

基于逆向云算法模型的工业控制系统工艺稳定性建模与攻击防护

蔺俊豪, 冯冬芹

(浙江大学控制科学与工程学院, 浙江 杭州 310027)

摘要: 与传统的网络安全防御手段相比, 基于工艺流程的工业系统安全防护研究愈发成为工业控制安全领域的重要研究方向。提出一种改进型 BC-1stM 无确定度逆向云算法, 通过对时间序列与工艺流程的正常状态进行建模, 实现在工业系统中基于工艺攻击方式的安全防护检测与告警, 并采用田纳西伊士曼化工过程平台进行验证。结果表明, 该模型在进行攻击行为检测与攻击点检测方面有很高的查准率, 提高了工业系统的安全防护能力。

关键词: 工业控制系统; 工艺流程; 正常状态模型; 入侵检测; 逆向云算法

中图分类号: TP309.2

文献标识码: A

doi: 10.11959/j.issn.2096-6652.202006

Process stability modeling and attack protection of industrial control system based on reverse cloud algorithm model

LIN Junhao, FENG Dongqin

Zhejiang University College of Control Science and Engineering, Hangzhou 310027, China

Abstract: Compared with traditional network security defense methods, industrial system security protection research based on process flow has become an important research direction in the field of industrial security. An improved backward cloud algorithm based on first order absolute central moment (BC-1stM) non-deterministic reverse cloud method was proposed, which was modeled by the time series and the normal state of the process flow. The security protection detection and alarm based on the process attack mode in the industrial system was realized, and Tennessee Eastman chemical process platform was adopted to validate the algorithm. The results show that the model had a high precision in the detection of attack behavior and detection of attack points, and improved the security protection capability of industrial systems.

Key words: industrial control system, process flow, steady state model, intrusion detection, reverse cloud algorithm

1 引言

在2010年“震网”病毒攻击伊朗核电站之后, 世界各国在近些年接连发生了多起工业控制网络安全事件: 2015年乌克兰电力系统被具有高度破坏性的恶意软件攻击, 导致大规模停电数小时; 2019年3月委内瑞拉玻利瓦尔共和国水电站遭受攻击导致大范围停电。这些工业控制网络攻击大多导致了工业生产停摆, 造成了严重事故。

对近年来工业控制系统遭受的攻击进行分析^[1-3],

可以得到这样一个结论: 对工业控制系统的网络攻击与破坏已经越来越深入、越来越隐蔽, 难以被及时察觉与防范, 造成了不可避免的损失。而传统意义上的网络安全防护更多的是针对攻击者的行为进行分析, 提取攻击特征进行研究和防护。但是, 如果攻击者只是渗透进入系统, 接管操作并且不按照工艺流程下达控制命令, 那么其完全能够在操作合法的情况下实施攻击, 造成减产停产等重大损失。因此, 针对工业控制系统进行工艺稳定性建模与攻击防护检测的研究就显得尤为重要。

收稿日期: 2019-01-01; 修回日期: 2020-02-26

通信作者: 蔺俊豪, linjunhao@zju.edu.cn

2 工业控制网络安全研究背景

目前,对工业控制系统的网络安全的研究还处在发展阶段,且研究思路主要分为网络信息传输安全与工艺安全2个方向。

对于网络信息传输安全的研究,李俊等人^[4]利用卡尔曼滤波器对工业控制系统中遭受的分布式拒绝服务(distributed denial of service, DDoS)攻击进行检测,但是其检测仅限于DDoS攻击,对于其他攻击类型很难有好的效果。杨伟等人^[5]基于IEEE 802.15.4e的工业互联网标准研究安全时钟同步策略,把工业控制网络时钟同步机制当作攻击者的首要目标进行防护,并提出单跳时间同步技术,但是该算法仍然在控制周期内部增加验证算法进行防护,这会影响对时延要求极高的工业控制系统的性能。

相比网络传输安全的局限性,针对特定工艺的攻击检测可以更好地适配工业控制系统不同类型攻击的安全防护,从系统层面保证系统的稳定运行。但是现有研究仍有局限性:李绍晖等人^[6]提出基于柯尔莫哥洛夫不等式理论设置累积和算法(cumulative sum based on Kolmogorov Inequality, CUSUM-KI)偏移常数的入侵检测方法,但是其更多是基于几个关键参数进行检测,无法做到在系统遭受未知攻击时从所有数据中检测出遭受攻击的时间和相关攻击点等信息,因此在大型控制系统中难有好的检测效果;王华忠等人^[7]利用主成分分析(principal components analysis, PCA)和粒子群优化(particle swarm optimization, PSO)-支持向量机(support vector machine, SVM)相结合的方法,实现了基于数据驱动的工业控制系统的3类攻击检测,但是未对通过降维剔除的“冗余信息”的无效性进行验证,且检测算法运算量巨大,只适合存量数据检测,无法做到实时检测;贾志伟等人^[8]利用K最邻近(K-nearest neighbor, KNN)算法对标记数据进行初始种子聚类,并用其辅助无标记数据进行聚类,从而对无标记数据的数据类别进行判断,实现入侵检测的功能,但是这项研究检测准确度不足,且更多的是基于互联网平台的数据研究,并没有在工业控制系统上加以验证。

