基于多目标决策的工控系统设备安全评估方法研究

贾驰千 [1] 冯冬芹 [1]

摘 要 目前的工业控制系统 (Industrial control systems, ICS) 安全评估方法中, 往往利用专家经验对系统设备受攻击的可能性进行赋值, 主观性较强. 针对这个问题, 本文提出了一种系统设备受攻击可能性的量化计算方法. 工控系统设备受攻击的可能性与两个因素有关, 该设备受攻击后, 造成系统损害的严重程度与异常检测算法发现异常的时间长短. 因此, 通过对工控系统中的各个设备发动相同攻击, 记录各个设备受攻击后系统敏感指标的变化情况与异常检测算法发现异常的时间, 将敏感指标变化情况与发现异常时间作为量化指标, 提出基于多目标决策的量化计算方法, 计算出各个设备受攻击的可能性. 本文以田纳西 – 伊斯曼过程 (Tennessee-Eastman process, TEP) 为例, 验证了计算方法的可行性, 得到了设备受攻击可能性的量化计算结果.

关键词 工控系统, 多目标决策, 安全评估, 量化方法

引用格式 贾驰千, 冯冬芹. 基于多目标决策的工控系统设备安全评估方法研究. 自动化学报, 2016, **42**(5): 706−714

DOI 10.16383/j.aas.2016.c150546

Industrial Control System Devices Security Assessment with Multi-objective Decision

JIA Chi-Qian[1] FENG Dong-Qin[1]

Abstract In security assessment of industrial control systems, it is considered too subjective to evaluate the possibility of attack on industrial control systems (ICS) devices using expert experience. So a quantitative assessment is proposed for the possibility of attack on ICS devices. The weight of ICS devices depends on two factors, the severity of damage to the system and the time of anomaly detection after the devices being attacked. Thus, a record is made to keep both the variation of critical system parameters and the time when the anomaly is detected after the same attack against each device is launched in the industrial control system. This record is regarded as the quantitative parameter. Moreover, a quantitative method with multi-objective decision is proposed, meanwhile the possibility of each device′s being attacked is then obtained. At last, the Tennessee-Eastman process (TEP) is set as an example to verify the feasibility of the method, and get the quantitative result of the possibility of attack on ICS devices.

Key words Industrial control system, multi-objective, security assessment, quantitative method

Citation Jia Chi-Qian, Feng Dong-Qin. Industrial control system devices security assessment with multi-objective decision. *Acta Automatica Sinica*, 2016, **42**(5): 706−714

随着工业控制系统的信息化建设加速发展, 工业化与信息化融合达到了新的高度. 传统工业控制系统在设计、部署之初采用的是专有的软硬件设施和工业控制协议, 很少考虑到系统开放性问题. 伴随着工业控制系统日益开放, 工业控制系统正在面临越来越多的威胁. 工业控制系统安全评估可以反映工控系统的安全状态, 判断工控系统的脆弱性所在, 属于对安全威胁的主动防御, 所以工控系统安全评估已经成为工控系统安全研究的热点课题. 目前, 不断有专家与学者对工控系统安全评估进行研究, 从方法论到具体的评估方法进行了全方位的探索与尝试[1−3]. 主要有基于概率论与图论相融合的贝叶斯网络 (Bayesian network, BN). Wang 等[4] 以贝叶斯网络为模型, 对影响风险等级的各种因素采用概率方法结合专家知识进行描述. 该方法不仅可以评估网络的总体风险, 还可以分别评估各个局部要素可能引起风险的程度. 但是贝叶斯网络模型输入节点通常为工控系统设备的受攻击可能性, 赋值较为困难, 没有客观的量化标准, 一般来说通过主观量化攻击设备的破坏性来进行赋值, 然后再进行贝叶斯网络图的概率计算.

收稿日期 2015-08-31 录用日期 2015-11-17
Manuscript received August 31, 2015; accepted November 17, 2015
国家自然科学基金 (61223004), 工控网络安全研究 (2015XZZX005-03) 资助
Supported by National Natural Science Foundation of China (61223004) and Research on the Security of Industrial Control Network (2015XZZX005-03)
本文责任编委 胡昌华
Recommended by Associate Editor HU Chang-Hua
1. 浙江大学智能系统与控制研究所工业控制技术国家重点实验室 杭州 310027
1. State Key Laboratory of Industrial Control Technology, Institute of Cyber-Systems and Control, Zhejiang University, Hangzhou 310027

另一具有代表性的工控系统安全评估方法是层次分析法 (Analytic hierarchy process, AHP). 如 Bian 等[5] 从风险因素、服务因素和公共因素三方面对信息安全态势进行评估; 卢慧康等[6] 以 NIST800-82 和 IEC 62443 为依据, 对工业控制系统安全进行安全评估. 层次分析法在层次权重赋值上主观性较强, 特别是将工控系统设备受攻击的可能性转化为系统设备相对权重赋值时, 过度依赖于专家的个人知识和经验. 有不少学者将模糊综合分析法与层次分析法结合[7−8], 但是这种方法还是缺乏一定的数据分析, 依然存在较强主观性.

