文章编号: 1001-0920(2007)04-0432-04

混合前馈型神经网络在入侵检测中的应用研究

姚 羽[1],高福祥[1],邓庆绪[1],于 戈[1],张守智[2]
(1. 东北大学 信息科学与工程学院, 沈阳 110004; 2. 辽宁省财政厅 信息中心, 沈阳 110002)

摘 要: 提出一种基于混沌神经元的混合前馈型神经网络,用于检测复杂的网络入侵模式. 这种神经网络具有混沌神经元的延时、收集、思维和分类的功能,避免了 MLP 神经网络仅能识别网络中当前的滥用入侵行为的弱点. 对混合网络进行训练后,将该网络用于滥用入侵检测. 使用 DARPA 数据集对该方法进行评估,结果表明该方法可有效地提高对具备延时特性的 Probe 和 DOS 入侵的检测性能.

关键词: 网络安全; 入侵检测系统; 前馈型神经网络; 混沌神经网络
中图分类号: TP393.08; TP183 **文献标识码**: A

Application of a hybrid feedforward neural network to intrusion detection

YAO Yu[1], *GAO Fu-xiang*[1], *DENG Qing-xu*[1], *YU Ge*[1], *ZHANG Shou-zhi*[2]
(1. College of Information Science and Engineering, Northeastern University, Shenyang 110004, China; 2. Information Center, Financial Department of Liaoning Province, Shenyang 110002, China. Correspondent: YAO Yu, E-mail: yaoyu@mail.neu.edu.cn)

Abstract: A hybrid feedforward neural network based on chaotic neuron is proposed to detect complicate network intrusion. The proposed neural network has the capability of time-delay, collection, thinking and classification, based on which the weakness of general neural network is avoided which can only detect current misuse intrusion. The neural network is trained and applied to misuse intrusion detection cases. This approach is evaluated by using DARPA data set. Results show that the system's capability of detecting time-delayed Probe and DOS attacks is enhanced effectively by using the proposed approach.

Key words: Network security; Intrusion detection system; Feedforward neural network; Chaotic neural network

1 引 言

随着计算机技术的不断发展,网络安全面临更加严峻的挑战. 入侵检测系统(IDS)作为网络安全研究领域中重要课题,得到了深入的研究,出现了大量研究成果.

文献[1]提出了基于 D-S 证据理论的网络异常检测方法,综合评判网络流量的特征值. 文献[2]提出了基于 KPLS 的网络入侵特征抽取及检测方法. 文献[3]提出了基于改进的竞争学习神经网络的入侵检测方法. 文献[4]提出了基于分级神经网络的入侵检测方法. 文献[5]采用 4 层 MLP(Multi-Level Perceptron),建立神经网络滥用入侵检测系统. 文献[6]采用基于入侵关键字累计技术的 MLP 网络进行入侵检测.

随着网络安全技术的不断发展,出现了分布协作式入侵方式. 该方式由多次独立行为组成,能有效地避开网络安全系统的防御策略. 在美国西点召开的 1999 年 CERT 年会上,文献[7]明确定义这种攻击行为是延时攻击,并指出延时攻击是危害极大且不易检测的入侵行为. 因此,神经网络方法需要更加有效地检测此类攻击.

文献[8]提出基于动态自组织影射神经网络的聚类方法进行入侵检测. 文献[9]中利用 SOM 完成预处理后,使用 BP 网络进行异常检测. 以上方法提高了神经网络识别具有延时特性的入侵行为的能力,但增加了神经网络结构及数据前处理的复杂性.

收稿日期: 2006-03-29; **修回日期**: 2006-07-14.
基金项目: 国家自然科学基金项目(60473073); 国家 863 计划项目(2004AA1Z2060); 国家 973 计划项目(2006CB303000); 广东省自然科学基金项目(04010589).
作者简介: 姚羽(1976—),男,沈阳人,讲师,博士,从事网络安全、非线性动力学等研究; 高福祥(1961—),男,山东淄博人,教授,博士,从事网络安全、嵌入式 Internet 等研究.