因此本文结合典型工业系统模型,对工艺流程攻击与威胁情况进行建模分析,结合现有研究基础,提出在系统的生产控制回路建立稳定性模型,

并利用BC-1stM无确定度逆向云算法实现在时间序列上的入侵检测与在控制模型回路上的攻击点检测,提升了工艺流程攻击检测的时效性与空间有效性。

3 工业控制系统模型分析与攻击建模

3.1 工业控制系统模型分析

工业控制系统的各项回路中包含各类控制器、具体执行控制操作的执行器、负责生产过程中数据采集的传感器以及负责数据传输的总线网络或局域网等。因控制系统的外界变量很多,所以可以使用控制原理建模方法简化得出控制过程模型,具体生产控制回路的简化模型为:

$$x(t+1) = Ax(t) + B\eta(t) \quad (1)$$

$$y(t) = \lambda x(t) \quad (2)$$

其中, $x(t) = x_m(t) \in R^n (m \in [0, n])$ 是生产回路控制状态参数, $\eta(t) = \eta_p(t) \in R^n$ 是输入的控制变量,

$A \in R^{n \times n}$ 是状态矩阵, $B \in R^{n \times p}$ 是输入矩阵。

$y(t) = y_k(t) \in R^n (k \in [0, n])$ 为系统中传感器测量值, $\lambda \in R^{k \times n}$ 为输出矩阵。其中3个矩阵 A 、 B 、 λ 均表示系统的相关信息。该模型为控制系统忽略外界噪声的简化模型,相关因素将在后文中分析。

3.2 生产工艺攻击建模

基于生产工艺攻击的方式有很多种,而其根本方式都是在控制闭环中加入攻击变量实现控制闭环的崩溃与破坏。本文主要关注的是关于虚假控制信息的注入型攻击。生产控制回路攻击示意如图1所示。

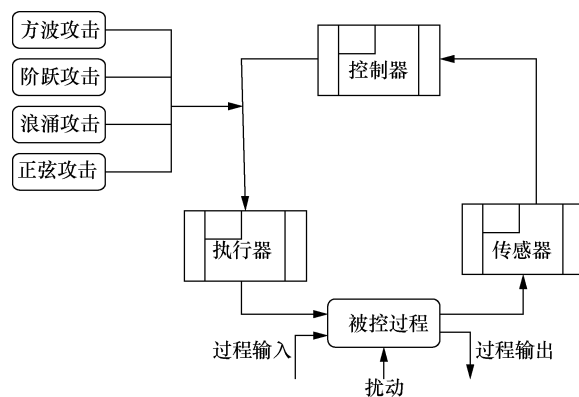


图1 生产控制回路攻击示意

图1主要描述了完整的工业控制系统模型的运行情况。在控制器和执行器中加入虚假控制信息注入型攻击从而破坏数据完整性与控制回路的稳定

性，函数表达式为：

$$x(t+1) = Ax(t) + B\eta(t) + \Delta_{\text{attack}} \quad (3)$$

可以看到，工艺攻击模型是在正常而稳定的工艺状态下，通过增加偏差量 Δ_{attack} 实现控制状态的改变。此处，笔者参照之前的研究，针对以下工艺控制类型攻击进行分析。

(1) 浪涌攻击

$$\tilde{y}_i(t) = \begin{cases} y_i(t), t \neq t_a \\ y_i(t_a) + C_{\max}, t = t_a \end{cases} \quad (4)$$

其中， t_a 为设定的周期值， $C_{\max}$ 为浪涌偏差量。

(2) 阶跃攻击

$$\tilde{y}_i(t) = \begin{cases} y_i(t), t \notin T_{\text{act}} \\ y_i(t) + c_i, t \in T_{\text{act}} \end{cases} \quad (5)$$

其中， T_{act} 为阶跃时间范围变量， c_i 为阶跃偏差量。

(3) 几何攻击

$$\tilde{y}_i(t) = \begin{cases} y_i(t), t \notin T_{\text{act}} \\ y_i(t) + \alpha_i \phi(t), t \in T_{\text{act}} \end{cases} \quad (6)$$

其中， T_{act} 为几何攻击时间范围变量， $\alpha_i \phi(t)$ 为几何方程。

基于现有的各项研究与定义，本文提出利用改进后云模型中 BC-1stM 无确定度逆向云算法对所有维度的特征进行正常工艺状态建模，并通过该算法实现实时攻击检测。

4 云模型算法

云模型拥有对不确定性内容进行表达和处理的能力，它建立了一种定量数据与定性概念双向转变的认知模型^[9]。其构造出期望 Ex、熵值 En 以及超熵值 He 这 3 个参数，通过相互融合，实现对定量数据到定性概念的转化，并定义为云滴。其中，期望 Ex 是每个变量在空间分布中的数学期望，即该变量的标定点；熵值 En 代表变量的不确定性度量范围，即该变量不确定性的量化描述方式；超熵值 He 则是变量与定性概念离散程度的表达方式，即其偏离期望的分布情况。

4.1 BC-1stM 无确定度逆向云算法

传统的逆向云发生器算法^[10]从给定数量的云滴中，还原出数域空间下的 3 个数学特征

(Ex, En, He)，以实现从定量数据到定性概念的转变。但是在计算参数时，计算参数确定度 μ_i 所需要的 En、He 这 2 个参数的最佳值难以选择，并且在高维扩展十分困难。

