

# 基于人工神经网络入侵检测模型的探讨

陈丹伟, 黄秀丽, 任勋益

(南京邮电大学 计算机学院, 江苏 南京 210003)

**摘要:**目前,对 ANN IDS 的研究,主要集中在 ANN 算法的改进和具体原型的实现上,而对其模型的探讨则很少。模型研究对 IDS 发展意义重大,ANN 技术在 IDS 中也具有其它技术不可替代的优越性,因此,对 ANN IDS 的探讨尤为重要。文中对 ANN IDS 模型结构、特点及其使用场合均进行了探讨,介绍了 IDS 模型现状;阐明了 ANN 技术在 IDS 系统中的应用优势和发展;介绍了 IDS 模型中典型的 CIDE,IDES 和 DIDS 模型,并着重分析了三种 IDS 系统通用模型框架基于 ANN 技术的实现和应用。

**关键词:**人工神经网络;入侵检测模型;异常检测;误用检测

**中图分类号:**TP393.08

**文献标识码:**A

**文章编号:**1673-629X(2009)12-0143-03

## An Approach to IDS Model Based on Artificial Neuron Network

CHEN Dan-wei, HUANG Xiu-li, REN Xun-yi

(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

**Abstract:**At present, people often focus on the research of the optimization of ANN algorithm and implementation of IDS model, few people care IDS model itself. But the research on IDS model is vital to the development of IDS, especially for IDS model based on ANN which is a key detect technique in IDS. So it is necessary to study ANN IDS model. Introduce the development of IDS model and the superiority of ANN firstly, then discuss all IDS models based on ANN in detail. Introduce the CIDE, IDES and DIDS models in IDS model. Analyse the implementation and application of the 3 kinds of IDS system model based on ANN.

**Key words:**artificial neuron network; IDS model; anomaly detection; misuse detection

## 0 引言

随着 IT 技术的高速发展,计算机网络进入复杂网络阶段,网络攻击进入复杂攻击阶段。针对这些复杂的攻击,单靠单一的 IDS 系统很难检测出来,需要 IDS 系统之间以及与其他系统之间的交互和协作,形成一个整体有效的安全保障系统<sup>[1]</sup>。为解决 IDS 系统之间以及与其他安全产品之间的互操作性,国际上的一些研究组织开展了标准化研究。

目前对 IDS 进行标准化工作的有两个组织:Common Intrusion Detection Framework(CIDE)和 IETF 的 Intrusion Detection Working Group(IDWG)。CIDE 所做的工作主要包括四部分:IDS 的体系结构、通信体制、描述语言和应用编程接口(API)。IDWG 主要负责制定入侵检测响应系统之间共享信息的数据格式和交换信息的方式,以及满足系统管理的需要。

对 IDS 模型的研究始于 CIDE 组织提出的通用入侵检测框架 CIDE,在此之后相继出现了另外两类典型 IDS 系统通用模型:入侵检测专家系统(IDES)<sup>[2]</sup>和分布式入侵检测系统(DIDS)。这三种模型是 IDS 模型发展史上最经典的三种模型,大多 IDS 的原型系统借鉴这些思想由这些模型发展演变而成。

IDS 从检测技术上划分为误用检测和异常检测,这两种检测均可采用 ANN 技术。与传统的误用检测技术和其他异常检测技术相比,ANN 技术的优势在于:1. 分析速度很快,可以用于实时分析;2. 能够较好地处理带噪声的数据。

目前,很多组织和个人展开了对 ANN IDS 技术的研究:Debar 等人采用递归型(Recurrent)BP 网络,并同时结合传统的专家系统进行入侵检测。Cannady 和 Mahaffey 将 MLP 模型和 SOM/MLP 混合模型应用到基于网络流量的滥用检测模型中;MIT 的 Lippmann 和 Cunningham 明确提出采用关键词和 ANN 相结合的方法进行网络入侵检测并针对 Telnet 服务会话进行了相关研究等。

收稿日期:2009-04-11;修回日期:2009-07-04

基金项目:国家十一五科技支撑计划项目(2007BAK34B06)

