文章编号: 1001-0920(2017)07-1223-06 DOI: 10.13195/j.kzyjc.2016.0551

基于改进C-SVC的工控网络安全态势感知

陆耿虹[1], 冯冬芹[2†]

(1. 浙江大学 工业控制技术国家重点实验室，杭州 310027；2. 浙江大学 智能系统与控制研究所，杭州 310027)

摘 要: 工控网络攻击类型多样、强度不一,在这种情况下,传统检测技术无法对多种类型的攻击进行有效识别,也无法给出全面准确的工控网络安全态势. 为此,提出工控网络安全态势感知模型: 首先采取改进的C-SVC算法对多源数据进行规则提取;然后利用决策融合算法进行决策层融合,获取最终态势感知结果. 实验结果表明: 所提出的模型和算法能够有效地识别多类型攻击,准确判断出系统遭受到的攻击,并形成态势感知结果.

关键词: 工业控制系统；网络安全态势感知；改进的C-SVC；决策融合

中图分类号: TP273 **文献标志码:** A

Industrial control network security situation awareness based on improved C-SVC

LU Geng-hong[1], *FENG Dong-qin*[2†]

(1. State Key Laboratory of Industrial Control Technology，Zhejiang University，Hangzhou 310027，China；Institute of Cyber-Systems and Control，Zhejiang University，Hangzhou 310027，China)

Abstract: The attacks against the industrial control network have different types and various attack intensity. Under this circumstance, the traditional detection techniques cannot identify the multiple types of attacks effectively, and can not assess the security situations of the industrial control network comprehensively and accurately. Therefore, the industrial control network security situation awareness model is proposed. Firstly, the rule extraction can be done by applying the improved C-SVC algorithm to the multi-sensor data. Then with the application of decision fusion algorithm, the decision-level fusion is completed and the results of situation awareness are procured. The simulation experiment results show that the proposed model and algorithms can distinguish multiple types of attacks effectively, identify the attacks that are launched against the industrial control system accurately, and generate the results of situation awareness.

Keywords: industrial control system；network security situation awareness；the improved C-SVC；decision fusion

0 引 言

基于网络的工控系统被称为工控网络,而随着工控系统的通信网络与外部网络连接程度的增加,使得工控网络极易受到外部入侵者的攻击[1].但不同于传统IT网络着重于网络层内的数据安全研究,在对工控网络进行研究时需要考虑物理层所受威胁.

强调物理层信息的重要性是由于工控网络信道内的数据一旦遭受攻击,会使得这些被篡改的信息通过反馈控制直接对物理过程产生影响. 如,震网病毒是通过对可编程逻辑控制器程序的篡改,获取设备的控制权,导致设备损伤[2],造成了伊朗布什尔核电站内大量离心机报废[3]. 攻击者依据已知的先验系统知识、窃取的系统数据以及现有的攻击手段[4],对工控系统施加不同类型的攻击,以破坏系统的可用性、完整性及保密性. 因此,对多种攻击进行有效识别与区分,有助于正确理解工控系统状态,提升系统安全能力.

安全态势感知技术不同于传统检测技术,能在获取系统数据信息的基础上,通过解析信息之间的关联性对数据进行融合,获取宏观的安全态势,准确判断系统是否遭受到攻击,并识别攻击类型,给出系统当前安全状态. Bass[5]提出了应用多传感器数据融合建立网络空间态势感知的框架,通过推理识别入侵者身份、速度、威胁性和入侵目标,进而评估网络空间的安全状态; Shifflet[6]采用本体论对网络安全态势感知相关概念进行了分析比较研究,并提出基于模块化的

收稿日期: 2016-05-03；**修回日期:** 2016-10-08.

基金项目: 国家自然科学基金项目(61223004).

作者简介: 陆耿虹(1992−), 女, 博士生, 从事工业控制系统网络安全态势感知等研究；冯冬芹(1968−), 男, 教授, 博士生导师, 从事现场总线、实时以太网、工业控制系统安全以及网络控制系统等研究.

†通讯作者. E-mail: fengdongqin@zju.edu.cn

技术无关框架结构;韦勇等[7]针对网络系统多源的特点,提出了一个网络安全态势感知的融合框架.