本文提出了一种基于敏感指标变化和异常检测时间的多目标决策的工控系统设备安全评估量化计算方法.

1) 通过主元分析方法 (Principal components analysis, PCA) 建立工控系统的主元模型, 并建立 T^2 和 SPE 统计图.

2) 通过记录、分析工控系统各设备在相同攻击输入模型作用下, 系统的主元指标 T^2 和 SPE 统计值变化情况, 得到异常检测时间.

3) 建立系统敏感指标和主元变化异常检测时间的多目标安全评估量化模型及其算法.

4) 以上述模型和算法作为决策依据, 可评估、判断出工控系统中最有可能被攻击的设备.

本文最后以 TE 过程为例, 对该方法进行验证, 结果表明, 利用系统敏感指标变化和主元变化异常检测时间的多目标决策方法, 得到的工控系统安全评估量化计算结果与实际情况相符, 证明了本方法的有效性.

1　设备安全评估原理

工控系统设备的安全评估就是对系统设备受攻击的可能性 P 的计算, 它由两方面因素决定.

1) 某个系统物理设备受到攻击 $a(k)$ 作用后, 工控系统敏感指标 s 的超限程度. 若分别攻击系统物理设备 A 和 B 后, $s_A > s_B$, 说明攻击 A 可能造成的破坏更大, 那么设备 A 受攻击的可能性 P 就越大;

2) 某个系统物理部件受到攻击 $a(k)$ 作用后, 异常检测算法检测出系统异常的时间 t. 若分别攻击系统物理部件 A 和 B 后, 异常检测算法检测异常的时间 $t_A > t_B$, 说明攻击设备 A 不易被检测算法发现, 那么设备 A 受攻击的可能性 P 就越大.

本文基于这两点考虑, 提出了工控系统设备受攻击可能性的量化计算方法. 设系统设备受攻击可能性为 P, 可用式 (1) 进行计算.

$$P = f(s,t) \tag{1}$$

其中, s 表示设备受攻击后系统敏感指标的最大值, t 表示异常检测算法检测出异常的时间.

工控系统设备受攻击的可能性 P 由 s 和 t 决定, 受攻击后, 敏感指数最大值 s 越大, 异常检测算法检测时间 t 越大, 该设备受攻击的可能性就越高. 本文提出的基于多目标决策的量化计算方法 f, 就是将 s 和 t 这两类标准统一起来, 量化计算出设备受攻击的可能性 $P = (p_1, p_2, \cdots, p_m)$, 其中 $p_{\max}$ 对应的设备就是最有可能受攻击的设备.

2　安全评估计算方法

2.1　建立攻击输入模型

攻击者发动攻击的动机主要有两类:

第一类攻击: 篡改原本正确的测量值 $z_i(k)$, 使计算单元接收到的测量值 $\tilde{z}_i(k)$ 与正常值 $z_i(k)$ 发生偏差, 诱导系统进入错误的控制, 做出不正确的响应, 从而造成损失;

第二类攻击: 攻击者攻击了系统的其他部分, 使系统处于非正常的运行模式, 同时将传感器测量值 $\tilde{z}_i(k)$ 篡改为正常情况下的数据 $z_i(k)$, 使系统无法做出正确的响应.

其手段主要有:

1) 恶意数据注入, 即攻击者在原数据上添加一个附加数据 $a(k)$;

2) 重放攻击, 针对第二类攻击动机, 攻击者采集原系统一段数据用以替换另一段运行时间内的数据.

本文引入检测算法的目的是根据攻击造成的敏感指标变化情况以及异常检测时间来对系统设备受攻击可能性进行量化, 因此, 针对第一类攻击动机进行计算.

一般性的攻击可以分为三种[9]: 浪涌攻击 (Surge attack)、偏差攻击 (Bias attack) 和几何攻击 (Geometric attack).

