工业控制系统网络攻击预测技术研究*

丁朝晖，张　伟，杨国玉，刘　腾
（中国大唐集团科学技术研究总院有限公司，北京 100043）

摘　要： 面对复杂的网络安全形式，攻击方常采用大量的信息侦查、漏洞利用和混淆技术在网络进行恶意活动或破坏行为。虽然当前网络安全态势感知平台尽可能地发现和监测新漏洞的利用过程，但是攻击预测的准确率和精确率都不尽如人意，需要在目前预测技术的基础上研究更加高级的算法将安全事件自动关联到对应的资产和攻击类型上，对可能发生的网络安全攻击进行预警和风险评估，实现对网络安全事件的精准预测。

关键词： 工业控制系统；网络攻击预测；神经网络
中图分类号： TN915.08　　**文献标志码：** A　　**DOI:** 10.16157/j.issn.0258-79982.222698

中文引用格式： 丁朝晖，张伟，杨国玉，等. 工业控制系统网络攻击预测技术研究[J]. 电子技术应用，2023，49(1)：86-90.
英文引用格式： Ding Zhaohui，Zhang Wei，Yang Guoyu，et al. Research on network attack prediction technology of industrial control system[J]. Application of Electronic Technique，2023，49(1)：86-90.

Research on network attack prediction technology of industrial control system

Ding Zhaohui，Zhang Wei，Yang Guoyu，Liu Teng
(China Datang Group Science and Technology Research Institute Co.，Ltd.，Beijing 100043，China)

Abstract： In the face of complex forms of network security，attackers often use a large number of information investigation，vulnerability utilization and confusion technologies to carry out malicious activities or destruction in the network. Although the current network security situational awareness platform finds and monitors the utilization process of new vulnerabilities as much as possible，the accuracy of attack prediction are not satisfactory. It is necessary to study more advanced algorithms based on the current prediction technology to automatically associate security events with the corresponding assets and attack types，carry out early warning and risk assessment for possible network security attacks to achieve accurate prediction of network security events.

Key words： industrial control system；network attack prediction；neural network

0 引言

为了实现有效的安全运营，企业和组织进行了大量的投入，纷纷成立了安全运营中心，建立了安全运营团队，搭建了安全运营平台，并逐步形成了一些安全运营流程。随着网络空间安全形势日趋恶化，网络安全地位日益提升，但受限于传统网络安全预测技术的缺陷，现有的安全运营工作面临诸多挑战。以下列举部分典型的网络安全预测面临的困难：

(1)预测不准确，安全运营人员忙于处理无关紧要的威胁警报，而没有时间处理真正重要的预警信息。加之，安全从业人员匮乏已是众所周知，安全运营人员尤其紧缺，在这种情况下，迫切需要提高预警的准确率。

(2)预警信息太多，处理起来费时费力，安全运营工作中最主要的工作之一就是预警处理。安全工具不断叠加部署造成预警数量与日俱增。如何高效处理海量预警信息已经成为安全运营的一个永恒话题。每种工具都在尽力减少警报，而安全信息和事件管理工具和传统的安全运营中心也花费了大量的精力在消除预警上，大数据分析技术、机器学习和人工智能技术纷纷引入，试图从多个维度降低预警，但效果依然有待改善。

网络安全已成为关系国家安全和发展、关系人民群众切身利益的重大问题，网络安全形势也是日益严峻，网络攻击危害政治安全、社会稳定、经济发展、文化建设，网络空间的国际竞争方兴未艾。潜在的网络攻击和威胁如果能被准确预测，在攻击成功之前采取有力措施，阻断攻击，甚至反击攻击者，已成为网络安全研究的新方向。

1 网络攻击预测技术原理

预测即根据过去的收集到的威胁情报推测未来可

* 基金项目：2020年大唐集团第一批科技项目(KJ20-002)

