doi: 10.3969/j.issn.0490-6756.2017.04.012

基于组合神经网络的启发式工控系统异常检测模型

唐彰国，李焕洲，张　健
(四川师范大学网络与通信技术研究所，成都 610066)

摘　要：为了提高工控系统入侵的检测率，讨论了传统工控入侵检测技术的原理，并从信息论的观点进行了对比研究.通过对工控系统特异性及其攻击手法的建模，归纳出工控攻击在协议栈、统计特性、通信行为等方面表现出的动态和静态指纹，基于一种新的异构信息的抽象方法，提出并实现了一个基于组合神经网络的启发式工控系统异常检测模型.测试结果表明该检测模型运行高效，相比一般智能方法检测结果更为准确.

关键词：异常检测；组合神经网络；工控系统；启发式；模型
中图分类号：TP393　　**文献标识码**：A　　**文章编号**：0490-6756(2017)04-0735-07

Heuristic anomaly detection model of industrial control system based on combined neural network

TANG Zhang-Guo, LI Huan-Zhou, ZHANG Jian
(Institute of Computer Network and Communication Technology, Sichuan Normal University, Chengdu 610066, China)

Abstract: In order to improve the intrusion detection rate of industrial control system, the principle of traditional industrial intrusion detection technology is discussed, and the comparative study is done from the viewpoint of information theory. The dynamic and static fingerprints of industrial control attacks in the protocol stack, statistical characteristics, and communication behavior are summarized based on the modeling of the specificity of the industrial control system and the attack methods. Based on a new abstract method of heterogeneous information, a heuristic industrial control system anomaly detection model based on combinatorial neural network is implemented. The test results show that the proposed model is more efficient, and the results are more accurate than the conventional intelligent methods.

Keywords: Anomaly detection; Combined neural network; Industrial control system; Heuristic; Model

1　引　言

随着信息化与工业化的深度融合，以及物联网和工业 4.0 的蓬勃发展，近年来出现了新型针对工控系统的高级攻击技术及攻击事件，如 Stuxnet、Duqu、Flame、Havex 等病毒武器造成了关键工业基础设施的巨大破坏并产生了深远影响.传统入侵检测方法及其产品大都以 IT 系统及互联网为研究对象，较少考虑工控系统自身的特异性.近年来针对工控系统的专用入侵检测研究但大多基于已知的入侵形式或参照了互联网中出现过的入侵[1-3]，而对未知形态的入侵研究还不够深入，其成果远没有互联网入侵检测成熟，表现在理论上还没有一个严谨普适的方法，没有深入揭示工控系统的构成要素及其特性，没有将入侵过程结合工控场景抽象成一般性过程并形成统一的数据模型，更没有从博弈论角度来进行理论上的建模.表现在实践上还没有成熟有效的自动化检测工具.基于此，本文

收稿日期：2017-01-14
基金项目：四川省教育厅青年基金(15ZB0026)
作者简介：唐彰国(1978－)，男，广西桂林人，硕士，副教授，研究方向为通信与信息安全.E-mail：tangzhangguo@sicnu.edu.cn

以工控系统的信息流为研究对象,通过对工控入侵控制机制和通信机制的特异性进行分析,归纳描述工控入侵的若干属性,发现其在协议通信特征、网络行为特征等方面的动态和静态指纹,并提出基于信息论的异构信息抽象思想,进而设计并实现一个基于组合神经网络的工控系统异常入侵检测模型,最后通过实验测试并与其他方法进行比对,验证该检测模型在普适性、准确性方面所具有的优越性.

2 主流工控系统入侵检测原理和现状

2.1 工控系统入侵检测的需求

传统IT信息系统的安全技术与方法不能直接应用于工控系统.工控系统在生态上是一种"人、机、物"一体系统,其安全诉求主要表现为对物理世界的可信感知以及对物理世界的可靠控制.而IT信息系统安全侧重对信息的保护,包括可信信息传输与处理,但并未触及到攻击如何作用于物理世界.因此,为了设计出适用于工控系统的异常检测方法,须分析工控系统自身的特异性及其安全需求的特有属性[4].工控系统的一大特征就是对实时可用性的要求,无论采用何种攻击手法,最终目的是实现对破坏物理设施的可用性,因此,作为工控系统专用的入侵检测,对其安全需求须从物理系统的角度逆向挖掘.须研究工控系统与物理世界的交互过程,研究工控攻击对于物理系统的影响路径及影响程度,研究攻击对于工控系统的状态预测的影响,研究工控协议、通信信道及其脆弱性,研究控制命令和传感器状态的因果逻辑等等,设计出一种能够自我识别和异常感知的智能算法,从而为工控系统的深度保护提供预警机制.