1) 浪涌攻击

攻击者通过篡改单个数据, 在最短的时间内达到尽可能最大程度的伤害, 如式 (2) 所示.

$$\tilde{z}_i(k) = \begin{cases} z_i(k) + a(k), & k = j \\ z_i(k), & k = 1, \cdots, N,\ \ k \neq j \end{cases} \tag{2}$$

其中, $z_i(k)$ 表示系统在 k 时刻的某个正常数值, $a(k)$ 表示 k 时刻的攻击.

2) 偏差攻击

攻击者小量地连续篡改多个数据, 即在对每个时刻的数据添加一个非零常数 c, 为了不被检测出, c 通常取值较小, 如式 (3) 所示.

$$\tilde{z}_i(k)=\begin{cases}z_i(k)+c_i, & k=j,\cdots,N\\ z_i(k), & k=1,\cdots,j-1\end{cases}\tag{3}$$

其中, $z_i(k)$ 表示系统在 k 时刻的某个正常数值, c_i 表示攻击常量.

3) 几何攻击

几何攻击可以看作是浪涌攻击和偏差攻击的结合, 攻击者一开始注入较小的偏差值, 可以在不被检测到的情况下累积攻击偏差值, 最后时刻加入尽可能大的偏差, 从而达到最大程度的破坏, 因此攻击者添加的偏差值通常为等比数列, 如式 (4) 所示.

$$\tilde{z}_i(k)=\begin{cases}z_i(k)+\alpha_i{\beta_i}^{k-j}, & k=j,\cdots,N\\ z_i(k), & k=1,\cdots,j-1\end{cases}\tag{4}$$

其中, $z_i(k)$ 表示系统在 k 时刻的某个正常数值, $\alpha_i{\beta_i}^{k-j}$ 表示几何攻击. 几何攻击结合了前两种攻击的优点, 攻击效果较好, 且较难被检测.

由于在量化评估中, 需要加大区分度, 如果一种攻击方式攻击任意设备都是很容易就检测出来的, 那就失去了该项指标的意义. 因此, 本文采用几何攻击作为攻击各个设备的攻击方法.

需要注意的是, 本文攻击建模中提到的攻击方法均属于数据篡改攻击, 而工控系统攻击方法还有许多, 如控制命令篡改等. 本文在系统设备安全评估过程中, 考虑的因素为系统设备受攻击后, 系统敏感指标与异常检测时间的变化情况, 这些因素受设备输入输出数据的变化影响. 从这一点上来说, 数据篡改、控制命令篡改等攻击的效果是一致的, 都影响设备的输入输出数据. 因此, 本文仅从数据篡改角度进行计算说明.

2.2 基于多变量统计分析的异常检测

2.2.1 主元分析法降低状态维数

主元分析是一种较为成熟的多元统计监测方法. 应用 PCA 的方法, 降低原始数据空间的维数, 从新的隐式变量中提取主要变化信息及特征. 这样既保留了原有数据信息的特征, 又消除变量间的关联, 简化分析复杂度[10].

以典型化工系统为例, 假设系统有 m 个状态变量, 有如式 (5) 所示的状态方程.

$$\dot{X}=AX+BU\tag{5}$$

由于变量数量较多, 再加上变量之间的相关性, 使得问题的分析复杂性大大提高. 因此, 可以运用主元分析方法对变量进行降维处理.

采集正常情况下系统状态向量数据 X, 经过归一化后, 分析其相关系数矩阵 R, 对相关系数矩阵的特征根 λ_i 进行从大到小排序, 将前 k 个特征根 λ 对应的状态变量取为主元变量 t_i. 利用主元向量 T 可以重构状态向量数据的估计值 $\hat{X}$, 如式 (6) 所示.

$$X=TP+E=\hat{X}+E\tag{6}$$

其中, $T=[t_1,t_2,\cdots,t_k]^{\mathrm{T}}$, $P=[p_1,p_2,\cdots,p_k]^{\mathrm{T}}$. T 代表新的主元变量组成的向量, E 代表状态向量估计值与实际值的残差, P 代表主成分系数矩阵, 即负载矩阵.