为了提高安全态势感知的准确性,本文引入多源融合技术,该技术可以最大限度地利用多源异构数据,提高系统的准确性和鲁棒性,从而获得对事件的准确判断[8]. 支持向量机(SVM)技术作为多源融合的技术之一,具有强大的推理与快速学习能力. Vapnik[9]在1995年最早提出了标准的支持向量机方法,称为C-SVC方法,这是最基本的SVM算法. 林肯实验室的Braun[10]提出了基于SVM技术的多数据源融合方法,并针对数据采集过程中,来自数据源的数据可能丢失问题,提出了解决方法. 之后,Braun等[11]提出了利用SVM技术对大量数据源数据的信息进行数据融合,对高维度的输入空间进行划分,保持数据完整性,并讨论了特征层融合与决策层融合之间的关系;Lu等[12]提出了利用SVM技术对多源多属性信息进行融合的态势评估方法.

本文在考虑工控系统网络安全问题时,依据攻击特点对攻击进行分析,并将攻击下物理层各个节点的信息以及信息间潜在的关联作为数据源进行研究,提出了基于改进的C-SVC技术的工控系统网络安全态势感知方法. 在建立工控系统网络安全态势感知模型的基础上,介绍了改进的C-SVC算法,以及决策融合算法:改进的C-SVC算法作为一种统计规则,能够对属于多个类别的数据源信息进行判别与分类;而决策融合算法是在构造多个不同的C-SVC基础上,将每个C-SVC输出结果result(label, Cl, μ)作为决策融合算法的输入,可在统计结果出现冲突,无法获取整体系统态势的情况下,利用置信水平Cl及匹配度μ对C-SVC输出可靠性进行定量计算,实现决策融合,并最终获取系统安全态势. 在本文的最后,对受到不同假数据注入攻击的单回路控制系统进行仿真实验,验证了模型和算法的准确性及有效性.

1 工业控制网络

1.1 工控网络模型介绍

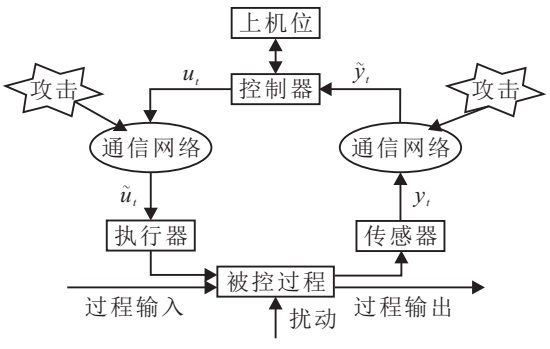

图 1 受到攻击的工控网络示意图

图1描述的是空间分布式的工控系统模型. 其中,被控过程的运行由控制器进行控制,控制器能够接收分布在不同地域的传感器测量值,并利用通信网络将控制信号传输至空间分布的执行器中[13]. 在工控系统运行时间T内,t时刻系统受到攻击者的恶意攻击,传感器(或控制器)输出的信号$y_i(t)(u_i(t))$与控制器(或执行器)接收到的信号$\tilde{y}_i(t)$(或$\tilde{u}_i(t)$)存在偏差:

$$\tilde{y}_i(t)=\begin{cases} y_i(t),\ t\notin T_{\rm atc};\\ a_i(t),\ t\in T_{\rm atc}; \end{cases} \tag{1}$$

$$\tilde{y}_i(t)\in Y_i,\ Y_i=[y_i^{\min},y_i^{\max}]; \tag{2}$$

$$\tilde{u}_i(t)=\begin{cases} u_i(t),\ t\notin T_{\rm atc};\\ a_i(t),\ t\in T_{\rm atc}. \end{cases} \tag{3}$$

其中:$y_i^{\min}$和$y_i^{\max}$分别为传感器检测范围内的最小值和最大值;$a_i(t)$为攻击者施加的攻击信号[14],攻击方式、目的不同,攻击信号也不同;$T_{\rm atc}$为系统遭受到攻击的时间,$T_{\rm atc}\subset T$.

定义1 系统正常normal. 如果$a_i(t)=0$,则称这个工控网络在时刻t是正常的;否则,称该系统在时刻t遭受攻击.

1.2 假数据注入攻击

假数据注入攻击是在攻击者知道系统组态的情况下对系统的测量值进行篡改,并不能被传统检测方式(通过对测量值与预测值两者残差的平方值进行评估,当该值超过某一阈值时发出警报)检测到的一类攻击[15],可用下式表示:

$$a_i(t)=\begin{cases} 0,\ t\notin T_{\rm atc};\\ a_i(t-1)+\mu\gamma^t,\ t\in T_{\rm atc}. \end{cases} \tag{4}$$

其中:μ、γ为常数,随着t的增长,γ^t呈指数增长.

