差较大. Curve 4 只在 10 一点出现异常,对应于片段 2 和片段 3 的评估值偏差较大. Curve 5 和 Curve 6 在曲线末端出现异常,因此片段 5 的评估出现偏差.

事实上,该 BP 网络不仅能检测出上述由于含有异常大(小)点而变得异常的曲线,而且还能检测出含有其他异常特征(如走势)的曲线. 但由于受图形分辨率的限制,我们没有选取异常走势的曲线作为本文的例子.



①曲线.

Fig. 6 23 curves and the evaluation results of six of them

图 6 23 条曲线和其中 6 条的评估结果

Table 1 Evaluation results of 6 curves

表 1 6 条曲线的评估结果

Evaluation results①	Segment② 1	Segment 2	Segment 3	Segment 4	Segment 5
Curve③ 1	1.004 7	0.991 3	0.969 7	0.950 6	0.972 2
Curve 2	0.994 5	0.985 4	1.032 7	1.038 1	1.019 7
Curve 3	0.979 8	0.740 0	1.449 1	0.834 8	1.039 2
Curve 4	1.001 1	0.906 5	0.910 2	1.028 6	1.002 7
Curve 5	1.005 8	1.020 5	0.971 3	1.016 3	1.130 3
Curve 6	1.015 0	0.980 8	0.948 7	0.952 9	0.868 3

①评估值,②片段,③曲线.

通过对上述数据的分析可以看出,这种 BP 网络确实具有综合能力和泛化功能. 这也正是神经网络与统计假设方法相比的明显优势. 我们希望将 BP 网络的应用从目前的监视全网络总流量推广到监视各子网流量和若干台服务器(例如,计费服务器、DNS 服务器等具有相对固定流量模式的服务器),从而有能力发现子网和单机上的异常流量. 这种多层次的综合监视将大大提高系统的入侵检测能力.

4 小 结

IP 陷阱、流量标本和神经网络是 DIDAPPER 系统的关键技术. 它们为 DIDAPPER 提供了认知能力,这正是 DIDAPPER 的重要特点. IP 陷阱、流量标本与 DIDAPPER 的知识共享机制相结合,可以提高整个网络的认知能力. 将 BP 网络应用于园区网络流量的模式识别有很强的可行性和实用性.

References:

[1] Zamboni, D., Spafford, E. H. A framework and protocol for a distrubuted intrusion detection system. Technical Report, 98-05, Purdue University, 1998.

[2] Crosbie, M., Spafford, E. H. Active defense of a computer system using autonomous agents. Technical Report, 95-008. Purdue University, 1995.

[3] Staniford-Chen, S., Cheung, S., Crawford, R., *et al*. GrIDS: a graph-based intrusion detection system for large networks. In: Proceedings of the 19th National Information Systems Security Conference. 1996. http://seclab.cs.ucdavis.edu/paper.html.

[4] Bonifacio, J. M., Cansian, A. M., de Carvalho, A. C. P. L. F., *et al*. Neural network applied in intrusion detection systems. In: Proceedings of the 1998 IEEE International Joint Conference on Neural Networks. New Jersey: IEEE Piscataway, 1998. 205~210.

[5] Staniford-Chen, S., Heberlein, L. T. Holding intruders accountable on the internet. In: Proceedings of the 1995 IEEE Symposium on Security and Privacy. New Jersey, IACR IEEE Piscataway, 1995. 39~49.

[6] Lunt, T. F. Detecting intruders in computer systems. In: Proceedings of the Conference on Auditing and Computer Technology. 1993. http://www.ccert.edu.cn/documents/intrusion.pdf.

[7] Jin, Fan, Fan, Jun-bo. Neural Network and Neural Computer. Chengdu: Southwestern Jiaotong University Press, 1991 (in Chinese).

[8] Lou, Shun-tian, Shi, Yang. MATLAB-Based System Analysis and Design. Xi'an: Xi'an Electronic Science and Technology University Press, 1998 (in Chinese).

附中文参考文献:

[7] 靳蕃,范俊波.神经网络与神经计算机.成都:西南交通大学出版社,1991.

[8] 楼顺天,施阳.基于MATLAB的系统分析与设计.西安:西安电子科技大学出版社,1998.

A Distributed Intrusion Detection System and Its Apperception Ability*

CHEN Shuo, AN Chang-qing, LI Xue-nong

(*Network Research Center, Tsinghua University, Beijing* 100084, *China*)

E-mail: shuochen@crhc.uiuc.edu; acq@tsinghua.edu.cn

http://www.tsinghua.edu.cn

Abstract: The DIDAPPER (distributed intrusion detector with apperception) system presented in this paper is a distributed intrusion detector with apperception. The distributed architecture, the apperception ability and the sharing of knowledge are evident characteristics of the DIDAPPER. This paper focuses on the apperception ability of DIDAPPER. Traffic specimens and IP traps are DIDAPPER's new concepts, which can capture and recognize abnormal traffics and are suitable for monitoring the large scale network attacks. The other aspect of DIDAPPER's apperception ability comes from the neural network algorithm. The BP neural network with learning ability has been applied to traffic analysis, and shows good effect on the recognition of traffic patterns.

Key words: IDS (intrusion detection system); large-scale automatic attack; traffic specimen; IP trap; pattern recognition; neural network, BP network

* Received September 8, 1999; accepted November 23, 1999
Supported by the National Technology Development Program of China under Grant No. 863-317 01-99