对图 1 所示化工系统中的反应炉控制系统进行攻击时, 假设对该控制系统的副回路传感器的输出值进行攻击, 加入攻击输入 $a(k)$, 就会引起化工系统中 m 个状态变量或部分相关状态变量的变化. 此时的状态估计值变为 $\hat{X}_{\mathrm{new}}$, 残差为 $E_{\mathrm{new}}=X_{\mathrm{new}}-\hat{X}_{\mathrm{new}}$.

$$\hat{X}_{\mathrm{new}}=T_{\mathrm{new}}P\tag{7}$$

$$E_{\mathrm{new}}=X_{\mathrm{new}}-\hat{X}_{\mathrm{new}}\tag{8}$$

2.2.2 建立 SPE 和 T^2 统计图

建立主元模型后, 可采用多变量控制统计图进行过程检测, SPE 图和 T^2 是最常见的多变量统计控制图[11].

T^2 图是得分向量的标准平方和, 表示每个采样在变化趋势和幅值上偏离模型的程度. T^2 表征 PCA 模型内部变化的一种测度, 定义如式 (9) 所示.

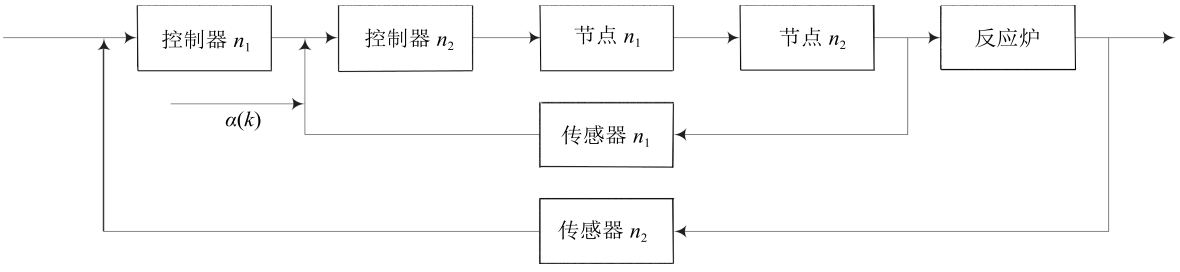


图 1 反应炉控制系统

Fig. 1 Reactor control system

$$T_i^2 = t_i \lambda^{-1} {t_i}^{\mathrm{T}} = X_i P \lambda^{-1} P^{\mathrm{T}} {X_i}^{\mathrm{T}} \tag{9}$$

其中, P 为负载矩阵, 由 PCA 建模过程中训练集协方差矩阵的前 k 个特征向量组成; λ 是由与前 k 个主元所对应的特征值所组成的对角均值.

当 $T^2 \le T_\alpha^2$ 时, 表示过程状态正常, T_α^2 表示 T^2 统计值的控制限. T_α^2 可以利用 F 分布按式 (10) 进行计算.

$$T_\alpha^2 = \frac{k(m-1)}{m-k} F_{k,m-1,\alpha} \tag{10}$$

其中, m 是样本个数, k 是所保留的主元个数, α 是检验水平, $F_{k,m-1,\alpha}$ 是对应于检验水平为 α, 自由度为 $(k, m-1)$ 条件下的 F 分布的临界值.

统计量 SPE 在 i 时刻的值是个标量, 它表示此时刻测量值 X_i 对主元模型的偏离程度, 是模型外部数据变化的一种测度. SPE 统计量也被称为 Q 统计量, 其定义如式 (11) 所示.

$$Q = E^{\mathrm{T}} E \tag{11}$$

这里 E 是残差向量.

当 $Q \le Q_\alpha$ 时, 表示过程状态正常. Q_α 表示 SPE 的控制限. Q_α 可按式 (12) ∼ (14) 进行计算.

$$Q_\alpha = \theta_1 \left[\frac{C_\alpha h_0 \sqrt{2\theta_2}}{\theta_1} + 1 + \frac{\theta_2 h_0 (h_0 - 1)}{\theta_1^2} \right]^{\frac{1}{h_0}} \tag{12}$$

$$\theta_i = \sum_{j=k+1}^{n} \lambda_j^i, \quad i = 1, 2, 3 \tag{13}$$

$$h_0 = 1 - \frac{2\theta_1 \theta_3}{3\theta_2^2} \tag{14}$$

其中, λ_i 是 X 协方差矩阵的特征值, C_α 是正态分布置信度为 α 的统计.

本文使用 PCA 作为设备受到攻击后的异常检测算法, 利用 T^2 统计值和 SPE 统计值来监测系统情况, 将统计值检测到攻击的时间作为评判攻击是否容易被检测出来的依据.