本文将混沌神经元[10]引入入侵检测系统,使系统以更加接近大脑的思维方式进行判断,提高识别能力.本文提出的 MLP/CNN 网络大大改善了神经网络系统的延时特性,可以推广到检测具有延时特性的复杂的入侵行为,如端口扫描,DOS 等.

2　混沌神经元延时检测模型

分布协作式攻击行为由若干次独立的网络通信组成,这些通信单独看是合法的,组合起来就构成了攻击.MLP 和 SOM/MLP 神经网络仅能识别网络中的单一入侵行为,其功能显然是不够的.

2.1　延时攻击

分布协作式攻击的最大优势是能够分阶段进行攻击,不暴露在实时检测之下,因而更加危险.

延时攻击指的是,需要持续一段时间完成或持续一段时间实现攻击企图的攻击行为[7].例如,端口扫描是入侵者对主机的 65535 个端口进行逐个探察,找出其中的弱点而发起的攻击[11].FTP 强力攻击的持续时间很难预测,可能是 1 min,1 h,或 1 d,2 d,甚至会持续更长的时间,是很难检测到的具有延时特征的入侵行为之一.

2.2　延时检测策略

军事部门采用提示与警告方法(I&W 方法)判定敌人的行动是否为军事入侵[7].在应用 I&W 方法时,只有当有意义的"提示"事件达到一定数量后,才能激活 I&W 系统发出"警告".若"提示"事件很少则不能触发"警告".

在入侵检测中,应采用相同的 I&W 策略确定异常行为或系统滥用[7].如果发现网络中的孤立的异常行为就判定为入侵,会导致误报率的增加,降低入侵检测的可信度.只有经过一段时间内的累积效果,才能得出入侵的结论.本文研究的神经网络方法就是利用混沌神经元的高阶信息处理能力对延时攻击进行延时分类检测.

2.3　混沌神经元

延时混沌神经元模型[10]如下:

$$O(t+1) = \gamma \cdot O(t) + I + \omega_s \cdot \sigma(O(t)). \quad (1)$$

其中:$O(t)$ 和 $O(t+1)$ 分别为 t,$(t+1)$ 时刻混沌神经元的值,代表神经元的内部状态;$\gamma(0 < \gamma \leq 1)$ 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;ω_s 为神经元的自权值,它的激发函数为 $\sigma(x) = (1 - e^{-\lambda x})/(1 + e^{-\lambda x})$ 双极性函数.当 ω_s 和 γ 在某一特定参数域内时,混沌神经元的状态呈现关于 I 的混沌、倒分岔的现象,如图 1 所示.

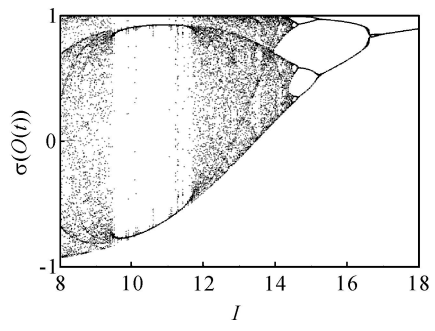


图 1　混沌神经元运行机制($\omega_s = -16$, $\gamma = 0.8$)

从图 1 可以看出,混沌神经元的状态随着输入 I 的增加,经历了混沌和有限的周期窗口后,当输入达到某一值时,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,说明该神经元具有输入增益效果和思考决策的功能.本文将混沌神经元的这一特性应用到入侵检测系统中.

3　混合前馈型神经网络模型

通过建立 MLP/CNN 混合前馈型神经网络,使入侵检测系统具有灵活的延时特性.

3.1　MLP/CNN 混合神经网络

通过训练 MLP 神经网络,当网络的 2 个输出结点输出 (0,1) 时表示网络数据流无误用行为,输出 (1,0) 时表示网络数据流中存在误用行为[12].