因此引入 BC-1stM 无确定度逆向云算法^[11]，通过对样本的分析，利用统计学的方法对数据样本进行参数估计，从而将一定数量的精确数据转化为以数字特征 (Ex, En, He) 表示的定性概念。仅利用云滴 x_i 的定量值还原出 m 维无确定度逆向云算法的期望、熵值和超熵值。

输入 N 个云滴 x_i ，计算该组数据的样本平均值 $\bar{x}$ 、 m 维样本绝对中心距 X^* 、 m 维样本方差 S^2 与 X 的期望 $E\hat{x}$ 。

$$\begin{aligned} \bar{x} &= \frac{1}{N} \sum_{a=1}^N x_a \\ X^* &= \frac{1}{N} \sum_{a=1}^N |x_a - \bar{x}| \\ S^2 &= \frac{1}{N-1} \sum_{a=1}^N (x_a - \bar{x})^2 \\ E\hat{x} &= \bar{x} = \frac{1}{N} \sum_{a=1}^N x_a \end{aligned} \quad (7)$$

X 的概率密度函数为：

$$f(x) = \int_{-\infty}^{+\infty} f_{X,Y}(x, y) dy = \frac{1}{2\pi\text{He}} \int_{-\infty}^{+\infty} \frac{1}{y} e^{-\frac{(x-\text{Ex})^2}{2y^2} - \frac{(y-\text{En})^2}{2\text{He}^2}} dy \quad (8)$$

根据 X 的概率密度函数求得 X 的一阶绝对中心矩为：

$$E|X - \text{Ex}| = \int_{-\infty}^{+\infty} |X - \text{Ex}| f(x) dx = \sqrt{\frac{2}{\pi}} \text{En} \quad (9)$$

则根据逆向云发生器定义，且设样本数为 N 时，通过期望 $E\hat{x}_b$ 可以得到 X 的熵 $E\hat{n}_b$ 。

$$E\hat{n}_b = \sqrt{\frac{2}{\pi}} \times \frac{1}{N} \sum_{b=1}^N |x_{ab} - E\hat{x}_b|, b=1, 2, \dots, N \quad (10)$$

最后根据 X 的熵 $E\hat{n}_b$ 和样本方差可求得 X 的超熵 $H\hat{e}_b$ 。

$$\begin{aligned} H\hat{e}_b &= \sqrt{\frac{1}{N-1} \sum_{b=1}^N (x_{ab} - E\hat{x}_b)^2 - E\hat{n}_b^2} \\ (b=1, 2, \dots, N) \end{aligned} \quad (11)$$

4.2 对 BC-1stM 无确定逆向云算法的优化

BC-1stM 算法可以在无须参数确定的情况下实现云滴的计算，但在实际计算过程中，由于样本的

参数估计会导致相应的计算误差,即在通过云滴的样本计算超熵时,并不能保证方差绝对值大于熵的绝对值,即需要满足 $S^2 - E\hat{n}_b^2 \geq 0$ 。此时差值若小于零,计算出的超熵值会为虚数,没有实际意义。

在现有研究中,一般对此情况有2种处理方式:一种是对方差绝对值小于熵绝对值的样本量直接采取丢弃处理;另一种是对计算结果进行二次与四次方处理,提高维度,避免出现该种情况。但是,这2种算法都有其局限性:对于直接采取丢弃处理的方法,若该数据组出现较多抛弃状况,则计算的准确度和可信度就有比较明显的下降;若采取二次方或者四次方处理的方式,那么会明显提高运算量,影响计算效率。

因此,本文利用 BC-1stM 无确定度逆向云算法只是计算超熵偏差量的绝对值,以此进行正常工艺模型波动范围系数的计算,判断异常攻击状态下系统模型波动量的放大值。根据熵与超熵的定义,熵是代表定性概念的不确定性度量,是由概念的随机性和模糊性共同决定的,而逆向云的超熵值是从定量数据向定性概念的转换,超熵值的大小由熵和期望的混乱度确定。计算包含熵小于期望与熵大于期望2种情况,而得到的超熵只表达了偏离的混乱程度,则可以暂定 $H\hat{e}_b$ 取数值绝对值,确保超熵定义的有效性。

$$H\hat{e}_b = \sqrt{|S^2 - E\hat{n}_b^2|} \quad (12)$$

5 云模型方法的工控安全模型

对于工业控制系统的工业领域模型来说,其安全防护手段除了传统的网络报文行为特征解析与防护之外,还需要对越来越多的潜伏到系统当中的、扰乱与破坏整个工艺流程的攻击进行有针对性的防护。因此,本文利用逆向云算法的思想,对拥有众多传感器的高维系统进行定性概念转化,训练出定性系统的稳定模型。

对于控制系统中的各项扰动信息来说,因逆向云模型算法是基于传感器、控制器等采集到的数据进行驱动的,其各项相关的数据仅包含数据的样本平均值、 m 维样本绝对中心距、 m 维样本方差与 X 的期望,得到的超熵 $H\hat{e}_b$ 也通过正常状态下训练集的训练 $H\hat{e}_{\text{train}} - H\hat{e}_{\text{test}}$,使扰动对安全检测不造成影响。