2.2 基于信息论观点的检测方法比较

从信息论的角度以及大数据思维看,描述工控系统入侵的信息具有稀疏性及异构性.为了从方法论层面便于比较,本文创造性地将现有工控系统入侵检测技术归纳为"四层四类".四层是从信息抽象级别角度划分为语法、语义、语用和画像,四类分别是特征检测、统计检测、行为检测和知识检测.其中,特征检测是指针对设备及其状态在数据包特定字段的定义,如字段内容表征设备是正常状态还是故障状态,即语法信息,该类方法适用于已知的入侵形式,而对未知及加密内容无效,也不能产生出关于攻击的知识;统计检测是基于工控系统运行数据的业务可解析性即语义信息,在数据上叠加的操作可形式化为通信协议多个数据包之间的相互关系(如序列化特征等);行为检测是基于信息操作与作用对象的匹配,识别操作的目的和效用价值等语用信息,如对工控系统网络建立流量基线模型并以此作为判断是否含有入侵流量的依据;而知识检测包括贝叶斯网、络神经网络、支持向量机、遗传算法等机器学习方法,如神经网络将攻击入侵的特征、规律及效用等信息通过神经元之间的连接构成"画像"来学习理解,能"优美"地表达变量间的非线性关系,从模式或图这样高维或超维层次建构信息,虽然这种图式不能显式的表达成有意义的解析式,但其固有的模糊性和高维特性较好的满足基于"全信息"的分类要求,因而分类的准确性高.几种典型工控入侵检测方法的差异如表1.

表1 现有工控系统入侵检测技术比较

Tab.1 Comparison of intrusion detection technology in industrial control system

方法	基于特征方法	基于统计方法	基于行为方法	基于知识方法
检测对象	设备状态及数据包	会话流	数据流量	数据流及数据回
信息层次	语法	语义	语用	画像
检测结果的准确性	漏报率较高	误报率较高	准确性中等	准确性高
检测结果可解析性	好	较好	一般	一般
未知异常识别能力	较差	较好	较好	好

3 工控系统的特异性建模

3.1 工控系统特异性分析

这里研究的特异性是相对于IT系统而言.关于工控系统与IT系统的差异虽有许多论文综述[4,5],但比较方式主要着眼宏观层面,难以直接转化成检测规则,这里从检测建模的角度进行二次归纳如下.

1)系统特异性:与传统互联网和IT系统相比,每个工业控制系统都是根据其特定物理过程、使用不同控制设备和软件定制开发的系统[5].不同工控系统在系统层面上具有唯一性、结构稳定性,

在业务层面表现出周期性、业务有限性，在行为层面上表现出规律性和可预测性. 该特异性表明，工控系统存在系统层次的指纹是合理的及可能的.

2）协议特异性：具有私有特性和安全缺陷特性. 工控系统发展初期是个封闭系统，各企业依靠自身开发的私有协议进行竞争，导致工控网络私有协议众多，因此传统基于公开 TCP\IP 的协议分析不适用，为了更能反映工控系统物理过程的特性，须专门研究基于工控协议级分析的异常检测. 同时，这些工控协议大多未考虑加密、认证、校验等安全措施，如 Modbus、DNP3、ICCP 等都存在大量漏洞以及包篡改、身份伪装等中间人攻击的安全隐患. 该特异性表明，对于基于协议漏洞的攻击在流量上可能无明显特异性，须对协议进行深度解析，包括格式逆向、内容破解、协议状态机以及事件序列等多维特征进行联合检测.