作者简介:陈丹伟(1971-),男,副教授,硕士研究生导师,研究方向为信息安全。

## 1 基于神经网络的入侵检测模型探讨

### 1.1 基于神经网络的 CIDEF 模型

#### 1.1.1 CIDEF 模型结构

通用入侵检测框架 CIDEF 是为了在不同的 IDS 系统、入侵响应系统之间共享信息而制定的一套标准。由 DARPA 提出的,最早由加州大学戴维斯分校安全实验室主持起草工作。CIDEF 根据 IDS 系统通用的需求以及现有的 IDS 系统的结构,将 IDS 系统的构成划分为四类功能组件:事件发生器、事件分析器、事件数据库、响应单元。

CIDEF 模型工作原理:事件发生器组件负责从监控环境获取信息,然后将信息传送给事件分析器和事件数据库,事件分析器对接收到的数据进行检测分析然后将分析结果告知响应模块和事件数据库,事件数据库存储来自其他模块的信息,响应模块对于分析的结果根据响应策略进行响应。

#### 1.1.2 基于神经网络的 CIDEF 模型

将神经网络技术用于 CIDEF,将得到两种基于神经网络的 CIDEF 模型:误用检测模型<sup>[3]</sup>和异常检测模型<sup>[4]</sup>,其检测流程图如图 1 所示。

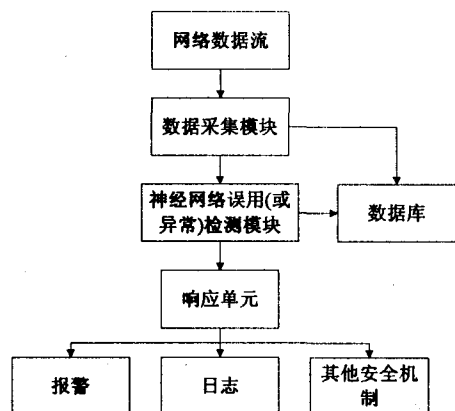


图 1 基于神经网络的 CIDEF 模型

误用检测模型能够快速准确地检测出已有的攻击类型,误报率低,缺点是只能发现已知的攻击,对未知的攻击无能为力。异常检测模型可以使系统检测出未知攻击或其它情况,缺点是误报率较高。

神经网络训练成功后,其响应速度非常快,因此,基于神经网络误用检测模型适用于误报率低、有实时性要求的场合;而基于神经网络异常检测模型适用于病毒更新快、有实时性要求的场合。

### 1.2 基于神经网络的 IDES 模型

#### 1.2.1 IDES 模型结构

入侵检测专家系统(IDES)是 Denning 和 Peter Neumann 从 1984 年到 1985 年研究并发展的

一个实时 IDS 模型。该系统包括一个异常检测器和一个专家系统,分别用于异常模型的建立和基于规则的特征分析检测。IDES 模型中有 6 个主要构件:审计数据源、模式匹配器、轮廓特征引擎、策略规则、异常检测器和警报报告产生器。

IDES 模型工作原理:该系统包含一个专家系统和一个异常检测器,审计数据源是从所要监控系统获取的监控信息,审计数据源模块将信息同时传送给该系统的专家系统和异常检测器,分别用于基于规则的特征分析检测和异常检测器的检测,警报/报告产生器对产生的检测结果进行融合。

#### 1.2.2 基于神经网络的 IDES 模型

技术层面上,误用检测模块和异常检测模块都可以采用 ANN 技术。模型层面上,按误用检测模块和异常检测模块的关系,划分为并行模型和串行模型。并行模型中根据误用检测和异常检测两个模块的合作关系又分为三种:互补模型<sup>[5,6]</sup>、辅助模型<sup>[7]</sup>和嵌套模型<sup>[8,9]</sup>。互补模型中,两个模块以独立并行工作为主、以相互动态更新为辅。辅助模型中,辅助模块对主检测模块以辅助处理为主、以辅助更新为辅。嵌套模型中,嵌入模块对主检测模块以动态自适应更新为主、以双重认证为辅。