再对从系统实时采集的数据进行模型告警能

力的有效性验证,量化其验证效果与各项性能指标问题。工艺建模与攻击防护方法构建如图2所示。

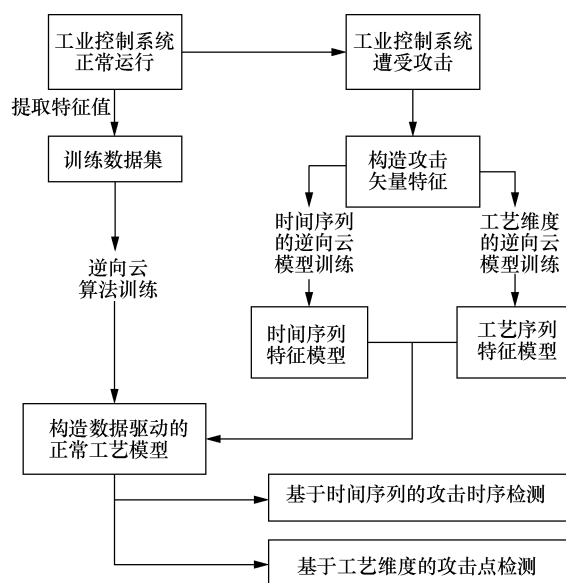


图2 工艺建模与攻击防护方法构建

6 实验结果与分析

6.1 实验验证平台介绍

本文采用工业控制界比较成熟的田纳西伊士曼(Tennessee Eastman, TE)化工过程仿真模拟进行有效性验证。其是由 Downs J J 和 Vogel E F^[12]两位工程师提出的,系统整体均为不可逆的放热反应,其反应速率与温度之间呈函数相关性,与反应浓度呈线性相关。

整个反应过程中包含5个操作单元14个操作变量,5个操作单元分别是反应器、产品冷凝器、气液分离器、循环压缩机以及汽提塔。

6.2 攻击策略

本次攻击测试并不直接通过控制指令改变操纵变量,而是从过程反应的工艺上出发,对反应器、分离器等控制值进行攻击,如通过进行有规律的逆工艺化的虚假控制信息注入攻击,验证该算法时间序列的检测效果及检测的时延,并进行空间序列上攻击维度的检测效果验证。

因此笔者对 TE 平台模型的反应器压力(reactor pressure)、反应器温度(reactor temperature)和分离器温度(separator temperature)进行4种常见的虚假控制信息的注入型攻击:正弦攻击、方波攻击、阶跃攻击与浪涌攻击。具体的攻击参数见表1。

表 1

4 种注入型攻击的参数

攻击参数	正弦攻击	方波攻击	阶跃攻击	浪涌攻击
攻击参数 1	频率 0.2 rad/s	周期 30 s	初始值 0 Pa	阶跃值 200 Pa
攻击参数 2	振幅±75 Pa	振幅±100 Pa	峰值 1 000 Pa	阶跃值 250 Pa
攻击参数 3	偏移度 0	脉冲比 50%	起始时间 60 s	阶跃值 300 Pa
攻击参数 4	相位 20 rad	起始时间 20 s	采样时间 70 s	间隔时间 20 s

6.3 模型训练与攻击检测结果分析

本文采取的 TE 过程验证主要分为无攻击的工艺稳定性建模与方波攻击、正弦攻击、阶跃攻击、浪涌攻击 4 种攻击方式的检测。对于工艺稳定性模型，笔者采用了仿真 12 800 个采样点的方式，按照时间维度和工艺维度 2 个方向进行训练。

首先对于时间维度来说，笔者先对每个维度的数据计算期望值，并以同一时间采集的数据为一组，在计算出期望与采集数据的偏差后计算出该时间下的熵值和超熵值。笔者按照时间维度进行了一万多次训练，组合形成了正常状态模型，并根据最大值群的平均 $Average(x_{\max 1}, x_{\max 2}, x_{\max 3})$ 的规则设定阈值。

其次进行工艺维度的工艺稳定性建模，按照每个维度的期望与采集值的偏差进行熵值和超熵值的计算，得到该维度正常状态下的偏移量值。

最后把攻击数据按照时间维度和工艺维度 2 个方向进行训练：期望仍然采取正常状态下的数值，对攻击过程运行的数据进行计算，在得到熵值和超熵值后，形成整个模型检测图，从而验证算法的有效性。

笔者把 54 维变量放入逆向云算法中进行正常模型训练，并针对反应器压力执行攻击检测，具体攻击检测效果如图 3~图 7 所示。

在训练过程中，时间序列的攻击阈值是按照 $Average(x_{\max 1}, x_{\max 2}, x_{\max 3})$ 规则选取的，且当攻击检测过程中出现连续 3 次以上的超阈值状态时判定为攻击，以此来避免控制周期初始收敛状态的误报攻击。而对于工艺维度的阈值训练来说，以该维度所有时间点的偏差值作为训练集，取偏差值最大的维度为阈值。对不同的攻击形式设置了不同的攻击次数进行验证，通过图 3~图 7 可以看到每种攻击的次数均可以被准确识别，因此笔者判断，对于整个攻击流程来说，其检测的准确