不同的参数设定会使得系统遭受到不同强度的攻击,从而对系统性能产生不同影响. 一般的假数据注入攻击的主要攻击方式有以下3种:

1) 浪涌攻击$\rm surge_{atc}$.

攻击目标:在最短的时间内,对被控过程造成尽可能最大程度的伤害.

2) 偏差攻击$\rm bias_{atc}$.

攻击目标:攻击者在每一时刻连续对数据进行篡改,即在前一时刻数据的基础上添加一个非零的较小的常数C,在保证不触发警报的前提下对系统造成伤害.

3) 几何攻击$\rm geom_{atc}$.

攻击目标:攻击者在开始攻击时对数据的篡改幅度较小,并不断累积攻击偏差值,在攻击的最后时

刻产生幅度较大的偏差值,试图对系统造成最大程度的伤害.

通过对这3类典型假数据攻击的识别,可有助于决策人员探知攻击者的攻击意图,从而做出准确的决策方案以保证系统持续、稳定、安全地运行.

针对多类型攻击识别的要求,本文在第3节中提出了工控网络安全态势感知模型以及相关的算法,以实现对工控系统态势的准确判断.

2　工控网络安全态势感知模型

工控网络安全态势感知模型如图1所示.

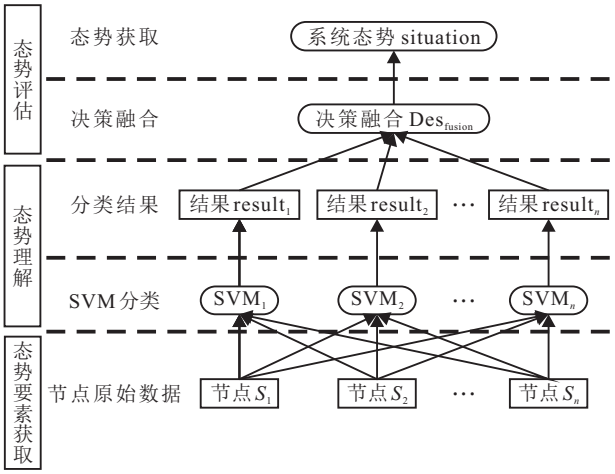

图 2　工控网络安全态势感知模型

为了叙述方便,在介绍工控网络安全态势感知模型之前,给出如下定义.

定义2　训练数据S^{train}. 在训练时段T_{train}内,采集到来自不同时刻t不同数据源i的数据,用于进行多类SVC训练.

$$S^{\text{train}}(t)=[S_1^{\text{train}}(t),\cdots,S_n^{\text{train}}(t)]^{\text{T}},t\in T_{\text{train}};\quad(5)$$

$$S^{\text{train}}=\{S^{\text{train}}(t)|t=1,2,\cdots,T_{\text{train}}\}.\quad(6)$$

定义3　测试数据S^{test}. 在测试时段T_{test}内,来自不同时刻t不同数据源i的数据,用于进行多类SVC测试.

$$S^{\text{test}}(t)=[S_1^{\text{test}}(t),\cdots,S_n^{\text{test}}(t)]^{\text{T}},\ t\in T_{\text{test}};\quad(7)$$

$$S^{\text{test}}=\{S^{\text{test}}(t)|t=1,2,\cdots,T_{\text{test}}\}.\quad(8)$$

定义4　置信水平Cl_{label}. 将测试时段T_{test}内的一组测试点类别标记为$\text{label}_{(i)}$的可靠程度.

$$\text{cl}_{\text{label}(i)}=\sum D_{\text{label}_{(i)}}\Big/\sum_{j=1}^{T_{\text{test}}}D_j.\quad(9)$$

其中: $D_{\text{label}_{(i)}}$是类别为$\text{label}_{(i)}$的测试点到决策分类面的距离, D_j是所有测试点到决策分类面的距离.

定义5　匹配度μ. 表征数据点x'与数组$X=\{x_1,x_2,\ldots,x_n\}$内各点的相似性,

$$\mu(x',X)=\sum_{i=1}^{n}F(x',x)\Big/n,\quad(10)$$

其中

$$F(x',x)=\frac{\sqrt{(x'\cdot x)}}{\sqrt{(x\cdot x)\cdot(x'\cdot x')}},\quad(11)$$

符号$(\cdot)$表示两个向量的内积.

定义6　结果result$(\text{label},\text{Cl},\mu)$: 测试阶段,C-SVC分类算法的输出结果可用三元组表示,即result$(\text{label},\text{Cl},\mu)$,其中label为C-SVC输出的类别标记.