3）流量特异性：具有稳定性、周期性及稀疏性. 稳定性是基于工控系统业务层面的“有限性”，“行为有限”即通信行为具有稳定特征及可预测的行为模式，“状态有限”即通信具有规律性，表现为规则的周期性通信流. 稀疏性是指 APT 等高明攻击手段缓慢渗透的入侵攻击流量稀少，相对于高维度的检测模型训练向量，攻击样本及流量呈现稀疏性. 传统机器学习方法处理的数据维度较小，在训练检测模型时缺乏对参数本身的限制与优化机制，不利于从稀疏样本中提取与入侵行为紧密相关的流量特征[4]. 该特异性表明，传统机器学习模型及其算法必须加以改进以适应工控系统的行为特性，这也是本文提出组合神经网络的缘由之一.

4）网络连接特异性：具有统计学意义. 基于工控系统拓扑稳定性即拓扑结构固定、服务、端口基本不变[6]，以及工控设备任务的稳定性即操作行为固定、操作对象固定、操作流程固定、操作人员固定，因此工控设备间通信的包长、包方向、到达时长、包间隔时间、包序列向量具有规律性和可预测性. 该特异性表明，工控系统网络连接的统计特性可作为一种运行时动态指纹特征量.

5）工控设备特异性：工控设备虽种类繁多，但对具体的工控系统而言设备的形态、用途具有稳定性以及拓扑位置的不变性. 该特异性表明，检测模型为了能区分“自我”和“非我”，可以将设备 ID、物理位置及设备任务类型绑定作为一种静态指纹. 同时，工控设备因为任务有限性和稳定性，其运行时的能耗功率谱具有规律性，该特异性表明，工控设备的功率谱特性亦可作为一种运行时动态指纹特征量.

3.2　工控系统攻击模型及其脆弱点建模

工业控制系统与传统 IT 信息系统的本质区别在于控制系统与物理世界存在交互关系，工控系统作为信息空间和物理空间的中介和接口[7]. 因此，可将工控系统抽象为一个数据链模型，如图 1 所示，从信息流向上既实现了信息空间对物理空间的感知和监视，也实现了信息空间通过决策反作用于物理空间. 在具体攻击手法上虽然形式多样，包括重放攻击、中间人攻击、远程修改 RTU 逻辑、多信道干扰、DoS 攻击、APT、挂马、协议漏洞攻击、网络钓鱼、信息泄露、社会工程学攻击等，但从模型视角仍然可根据图示中的四类数据流分为对感知流、监视流、决策流和控制流的攻击. 因此，实际对工控系统的入侵亦可抽象为对应的两种类型：

1）对信息空间的攻击：表现为对 A_1、A_2 的攻击，如工控设备无法上传数据、上传假数据，或冒充合法工控设备等.

2）对物理空间的攻击：表现为对 A_3、A_4 的攻击，如更改设备运行逻辑、执行未授权指令等.

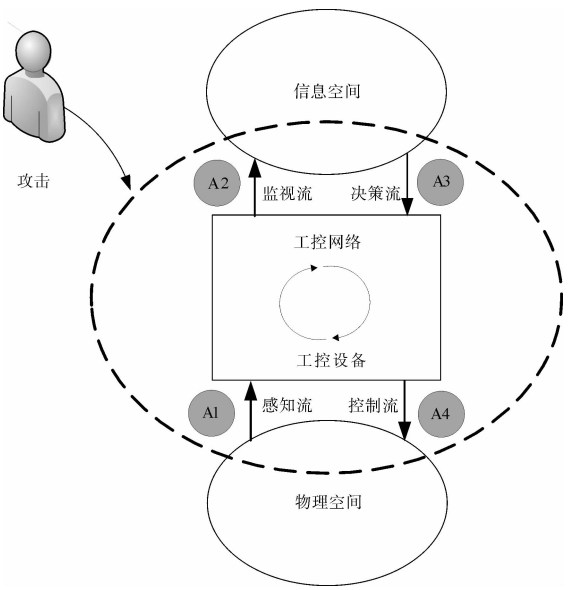

图 1　工控系统攻击的信息流视图

Fig. 1　Information flow view of industrial control system attack

为了使模型更具可操作性，本文通过对相关文献及实战案例的研究，综合各攻击手法的攻击对象、攻击点、攻击位置以及与工控系统脆弱点信息绘制出了一种场景式的攻击全景图，如图 2.

