文章编号：1000-1190(2012)05-0537-03

基于协同神经网络的网络流量异常检测

马 卫*，熊 伟

(中南民族大学 计算与实验中心，武汉 430074)

摘 要：针对网络流量具有复杂的动力学特性，提出了一种应用自上而下的协同神经网络进行网络流量异常检测的方法. 首先选择包含正常网络流量和异常攻击流量的数据集作为原型模式，然后通过协同神经网络进行序参量的动力演化，最终根据原型模式对应的序参量的演化结果来判定检测结果. 实验结果证明，该方法能有效的识别出正常流量和异常攻击的种类.

关键词：网络流量；异常检测；协同神经网络；序参量

中图分类号：TP393.06 文献标识码：A

随着互联网和网络应用的快速发展，网络安全问题越来越引起人们的重视. 网络流量异常检测是其中的重要问题之一. 导致网络流量异常的原因有很多，除正常的网络设备运行故障之外，恶意的网络攻击则是导致网络流量异常的主要原因，它发作突然，先兆特征不明显，短时间内会对网络用户及管理者带来极大的危害，因此，采取有效的方法进行网络流量异常检测对提高网络性能和改善网络服务质量具有重要意义[1].

但目前众多的网络流量异常检测方法是在基于网络流量是线性的、平稳性的假设前提下进行的，即假定在某一个时间段内，反应网络流量特征的特征量保持不变或呈线性变化，通过观察该特征量的变化情况来判断网络流量是否异常[2]. 然而，网络作为一个远离平衡态的开放系统，网络流量受诸多因素的影响，如拓扑结构、网络设备、传输协议及网络用户之间的合作与竞争等，因此，实际网络流量往往呈现出非线性、非平稳性的复杂的动力学特性[3]. 针对该特性，本文提出了一种应用自上而下的协同神经网络[4] 进行网络流量异常检测的方法. 该方法首先选择包含正常网络流量和异常攻击流量的数据集作为原型模式，然后通过协同神经网络进行序参量的动力演化，最终根据原型模式对应的序参量的演化结果来判定检测结果.

1 协同神经网络模型

协同学的一个重要观点是：模式识别的过程即为模式形成的过程. 系统模式形成过程是初始状态的配置，其中也包括部分有序化的子系统，属于这个子系统的序参量在竞争中取胜，最后支配整个系统并使其进入这个特定的有序状态，完成了系统的宏观质变. 协同神经网络是用协同学理论所构造的，与传统的从研究单个神经元的特性、配置和连接的构造方法完全不同，它是一种自上而下的神经网络.

协同神经网络的基本原理[5] 是构造非线性动力学系统中的动态过程，完成模式识别及联想记忆的功能. 在模式识别时，对待识别模式 q 可构造非线性动力学系统的动态过程：使 q 经过中间状态 $q(t)$ 进入到诸原型模式中的一个原型模式 v_k，即这个原型模式与 $q(0)$ 最为靠近，也即拉它使其处于这个原型模式的吸引谷底，可描述为 $q(0) \to q(t) \to v_{k0}$.

假设原型模式数为 M，原型模式向量维数为 N，要求 $M \leqslant N$，动力学方程为：

$$\dot{q} = \sum_k \lambda_k v_k (v_k^+ q) - B \sum_{k \neq k'} (v_{k'}^+ q)^2 (v_k^+ q) v_k - C(q^+ q) q + F(t) , \quad (1)$$

式中，q 是以输入模式 q_0 为初始值的状态向量，为待识别的模式向量. λ_k 为注意参数，只有当它为正的时候，模式才能被识别；$F(t)$ 为涨落力，可忽略不记；B 和 C 为指定系数，且都大于 0；v_k 为原型模式向量，$v_k = (v_{k,1}, v_{k,2}, \cdots, v_{k,N})^T$. v_k^+ 为 v_k 的伴随向量，且需满足：

收稿日期：2012-03-09.
基金项目：中南民族大学校级基金项目(YZQ09006).
* E-mail：mw0626@163.com.