本文提出的网络安全态势感知模型,主要包括3个层次,自下而上分别为态势要素获取层、态势理解层和态势评估层.

态势要素获取层: 对工控网络中的各节点数据进行采集,获取训练数据集S^{train}和测试数据集S^{test}.

态势理解层: 利用C-SVC分类算法对接收到的数据进行判断,并输出分类结果result$(\text{label},\text{Cl},\mu)$.

态势评估层: 对得到的分类结果进行评估,通过决策融合算法$\text{Des}_{\text{fusion}}$获取最终系统态势.

3　工控网络安全态势感知算法

本文提出的算法是在获取物理层各传感器数据源的基础上,采用C-SVC分类算法对系统状态进行模式识别和分类,并将C-SVC分类算法的输出结果作为决策融合算法的输入,实现对系统态势的整体感知.

需要注意的是,本文只考虑系统稳定运行过程中,遭受到假数据注入攻击时的情况. 对于一些特殊事件,如系统紧急关停时可能存在的系统异常状况,将不在文中进行分析.

3.1　C-SVC算法

SVM技术是在结构风险最小化和统计学理论基础上提出的一种模式识别方法. 该方法是对线性可分情况下的最优分类超平面进行求解. 而C-SVC技术作为最基本的SVM方法,通过引入惩罚参数C,软化超平面的几何间隔,以使得分类间隔增大,错划程度减小. 本文首先对C-SVC算法[16]进行介绍.

假设有训练集:

$$\text{Train}_{\text{data}}=\{(x_1,y_1),\cdots,(x_l,y_l)\}\in(\boldsymbol{X},\boldsymbol{Y}).\quad(12)$$

其中: $x_i\in\boldsymbol{X}=R^n\,(i=1,2,\cdots,l)$为输入数据, $y_i\in\boldsymbol{Y}=\{1,-1\}$为类别标记. 待求目标函数为

$$\begin{aligned}&\min\frac{1}{2}\|w\|^2+C\sum_{i=1}^{l}\xi_i;\\&\text{s.t. }y_i(w^{\text{T}}x_i+b)\geqslant 1-\xi_i,\\&\qquad\xi_i\geqslant 0,\ i=1,2,\cdots,l.\end{aligned}\quad(13)$$

其中: w为权系数向量, b为分类阈值, C为惩罚参数, ξ_i为松弛变量. 通过对式(13)引入Lagrange乘子α,构造并求解最优化问题:

$$\min_{\alpha}\frac{1}{2}\sum_{i=1}^{l}\sum_{j=1}^{l}y_iy_j\alpha_i\alpha_jK(x_i,x_j)-\sum_{j=1}^{l}\alpha_j;$$

$$\text{s.t.}\ \sum_{i=1}^{l}y_i\alpha_i=0,\ 0\leqslant\alpha_i\leqslant C,i=1,2,\cdots,l. \quad (14)$$

得最优解$\alpha^*=(\alpha_1^*,\alpha_2^*,\cdots,\alpha_l^*)^{\mathrm{T}}$,并选取$\alpha^*$的一个小于$C$的正分量$\alpha_j^*$,据此可获得决策函数:

$$y(x)=\mathrm{sgn}\Big[\sum_{i=1}^{l}\alpha_i^*y_iK(x,x_i)+b^*\Big], \quad (15)$$

$$b^*=y_j-\sum_{i=1}^{l}\alpha_i^*K(x_i,x_j), \quad (16)$$

其中$\mathrm{sgn}(\cdot)$为符号函数.

3.2 改进的C-SVC算法

原始C-SVC算法是针对二分类问题直接输出分类结果,其分类结果的可靠程度无法获得.

改进的C-SVC算法是在原始算法的基础上,引入置信水平Cl和匹配度μ的概念;在考虑C-SVC方法输出分类结果(设结果标记为label)的可靠程度时,可以用这两个值进行定量衡量.

置信水平Cl表示的是标记为label的一组数据点到决策面的距离占所有数据点到决策面距离的比值,该值越大说明该决策面的分类效果越佳.

匹配度μ表示的是标记为label的一组数据中,各点之间的紧密度大小,μ值越大说明该类别内的数据越相似,分类结果越好.

在介绍改进的C-SVC算法之前,需要说明的一点是,由于实际样本一般是线性不可分的,本文采用径向基核函数$K(x,x')$将原始输入空间映射到高维特征空间,获取高维空间中输入变量与输出变量之间的线性关系,并在此新空间中求取最优线性分类面[17]对数据进行分类.

$$K(x,x')=\exp\Big(-\frac{\|x-x'\|}{2\sigma^2}\Big), \quad (17)$$

其中σ为高斯核宽度.