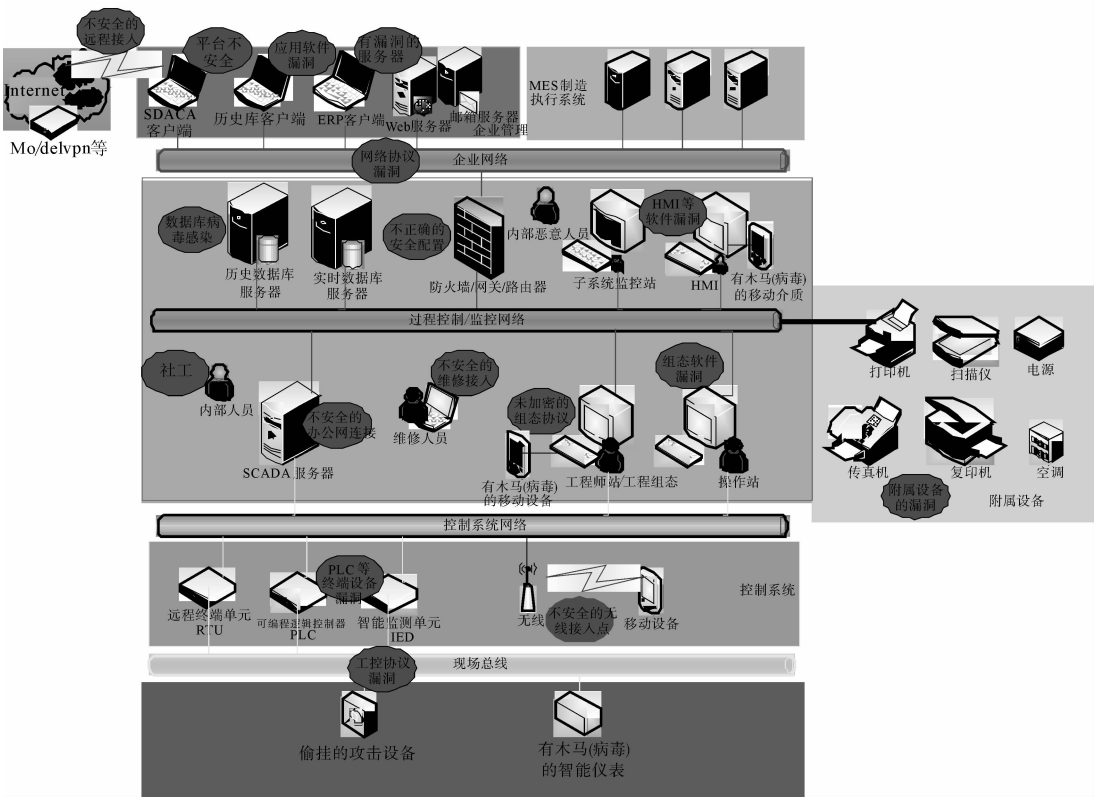

图 2 工控系统脆弱点及其攻击场景图

Fig. 2 Vulnerability of industrial control system and its attack scene

4 基于组合神经网络的启发式工控系统异常检测

4.1 异常检测模型及流程

由于异常检测的复杂性,采用混合方法已成为异常检测技术发展的一大趋势[8,9]. 工控系统的特异性是异构的多维信息,根据 2.2 节的结论本文选择并设计一种基于知识的检测即组合神经网络方法. 神经网络的结构设计尚无系统的方法,组合神经网络的核心思想是“以结构对异构”,通过多个“面向对象”的子神经网络的融合实现一种组合放大效应,以空间复杂度换取检测的性能,不仅能降低单个神经网络的复杂度,更能有效利用领域知识、先验知识降低整个神经网络的训练收敛时间及检测时间. 工控系统不同维度的特异性分别对应不同的、异构的子神经网络,而工控系统流量及样本的稀疏性使得单一的子神经网络无须大的网络结构. 基于此,模型引入静态指纹和动态指纹结合的思想,遵循信息抽象的级别,设计基于组合神经网络的识别模型,分为客体对象层、检测对象层、指纹标识层及画像表示层 4 个层级,整体架构如图 3. 针对设备侧对象,其静态指纹为设备 ID、物理位置及设备任务类型的绑定,其动态指纹为设备运行时的功率谱特性. 针对网络侧对象,其动态指纹包含多维属性,如协议特征(五元组、包载荷、功能代码,PLC 梯形逻辑等)、行为特征(流量变化、流量是否来源于规定区域、非授权登录等)、统计特征(包间隔、包延迟、包大小等). 将这些动静指纹作为神经网络的输入而不是使用原始数据包,其优点是由于在输入层加入先验信息和分类信息,这种分层启发式方法能在复杂背景噪声条件下保证较高识别准确度的同时,大幅缩减输入信息的维度和分析量,较好适应了工控环境设备计算能力受限的约束条件.

