基于混沌神经元的延时滥用入侵检测模型

姚 羽,高福祥,于 戈
(东北大学信息科学与工程学院,辽宁沈阳 110004)

摘 要: 在研究混沌神经元延时特性的基础上,构建了 MLP/CNN 混合前馈型神经网络.提出基于混沌神经元的滥用入侵检测模型,它既具备 MLP 的分类功能,又具有混沌神经元的延时、收集和思维判断功能,具有灵活的延时分类特性,因而能够有效地识别分布式入侵.使用从网络数据流中获取的样本,以 FTP 口令穷举法入侵为例,对该模型进行仿真和整体测试,结果表明可以依据实际情况设置入侵判据,本文对 FTP 入侵检测的精确率在 98 %以上,误报率和漏报率均小于 2 %.该模型可以推广到检测分布式 DOS 等具有延时特性的攻击行为和具有延时分类要求的其它系统中.

关键词: 滥用入侵检测; MLP/CNN 混合神经网络; 混沌神经元; 延时分类
中图分类号: TP309 **文献标识码**: A **文章编号**: 0372-2112 (2004) 08-1370-04

A Time-Delayed Misuse Intrusion Detection Model Based on Chaotic Neuron

YAO Yu, GAO Fu-xiang, YU Ge
(Faculty of Information Science and Engineering, Northeastern University of China, Shenyang, Liaoning 110004, China)

Abstract: A hybrid MLP/CNN neural network is constructed based on research on time-delayed characteristic of chaotic neuron. A misuse detection Model based on chaotic neuron is proposed, which has both the capability of classification which MLP has and the functionality of time-delay, collection and judgment which chaotic neuron has. Because this intrusion detection system has flexible time-delay characteristic, it can identify distributed intrusion effectively. The simulation and test is conducted using samples captured from data traffic. The detection rate of FTP (File Transfer Protocol) brute-force attack is up to 98 %. The false alarm and false negative rates are both less than 2 %. The model proposed in this paper may be generalized to time-delayed intrusion detection systems such as distributed DOS etc. and other time-delayed classification systems.

Key words: misuse intrusion detection; hybrid MLP/CNN neural network; chaotic neuron; time-delay classification

1 引言

随着计算机及网络技术的不断发展和普及,网络安全问题已经成为人们日益关注的问题,入侵检测系统是网络安全研究领域中的重要课题之一.由于滥用入侵检测具有高效率,高精度,低误报率的特点,是目前面向应用的系统中常用的入侵检测实现方式.滥用入侵检测可以采用模式匹配,协议分析,专家系统和神经网络等方法实现.其中,MLP (Multiple-level perceptron) 神经网络被引入入侵检测专家系统[1],初步实现了对入侵事件的识别,为将神经网络应用到入侵检测领域开辟了道路.MLP 神经网络入侵检测模型虽然具有并行处理,高效决策的特点,但是它仅能对孤立的网络事件进行分类,因此,不能有效的识别分布协作式入侵.

本文首次提出一种新的基于混沌神经元的延时滥用入侵检测模型.该模型利用 MLP 神经网络识别孤立的网络事件,再利用混沌神经元的延时特性,识别分布式入侵,使新模型具备了灵活的延时分类特性,提高了模型的整体性能.

2 滥用入侵判据

随着入侵手段的不断发展,大规模、分布协作式攻击逐渐成为网络入侵的主要趋势.这些攻击由若干次相对独立的网络通信组成,这些通信虽然单独看起来是合法的,而组合起来就构成了攻击.如 FTP 用户口令穷举法入侵.由于入侵行为持续时间存在不确定性,可能是 1 分钟、1 小时、或 1 天,2 天,或者因为入侵的"重要性"和艰巨性,以及由于网络的安全措施完备等原因,甚至会持续更长的时间.因而,检测出一次或若干次 FTP 用户口令输入错误,不能确定是否存在入侵事件,只有通过较长时间的监测,才能得出结论,这就是入侵的延时特性.为了综合分析网络事件,提出新的定义:

定义 1(误用行为) 组成一次入侵事件序列中的孤立网

收稿日期:2003-09-15;修回日期:2004-04-19
基金项目:国家自然科学基金(No. 60173051);国家教育部博士点基金(No. 20030145029);教育部高等学校优秀青年教师教学和科研奖励基金;国家 863 项目(No. 2003AA414210)

络事件,是误用行为.例如一次 FTP 用户口令输入错误就是一次误用行为.

