计算机网络安全中神经网络算法的应用分析

刘君行

（西北民族大学　甘肃兰州　730030）

摘要：随着计算机网络技术的不断更新以及广泛应用，计算机网络对信息时代的社会发展起到了关键作用，但也不可忽视网络安全的重要性。尤其是深处大数据时代，传统的计算机网络技术面对错综复杂的网络安全形势显得力不从心。神经网络算法可以让计算机像人类的思维一样记忆和思考，并做出判断，进而更好地推动计算机网络安全技术的进步。基于此，本文以 BP 神经网络算法为典型展开研究，并分析其在计算机网络安全中的应用表现。

关键词：计算机网络安全；神经网络算法；BP 神经网络；应用

引言：

计算机网络深深地改变了社会发展的面貌，人们在享受计算机网络带来的便利的同时，也一直面对着严峻的计算机网络安全形势。从计算机病毒传播到个人信息泄露，计算机网络安全引起的重大损失事件数不胜数，这也就更需要相关技术人员运用神经网络算法解决新形势下的计算机网络安全问题，捍卫网络空间的安全。

1.人工神经网络在计算机网络安全中的优势

1.1 人工神经网络的概念

人工智能领域早在上世纪 80 年代就将人工神经网络（Artificial Neural Network，即 ANN）作为研究热点，而在计算机科学角度将人类神经元进行抽象并作为运算模型的思想可以追溯至更早时期。人工神经网络将每个需要分析的数据视作一个神经元节点，亦或称之为基础节点，对该节点进行分析以获取其信息，再分析该节点与其他所有节点的联系，即可得到整体的信息特征。分析完毕后将所有分析结果都导入训练库中，那么在遇到相同信息时可以迅速根据训练库特征匹配机制对信息进行识别，并对信息进行定义。

值得一提的是，当下的集成电路水平理论上还不足以支持计算机像人脑一样处理和解决问题，因此研究神经网络算法依旧是十分有必要的。

1.2 应用优势

人工神经网络由于模拟了人类神经元的组织方式，进而拥有了类似人类的思维能力，因此在计算机网络方面具有很多优势。具有代表性的优势有以下：

（1）可学习性

人工神经网络的典型特点之一是可以存储大量的信息，并根据学习算法不断地自动学习，完善信息的存储。例如，当人工神经网络遭遇未知的计算机病毒时，将标记这类未知的信息并暂停其运行，紧接着对其中的信息进行解析。解析完成后，根据人工神经网络的运行逻辑得到新的神经元节点，根据所有节点的联系得到整体的运行情况，并将新的信息特征放入训练库中，以便应对下次类似的未知来源攻击。同理，人工神经网络也可以利用样本来模拟现实环境，也就是对输入进行自适应学习，不断完善信息的存储。

（2）运行效率优势

相当部分的计算机网络安全维护工作依赖于人工，各种信息处理的速度和效率通常存在劣势。而人工神经网络基于信息技术，得益于硬件的支持，在运行量级和处理速度上与人工操作有着本质的区别，能够迅速完成千万级甚至指数增长级的数据处理并做出响应，大幅提升计算机网络安全工作的效率。

（3）高度并行性和分布式处理

人工神经网络的神经元排列并非是杂乱无章的，通常呈一种规律或有层次的排列。在人类神经系统中，信号可以同时到达多个神经元进行输入，人工神经网络亦是如此，这种结构显然十分适合并行处理。假设将每个神经元看作是一个处理单元，则整个人工神经网络可以视为一个分布式计算系统，进而避免了“无限递归”或“匹配冲突”等问题，信息的处理速度与效果亦将大幅提升[1]。

2.BP 神经网络分析

2.1 BP 神经网络基本思想

BP 神经网络（Back-Propagation Neural Network）是人工神经网络中应用最广泛的算法之一，其基本思想是梯度下降法，以网络的实际输出值和期望输出值的误差均方差最小为目的，并结合非线性信息动力学实现输入到最终输出呈非线性映射。因此，该算法的整个过程表现出很好的自适应性和容错性。

2.2 BP 神经网络算法

BP 神经网络是一种严格遵循误差逆向传播算法训练的多层前馈神经网络。

从结构上看，理解归纳神经网络所模拟的本质，BP 神经网络主要包含三个部分：输入层、输出层、隐藏层。值得注意的是，隐藏层是在输入层和输出层之间增加的一层或多层神经元，这些神经元也可称为隐单元，其状态的改变会影响到输入与输出。