能面临的安全威胁。依据预测的性质、任务来划分，主要分定量预测和定性预测两类[1]。定量预测主要利用数学模型和方法，依据收集的原始数据和信息，通过对这些数据和信息进行分析，找出网络攻击成功事件与这些数据和信息的对应关系，得到工业控制系统中可能发生的网络安全事件或者变化规律，达到预测的目的，其分析方法主要包括时间序列、回归分析、人工神经网络等。定性分析主要依靠经验积累和能力，利用有限原始数据进行推理、判断和估测，其方法主要包括类推法、判断分析法等[2]。本文重点介绍定量预测方法。

1.1 基于时间序列的预测方法

时间序列[3]是指由某一随机过程在不同时刻的相继观察到的数值排列而形成的一组数字序列。在一个时间序列里，这组数值与聚集的时间粒度密切相关，且按时间顺序排列。

由此可以看出，时间序列预测技术是一种统计预测的方法，通过时间序列对应的事件状态、趋势、维度和规律推理分析，预测事件走向和严重程度的方法。它研究预测目标与时间过程的演变关系，建立函数$\boldsymbol{y}=f(t)$，$\boldsymbol{y}$即网络安全态势值，该值由态势评估获取而来，为非线性。根据统计规律性构造拟合$f(t)$的数学模型，设定时间序列为$t_1<t_2<\cdots<t_n$，以时间t为自变量、离散化的有序集合$f(t_1),f(t_2),\cdots,f(t_n)$为网络安全态势值的时间序列，可以有不同的物理意义，如网络攻击的次数、网络流量大小、设备资源使用率等，通过一系列已发生网络异常或攻击情况的态势值推算未来的网络安全态势值[4]。

时间序列预测法简单方便，可操作性好。但是，如果需要预测结果更加精确预测，则需要模型阶数和参数的最佳估值，要达到这样的效果，建模过程相当复杂。

1.2 基于回归分析的模型预测方法

基于回归分析模型的预测方法是在分析各种因变量和自变量之间关联关系的基础之上，确定自变量（态势值）和因变量（评估指标）之间的逻辑、函数关系，达到预测态势的目的[5]。

回归分析的基本思想：首先从一组观测到的样本数据出发，建立变量之间的函数关系；然后对这些函数关系的可信度进行验证，确定影响某主要结合值的各变量的影响程度；再进一步利用函数关系，确定一个或几个变量的取值来影响另一个特定结果变量的取值，并量化该影响的精确程度。

回归分析预测方法的一般步骤[6]：

(1)平稳性判断。根据平稳时间序列的特征对其平稳性进行判断。

(2)模型识别。在得到平稳序列后，进行模型的初步识别和定阶，初步识别自相关函数（ACF）和偏相关函数（PACF），根据ACF和PACF的拖尾或截尾性质，确定采用的回归序列预测模型。

(3)选定模型阶数。经过模型识别后，需要减少预测误差，通过选定合适的模型阶数，来达到使模型拟合程度更好、误差最小的目标。

(4)参数估计。确定了事件序列的模型和阶数后，还需要对模型的参数进行计算。

(5)模型校验。回归预测模型是否可用于实际预测，取决于对回归预测模型的检验和对预测误差的计算。回归模型只有通过各种检验，残差序列为白噪声时，序列有用信息提取充分，才能将回归模型作为预测模型进行预测；否则说明有用信息没有提取完整，需对模型进行修改或重新建模[7]。

1.3 基于神经网络预测方法

人工神经网络[8]简称神经网络，它是一种模拟大脑神经的结构进行信息处理、分析、设计、思考、学习等思维活动的数学模型，用以解决和处理复杂的问题。

神经网络由简单的处理单元——神经元组成，神经元具有存储信息、学习知识，总结经验的功能，利用神经网络通过学习从输入信息中获取知识，通过自学习能力，还可多次从新的输入中进行联想、概括、类比和推广，调整认知，从而产生更准确的输出。因此，神经网络具有自学习、自完善、创新性、健壮性、容错性等特点。