定义 2(有效延时时间)　入侵检测系统有效检测一次入侵所持续的最长时间,为系统的有效延时时间.

根据上面的定义,一次入侵行为需要依据三元组:

〈误用行为,有效延时时间,误用极限值〉

来判别.例如,对 FTP 用户口令的穷举法入侵检测的依据可以记作 < FTP password error, M minute, N〉,表示在 M 分钟内识别出 N 次 FTP password error 时,则认为发生了一次入侵.

3　混沌神经元

MLP 神经网络的神经元只有两种状态:抑制状态和兴奋状态,不能模拟大脑的思维过程.医学界已经证实,大脑思维时脑电波呈现混沌状态,而睡眠时为周期性电波.为了使神经网络具有与大脑活动类似的收集、思维和分类的高级功能,需要使用更加复杂的神经元来实现,这就是混沌神经元.

3.1　混沌神经元数学模型

F Pasemann 提出的混沌神经元数学模型如下[2]:

$$O(t+1) = \gamma \cdot O(t) + b + I + \omega_s \cdot \sigma(O(t)) \qquad (1)$$

其中,$O(t)$、$O(t+1)$分别为 t、$(t+1)$时刻混沌神经元的值.$\gamma(0 < \gamma \leq 1)$为混沌神经元记忆衰减率,$\gamma \cdot O(t)$反映了它的记忆衰减特性.$I$为混沌神经元的输入,$b$为阈值,$\omega_s$为自权值,激发函数为 Sigmoid 函数.

本文将 MLP 的分类结果作为混沌神经元的输入,模型(1)转换为:

$$O(t+1) = \gamma \cdot O(t) + b + \sum_{k=1}^{n}\sum_{j=1}^{n_y}\omega_j y_{ki} + \omega_s \cdot \sigma(O(t)),$$
$$t = 1, 2, \cdots, n_p \qquad (2)$$

式 $\sum_{k=1}^{n}\sum_{j=1}^{n_y}\omega_j y_{ki}$ 为混沌神经元的第 k 次输入,n 为 MLP 网络输出次数;n_y 为输入结点的个数,等于 MLP 网络输出结点个数;y_{ki} 为 MLP 网络的第 i 个结点的第 k 次输出,ω_j 是 MLP 到混沌神经元的连接权值,n_p 为迭代次数,其余符号与公式(1)相同.

式 $\sum_{k=1}^{n}\sum_{j=1}^{n_y}\omega_j y_{ki}$ 代表该神经元对过去的事物具有记忆和收集功能,弥补了普通神经元只能处理当前信息的弱点,实现识别延时系统中的复杂入侵行为.

3.2　混沌神经元参数

模型(1)具有多个参数,都可以作为混沌分岔参数,如 γ、ω_s 和 I.本文研究混沌神经元的输入与输出之间的关系,因此选取输入 I 作为分岔参数.

对于某一具体的神经元,参数 γ、b 和 ω_s 应为常数.当 γ、b 和 ω_s 选取不同值时,混沌神经元的运行机制不同.

本文选取 $\omega_s = -16$、$\gamma = 0.6$、$b = 7$.该混沌神经元运行机制如图 1 所示,呈现出关于输入的混沌、倒分岔现象.混沌神经元的内部状态随着输入的增加,经历了混沌和有限的周期窗口后,倒分岔结束,进入稳定的 $P-1$ 解,从而使网络状态的奇怪吸引子达到一个稳定的平衡点,混沌表现为自相似结构的暂存状态.

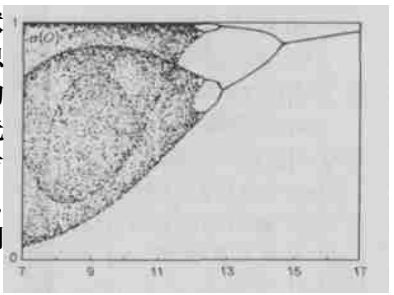

图 1　混沌神经元运行机制
($w_s = -16$、$\gamma = 0.6$)

神经元处于混沌状态时,模拟神经元的思考阶段;处于倒分岔的多周期解时,为神经元的思维整理阶段,只有进入稳定的 P-1 解时,混沌神经元才能做出判断.

根据 Elman 网络的功能特点和混沌神经元的数学模型,采用双 Elman 网络描述混沌神经元.

4　MLP/CNN 混合神经网络模型

下面说明混合神经网络模型的建立、训练及仿真测试.

4.1　MLP/CNN 模型的建立

分别建立 MLP 和混沌神经网络模型,然后形成混合网络模型.