模型包括离线训练模式和在线工作模式,通过数据采集导入数据报文或数据包文件后进行分类预处理,预处理包括特征提取和归一化,如异构工控设备的特征提取,通过协议逆向和自动分析提取包含操作系统、协议和硬件指纹的多维度静态指纹,按照设备、协议、统计和行为四方面分别进行归一化处理,并作为指纹特征向量输入相应的量子神经网络,通过开关训练并使用该网络,最后通过一定的识别逻辑对三个神经网络的输出进行数据融合,从而实现对异常的自动识别和分类.

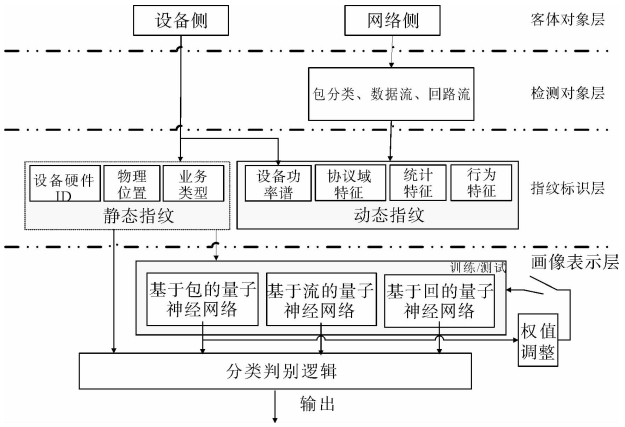

图 3　组合神经网络模型的层级架构图

Fig. 3　Hierarchical architecture of combined neural network model

4.2　基于动静指纹的输入向量

神经网络算法是一个数值计算过程，须对特征指纹进行编码形成 n 维向量. n 维向量表征了某个时刻工控系统的状况，为便于归一化，按照先验知识对指纹载体进行分类，包括数据包、会话流、数据回三个层次. 其中，数据包作为设备指纹、高危控制命令、异常参数等语法型特征信息载体，如 Modbus、DNP3、ICCP 等协议的分段标志、偏移、载荷等. 流特征针对隐藏在连续的多个数据包中的统计异常信息，包括包序列、命令序列等. 数据回特征观察双向信息流是否满足特定业务约束，包括业务类型、链路特征、流量特征及时间窗口等. 包、流和回作为通信要素共同作用形成高维图式，对工控入侵进行画像.

表 2　工控入侵指纹特征输入向量

Tab. 2　The input vector of intrusion fingerprint feature in industrial control system

信息类型	信息载体	输入向量	数据类型性	特征含义
语法(特征类)	数据包	特定协议域	字符型、数值型	误用识别
语义(统计类)	会话流	包大小、包序列等	数值型	规律理解
语用(行为类)	数据回	业务、流量、时间等	数值型、布尔型	合法判断
画像(知识类)	训练集	指纹	数值型	图式分类

神经网络不能直接和外界通信，神经网络算法是一个数值计算过程，其输入和输出都是数值向量，因此需要将外部输入样本转换为输入向量并规格化到 [0,1] 区间[10].

(1) 字符型：如工控协议域指纹一般用字符型表示，须进行字符数值化预处理，可将 Modbus、DNP3 等协议进行十进制编码，如用 1 表示 Modbus，2 表示 DNP3 等. 计算公式为 $y=\dfrac{x}{a+1}$，式中 x 为协议的序号；a 为最大序号；y 为转化后的实数值.