一个典型的人工神经元模型由输入$\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$、网络权值$\boldsymbol{W}=(w_1,w_2,\cdots,w_n)$、阈值$V$、求和单元$\sum$、激励函数$f$、输出$\boldsymbol{Y}$组成，如图1所示。

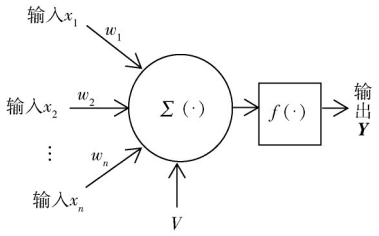

图1　典型人工神经元模型

在网络安全态势预测中，通过对输入层信息进行函数计算，得到各个输出节点的值，这个值代表网络攻击成功概率和严重程度，数值越大，网络攻击成功概率越大，严重程度越高，需要尽快进行安全加固[9]。

2 工业控制系统中网络攻击预测的实现

RBF神经网络[10]是一种3层神经网络，包括输入层、中间层、输出层。输入RBF神经网络的矢量直接映射到中间层，并不通过权连接。当RBF神经网络的中心点确定以后，这种映射关系也被确定。而中间层空间到输出空间的映射是线性的，即网络的输出是隐单元输出的线性加权和，此处的权即为网络可调参数。其中，隐含层的作用是把向量从低维度映射到高维度，这样低维度线

性不可分的情况到高维度就可以变得线性可分了。这样，网络由输入到输出的映射是非线性的，而网络输出对可调参数而言却又是线性的。网络的权就可由线性方程组直接解出，从而大大加快学习速度。RBF神经网络由于中间层较少（只有一个），因此，其训练速度快，训练简洁。目前已经证明RBF网络能够以任意精度逼近任意连续的函数，且具有全局逼近能力，从根本上解决了BP网络的局部最优问题，而且拓扑结构紧凑，结构参数可实现分离学习，收敛速度快[11]。

本次设计RBF神经网络预测实验模型采集数据主要来自普通网络攻击者，根据普通网络攻击者一般对一个工控系统展开为期两天的攻击，如果没有结果，会放弃本次攻击。因此，本次模拟实验，收集两天的攻击数据样本，预测普通网络攻击者是否已经获取工控系统服务器权限或者即将获取工控系统服务器权限，其模型参数选取如表1所示。

表1　RBF神经网络攻击预测实验模型参数

参数值参数	维数	数量	采集时段
输入向量 $\boldsymbol{X}$	20	1 000	2021.10.01 ~2021.10.02
输出向量 $\boldsymbol{Y}$	6	$1 \leqslant n \leqslant 1\ 000$	/

本次RBF神经网络训练样本数量为1 000，如果训练样本过多，可能出现过拟合现象[12]；如果训练样本过少，则预测结果误差较大。因此，选择训练样本数量为1 000，训练过程如图2所示。

下面以某电厂的电力控制系统为例，基于工业协议（如Siemens S7、Modbus、Bacnet、Ethernet/IP等）来开展各种维度的监测、分析等，获取流量中的疑似恶意攻击行为，在本文中主要研究工业态势感知系统捕获到对电力控制系统的工程师站和操作员站主要7种网络安全攻击。本次实验中输入样本数据范例如表2所示，这样的样本数据共有1 000个，每个样本参数有20个，通过对这些样本进行分析，预测系统中可能发生的安全事件位置和事件严重程度、发生的概率等，减少误报和重复预警。

严重程度越高代表预测该攻击发生概率高，网络攻击成功概率和严重程度成正比，网络攻击成功概率越高，严重程度越高，需要尽快进行安全加固。网络攻击严重程度划分如表3所示。

通过对电力工控网络攻击样本进行分析，使用RBF神经网络攻击预测实验模型实现预测，经过训练收敛后，使用剩余样本获得网络攻击成功可能性预测值。在训练中，学习率取0.03，首先，各层的权值随机输入[13]。然后，根据训练目标对各层的权值进行调整，并判断预测值与标签的均方误差是否满足MSE≤0.1，当均方误差