算法1 改进的C-SVC算法.

Step 1: 依据已知的训练数据S^{train}以及与数据对应的系统态势构造训练集$\mathrm{Train}_{\mathrm{data}}$;

Step 2: 将训练集输入C-SVC,挑选合适的参数C与σ,并进行规则提取,获取式(13);

Step 3: 完成训练后,将测试数据S^{test}输入C-SVC,利用Step 2中所求规则求取测试数据中每一个点i所对应的输出$y_i(x)$;

Step 4: 利用式(8)求取$\mathrm{Cl}_{\mathrm{label}}$,其中参数$D_i$可用下式求取:

$$D_i=\frac{w^{\mathrm{T}}S^{\mathrm{test}}+b^*}{\|w\|}; \quad (18)$$

Step 5: 利用下式判断测试数据的整体类别:

$$\mathrm{label}=\mathrm{sgn}\Big[\frac{\sum y_{\mathrm{label}}(x)}{\sum|y_i(x)|}\Big], \quad (19)$$

其中y_{label}表示对所有相同的输出类别求和,此处的label用$+1,-1$或0表示;

Step 6: 判断label是否为0,若是,则执行下一步,否则执行Step 8;

Step 7: 计算两类各自的$\mathrm{Cl}_{\mathrm{label}}$,取值大的一类为测试数据的整体label;

Step 8: 利用式(10)计算每个时刻t下,测试数据$S^{\mathrm{test}}(t)$对所有训练数据的匹配度$\mu(S^{\mathrm{test}}(t),S^{\mathrm{train}})$;

Step 9: 计算整体匹配度

$$\mu=\frac{\sum_{t=1}^{T_{\mathrm{test}}}\mu(S^{\mathrm{test}}(t),S^{\mathrm{train}})}{T_{\mathrm{test}}}; \quad (20)$$

Step 10: 输出该组测试数据的整体类别结果$\mathrm{result}(\mathrm{label},\mathrm{Cl},\mu)$.

3.3 决策融合算法

改进的C-SVC算法具有实现测试数据整体类别划分的能力,为了对工控系统中可能存在的多种类型攻击及其相应的多种安全态势进行区分,本节提出了决策融合算法的概念.

该算法是在使用C-SVC的基础上,即在利用$\frac{K(K-1)}{2}$个C-SVC对系统内存在的K种安全态势进行两两分类的基础上,对C-SVC输出的$\frac{K(K-1)}{2}$个结果(每个C-SVC的决策输出)$\mathrm{result}(\mathrm{label},\mathrm{Cl},\mu)$进行决策融合,即对$\frac{K(K-1)}{2}$个结果标记label数量进行统计,选取数量最多的标记作为系统整体态势标记;当出现有2个及以上的标记有相同的最多数量时,利用置信水平Cl及匹配度μ定量计算输出结果的可靠性$r_{\mathrm{label}_{(i)}}^{\max}$,选取$r_{\mathrm{label}_{(i)}}^{\max}$最大值所对应的态势作为系统整体态势.

算法2 决策融合算法.

Step 1: 将$\frac{K(K-1)}{2}$个$\mathrm{result}^i(\mathrm{label}^i,\mathrm{Cl}^i,\mu^i)$作为输入函数,其中$\mathrm{result}^i$表示为第$i$个C-SVC的输出结果.

Step 2: 查找所有类别标志为$\mathrm{label}_{(i)}$的$\mathrm{result}^j(\mathrm{label}_{(i)}^j,\mathrm{Cl}^j,\mu^j)$,并记录其总数为$N_{\mathrm{label}_{(i)}}$.

Step 3: 将Step2计算得到的k个$N_{\mathrm{label}_{(i)}}(i=1,2,\cdots,k)$进行比较,获取与最大值对应的标记$\mathrm{label}_{(i)}^{\max}$,并记录这些标记的数量为$N_{\mathrm{dif}}$. 需要注意的是,与最大值对应的类别标记可能不止一种.

Step 4: 判断N_{dif}的值是否大于1,若是,则执行下一步,否则进入Step 8.

Step 5: 获取所有包含标记 $\text{label}_{(i)}^{\max}$ 的输出结果 $\text{result}^j(\text{label}_{(i)}^{\max},\ \text{Cl}^j,\ \mu^j)$.