将 MLP 网络的输出作为后续的混沌神经元的输入,建立混合神经网络.混沌神经元模型为

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

式中:$\sum_{k}^{n}\sum_{j}^{n_y}\omega_j y_{ki}$ 为混沌神经元的第 k 次输入,n 为所计算的最大输入次数,n_y 为混沌神经元的输入结点数量,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,b 为输入偏移量,n_p 为混沌神经元的延时次数,其余与式(1)中相同.

$\sum_{k}^{n}\sum_{j}^{n_y}\omega_j y_{ki}$ 代表该神经元对过去的事物具有记忆和收集的功能.普通神经元只能处理神经元当前接收到的信息,而式(2)的输出不仅与 MLP 的当前状态有关,且与前 k 次状态的累积效果相关,以实现识别延时系统中复杂的入侵行为.

3.2　网络训练

为避免递归网络算法复杂、训练费时的缺点,应用前馈静态网络成熟的算法,使用开环训练、闭环再训练的算法对网络进行训练[13].

首先构建并训练 MLP 神经网络[14].然后利用

开环训练混沌神经网络,生成 0,1 编码. 1 代表存在误用,0 代表正常通信. 将每个编码与其反码组成 2 元组,形成二元组序列,作为混沌神经网络的输入. 当规定二元组序列中的"1"编码的个数小于 n_{max} 时,神经元处于混沌状态;当接近于 n_{max} 时,神经元处于倒分岔中;只有当大于 n_{max} 且神经元进入稳定解时,认为发生了入侵事件. 最后,利用 BP 算法闭环再训练,得到 MLP 网络与混沌神经网络之间的连接权值.

3.3 网络测试

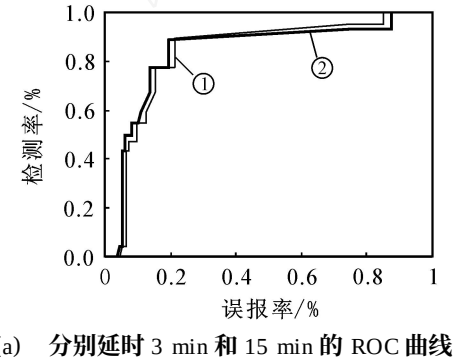
为了验证 MLP/CNN 混合神经网络识别模拟数据流的能力,使用 FTP-brute force 攻击,对网络进行 5 次检测. 测试结果见表 1. 当案例中没有 FTP 攻击模式时,混沌神经元处于混沌状态;而当案例中存在 33 个 FTP 攻击事件时,混沌神经元处于 P-1 状态. 测试结果有力地证明了混合神经网络模型具有检测复杂入侵行为的能力.

表 1 MLP/CNN 混合前馈型神经网络测试结果

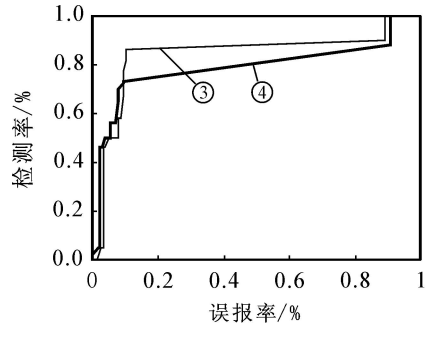
误用次数	0	8	12	25	33
测试结果	混沌状态	周期窗口	混沌状态	倒分岔周期 4	周期 1

4 评估及性能对比

为了验证本文方法的整体性能,采用林肯实验室发布的 DARPA 数据集[15]进行离线评估.



(a) 分别延时 3 min 和 15 min 的 ROC 曲线



(b) 分别延时 30 min 和 2 h 的 ROC 曲线

图 2 4 个不同延时时间的滥用检测结果

4.1 评估结果

在 MLP/CNN 神经网络模型中,采用不同的延时时间会产生不同的 ROC 曲线. 分别取延时时间为 3 min,15 min,30 min 和 2 h,得到 ROC 曲线如图 2 所示. 其中:①为延时 3 min;②为延时 15 min;③为延时 30 min;④为延时 2 h. 计算 ROC 曲线下面积,使用阳性似然比和 Youden 指数分析获得最佳工作点[16],如表 2 所示.