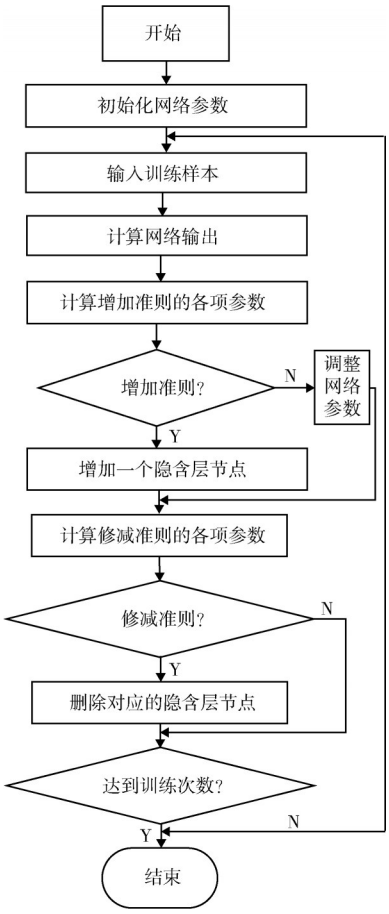

图2　神经网络学习流程图

达到要求时，训练结束，神经网络的参数随之确定，用训练好的神经网络参数对剩余200个样本点进行预测，预测结果如表4所示。

通过使用本文中描述的RBF神经网络，使用表1的训练集数据，得到表2的输出结果集，与验证集中的数据进行对比，如同一目标有两条攻击路线，则选择概率高的作为结果，预测模型的预测结果与网络攻击实际结果（验证集）进行对比，攻击可能性大于90%的攻击实际发生率为99.9%，如表5所示，可见该算法对于网络攻击预测准确率极高[14]。

3　结论

随着网络态势感知走向动态网络防御，网络攻击预测的发展方向是利用各种数据进行深度机器学习。围绕网络中关键资产可能被混淆、存在噪声的数据以及有限的防御手段等，本文利用深度学习技术来动态地学习和创建针对0-day漏洞等新攻击技术的防御策略与防护模型[15]，实现了工业控制系统中网络安全威胁事件的更加精准预测。下一阶段将对网络攻击进行及时阻断，保障工业控制系统的正常稳定运行。

参考文献

[1] 李纪真，孟相如，温祥西，等. 萤火虫群算法优化高斯过

表2　网络安全事件输入样本数据范例(部分)

序号	事件	发生时间	源IP	目标IP	源帐户	目标帐户
1	扫描	2021.10.01 17:20	*.*.72.8 *.*.72.12	*.*.72.100-254	/	/
2	执行越权指令	2021.10.01 18:30	*.*.72.8	*.*.72.100	/	administrator
3	非法输入尝试	2021.10.01 19:25	*.*.72.20	*.*.72.102	test	/
4	口令探测	2021.10.01 19:50	*.*.72.8	*.*.72.105	root	root
5	口令探测	2021.10.01 19:50	*.*.72.8	*.*.72.109	root	root
6	口令探测	2021.10.01 19:50	*.*.72.8	*.*.72.107	root	root
7	恶意软件活动	2021.10.01 20:30	*.*.72.8 *.*.72.12 *.*.72.20	*.*.72.107	/	/
8	用户名探测	2021.10.02 06:55	*.*.72.20	*.*.72.112	test	administrator admin root
9	远程溢出攻击探测	2021.10.02 12:46	*.*.72.8 *.*.72.12 *.*.72.20	*.*.72.125	administrator	/

表3　网络攻击严重程度划分

序号	严重程度	攻击成功概率%	描述
1	极低	1~20	工程师站和操作员站未受到严重的网络攻击
2	低	21~40	工程师站和操作员站受到一般网络攻击
3	中	41~60	工程师站和操作员站受到较为严重网络攻击
4	高	61~80	工程师站和操作员站将受到严重网络攻击
5	紧急	81~10	工程师站和操作员站将受到很严重网络攻击

表4　网络攻击严重程度预测(部分)