Step 6: 针对不同的类别标记 $\text{label}_{(i)}^{\max}$, 利用下式对 Step 5 中同一类别标记对应的所有 result^j 中的参数 Cl^j 和 μ^j 进行计算, 以衡量分类结果的可靠性:

$$r_{\text{label}_{(i)}^{\max}} = \sum \text{Cl}^j \times \mu^j,\ j \in \left[1, \frac{K(K-1)}{2}\right]. \quad (21)$$

Step7: 将各个 $r_{\text{label}_{(i)}^{\max}}$ 进行比较, 记录最大 $r_{\text{label}_{(i)}^{\max}}$ 所对应的类别 $\text{label}_{(i)}$.

Step8: 依据最终获取的类别标记, 输出当前系统的态势结果.

在构造C-SVC (对C-SVC进行训练)时, 需要注意的是: 由于改进的C-SVC算法输出标记label值为1或 -1, 对于多分类问题, 可将需要进行分类的第 k 类和第 j 类的原始类别标记 $\text{label}_{(k)}$ 和 $\text{label}_{(j)}$, 分别标记为1和 -1, 以构造完整的训练集; 在测试过程中进行结果输出时, 将 $\text{label}_{(k)}$ (或 $\text{label}_{(j)}$) 回代至相应的数值, 此时, 输出结果 $\text{result}(\text{label}, \text{Cl}, \mu)$ 中的label不再是某个值, 而是用字符表示的多个类别标记.

4　仿真实验与结果

为了验证本文所提出模型和算法的有效性, 首先将单回路控制系统作为仿真对象搭建仿真模型, 再在反馈回路中施加不同种类的攻击, 最后利用本文提出的算法进行系统态势感知, 获取态势结果并计算算法准确率.

在本文中, 各类别标记label存在4种情况: $\text{label} \in \{\text{normal}, \text{surge}_{\text{atc}}, \text{bias}_{\text{atc}}, \text{geom}_{\text{atc}}\}$.

各类别标记含义如下: normal —— 系统正常; $\text{surge}_{\text{atc}}$ —— 浪涌攻击; bias_{atc} —— 偏差攻击; geom_{atc} —— 几何攻击.

4.1　仿真模型搭建

某精馏塔提馏段温度单回路控制方案[18], 如图3所示, 图中表示了蒸馏塔的提馏段, 提馏段某块板的温度为主变量. 其中: Q 为蒸汽流量, f_v 用于表征控制阀开度; p_v 为蒸汽控制阀阀前压力; p 为蒸汽控制阀阀后压力; F 为进料量, B 为塔底产品馏出液.

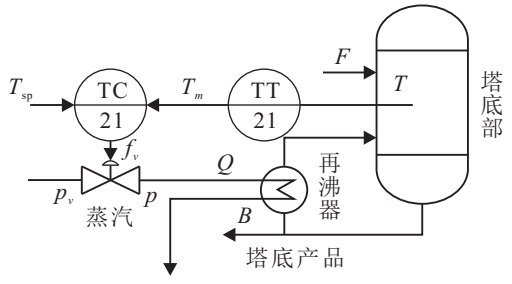

图 3　提馏段温度单回路控制方案

该系统中有一个温度传感器TT 21, 能对提馏段的温度 T_m 进行检测, 其中 T_{sp} 为 T 的设定值, 控制器TC 21通过控制信号 u 控制蒸汽控制阀, 对温度进行控制, 且控制阀门开度处于0% ~ 100%之间, 即控制阀完全关闭或完全打开.

4.2　仿真过程及结果

针对上节的仿真对象, 利用本文提出的算法进行仿真. 对于不同的攻击场景, 设置相关参数, 重现各类攻击, 并将温度传感器输出值 T_m、控制器输出值 u 作为数据源, 每次仿真时间 $t = [0, 300]$.

1) 浪涌攻击

$$a_i(t) = \begin{cases} 0,\ t \neq 101; \\ 10,\ t = 101. \end{cases} \quad (22)$$

2) 偏差攻击

$$a_i(t) = \begin{cases} 0,\ t \notin T_{\text{atc}}; \\ (t-1) + 0.1,\ t \in T_{\text{atc}}; \end{cases} \quad (23)$$
$$T_{\text{atc}} = [101, 151].$$

3) 几何攻击

$$a_i(t) = \begin{cases} 0,\ t \notin T_{\text{atc}}; \\ (t-1) + 0.05 \times 1.01^t,\ t \in T_{\text{atc}}; \end{cases} \quad (24)$$
$$T_{\text{atc}} = [101, 116].$$