从计算过程和方向上看，BP 神经网络计算过程主要分为正向传播和误差逆向传播两种计算过程。在正向传播过程中，信号从输入层进入并逐层处理，最后转向输出层。同理，如果在输出层未能得到预期的结果，则进入误差反向传播的过程，将误差信号沿原路返回。此时沿着相反方向不断进行，并在该过程中修改神经元的权值和阈值，尽可能使误差信号最小。在正向传播的过程中，主要通过隐藏层来实现输入信号到达输出层，采用非线性变换法来产生强烈的输出信号。若出现实际输出与预期输出不符的情况，则自动转换到误差的逆向传播过程，同样地，输出误差也通过隐藏层传输到输入层。前文提到，BP 神经网络的神经元排列是有规律、层次的，那么，其计算过程也必然严格按照逐层的原则。例如，在误差信息逆向传播的过程中，误差信息将被分配到输入层、输出层、隐藏层中的所有单元，因而在输入层、输出层、隐藏层中也能获得误差信息，保障了各部分之间的联结程度的可靠性。

综上所述，BP 神经网络可以高效实现信息从输入到输出的非线性映射，并表现出良好的可学习、泛化、容错的特性。BP 神经网络通常使用 Sigmoid 函数来表示，Sigmoid 函数源自于生物学，也被称为 S 型生长曲线，在 BP 神经网络中常用作激活函数[2]。为了更好地分析 BP 神经网络算法，引入代理模型分析其训练过程。注意，这里引入的代理模型是基于大量数据的基础之上，并且其本身也是 BP 神经网络。

基于 BP 神经网络的特点，引入非线性信息动力学公式：

$$D(k) = \{(x_i, F(x_i)), i = 1,2,3,\dots,N_k\}$$

其中，k 指将用于训练的数据分成若干个 k 份。选取其中的一份数据用于训练，考虑到 BP 神经网络的结构特点，为了使每一层

都具有能接收任意输入并使得输出具有连续的映射能力，此时引入 Sigmoid 函数$S(x)=\frac{1}{1+e^{-x}}$用于传递。输入层中的神经元节点数量是由一系列个体x_i组成的，令输出层的神经元节点数为 o，则理想隐藏层神经元节点数为$\frac{i+o}{2}$。以 MSE 度量为标志结束训练，即 $MSE=\frac{1}{N_k}\sum_{i=1}^{N_k}[\bar{F}(x_i)-F(x_i)]^2$满足要求的误差精度，并使用梯度下降技术动态调整输入层和隐藏层，由此建立了基于 BP 神经网络的认知代理模型。这一经典模型的功能是预测区间适应值的变化，进而降低用户的操作负担。

通常地，该代理模型部分进化个体的适应值很可能偏离预期的情况。需要代理模型具备自动更新的能力来解决这个问题。也就是说，代理模型不仅需要大量的数据作为支撑，也需要对代理模型进行同步的数据更新。不难得知，该代理模型的训练是多代进化的过程，在该过程中需要保存每一代最优的结果，并呈现多代进化后最终的最优结果集。应用代理模型下的粒子群算法可很好完成这一过程，其基本思想是种群初始化后确定历史最优 Hbest 和全局最优 Tbest，利用代理模型更新种群并依照 PSO 粒子群算法更新粒子的速度和位置，同时更新 Hbest 和 Tbest 的值，最后分析 Tbest 的值或更新其适应值。若最终 MSE≥e，e 在此表示误差精度，则说明该基于代理模型的 BP 神经网络可以实现自动更新。

3.BP 神经网络的实际应用

计算机网络自诞生起就肩负着改变世界的使命，从 ARPANET 到以因特网为代表的互联网，再到如今的大数据时代，计算机网络的规模和复杂性发生了成倍的变化，计算机网络面临的安全形势日益严峻。网络空间通常被视为看不见的领土，其重要性不言而喻。世界上每天都在发生网络攻击，考虑到计算机网络的发展程度和人工智能日益强大的学习性、自适应性，当前的入侵检测技术更多与人工智能技术结合使用，BP 神经网络就是典型的应用。

3.1 入侵检测

入侵检测的分类比较庞大，这里特指网络入侵检测（NIDS）。BP 神经网络主要在网络中收集并分析各种信息，判断各种行为是否符合安全原则以及网络本身是否受到网络攻击，其相应的手段主要包括记录危险事件、隔离网络环境等，并立即发送警告通知。

入侵检测需要使用数据集来检测和检验防御效果，本文采用 UNSW-NB15 数据集进行模拟检测分析，并生成一种真实的现代正常活动和合成的当代攻击行为的结合体。通过使用 12 种算法，将网络活动总结为 49 种特征，这些特征又分为时间特征、内容特征、标签特征等六大类特征，这些特征可以代表模拟网络活动的进行情况。在入侵检测中，时间特征和基础特征是尤其重要的参考指标，涉及到流量、TCP 连接的传输间隔和目标到源的传输信息等。注意，标签特征中的 attack_cat 标签也是重要的参考指标，因为它直接指出当前环境的流量是否正常以及具体遭受了哪种类型的攻击。但 BP 神经网络不能确保收敛至全局最小点，网络结构也不易确定，有必要引入遗传算法与 BP 神经网络进行综合[3]。