序号	目标IP(被攻击目标)	攻击预测	攻击成功可能性/%	严重程度	源IP
1	*.*.72.100	指令篡改	99.9	紧急	*.*.72.8
2	*.*.72.102	指令篡改	80	高	*.*.72.12
3	*.*.72.105	远控主机	78	高	*.*.72.20
4	*.*.72.109	远控主机	99.9	紧急	*.*.72.20
5	*.*.72.107	远控主机	92	紧急	*.*.72.8
6	*.*.72.102	远控主机	85	紧急	*.*.72.8
7	*.*.72.105	远控主机	80	高	*.*.72.8
8	*.*.72.102	远控主机	50	中	*.*.72.8
9	*.*.72.105	远控主机	20	极低	*.*.72.8
10	*.*.72.109	远控主机	93	紧急	*.*.72.8
11	*.*.72.107	指令篡改	80	高	*.*.72.8

表5　预测模型与实际值对比表(部分)

序号	攻击种类	目标IP(被攻击目标)	实际值	攻击可能性/%
1	指令篡改	*.*.72.100	发生	99.9
2	指令篡改	*.*.72.102	未发生	85
3	远控主机	*.*.72.105	未发生	80
4	远控主机	*.*.72.109	发生	99.9
5	远控主机	*.*.72.107	发生	92

程的网络安全态势预测[J]. 系统工程与电子技术,2015(8):1887-1893.

[2] 张威. 网络安全告警的时间序列分析及预测[D]. 武汉:华中科技大学,2008.

[3] 王雪. 基于时间序列分析的网络安全态势预测模型研究[D]. 北京:北京邮电大学,2014.

[4] 陈兴蜀,江天宇,曾雪梅,等. 基于多维时间序列分析的网络异常检测[J]. 工程科学与技术,2017,49(1):144-150.

[5] 王宇飞,沈红岩. 基于改进广义回归神经网络的网络安全态势预测[J]. 华北电力大学学报,2011,38(3):91-95.

[6] 黄亮亮. 网络安全态势评估与预测方法的研究[D]. 兰州:兰州大学,2016.

[7] 张然,刘敏,张启坤,等. 基于SOA_BP神经网络的网络安全态势预测算法研究[J]. 微电子学与计算机,2020,37(6):62-65,69.

[8] 李天骐. 基于神经网络的网络安全态势评估与预测技术研究[D]. 北京:华北电力大学,2016.

[9] 薛丽敏,李忠,蓝湾湾. 基于在线学习RBFNN的网络安全态势预测技术研究[J]. 信息网络安全,2016(4):23-30.

[10] 杨武俊. 基于BP神经网络的网络安全态势预测[J]. 网络安全技术与应用,2020(10):23-24.

[11] 邵伯乐. 基于禁忌算法和RBF神经网络的网络安全态势预测[J]. 兰州工业学院学报,2018,25(3):54-57.

[12] 杨鹏,马志程,靳丹,等. 面向智能电网的网络态势评估模型及感知预测[J]. 兰州理工大学学报,2015,41(4):99-103.
[13] 郝怡然,盛益强,王劲林,等. 基于递归神经网络的网络安全事件预测[J]. 网络新媒体技术,2017,6(5):54-58.
[14] 杜涛. 基于BP神经网络技术的网络流量预测模型[J]. 网络安全技术与应用,2016(7):55,57.
[15] 李方伟,张新跃,朱江,等. 基于APDE-RBF神经网络的网络安全态势预测方法[J]. 系统工程与电子技术,2016,38(12):2869-2875.

(收稿日期:2022-03-03)

作者简介:

丁朝晖(1977-),女,硕士研究生,高级评估师,主要研究方向:网络安全、工控系统安全。

张伟(1976-),男,硕士研究生,高级工程师,主要研究方向:网络安全、工控系统安全。

杨国玉(1980-),男,硕士研究生,高级经济师,主要研究方向:信息化与网络安全管理。

扫码下载电子文档

版权声明