训练过程构造与各态势相关的训练集:

1) 正常状态

$$\text{Train}_{\text{data}}^1 = \{(T_{m1}^1, u_1^1, y_1^1), \cdots, (T_{ml}^1, u_l^1, y_l^1)\}. \quad (25)$$

2) 浪涌攻击

$$\text{Train}_{\text{data}}^2 = \{(T_{m1}^2, u_1^2, y_1^2), \cdots, (T_{ml}^2, u_l^2, y_l^2)\}. \quad (26)$$

3) 偏差攻击

$$\text{Train}_{\text{data}}^3 = \{(T_{m1}^3, u_1^3, y_1^3), \cdots, (T_{ml}^3, u_l^3, y_l^3)\}. \quad (27)$$

4) 几何攻击

$$\text{Train}_{\text{data}}^4 = \{(T_{m1}^4, u_1^4, y_1^4), \cdots, (T_{ml}^4, u_l^4, y_l^4)\}. \quad (28)$$

进行C-SVC训练, 并将不同的态势进行两两组合, 构造6个C-SVC, 如表1所示.

表 1　各C-SVC与相应的训练集

	相关态势	训练集 $\text{Train}_{\text{data}}$
C-SVC1	$\text{surge}_{\text{atc}} - \text{bias}_{\text{atc}}$	$[\text{Train}_{\text{data}}^2 \ \ \text{Train}_{\text{data}}^3]^{\text{T}}$
C-SVC2	$\text{surge}_{\text{atc}} - \text{geom}_{\text{atc}}$	$[\text{Train}_{\text{data}}^2 \ \ \text{Train}_{\text{data}}^4]^{\text{T}}$
C-SVC3	$\text{bias}_{\text{atc}} - \text{geom}_{\text{atc}}$	$[\text{Train}_{\text{data}}^3 \ \ \text{Train}_{\text{data}}^4]^{\text{T}}$
C-SVC4	$\text{surge}_{\text{atc}} - \text{normal}$	$[\text{Train}_{\text{data}}^2 \ \ \text{Train}_{\text{data}}^1]^{\text{T}}$
C-SVC5	$\text{bias}_{\text{atc}} - \text{normal}$	$[\text{Train}_{\text{data}}^3 \ \ \text{Train}_{\text{data}}^1]^{\text{T}}$
C-SVC6	$\text{geom}_{\text{atc}} - \text{normal}$	$[\text{Train}_{\text{data}}^4 \ \ \text{Train}_{\text{data}}^1]^{\text{T}}$

2) 为了验证所提出算法的正确性, 分别对3种不同的攻击场景以及无攻击的场景进行仿真. 在每次仿真中, 将测试得到的 T_m 和 u 作为测试数据, 构造相应的测试集

$$S^{\text{test}} = \{(T'_{m1}, u'_1), \cdots, (T'_{mn}, u'_n)\}. \quad (29)$$

运行改进的C-SVC算法进行测试,每个测试集在输入不同的C-SVC后均能得到相应的测试结果.

将每个C-SVC的输出结果输入到决策融合算法中,获取系统最终态势. 表2所示为4组测试数据在每个C-SVC下的输出以及最终的系统态势结果,且每组测试数据的最终系统态势判定,均符合测试时的攻击场景.

表 2 测试结果及最终态势输出

	S_1^{test}	S_2^{test}	S_3^{test}	S_4^{test}
C-SVC1	$\text{surge}_{\text{atc}}$	bias_{atc}	bias_{atc}	bias_{atc}
C-SVC2	$\text{surge}_{\text{atc}}$	geom_{atc}	geom_{atc}	geom_{atc}
C-SVC3	bias_{atc}	bias_{atc}	geom_{atc}	bias_{atc}
C-SVC4	$\text{surge}_{\text{atc}}$	normal	normal	normal
C-SVC5	bias_{atc}	bias_{atc}	bias_{atc}	normal
C-SVC6	geom_{atc}	geom_{atc}	geom_{atc}	normal
系统态势	$\text{surge}_{\text{atc}}$	bias_{atc}	geom_{atc}	normal

5 结 论

本文提出了基于改进的C-SVC技术的工控网络安全态势感知方法. 该方法在获取来自多传感器数据源的基础上,利用改进的C-SVC算法提取不同种类攻击的攻击规则,通过算法对输入的测试数据进行测试,并获取算法输出结果;在此基础上,利用决策融合算法进行决策层融合可完成对系统的态势感知,获取准确的系统态势. 实验表明,本文所提出的算法能够有效地进行工控网络安全态势感知,并实现对系统当前所遭受攻击的识别,为安全管理人员提供可靠有效的决策依据.