$$(v_k^+, v_{k'}) = v_k^+ v_{k'} = \delta_{k,k'} = \begin{cases} 1, & k = k'; \\ 0, & k \neq k', \end{cases}$$

v_k 必须满足归一化和零均值条件：

$$\sum_{l=1}^{N} v_{k,l} = 0, \| v_k \|_2 = \left(\sum_{l=1}^{N} v_{k,l}^2 \right)^{1/2} = 1. \quad (2)$$

使用序参量 $\xi_k = (v_k^+, q) = v_k^+ q$ 和 $D = (B + C) \sum_k \xi_k^2$，可以得到用序参量描述的动力学演化方程为：

$$\dot{\xi}_k = \xi_k (\lambda - D + B \xi_k^2). \quad (3)$$

根据上述所建立的序参量方程，构造如图 1 所示协同神经网络模型[6]，网络分为 3 层. 上层是输入层，输入层的单元 j 接收待识别模式向量初始值 $q(0)$ 的分量 $q_j(0)$. 中间层表示各个序参量神经元，序参量 ξ_k 是由每个输入值 $q_j(0)$ 乘以相连接的 $v_{k,j}^+$，并对全部角码 j 求和所得. 具有活性 ξ_k 的各个神经元识别出角码 k 确定的特定原型模式. 网络按照动力学方程运行和演化，随时间的发展达到终态，通过 D 相互作用(侧抑制)，进行竞争，最后只有一个序参量能幸存，可得到 q_j. 下层是输出层，输出层的模式可表达成 $q_j(t) = \sum_k \xi_k(t) v_{k,j}$，$q_j$ 是输出层单元 j 的活性，ξ_k 是中间层的最终状态. 当 $k = k_0$ 时，$\xi_k = 1$；其它情况下，$\xi_k = 0$. $v_{k,j}$ 是原型向量的第 j 个分量，通过用 $u_{k,j}$ 替换向量分量 $v_{k,j}$，识别出用 $u_{k,j}$ 描述的属于角码 k 的新模式.

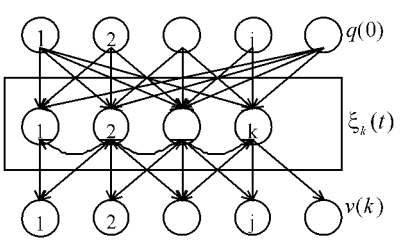

图 1 协同神经网络

Fig. 1 Synergetic neural network

2 网络流量异常检测

为了检测网络流量中存在的异常，需要根据已有的网络流量知识库，建立网络攻击流量的知识库，在此基础上，对于待识别的未知网络流量的攻击，分别选取不同类别的网络攻击流量作为其原型模式，利用上述建立的动力学方程，建立自顶向下的协同神经网络，对未知的网络流量的攻击进行识别.

进行异常检测时，首先选择包含正常网络流量和异常攻击的原型模式初始集，进行学习训练，根据协同神经网络模型，协同神经网络的学习算法是通过原型模式求其伴随向量的训练过程，而协同神经网络的识别则是在输入层输入实验模式向量，然后通过计算得出网络中间层的序参量 ξ_k 的初始值 $\xi_k(0)$，根据协同支配原理，具有最大初始序参量值所对应的模式最终将在协同竞争中胜出，从而识别出模式的归属. 具体步骤如下，

1) 将训练模式向量化，根据式(2)，计算出满足归一化和零均值条件的原型模式向量 $v_k = (v_{k,1}, v_{k,2}, \cdots v_{k,N})^T$，$k = 1, 2, 3, \cdots, M$，为原型模式的个数，为原型模式的向量维数，只要满足 $M \leqslant N$，个模式向量就可组成原型模式的向量集；

2) 计算原型模式 v_k 的伴随向量 v_k^+，从而获得网络输入层到中间层的连接权值；

3) 计算满足归一化和零均值条件的输入层实验模式向量 $q(0)$，然后根据序参量计算公式 $\xi_k = (v_k^+, q) = v_k^+ q$，计算出序参量 ξ_k 的初始值 $\xi_k(0)$；

4) 在协同神经网络中，对 $\xi_k(0)$ 按式(3) 进行协同动力学演化，将演化稳定的序参量投影到网络的输出层，系统的最终演化结果取决于实验模式向量对应的序参量初始值，即具有最大初始序参量值所对应的模式最终将在协同竞争中胜出，从而完成模式的识别.