考虑到 UNSW-NB15 数据集自身的规范性，数据预处理环节中的清洗步骤几乎可以省略。基于入侵检测的特点，数据转换更适合使用归一法进行操作，其公式为：

$$x_{res}=\frac{x-x_{min}}{x_{max}-x_{min}}$$

其中，x_{res}指归一化计算后的结果，x 指归一化计算前的数据，x_{max}和x_{min}分别指当前数据所在特征列的最大、最小数据。前文提到，BP 神经网络中每个神经元的权值和阈值会直接影响非线性函数的模拟结果。假设有 m 层输入层、n 层输出层、p 层隐藏层，基于非线性信息动力学公式，输入为x_i（i=1，2，3，…m），输出为y_k（k=1，2，3，…n）。设隐藏层的输出为O_j，阈值为θ_j，且有 j=1，2，3，…，k。隐藏层的激励函数为f_1为 Sigmoid 函数，输入层到隐藏层的权重为w_{ij}。那么，输入层到隐藏层的输出O_j的公式为$O_j=f_1(\sum_{i=1}^{m}w_{ij}x_i-\theta_j)$。同理，设输出层的阈值为$\theta_s$，输出层的激励函数为$f_2$，输出层到隐藏层的权重为$w_{js}$，那么隐藏层到输出层的第 k 个输出为$y_k=f_2(\sum_{j=1}^{k}w_{js}O_j-\theta_s)$。设该神经网络趋近的非线性期望输出为$R_k$。为了达到最佳目的，需要不断降低$R_k$与$y_k$之间的差距，同时不断调整权值和阈值。

综上，遗传算法可以很好地解决 BP 神经网络自身不能保证收敛到全局最小点、收敛速度慢等问题。基于 BP 神经网络的入侵检测可利用公式$Delta=\sum_{k=1}^{n}(R_k-y_k)^2$比较$R_k$与$y_k$之间的差值，并判断其是否满足事先设置的最小误差范围。因此，输入任意一组网络活动的数据即可输出其是攻击行为还是正常行为，以此达到入侵检测的目的。

3.2 计算机网络安全评价

计算机网络安全评价在网络安全中十分重要，其目的是对各种隐患或危险进行评估，对其进行防范，并采取一系列有效措施。在构建网络安全评价方案或体系时，应当遵循以下原则：第一，准确性，每个指标都能准确地反映出存在的问题。第二，完整性，每个指标都能全方位多方面立体地覆盖被评价对象。第三，独立性，每个指标之间不能重复作用且不得有过高的耦合度，否则将产生结果的冗余或增加误差。第四，简洁性，每个评价指标应具有代表性，为相关人员提供操作便利性。

如今身处大数据时代，网络安全评价手段愈发多元化，BP 神经网络由于其优势也得到了有效应用。要构建出完整的基于 BP 神经网络的网络安全评价体系，应当结合 BP 神经网络结构中的输入层、隐藏层、输出层。第一，输入层的构建，设计该安全评价体系和使用工具的实际情况时，指标的总量一定要和输入的神经元点保持一致，即神经元点数量要和所用工具总量保持一致。第二，隐藏层的构建，隐藏层在大部分神经网络的应用中都起到十分重要的作用。若隐藏层中的隐节点设置过多，则会明显导致该 BP 神经网络的学习和训练时间延长，反之隐节点过少会导致容错性受到较大的影响。第三，输出层的构建，输出层很大程度上影响将安全评价呈现出来的结果，并需要通过各种符号来表示其是否安全，将协助相关操作人员在应用 BP 神经网络时做出准确的判断。

实现 BP 神经网络模型在计算机网络安全评价中的应用时，应加强其学习性并把学习效果作为主要的参考指标。在设置相应安全评价参数时，需同时将这些参数通过输入层输入到模型中，进而知晓其实际运行效果，保证其在网络安全评价中的实际效果。最后，针对学习效果做出优化，使得网络安全评价体系拥有良好的容错性和适应性。

结语：

计算机网络安全长期以来一直是人们关注的问题，人工神经网络以其优势推动着网络安全的发展和进步，使其更具有实效性，提高安全防护效率。随着时代的发展，信息世界已在我们的手掌之中，相信未来神经网络算法将成为引领时代的技术，计算机网络安全的攻防也更加智能化，建立面向未来的更高阶信息时代，推动人类社会乃至文明的进步。

参考文献：

[1]张艳艳，徐亮. 浅谈计算机网络安全检验中神经网络的应用研究[J]. 网络安全技术与应用，2020，9：19-20.

[2]胡兆文. 神经网络算法在计算机网络安全中心中的应用研究[J]. 信息与电脑，2021，16：77-79.

[3]赵志伟. BP 神经网络在入侵检测中的研究与应用[J]. 信息通信，2012，2：118-119.

作者简介：刘君行，男，汉族，（2001·12——），本科，重庆南川人。研究方向：计算机科学。