(2) 数值型：数据流的包长、时间间隔等指纹一般用数值型表示. 归一化方法可采用线性插值法将其映射到 [0,1] 区间内数值，方法是若有一数组 $[a_i]$ 在区间 $[a_1,a_n]$ 内，通过公式 $x_i=x_1+(x_n-x_1)\dfrac{a_i-a_1}{a_n-a_1}$ 可将其中的 a_i 映射到区间 $[x_n,x_1]$ 内的数.

(3) 布尔型：行为类语用指纹如流量是否超过基线、峰值流量是否在时间窗口内等，其值为两个相反的逻辑状态，数值化方法为若状态值为真则在指纹数组中相应字段用 1.0 表示，反之用 0.0 表示.

4.3　组合量子神经网络的构造及算法选择

工控系统入侵检测的实质是一个分类问题. 采用量子理论量子叠加思想的量子神经网络相比 BP 等传统类型的神经网络，其隐层的激励函数采用了多个 sigmoid 函数的线性叠加，因而隐层的神经元能够表示更多的状态，理论和实验均证明多层激励函数的量子神经网络对具有不确定性、两类模式之间存在交叉数据的分类问题具有更高的自由度，因此将它应用到工控系统场景对特异性及异构性的动静态指纹进行图式理解和分类更具优越性[10].

为了减少单个神经网络的复杂度，基于对工控系统动态指纹的分类，相应地构造了 3 个独立的 3 层结构量子神经网络，其中，基于包的神经网络以协议字段为输入向量，其结构设计为 9-18-1；基于流的神经网络以统计特征为输入向量，其结构设计为 6-18-1；基于回的神经网络以数据流的行为特征为输入向量，其结构设计为 4-12-1. 三个神经网络的输出采用模糊逻辑进行信息融合. 在算法上，以文献[10,11]成果为基础进行了必要的适应性改造，如图 4，DR-QSOFM 神经元模型由输入向量、权重向量、量子旋转门、传递函数等组成，算法主要思想和过程是，模型以样本的领域信息作为先验知识进行输入，与样本的指纹向量一起参与权重向量

的调整. 转换函数 f_m 将处于实数态的特征向量 X 和目标向量 T 转换成对应的量子态输入 $|X\rangle$ 和 $|T\rangle$,权重向量也为量子态,$|W\rangle$ 表示特征向量与量子旋转门 U_i 的连接权重,$|V\rangle$ 表示目标向量与 U_i 的连接权重;量子旋转门 U_i 在量子态特征向量、目标向量和权重向量的作用下进行相位旋转,然后再反作用于 $|W\rangle$,使权重向量的方向朝着输入模式的方向进行调整,不断地向样本的中心位置移动,f_o 表示传递函数,最终将 DR-QSOFM 神经元的输出映射成一个分类实数,从而完成对工控系统入侵的画像理解.

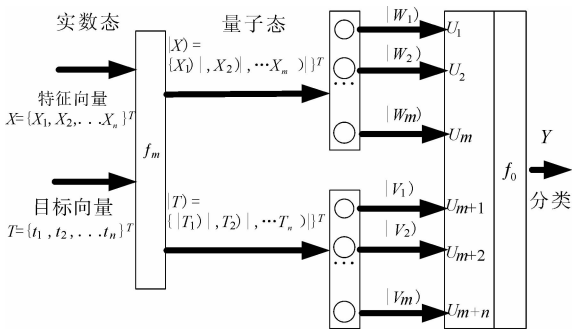

图 4 DR-QSOFM 神经元算法模型

Fig. 4 DR-QSOFM neuron algorithm model

5 测试及结果分析

5.1 测试环境及数据

搭建工控模拟系统及其场景,并在网络侧部署网络抓包软件,实验数据来源于实战案例模拟系统产生的数据以及部分 KDD Cup 1999 网络数据集. 数据集包括 DoS(拒绝服务攻击)、Probe(各种端口扫描和漏洞扫描)、U2R(各种权限提升)、R2L(远程权限获取)等 4 类攻击. 针对 Stuxnet、Duqu、Flame、Havex 以及 shodan 等部分实战样本的攻击行为,限于工控模拟系统的条件仅对其关键手法进行了仿真模拟,另外还有作者针对部分工控协议漏洞成功进行的中间人攻击数据,这些数据被随机地分为训练数据集和测试数据集,其中训练数据集选取包含实战攻击模拟数据、漏洞中间人攻击数据以及部分 KDD 攻击数据共计 12000 条记录,其中正例和反例各为 6000 条用于神经网络对“自我”及“非我”的画像. 各攻击类型所占比例如图 5 所示.