3 实验结果与分析

为了验证本文所提方法的效果，实验采用美国国防部高级计划研究署离线评估数据集[7](简称 DARPA 数据集) 中的第 5 周第 2 d 的数据进行网络流量异常检测的性能评估[8]. 使用第 4 周，第 5 d 的 DARPA 数据进行实验测试，其中采用了正常网络流量、U2R 攻击流量、R2L 攻击流量、DOS 攻击流量、PROBING 攻击流量 5 类数据集中的 350 个点作为协同神经网络中的原型模式向量 v_k，然后通过协同神经网络进行动力演化，最终根据原型模式对应的序参量的变化情况来判定检测结果，在序参量的演化竞争中，具有最大初始序参量的原型模式向量 v_k 获胜，其序参量 ξ_k 趋向于 1，而其他模式序参量趋向于 0.

实验结果如图 2 ～ 图 6 所示，从图中可以看出序参量起着决定性作用，当某一种网络流量所对应的序参量 ξ_k 趋向于 1，即获得了该流量所对应模式的检测结果.

4 结论

本文介绍了一种采用自顶向下的协同神经网

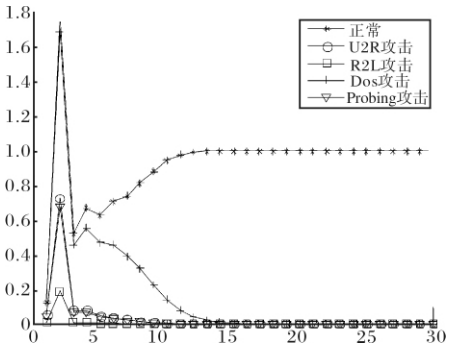

图 2　正常网络流量

Fig. 2　Normal network traffic

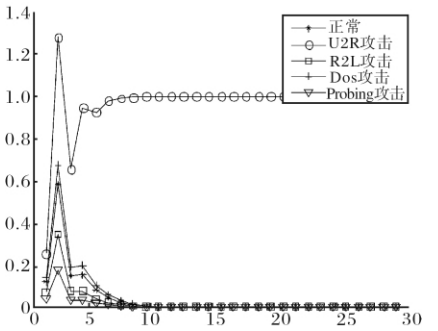

图 3　U2R 攻击

Fig. 3　U2R attack

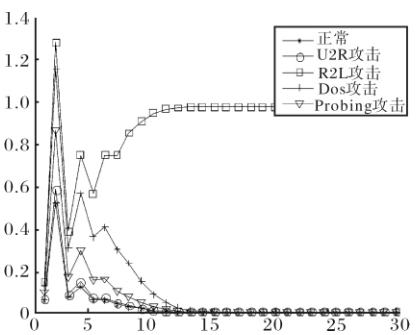

图 4　R2L 攻击

Fig. 4　R2L attack

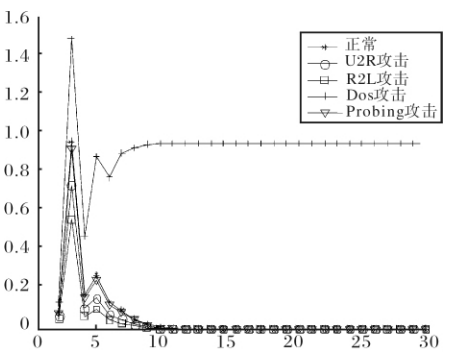

图 5　DOS 攻击

Fig. 5　DOS attack

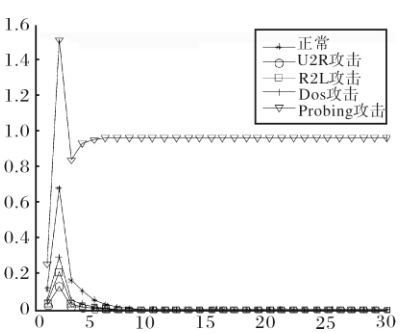

图 6　Probing 攻击

Fig. 6　Probing attack

络进行网络流量异常检测的方法，并通过实验证明了该方法的有效性. 下一步工作的研究重点则是探究非平衡注意参数在协同神经网络的学习过程中的作用，进一步优化网络的动力演化过程.

参考文献：

[1] Dickerson J E, Justin J, Koukousoula O, et al. Fuzzy intrusion detection[A]. IFSA World Congress and 20th NAFIPS International Conference [C]. Vancouver, BC: IEEE, 2001, 1506-1510.

[2] Sang A, Li S. A predictability analysis of network traffic [J]. Computer Networks, 2002, **39**(4): 329-345.

[3] 吕　军，李　星. 一种网络流量异常检测算法[J]. 计算机应用研究，2006, **32**(11): 217-219.

[4] Hanken H. Synergetic Computers and Cognition—A Top-Down Approach to Neural Nets[M]. Berlin: Springer-Verlag, 1991.

[5] Haken H. 协同计算机和认知—神经网络自上而下方法[M]. 杨家本译. 北京：清华大学出版社，1994.

[6] 陈永强，胡汉平，李新天. 基于协同神经网络的图像数字水印算法[J]. 中国图像图形学报，2005, **10**(7): 894-899.

[7] Lippmann R, Haines J, Fried D, et al. The 1999 DARPA off-line intrusion detection evaluation [J]. Computer Networks, 2000, **34**(4): 579-595.

[8] 熊　伟，胡汉平，王祖喜，等. 基于突变级数的网络流量异常检测[J]. 华中科技大学学报：自然科学版，2011, **39**(1): 28-31.

（下转第 568 页）

The exploration of the selective reduction of nitroarenes in CO_2-H_2O system

LIU Shijuan[1], JIANG Jingyang[2]