表 2 MLP/CNN 混合神经网络模型评估结果

延时 min	面积	最佳工作点					
		阳性似然性			Youden		
		检测率%	误报率%	似然比	检测率%	误报率%	指数
3	0.687	43.3	6.3	6.87	89.2	21.4	0.678
15	0.711	43.3	5.1	8.49	88.4	19.5	0.689
30	0.736	46.2	3.2	14.44	86.2	10.3	0.759
2	0.697	46.2	2.2	21.00	73.2	9.5	0.637

4.2 性能对比

对现有的几种神经网络入侵检测方法使用 DARPA 数据集评估,得到的结果见表 3. 通过对比可以看出,MLP/CNN 混合神经网络对 Probe 攻击的检测率为 92.1%,对 DOS 攻击的检测率为 93.5%. 这表明 MLP/CNN 混合神经网络对 4 种攻击的综合检测率高,它的整体性能指标最好.

表 3 神经网络入侵检测方法的检测率/误报率

检测方法	检测能力	Probe	DOS	U2R	R2L	文献
MLP	DR	0.787	0.872	0.132	0.156	[12]
	FPR	0.704	0.085	0.003	0.015	
SOM	DR	0.721	0.864	0.115	0.103	[9]
	FPR	0.062	0.071	0.001	0.012	
SOM/MLP	DR	0.801	0.886	0.117	0.074	[6]
	FPR	0.062	0.074	0.003	0.022	
MLP/CNN	DR	0.921	0.935	0.056	0.553	本文
	FPR	0.124	0.026	0.002	0.006	

MLP/CNN 方法整体性能高的原因,在于它利用混沌神经元的高阶处理能力,提供了灵活的延时手段,提高了对延时入侵行为的检测能力. 但是,该神经网络对于 U2R 和 R2L 攻击行为的检测能力较差,原因是该方法仅能对基于网络的入侵行为进行检测. 在需要检测新型的攻击时,MLP/CNN 的性能明显下降,这主要由于基于滥用入侵检测的 MLP 无法对已知的知识进行推广,这需要在今后的研究中加以改进.

5 结 语

通过实验结果可以看出,利用混沌神经元的高阶处理能力,能够对复杂的延时攻击行为进行有效地检测. 本文提出的混合前馈型神经网络能够有效地检测具有延时特性的入侵行为,具有结构稳定性和属性稳定性,有效地提高了系统的检测能力. 但是,该方法仍然没有完全发挥出混沌神经元的高阶处理能力,在检测性能上仍有提高空间. 另外,本文

方法所实现的算法复杂度仍然较高,需要进一步简化算法.同时,本系统是一个模型系统,要建立起一个完整高效的、有实用价值的网络入侵检测系统,仍需要进行大量的研究工作.

参考文献(References)

[1] 诸葛建伟, 王大为, 陈昱, 等. 基于 D-S 证据理论的网络异常检测方法[J]. 软件学报, 2006,17(3): 463-471.
(Zhuge J W, Wang D W, Chen Y, et al. A network anomaly detector based on the D-S evidence theory[J]. J of Software, 2006,17(3): 463-471.)

[2] 杨辉华, 王行愚, 王勇,等. 基于 KPLS 的网络入侵特征抽取及检测方法[J]. 控制与决策, 2005, 20(3): 251-256.
(Yang H H, Wang X Y, Wang Y, et al. KPLS approach for network intrusion feature extraction and detection[J]. Control and Decision, 2005, 20(3): 251-256.)

[3] Le J, Ghorbani A. Network intrusion detection using an improved competitive learning neural network[C]. Proc of the 2nd Annual Conf on Communication Networks and Services Research. Fredericton: CA Press, 2004: 190-197.