各种模型流程图如图 2~图 4 所示。

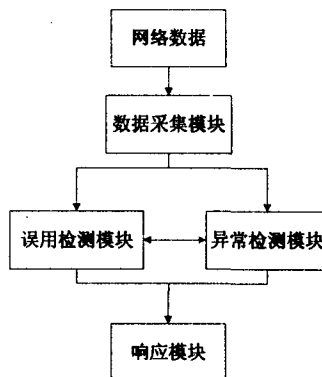


图 2 互补模型

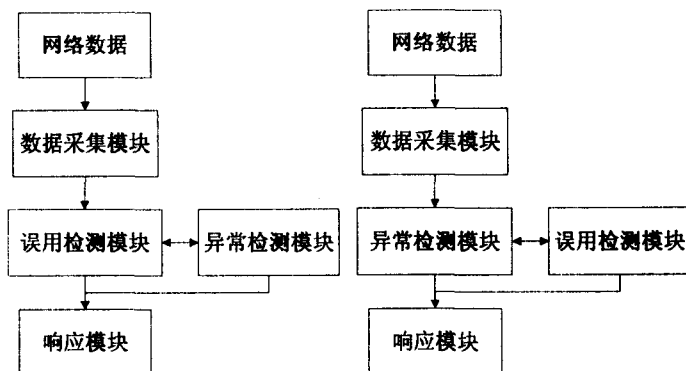


图 3 辅助模型的两种情况

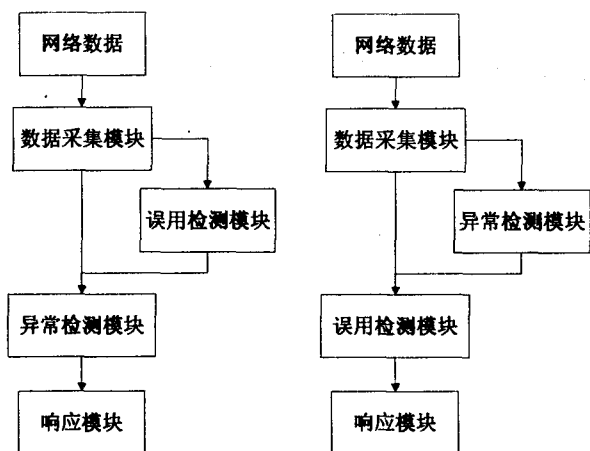


图 4 嵌套模型两种情况

IDES 模型将误用检测和异常检测技术结合起来,通过提高 IDS 的效率,降低误警率和漏警率,提供了更高的安全性能。

几种基于神经网络的 IDES 模型中:互补模型中,两种检测同时进行,实时性和安全性最好,缺点是误报率高,适合实时性要求高的场合;辅助模型中,检测效率和误报率优于互补模型,实时性不如互补模型,适合安全性和实时性要求稍低的场合;嵌入模型中,自适应更新能力最强,适合在新病毒频发的场合。

### 1.3 基于神经网络的 DIDS 模型

#### 1.3.1 DIDS 模型介绍

1998 年的 Internet 蠕虫事件之后,网络安全引起了军方、学术界和企业的高度重视。美国空军、国家安全和能源部共同资助空军密码支持中心、劳伦斯利弗摩尔国家实验室、加州大学戴维斯分校、Haystack 实验室,开展对分布式入侵检测系统(DIDS)的研究,将基于主机和基于网络的检测方法集成在一起。DIDS 模型中有四类主要部件:控制器、代理、事件发生器、监视器。

DIDS 模型工作原理:检测器负责检测其所在网段上的数据流,进行实时自动攻击识别和响应。检测器有代理、事件发生器和监视器组成,其中监视器和事件发生器监视数据流并采集数据,代理负责检测和 DIDS 通信。DIDS 控制器完成整个分布式安全检测预警系统的管理和配置。

#### 1.3.2 基于神经网络的 DIDS 模型

DIDS 模型是多点监控 IDS<sup>[10]</sup>,而 CIDF 模型以及 IDES 模型都是单点监控 IDS。技术层面上,DIDS 模型中的单点检测部件均可采用 CIDF 或 IDES 模型实现。模型层面上,DIDS 模型分为三类:集中控制模型、分层控制模型、基于 P2P 模型。