构造组合神经网络,输入层神经元的数量根据预处理后每条数据所保留属性的数量来确定. 针对 Stuxnet、Duqu、Flame 等实战样本所使用的攻击载体及其特异性进行分析,Stuxnet 是世界上首个专门针对工业控制系统编写的破坏性病毒,能够针对

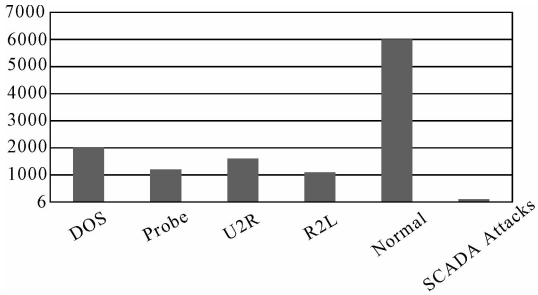

图 5 实验数据集攻击类型分布

Fig. 5 Attack type distribution of experimental data set

西门子的 SIMATIC WinCC 监控与数据采集(SCADA)系统进行攻击,在设备侧,Stuxnet 通过修改 PLC 来改变工业生产控制系统的行为,修改并注入新的 PLC 代码块,进而利用 Rootkit 功能隐藏 PLC 感染并躲避检测. 在网络侧 Stuxnet 拦截发送给 PLC 的读/写请求,以此判断系统是否为潜在的攻击目标. Duqu 在工控系统中被用来收集与其工控攻击目标有关的各种情报,与 C&C 通信的是一个采用一种未知编程语言编写 DLL 载荷. Duqu 最大的特异性表现在恶意代码只驻留在被感染机器的内存里,当目标机器重启时虽会被清除,但只要该及其还能连上内网,恶意代码就会从另一台感染机器传过来,这一手法是前所未见的. 从检测角度看,Duqu 在网络侧通过多种途径诸如 HTTP 请求、网络端口和代理服务器与 C&C 及内网机器连接通信. 而感染 Flame 的设备能自动分析自身的网络流量规律,自动录音,记录用户密码和键盘敲击规律,在设备侧通过流量混淆变形将信息及文件发送给远程服务器,在设备侧 Flame 检测并配置被控设备的蓝牙工作状态,当检测到其他设备靠近被感染机器时就通过蓝牙收集设备的信息. 基于以上工控系统及其攻击样本的特异性,设计相应子神经网络结构的输入向量,包括设备侧选择了设备功率谱、时间窗口作为输入,网络侧的基于包的神经网络选取了 Modbus、DNP3、ICCP 等工控协议以及 HTTP 的分段标志、偏移、载荷、命令参数等 9 个特征字段作为输入,基于流的神经网络选取了包长、包方向、包比例、到达时长、包间隔时间、包序列向量等 6 个对象作为输入,基于回的神经网络将业务类型、链路、流量和时间窗口等 4 个对象作为输入.

5.2 测试过程与分析

在模型工作阶段,以正常 KDD 数据为背景噪

声，将某种攻击数据分别叠加到多种不同的噪声文件上去，观察模型在复杂噪声下的识别结果并进行统计分析.

为了测试并比较组合神经网络模型相比普通神经网络在已知样本的辨识能力及区分能力上的差异，分别将模拟的 Stuxnet、Duqu 以及 Shadon 扫描和协议漏洞为攻击样本进行训练及测试，对比的统计结果如表 3 所示. 可见，基于组合神经网络的检测模型的统计检测率均在 95% 以上，对相同的数据样本其检测率和虚警率相比 BP 神经网络有明显优势.