率是 100%，数据维度上的查准率是 99.98%，即一般在攻击检测运行伊始有 1~2 个点的误报情况发生。

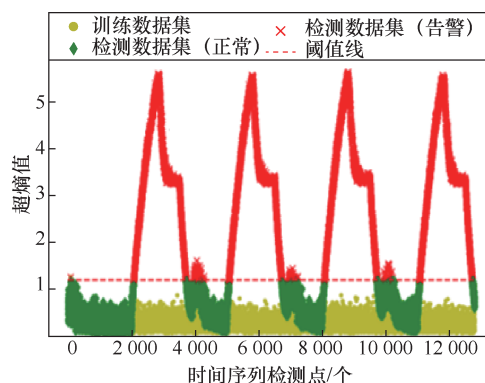


图 3 反应器压力方波攻击时间序列攻击检测效果

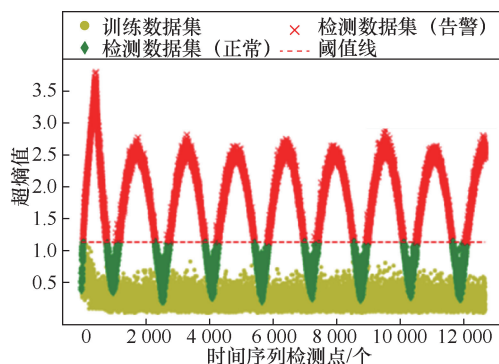


图 4 反应器压力正弦攻击时间序列攻击检测效果

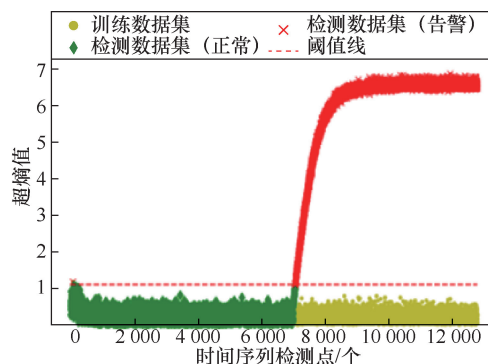


图 5 反应器压力阶跃攻击时间序列攻击检测效果

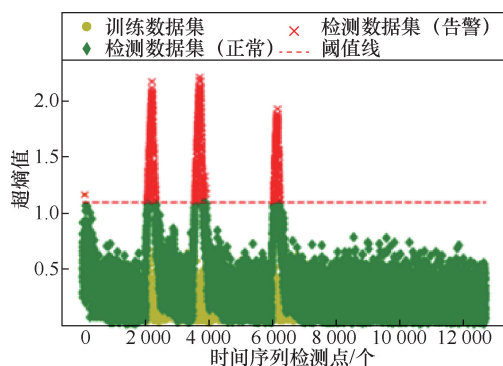


图6 反应器压力浪涌攻击时间序列攻击检测效果

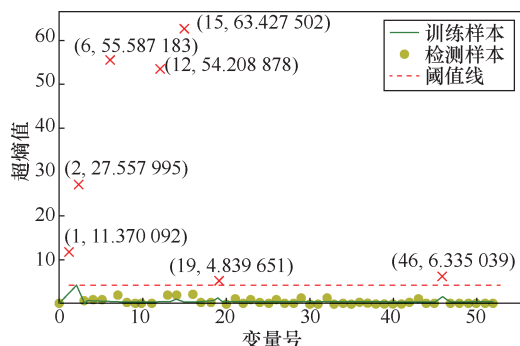


图7 反应器压力浪涌攻击下工艺维度序列攻击点散点图示意

由图3~图7可以看出,在128 s时间序列上的攻击检测当中,每种攻击检测都能很好地反映攻击,并且能够根据该攻击发生的强度进行攻击图谱的绘制。在该时间点的超熵值突破了工艺稳定建模的超熵值之后,该攻击检测模型才会把此时间判定为“告警”。时间序列上攻击检测时延见表2。

表2 时间序列上攻击检测时延

攻击类型	平均时延/ms	最大时延/ms
正弦攻击	810	1 280
方波攻击	511	645
阶跃攻击	553	553
浪涌攻击	773	822

对于超过标定阈值的变量维度,基本上在变量号为1、2、6、12、15和46的这6个维度产生。且根据偏差量的差距可以判断出攻击点所在的位置。表3为特征工艺点参数。

由图7可以看出,除了基础的E物料流量发生较大偏差外,反应器、产品分离器和汽提塔的压力都出现了与工艺相关的超熵值扩大,且真正的攻击点反应器压力的偏差值仅次于汽提塔的工艺连锁反应偏差值,可以有效地检测出攻击点可能的范围。

但是工艺维度检测效果仍有优化的空间,使真正攻击点的偏差值最为明显。

表3 特征工艺点参数

变量号	变量名	变量标准值	单位
1	D 物料流量	3 664.0	kg/h
2	E 物料流量	4 509.3	kg/h
6	反应器压力	2 705.0	KPa
12	分离器压力	2 663.7	KPa
15	汽提塔压力	3 102.2	KPa
46	放空阀操作量	40.064%	—