集中控制模型由数据收集组件和数据处理组件组

成。它的弱点是:容易单点失效、系统可扩展性差、网络负载重。集中控制是最早的分布式模型,适用于小型网络。

分层控制模型解决了集中控制模型中的一些缺点。数据处理组件按层次分布,划分为多个级别,呈树状分布。它的缺点是:体系灵活性差、层上存在瓶颈。分层控制适用于中型网络,AAFID<sup>[11]</sup>、EMERALD<sup>[12]</sup>和 SHOMAR<sup>[13]</sup>是分层控制模型的例子。

基于 P2P 的 DIDS 模型是完全分布式协同检测模型,避免了层次化系统检测结构存在的缺点。在这种模型中,所有组件是对等的,不存在逻辑上的从属关系,提高了系统的可靠性。完全分布式(对等)协同检测模型是刚刚兴起的一项研究<sup>[14]</sup>。芝加哥大学提出了一个分层结构的 P2P IDS 模型 - INTCTD<sup>[15]</sup>,它由数据收集模块、学习模块、状态声明模块、通信模块和加密模块组成。基于 P2P 的 DIDS 模型主要用于大型网络。

## 2 结束语

随着 ANN 技术的不断进步和 IDS 模型的不断创新,基于神经网络的 IDS 系统将会有更高的性能和效率。文中总结了各种 ANN IDS 模型,并进行了详细分析。一个好的 IDS 模型需要能够满足系统各方面要求,在实际应用中,应该结合系统的实际情况,来采用合适的 IDS 模型。

### 参考文献:

- [1] Hooper E. Intelligent Detection and Response Strategies for Complex Attacks[J]. IEEE A&E Systems Magazine, 2007, 22(11):3-12.
- [2] Denning D E, Neumann P G. Requirements and Model for IDES - a Real - time Intrusion - detection Expert System [R]. SRI International, USA: Computer Science Laboratory, 1985.
- [3] Cannady J. Artificial neural networks for misuse detection [C]//National information systems security conference. Arlington, VA, USA: National Computer Security Center, 1998.
- [4] de Lima I V M, Degaspari J A, Sobral J B M. Intrusion Detection Through Artificial Neural Networks[C]//Network Operations and Management Symposium. Salvador da Bahia, Brazil: [s. n.], 2008:867-870.
- [5] 许占文,王鹤翔,张 锦.一种神经网络和模式匹配相结合入侵检测系统[J].沈阳工业大学学报,2007,29(3):336-339.
- [6] 李之棠,李家春.模糊神经网络在入侵检测中的应用[J].

(下转第 161 页)

式具体说明如下:

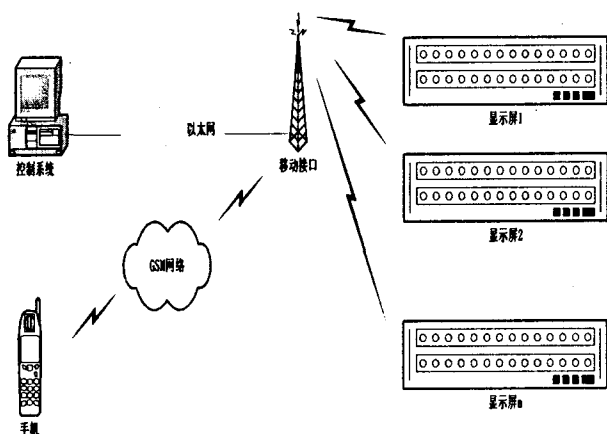


图 6 大规模应用模式

(1)由控制系统统一设置 1 号用户,1 号用户具有最高权限。1 号用户能授权给 2、3、4 号用户,也能解除 2、3、4 号用户的权限。1 号用户能向所有信息位置发送信息、查询信息或删除信息。

(2)2、3、4 号用户没有用户授予权,只有发布信息、查询信息的权限。

(3)如果遇到移动公司进行号码升位、修改等情况时,用户权限设置更改方案如下:a.1 号用户用<ALOCK>指令更改 1 号用户的号码。b.1 号用户用<ALOCK>指令更改 2、3、4 号用户的手机号。