目前,尚无选择 MLP 最佳网络拓扑结构的理论依据,本文通过测试网络结构的方法.根据网络数据流,MLP 网络具有 9 个输入和 2 个输出.用 1、0 和 0、1 代表误用行为和正常行为.输入数据结构如下:

ProtocolID	0:代表运输层协议为 TCP;
	1:代表运输层协议为 UDP;
SourcePort	源端口号.如 21,22,80;
DestPort	目的端口号;
SourceAddr	ABC 类地址;
DestAddr	ABC 类地址;
ICMPTypeID	ICMP 类型;
ICMPCodeID	ICMP 代码;
RawDataLength	Random;
RawDataID	Random.

用户可以自定义误用发生的条件.本文误用发生的条件为:TCP 协议(*ProtocolID* = 0),Server 端在 21 端口发送的 RawDataID 为 1000.文中的样本未经特殊说明,均采用这种数据结构.网络数据流样本举例如表 1 所示.

为了确定 MLP 网络是否能够鉴别那些端口号十分接近,如 21,20,22,而 RawDataID 又相同的样本,生成300组测试样

表 1　样本举例

Prot ID	Source port	Dest port	Source Address	Destination Address	ICMP TYPE ID	ICMP CODE ID	Raw Data Length	Raw Data ID	Attack
0	20	7952	2626939000	2941786000	9999	9999	4829	1000	0 1
0	22	29787	432674100	284201000	9999	9999	636467	1000	0 1
0	21	62660	3770657000	2278177000	9999	9999	46043	1000	1 0
0	8080	43704	1838977000	635998300	9999	9999	35578	38562	0 1

本. 表 1 中的第一和第二组样本为正常行为,而第三组为误用行为. 采用 BP 算法,分别对 5 层、4 层、3 层结点的网络进行测试,最后选择了 9-6-2 三层结点网络. 该模型神经元结点总数少并可达到分类要求.

4.2 MLP/ CNN 模型的训练

为了避免直接训练混合网络算法过于复杂及费时等缺点. 首先单独训练 MLP 和 CNN,然后训练整个网络.

从计算机网络数据流中采集的数据,经过前处理,形成 10000 组数据作为 MLP 训练样本. 训练参数:初始连接权值为 - 0.002 到 0.002 之间的随机数,学习速率为 10. 采用 BP 算法,经过 200EPOCH 训练,计算结果与期望值的差小于或等于 2.60E-5. 结果表明,该 MLP 网络具备识别 FTP 误用行为的功能.

CNN 网络的输入是 MLP 的输出,所以 CNN 网络的输入数据均为 0 或 1. 首先生成 0、1 编码序列,1 代表一次误用,0 代表正常通信. 将每一个编码与其反码组成 2 元组,形成二元组序列,作为 CNN 网络的输入. 共 2000 组数据,其中包含 300 组误用行为,作为 CNN 网络训练样本. 用户根据需要自定义判断一次入侵所依据的三元组. 本文规定〈FTP password error ,24 hours ,30〉,〈FTP password error ,48 hours ,50〉,〈FTP password error , 24 hours , 100〉,〈FTP password error ,24 hours , 200〉,〈FTP password error , 48 hours ,300〉5 个三元组为入侵行为判定条件. 即二元组序列中的‘1’编码的个数大于或等于期望值 Intrusion 时,发生入侵事件. 采用 BP 算法训练,使期望值与计算结果误差小于定值.

MLP/ CNN 混合网络训练入侵行为判定条件与上面相同. 网络的初始参数是训练后的 MLP 和 CNN 网络参数. 采用 BP 算法,使用训练 MLP 的 10000 组样本训练混合网络,当期望值与网络输出的差小于定值时训练结束.

4.3 MLP/ CNN 模型的仿真测试

在局域网环境下,对 FTP 服务器进行 5 轮用户口令的穷举法攻击,每轮攻击包含 245 次 FTP 误用. 截获网络数据,经过前处理后形成 5 组测试样本,判别依据与 4.2 节相同. 仿真测试结果列于表 2 中.

表 2 FTP 攻击测试结果

三元组判别条件	实测误用次数	误差 %	入侵次数	误报率 %	漏报率 %
1	31	3.33	8	0.0	1.25
2	49	2.0	4	0.0	0.0
3	100	0.0	2	0.0	0.0
4	202	1.0	1	0.0	0.0
5	无	0.0	无	0.0	0.0

本文仅对 FTP 用户口令穷举攻击进行检测,测试结果表明,MLP/ CNN 混合神经网络能够检测分布式 FTP 入侵行为. 对其他入侵行为的检测能力仍需进一步测试.