同理,笔者把攻击点换成TE平台模型的反应器温度,依然采取相同的4种工艺攻击手段,可以得到每种攻击时间序列攻击检测效果与工艺维度攻击点散点图,如图8~图12所示。

可以看出,相较于针对“反应器压力”的检测,“反应器温度”的检测效果略逊一筹,区分度没有“反应器压力”检测明显。其中2变量即E物料流量的变化偏差量有很明显的升高,并通过工艺模型的特性中“反应器温度升高物料阀门开度更大”的反应特点,可以判断出操作单元通过反应器温度攻击手段导致的物料阀门偏差过大。

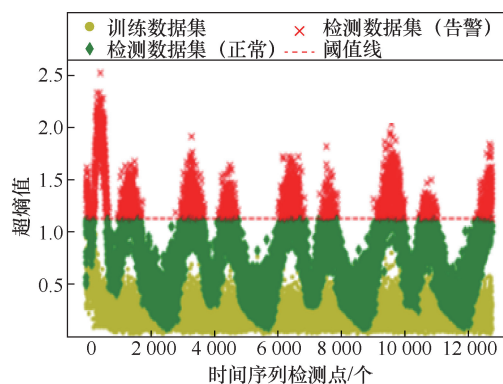


图8 反应器温度正弦攻击时间序列攻击检测效果

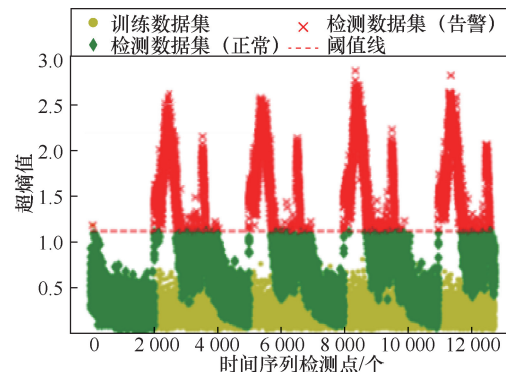


图9 反应器温度方波攻击时间序列攻击检测效果

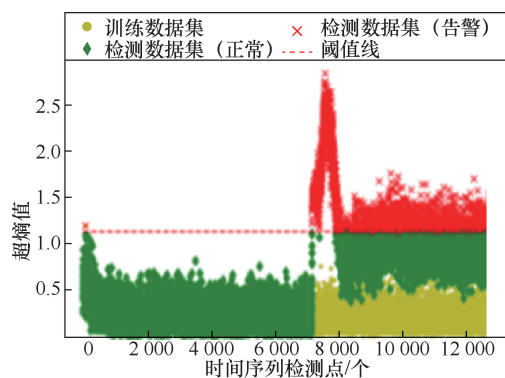


图10 反应器温度阶跃攻击时间序列攻击检测效果

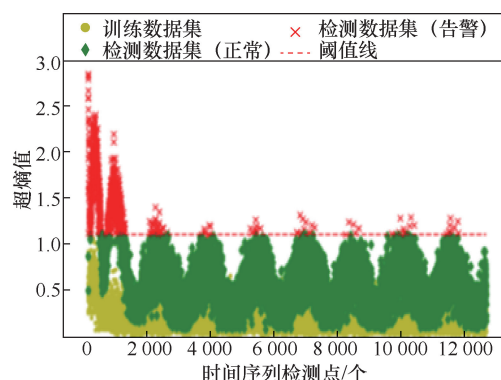


图13 分离器温度正弦攻击时间序列攻击检测效果

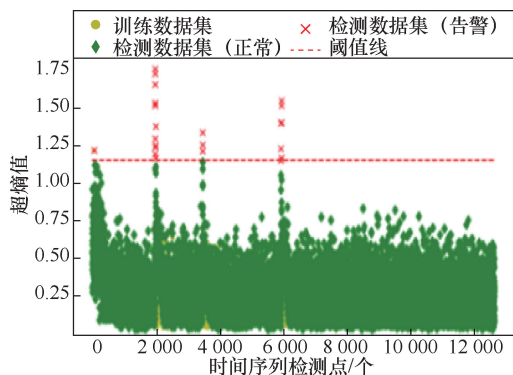


图11 反应器温度浪涌攻击时间序列攻击检测效果

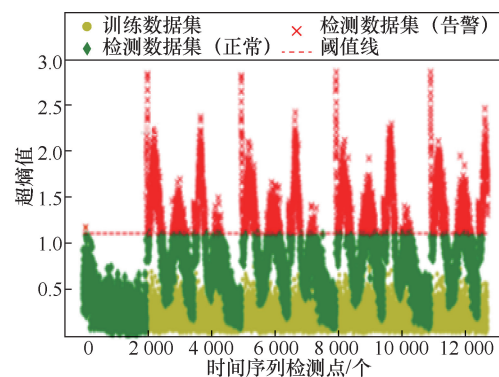


图14 分离器温度方波攻击时间序列攻击检测效果

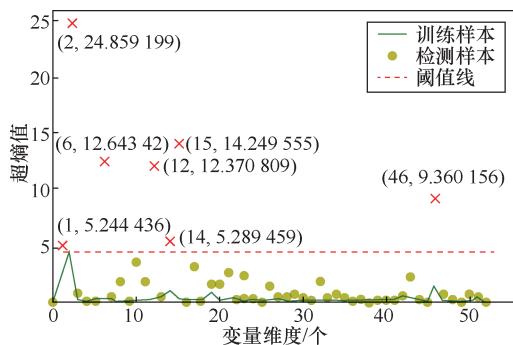


图12 反应器温度攻击下工艺维度序列攻击点散点图

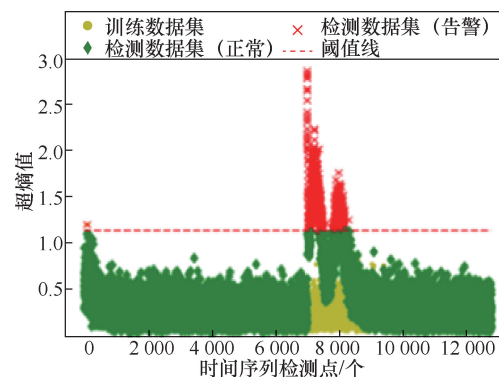


图15 分离器温度阶跃攻击时间序列攻击检测效果

其在时间序列上攻击检测的整体图谱模型与攻击模型有明显的时延，因为该检测时延主要与攻击方式本身相关度较高，如浪涌攻击持续时间很短且添加的恶意值幅值很大，则算法可以在短时间内检测出攻击行为；几何攻击为添加一个小偏差量，不断增大幅值，则在对系统影响较小的情况下算法无法检测出攻击，只有当攻击对系统造成一定影响后才检测出攻击行为。