(4)每收到新的短消息后,在当前显示的短信完成后,先显示当前短信,再按照短信位置循环显示。

(5)每条短信字体大小,字间距按照具体屏大小设置。

(6)显示屏每收到一条正确的指令后均由蜂鸣器发出长鸣表示操作已成功(如指令正确而屏不支持此功能也发出长鸣),如指令错误则发出间断声音表示指

令不正确。

## 4 结束语

该系统结合了 GSM 网络,采用无线传输,组建方便,易于实现,动态管理<sup>[8]</sup>。同时系统具有很好的扩展功能,可根据需要增加其他功能或裁减现有功能。该系统附加语音播报、应急闪烁、各种传感器等功能,广泛应用于高速公路广告和交通指示、生产现场的滚动显示生产看板、广场等公共场所的室内外广告发布和音视频传输放映系统、气象信息发布和自然灾害应急指挥系统,公共安全防范系统等方面。

## 参考文献:

- [1] 吴玉田,王瑞光,郑喜凤,等. GSM 模块 TC35 及应用[J]. 计算机测量与控制,2002,10(8):557-560.
- [2] 杨素英,刘会景,李 琨. 基于 GSM 短消息的远程无线数据采集系统的设计[J]. 计算机技术与发展,2007,17(11):103-105.
- [3] Zhang Guiming. Research and design of remote control and alarm system based on GSM/SMS[J]. Journal of Sichuan Normal Univeristy: Natual Science,2004,27:51-53.
- [4] Siemens Mobile, TC35i AT Command Set, Version 00.01, DocID TC35i-ATC-V00.01(2003)[M]. [s.l.]:[s.n.], 2003.
- [5] AT Command Set(Siemens Cellular Engines) Version 03.10 [DB/CD]. 北京:西门子(中国)有限公司,2002.
- [6] 诸昌铃.LED 显示屏系统原理及工程技术[M]. 成都:电子科技大学出版社,2000.
- [7] 徐妙君,张晓霞. 短消息控件的设计与实现[J]. 计算机技术与发展,2007,17(8):64-66.
- [8] 贾玉涛. 实用移动无线通信[M]. 北京:国防工业出版社,1995.

(上接第 145 页)

小型微型计算机系统,2002,23(10):1235-1238.

- [7] 马海峰,孙名松. 基于多层前向神经网络入侵检测系统的研究[J]. 哈尔滨理工大学学报,2004,9(2):52-55.
- [8] 刘美兰,姚京松. 神经网络在入侵检测系统中的应用[J]. 计算机工程与应用,1999,35(6):37-42.
- [9] 刘道群,孙庆和. 基于遗传神经网络的入侵检测模型[J]. 激光杂志,2005,26(6):73-74.
- [10] 马海峰,岳 新,孙名松. 基于神经网络的分布式入侵检测研究[J]. 计算机应用,2006,26:63-65.
- [11] Bal: asubra maniyan J S, Garcia - Fernandez J O, Lsacoff D. Architecture for intrusion detection using autonomous agents [M]. [s.l.]:COAST Laboratory,Purdue University,1998.
- [12] Porras P A, Neumann P G. EMERALD: Event monitoring enabling responses to anomalous live disturbances[C]//The

20th National Information Systems Security Conf (NISSC). Baltimore, MD, USA:[s.n.],1997.

- [13] Undercoffer J, Perich F, Nicholas C. SHOMAR: An Open Architecture for Distributed Intrusion Detection Services[R]. Baltimore County: University of Maryland,2002.
- [14] Locasto M E, Parekh J J, Keromytis A D, et al. Towards Collaborative Security and P2P Intrusion Detection[C]//Information Assurance Workshop, Proceedings from the Sixth Annual IEEE SMC. NY, USA: IEEE,2005:333-339.
- [15] Dumitrescu C L. INTCTD: A Peer-to-Peer Approach for Intrusion Detection[C]//Sixth IEEE International Symposium on Cluster Computing and the Grid. Singapore: IEEE, 2006:89-92.