5 MLP/ CNN 与其它神经网络的比较

最近几年,为了识别具有延时特性的入侵行为,出现了多种神经网络入侵检测系统.

本文认为必须对基于神经网络的入侵检测系统的性能评价进行修改,以适应当前入侵手段的不断变化并能体现出神经网络的所具备的特性.

首先,应具备灵活的延时特性.

其次,应具备结构稳定性和属性稳定性. 也就是说,当改变延时特性时,不需改变神经网络的结构,同时不需要重新组织样本、重新训练网络.

本文提出的 MLP/ CNN 网络,用户可以根据实际情况给出三元组,作为判别入侵的依据. 本文以检测 FTP 口令穷举法入侵作为应用实例,这种网络可以推广到其它具有延时特性的入侵行为,如端口扫描,DDOS 等. 表 3 对现行的各种神经网络进行了比较.

表 3 神经网络入侵检测系统比较

特性 / 类型	网络类型	延时时间	实时性	网络结构稳定性	网络属性稳定性	FTP 滥用检测(%)			延时入侵检测能力	备 注
						检测率	误报率	漏报率		
异常	KSOM	-	一般	稳定	不稳定	-	-	-	无	文献[4]
	SOM/ MLP	用户自定义	较好	不稳定	不稳定	24	0	76	有	文献[5]
	SOM/ RPROP	用户自定义	较好	不稳定	不稳定	97.9	4.191	6	有	文献[6]
滥用	MLP	-	差	稳定	不稳定	< 100	-	-	无	文献[1]
	SOM/ MLP	3 分钟	较好	稳定	不稳定	< 100	-	-	有限	文献[3]
	MLP/ CNN	用户自定义	好	稳定	稳定	98	2	2	灵活	本文

6 结论

本文构建的 MLP/ CNN 混合神经网络,首次将混沌神经网络应用到入侵检测系统中. 结果表明,混合网络分布式入侵检测的误报率和漏报率小于 2 %. 得到结论如下:

(1) MLP9-6-2 神经网络入侵检测系统训练收敛速度快,对 FTP 误用行为检测成功率达到 100 %.

(2) 验证了混沌神经元在入侵检测系统中的可行性和 MLP/ CNN 混合神经网络具备延时分类要求的特性.

(3) MLP/ CNN 入侵检测成功的经验,可以推广到其它形式的延时入侵检测系统中,如 DDOS 等.

参考文献:

[1] J Cannady. Neural networks for misuse detection: Initial results [A]. Recent Advances in Intrusion Detection ’98 Conference Proceedings [C]. Louvain-la-Neuve ,Belgium ,1998. 9. 31 - 47.

[2] F Pasemann. A simple chaotic neuron[J]. Physica D ,1997 ,104:205 - 211.

[3] J Cannady. Artificial neural networks for misuse detection [A]. 1998 National Information Systems Security Conference Proceedings[C]. Ar-

lington ,VA ,1998. 10. 443 - 456.

[4] B Rhodes ,et al. Multiple self-organizing maps for intrusion detection [A]. The 23rd National Information Systems Security Conference[C]. Baltimore ,MD ,2000. 10 - 14.

[5] A Bivens ,et al. Network-based intrusion detection using neural networks[J]. (2002) Artificial Neural Networks In Engineering proceedings. St. Louis ,Missouri ,2002. 11. 579 - 584.

[6] C Jirapummin ,et al. Hybrid neural networks for intrusion detection system[A]. The 2002 International Technical Conference on Circuits/ Systems ,Computers and Communications proceedings[C]. Phuket , Thailand ,2002. 7. 928 - 931.

作者简介:

姚　羽　男,1976 年 2 月生于辽宁沈阳,2001 年获东北大学工学硕士学位,现为东北大学信息科学与工程学院博士研究生,主要研究方向为:网络安全,混沌神经网络.

高福祥　男,1961 年 10 月生于山东省淄博市,现任东北大学信息科学与工程学院教授,研究领域为计算机及应用,主要研究方向为计算机网络及多媒体技术.

于　戈　男,1962 年生于辽宁大连,1996 年于日本九州大学获博士学位,东北大学教授,博士生导师,主要研究领域为数据库理论与技术、分布与并行式系统、网络信息安全等,中国电子学会高级会员、美国 ACM 和 ACM SIGMOD 会员、美国 IEEE 和 IEEECS 会员、日本 IPSJ 会员.