同样，笔者把攻击点换成 TE 平台模型的分离器温度，依然采取 4 种攻击，可以得到每种攻击时间序列攻击检测效果与工艺维度攻击点散点图，如图 13~图 17 所示。

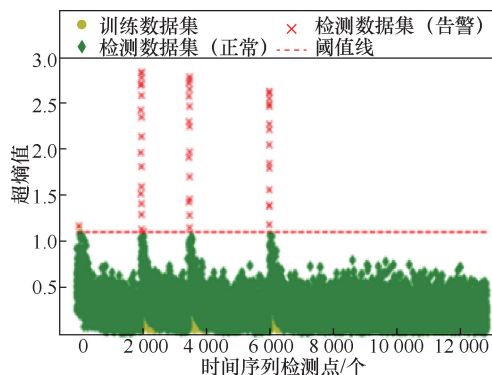


图16 分离器温度浪涌攻击时间序列攻击检测效果

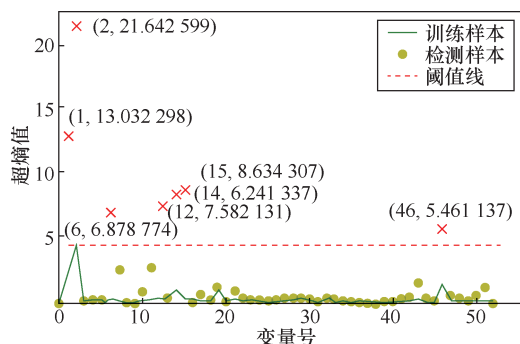


图 17 分离器温度攻击下工艺维度序列攻击点散点图

可以看到其时间序列的检测性能和准确度与工艺序列的维度与“反应器温度”检测效果相似。其工艺点检测中很明显 1、2 变量即 D 物料流量和 E 物料流量的变化偏差量有很明显的升高，并通过工艺模型的特性中“分离器温度升高反应速率加快，则反应器整体浓度增大，物料阀门开度更大”的反应特点，可以判断出操作单元可能因分离器温度攻击导致物料阀门偏差过大。但是相比反应器，分离器对控制循环的关联性影响更小，工艺超熵量偏差普遍变小，其时间序列维度的检测时延会更加明显。

6.4 模型性能与特点评价

与其他关于攻击防护与入侵检测方式相比，基于 BC-1stM 无确定度逆向云算法首先无须定义正常状态的各项参数，只需要在系统重启与保证正常的状态下，把检测到的数据传入 BC-1stM 无确定度逆向云算法中就能够确定正常状态的运行模型，以此为检测基准进行攻击检测能够更加真实地反映出该系统的特性，与其他需要设定训练参数、确定工艺场景的检测机制相比，该方法能够降低检测场的局限性，使其适用范围更加广泛。

同时，基于 BC-1stM 无确定度逆向云算法在执行攻击防护时的算法复杂度较低，运算量较小。在和其他攻击检测方法检测精度基本相同的情况下^[7-8]，其运算量有明显的降低，能够明显提高检测效率，满足工业控制网络对于低时延的要求。

由以上反应器压力、反应器温度以及分离器温度 3 个工艺流程点，通过 4 种不同的攻击，对攻击检测效果进行分析后，可以看到基于逆向云算法的工业控制系统工艺稳定性建模的检测有效性和准确性较高，但是在时间维度上，检测告警的时间点相比攻击的时间点有明显的时延，分析得到该模型是由采集的数据构建的，则当攻击发生时因不同攻