[4] Zhang C L, Jiang J, Mohamed Kamel. Intrusion detection using hierarchical neural networks [J]. Pattern Recognition Letters, 2005, 26(6): 779-791.

[5] Cannady J. Neural networks for misuse detection: Initial results[C]. Proc of Recent Advances in Intrusion Detection'98 Conf. Louvain-la-Neuve: CA Press, 1998: 31-47.

[6] Bivens A, Palagiri C, Smith R, et al. Network-based intrusion detection using neural networks[C]. Proc of Intelligent Engineering Systems through Artificial Neural Networks. NY: IEEE Press, 2002: 579-584.

[7] Campbell W. Traditional indications and warnings for host based intrusion detection, indication and warning methodology [C]. Proc of CERT Conf '99. West Point: CA Press, 1999: 232-236.

[8] Feng Y, Wu K G, Wu Z F, et al. Intrusion detection based on dynamic self-organizing map neural network clustering [C]. Proc of the 2nd Int Symposium on Neural Networks. Chongqing: Springer LNCS, 2005: 428-433.

[9] Ramadas M, Ostermann S, Tjaden B. Detecting anomalous network traffic with self-organizing maps [C]. Proc of Recent Advance in Intrusion Dection 2003. Pittsburgh: FL Press, 2003: 46-55.

[10] Pasemann F. A simple chaotic neuron[J]. Physical D, 1997, 104(2): 205-211.

[11] Otey M, Parthasarathy S, Ghoting A, et al. Towards NIC based intrusion detection [C]. Proc of the 9th ACM SIGKDD Int Conf on Knowledge Discovery and Data Mining. Washington D C: VA Press, 2003: 723-728.

[12] Cannady J. Artificial neural networks for misuse detection [C]. Proc of 1998 National Information Systems Security Conf. New York: IEEE Press, 1998: 443-456.

[13] 张若青,裘丽华. 基于动态神经网络的液压伺服系统故障检测[J]. 机械工程学报, 2002, 38(3): 46-49.
(Zhang R Q, Qiu L H. Fault detection of hydraulic servo-system based on dynamic neural network [J]. Chinese J of Mechanical Engineering, 2002, 38(3): 46-49.)

[14] 姚羽, 高福祥, 于戈. 基于混沌神经元的延时滥用入侵检测模型[J]. 电子学报, 2004, 32(8): 62-65.
(Yao Y, Gao F X, Yu G. The application of chaotic neural network to misuse detection [J]. Acta Electronica Sinica, 2004, 32(8): 62-65.)

[15] Cunningham R, Lippmann R, Fried D, et al. Evaluating intrusion detection systems without attacking your friends [C]. Proc of 3rd Conf and Workshop on Intrusion Detection and Response. San Diego: CA, 1999: 35-42.

[16] 姚羽, 高福祥, 于戈. 基于 ROC 曲线的入侵检测评估方法[J]. 通信学报, 2005, 26(1A): 113-115.
(Yao Y, Gao F X, Yu G. IDS evaluation approach based on ROC curves [J]. J of China Institute of Communications, 2005, 26(1A): 113-115.)

(上接第 427 页)

[9] 刘镔, 张永强, 刘粉林. 一种新的数字化混沌扰动方案[J]. 计算机科学, 2005, 32(4): 71-74.
(Liu B, Zhang Y Q, Liu F L. A new scheme on perturbing digital chaotic systems [J]. Computer Science, 2005, 32(4): 71-74.)

[10] Luo X Y, Liu B, Liu F L. Improved RS method for detection of LSB steganography[C]. Proc the 2005 Int Conf on Computational Science and Its Applications. Berlin: Springer-Verlag, 2005: 508-516.

[11] Lu P Z, Luo X Y, Tang Q Y. An improved sample pairs method for detection of LSB embedding[C]. Proc the 6th Information Hiding Workshop. Berlin: Springer-Verlag, 2004: 116-128.