下一步研究的方向为: 1)将算法与经验学习,即学习安全管理人员对系统遭受攻击的判断经验相结合,进行工控网络安全态势感知模型与算法的改进,以自动实现系统态势感知; 2)考虑特殊情况,如系统紧急关停时的工控网络安全态势,通过对复杂多样的异常产生原因进行分析,建立可区分多种异常行为的态势感知算法.

参考文献(References)

[1] 冯冬芹,褚健,金建祥,等. 实时工业以太网技术——EPA及其应用解决方案[M]. 北京:科学出版社, 2012: 150-164.
(Feng D Q, Chu J, Jin J X, et al. Real-time industrial Ethernet technology — EPA and its application solutions[M]. Beijing: Science Press, 2012: 150-164.)

[2] David A, Paul B, Christina W. Did stuxnet take out 1,000 centrifuges at the natanz enrichment Plant?[R]. Washington: Institute for Science and International Security Report, 2010.

[3] Hespanha P, Naghshtabrizi, Xu Y. A survey of recent results in networked control systems[J]. Proc of IEEE, 2007, 95(1): 138−162.

[4] Andre T, Daniel P, Henrik S, et al. Attack Models and Scenarios for Networked Control Systems[C]. ACM Int Conf on High Confidence Networked Systems. Beijing: ACM Press, 2012: 54-64.

[5] Bass T. Intrusion systems and multisensor data fusion: creating cyberspace situational awareness[J]. Communications of the ACM, 2000, 43(4): 99-105.

[6] Shifflet J. A technique independent fusion model for network intrusion detection[J]. Proc of Midstates Conf on Under Graduate Research in Computer Science and Mathematics, 2005, 3(1): 13-19.

[7] 韦勇,连一峰,冯登国. 基于信息融合的网络安全态势评估模型[J]. 计算机研究与发展, 2009, 46(3): 353-362.
(Wei Y, Lian Y F, Feng D G. A network security situational awareness model based on information fusion[J]. J of Computer Research and Development, 2009, 46(3): 353-362.)

[8] Yang S J, Stotz A, Holsopple J, et al. High level information fusion for tracking and projection of multistage cyber attacks[J]. Information Fusion, 2009, 10(1): 107-121.

[9] Vapnik V. The nature of statistical learning theory[M]. New York: Springer, 2000: 123-167.

[10] Jerome J Braun. Sensor data fusion with support vector techniques[J]. Proceedings of SPIE, 2002, 4731: 98-109.

[11] Jerome J Braun, Sunli P J. Information fusion of large number of sources with support vector machine techniques[J]. Proc of SPIE, 2003, 5099: 13-23.

[12] Lu J, Yang X, Zhang G. Support vector machine-based multi-source multi-attribute information integration for situation assessment[J]. Expert Systems with Application, 2008, 34: 1333-1340.

[13] 李硕,戴欣,周渝霞. 网络安全态势感知研究进展[J]. 计算机应用研究, 2010, 27(9): 3227-3232.
(Li S, Dai X, Zhou Y X. Research progress of network security situation awareness[J]. Application Research of Computer, 2010, 27(9): 3227-3232.)

[14] Cárdenas A A, Amin S, Lin Z S, et al. Attacks against process control systems: Risk assessment, detection, and response[C]. Proc of the 6th ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2011: 355-366.

[15] Yao Liu, Peng Ning, Michael K R. False data injection attacks against state estimation in electric power grids[J]. Proc of the 2009 ACM Conf on Computer and Communications Security, 2009, 14(1): 21-32.

[16] 邓乃扬,田英杰. 数据挖掘中的新方法:支持向量机[M]. 北京:科学出版社, 2004: 164-223.
(Deng N Y, Tian Y J. A new method of data mining: Support vector machine[M]. Beijing: Science Press, 2004: 164-223.)

[17] 边肇祺,张学工. 模式识别[M]. 北京:清华大学出版社, 1999: 257-258.
(Bian Z Q, Zhang X G. Pattern recognition[M]. Beijing: Tsinghua University Press, 1999: 257-258.)

[18] 戴连奎,于玲,田学民,等. 过程控制工程[M]. 北京:化学工业出版社, 2012: 85-116.
(Dai L K, Yu L, Tian X M, et al. Process control engineering[M]. Beijing: Chemical Industry Press, 2012: 85-116.)

(责任编辑:齐 霁)