击手段对控制系统造成破坏效果的时延不同，其会出现检测延后的情况。之后可从降低检测时延的角度进行进一步的研究。

7 结束语

本文将无确定度逆向云算法模型与时间序列和工艺维度序列结合进行训练与分析，提出了改进型 BC-1stM 无确定度逆向云算法，实现工业控制领域中的工艺稳定性建模与攻击防护。该方法利用了云模型从定量数据到定性概念转化的特性，完成正常工艺状态的稳定性建模，并且利用模型特性检测入侵行为，当攻击对控制系统稳定性造成危害时能够及时发现并做出预警，与此同时能够通过攻击点相关变量的熵值变化对攻击点进行定位。通过对 TE 工业模型平台的 4 种不同虚假控制信息注入的攻击方式进行验证，证明该方法能够在有限的时延下有效地实现工业控制系统针对工艺流程相关的攻击防护检测，为工控系统安全防护策略提供有效的扩充。

参考文献:

- [1] 梁耀, 冯冬芹, 徐珊珊, 等. 加密传输在工控系统安全中的可行性研究[J]. 自动化学报, 2018, 44(3): 434-442.
LIANG Y, FENG D Q, XU S S, et al. Feasibility analysis of encrypted transmission on security of industrial control systems[J]. Acta Automatica Sinica, 2018, 44(3): 434-442.
- [2] BABU B, IJYAS T, MUNEER P, et al. Security issues in SCADA based industrial control systems[C]// International Conference on Anti-cyber Crimes. Piscataway: IEEE Press, 2017.
- [3] 陆耿虹, 冯冬芹. 基于粒子滤波的工业控制网络态势感知建模[J]. 自动化学报, 2018, 44(8): 1405-1412.
LU G H, FENG D Q. Modeling of industrial control network situation awareness with particle filtering[J]. Acta Automatica Sinica, 2018, 44(8): 1405-1412.
- [4] 李俊, 郭娟, 孙军. 基于扩展 Kalman 滤波的工业控制系统 DDoS 攻击检测[J]. 电子技术应用, 2016, 42(4): 73-77.
LI J, GUO X, SUN J. The detection of DDoS attack for industrial control systems based on extended Kalman filtering [J]. Application of Electronic Technique, 2016, 42(4): 73-77.
- [5] 杨伟, 何杰, 万亚东, 等. 基于 IEEE802.15.4e 标准的工业物联网安全时间同步策略[J]. 计算机研究与发展, 2017, 54(9): 2032-2043.
YANG W, HE J, WAN Y D, et al. Security countermeasures for time synchronization in IEEE802. 15. 4e-based industrial IoT[J]. Journal of Computer Research and Development, 2017, 54(9): 2032-2043.
- [6] 李绍晖, 刘纪伟. 一种面向工业控制系统的改进 CUSUM 入侵检测方法[J]. 电子技术应用, 2015, 41(9): 118-121.
LI S H, LIU J W. An improved CUSUM algorithm in intrusion detection for industry control systems[J]. Application of Electronic Technique, 2015, 41(9): 118-121.

- [7] 王华忠, 杨智慧, 颜秉勇, 等. 融合 PCA 和 PSO-SVM 方法在工控入侵检测中的应用[J]. 科技通报, 2017, 33(1): 80-85.
WANG H Z, YANG Z H, YAN B Y, et al. Application of fusion PCA and PSO-SVM method in industrial control intrusion detection[J]. Bulletin of Science and Technology, 2017, 33(1): 80-85.
- [8] 贾志伟, 关忠仁, 赵建芳. 一种基于半监督学习的入侵检测算法[J]. 成都信息工程学院学报, 2012, 27(6): 560-563.
JIA Z W, GUAN Z R, ZHAO J F. Intrusion detection algorithm based on semi-supervised learning[J]. Journal of Chengdu University of Information Technology, 2012, 27(6): 560-563.
- [9] 李金武. 基于云模型主机安全评估方法[J]. 洛阳师范学院学报, 2017, 36(2): 59-63.
LI J W. An assessment method of host security based on cloud model[J]. Journal of Luoyang Normal University, 2017, 36(2): 59-63.
- [10] 王辉, 秦术, 刘少英, 等. 曲线拟合的逆向云改进算法[J]. 智能系统学报, 2014, 9(5): 590-594.
WANG H, QIN S, LIU S Y, et al. An improved algorithm of backward cloud based on curve fitting[J]. CAAI Transactions on Intelligent Systems, 2014, 9(5): 590-594.
- [11] 刘常昱, 冯芒, 戴晓军, 等. 基于云 X 信息的逆向云新算法[J]. 系统仿真学报, 2004, 16(11): 2417-2420.
LIU C Y, FENG M, DAI X J, et al. A new algorithm of backward

cloud[J]. Journal of System Simulation, 2004, 16(11): 2417-2420.

- [12] DOWNS J J, VOGEL E F. A plant-wide industrial process control problem[J]. Computers and Chemical Engineering, 1993, 17: 245-255.

[作者简介]



蔺俊豪(1994-), 男, 浙江大学控制科学与工程学院硕士生, 主要研究方向为工业控制系统、网络安全与深度学习等。



冯冬芹(1968-), 男, 浙江大学控制科学与工程学院教授、博士生导师, 主要研究方向为工业装备自主安全总线标准与芯片设计以及工控系统网络安全建模、评估和防护。