表 3　模型对异常样本的识别能力对比

Tab. 3　Comparison of the recognition ability of the model to the abnormal samples

样本	BP 神经网络		组合量子神经网络	
	检测率	检错率	检测率	检错率
Stuxnet 模拟	84.3	15.7	96.1	3.9
Duqu 模拟	81.3	18.7	95.7	4.3
Shadon 扫描	94.9	5.1	100	0
协议漏洞攻击	83.5	16.5	96.8	3.2

为了进一步验证模型的对未知攻击的识别能力，以 Havex 及其变种的攻击手法作为未知入侵进行模拟测试. Havex 病毒样本 mbcheck. dll 是专门针对工控系统的新型攻击，其手法涵盖了社会学攻击和水坑攻击，据不完全统计国际安全研究机构已收集并分析 Havex RAT 的变种超过 80 个. Havex 及其变种有很多值得关注的特征，如版本众多且更新速度快，每个变种的特征也不断变化，攻击手法特别，可以直接控制 OPC 客户端对 OPC 服务器发出非法指令操作 PLC 和现场设备，使用自定义私有协议实现不同 C&C 服务器之间的通信等. 实验模拟了 20 种 Havex 变种的攻击手法，分为 2 组置于不同的背景流量中，模型的识别结果如表 4 所示.

表 4　模型对 Havex 及其变种的识别能力

Tab. 4　The recognition ability of the model to Havex and its variants

样本	检测率	检错率
前 10 组	96.5	3.5
后 10 组	95.3	4.7

综和以上测试可以发现，基于量子神经网络的识别方法相比传统的 BP 神经网络在噪声免疫力、检测准确性、可靠性以及鲁棒性等方面优势明显，从技术上分析其原因可解析为：动静指纹组合的高维特性对攻击变异具有一定自适应能力，三个不同的量子神经网络的组合在特征表达方面的互补性提高了检测率.

6　结　论

工控系统及其入侵方法目前处于快速发展和动态演化的进程之中，文章着眼于工控系统的特异性，引入动静结合的系统指纹概念，采用启发式的组合检测思想，实现了一种通用型的工控系统异常检测模型，取得了较好的实验结果. 未来的工作：(1)针对不同工控系统入侵手法的特点，研究统一化、规范化、形式化的数据模型及其特征描述方法；(2)采用证据理论等方法对多个神经网络模型的可信度进行分析评价和融合，进一步提高模型预测的精度和粒度；(3)进一步增强模型对于“自我”的表达能力，结合大数据的思想对工控系统所在的领域知识、业务知识，更好地指导模型的建模及算法的优化.

参考文献：

[1] Pleijsier E. Towards anomaly detection in SCADA networks using connection patterns [C]//Proceedings of 18th Twente Student Conference on IT. Enschede, Holland: University of Twente, 2013.

[2] 董超，周刚，刘玉娇，等. 基于改进的 Adaboost 算法在网络入侵检测中的应用 [J]. 四川大学学报：自然科学版，2015，52：1225.

[3] 宿娟，何志蓉. 一维 Hopfield 神经网络模型的多稳态分析 [J]. 四川大学学报：自然科学版，2016，53：260.

[4] 杨安，孙利民，王小山，等. 工业控制系统入侵检测技术综述 [J]. 计算机研究与发展，2016，53：2039.

[5] 李琳，尚文利，姚俊，等. 单类支持向量机在工业控制系统入侵检测中的应用研究综述[J]. 计算机应用研究，2016，33：8.

[6] 彭勇，向憧，张淼，等. 工业控制系统场景指纹及异常检测 [J]. 清华大学学报：自然科学版，2016，56：14.

[7] 谢丰，彭勇，赵伟，等. 工业控制设备安全测试技术 [J]. 清华大学学报：自然科学版，2014，54：29.

[8] 郭通. 基于自适应流抽样测量的网络异常检测技术研究 [D]. 郑州：解放军信息工程大学，2013.

[9] 屈洪春，王帅. 一种基于进化神经网络的混合入侵检测模型 [J]. 计算机科学，2016，43：335.

[10] 唐彰国，李焕洲，钟明全，等. 基于量子神经网络的启发式网络隐蔽信道检测模型 [J]. 计算机应用研究，2012，29：3033.

[11] 张亮，陆余良，房珊瑶. 基于量子自组织神经网络的 DeepWeb 分类方法研究 [J]. 计算机科学，2010，38：205.