(1. College of Chemistry, Jilin Normal University, Siping, Jilin 136000;
2. State Key Laboratory of Fine Chemicals, Faculty of Chemical Environmental and Biological Science and Technology, Dalian University of Technology, Dalian, Liaoning 116012)

Abstract: Nitroarenes are selectively reduced to the corresponding N-arylhydroxylamines using Zn dust in CO_2-H_2O system, and the different factors are studied. The yield of N-phenylhydroxylamine from nitrobenzene is 76% when the reaction is carried out at 40 °C for 3 hours with a Zn to nitrobenzene molar ratio equal to 3 under 0.5 MPa CO_2 pressure. The method demonstrates high selectivity, other nitroarenes, which contain reducible functionality other than nitro group, are also selective reduced to the corresponding N-arylhydroxylamines, the reducible functionality other than a nitro group is not reduced. Nitroarenes bearing electron-withdrawing groups favor the reaction.

Key words: CO_2-H_2O; nitroarene; selective reduction; N-arylhydroxylamine

(上接第 539 页)

Network traffic anomaly detection based on synergetic neural network

MA Wei, XIONG Wei

(Center of Computing and Experimenting, South Central University for Nationalities, Wuhan 430074)

Abstract: For network traffic with complex dynamics characteristic, a method is proposed for network traffic anomaly detection, which based on a top-down synergetic neural network. First select the datasets that contain normal network traffic and abnormal attack traffic as a prototype pattern, and then calculate order parameter by synergetic neural network. Finally the detection result is obtained according to the evolution result of the order parameter corresponding to the prototype pattern in the end. Experimental results show that this method can effectively identify normal traffic and types of abnormal attacks.

Key words: network traffic; anomaly detection; synergetic neural network; order parameter