需要说明的是, 在攻击检测中, 应该对检测出的异常是属于常规设备故障造成还是属于人为攻击造成进行区分. 但是在系统安全评估中, 并不需要区分是由人为攻击造成的异常还是设备故障造成的异常, 只关注某个传感器或执行器发生故障后, 可能造成的损失大小进行评估. 即在系统安全评估中, 传感器 A 发生异常 (攻击或故障) 造成的系统损失比传感器 B 发送异常 (攻击或故障) 造成的系统损失更大, 那么, 攻击者会更倾向于攻击传感器 A.

因此, 在系统安全评估中, 无论是采用异常检测的算法或是故障检测的算法来发现异常都是可行的, 并不区分是由人为攻击造成的异常还是设备故障造成的异常, 因为只需要知道, 某个系统设备发生异常后, 对系统造成的影响和损失更大.

2.3　基于多目标决策的量化计算方法

本文统一采用几何攻击作为攻击信号, 采用敏感工艺指标的最大值情况与异常检测时间的长短作为设备重要性计算的依据. 假设设备为 x_i, 各项评判依据为 x_{ij}, 得到如表 1 所示的量化评判表.

表 1　量化评判表

Table 1　Quantitative evaluation table

设备	工艺指标 1	工艺指标 2	T^2 异常检测时间	SPE 异常检测时间
x_1	x_{11}	x_{12}	x_{13}	x_{14}
x_2	x_{21}	x_{22}	x_{23}	x_{24}
⋮	⋮	⋮	⋮	⋮
x_m	x_{m1}	x_{m2}	x_{m3}	x_{m4}

根据量化评判表的数值, 我们构造一个决策矩阵 R, 矩阵 R 内的各个元素 r_{ij} 即量化评判表内的各个值 x_{ij}. 但是, 考虑到量化评判表内的各个评价指标的数据单位不同, 意义不同, 需要对 x_{ij} 进行一定的处理.

1) 处理评价指标的意义不同的问题. 本文认为, 在受到攻击后, 敏感工艺指标达到的最大值越大, 可能造成的破坏越大, 该设备受攻击可能性越大; 异常检测时间越长, 说明攻击该设备越不易被发现, 可能造成的破坏就越大, 该设备受攻击的可能性就越大. 因此, 工艺指标和异常检测时间这两类评判依据和系统设备受攻击的可能性之间都是存在正相关的关系, 可以认为在安全评估中, 这两类指标的意义是一致的.

2) 对于评价指标的单位不同, 本文利用式 (15) 对 x_{ij} 进行归一化处理. 同时, 为了在下文计算与极大向量、极小向量的欧氏距离时方便计算、形式一致, 采用平方和的形式作为分母进行归一化处理. 归一化后, 各个设备的同一指标值的平方和为 1. 决策矩阵 R 如式 (16) 所示.

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \tag{15}$$

$$R = [r_{ij}] \tag{16}$$

由于量化评判表中有多个评价指标, 因此, 必须考虑各个评价指标对于评价结果的影响大小. 设 n 项评价标准的相对权重向量为 W, 那么, 可以构造一个加权规范化矩阵 V, 如式 (17) 和式 (18) 所示.

$$V = R \times W = \begin{bmatrix} w_1 r_{11} & w_2 r_{12} & \cdots & w_n r_{1n} \\ w_1 r_{21} & w_2 r_{22} & \cdots & w_n r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ w_1 r_{m1} & w_2 r_{m2} & \cdots & w_n r_{mn} \end{bmatrix} \tag{17}$$

$$W = \begin{bmatrix} w_1 & 0 & 0 & 0 \\ 0 & w_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & w_n \end{bmatrix} \tag{18}$$

此时, 得到的加权规范化矩阵 V 还是由各个设备的各项指标值组成, 需要将第 i 个设备的 n 项评价指标进行综合考虑, 得到第 i 个设备的一个综合评价值. 因此, 根据矩阵 V 做如下处理. 首先, 从矩阵 V 中选取 n 项指标中各项指标的最大值, 组成向量 v^*, 表示在当前情况下, 各项指标能达到的一种最具有威胁性的情况. 然后, 从矩阵 V 中选取 n 项指标中各项指标的最小值, 组成向量 v^-, 表示在当前情况下, 各项指标能达到的一种最安全的情况. 将第 i 个设备的 n 项评价值分别与最大向量 v^* 和最小向量 v^- 进行比较, 利用式 (19) 和式 (20), 得到第 i 个设备的指标向量值到最大向量 v^* 和最小向量 v^- 的欧几里得距离 S_i^* 和 S_i^-. S_i^* 越小, 表示设备 i 的评价值距离最大向量越近; S_i^- 越小, 表示设备 i 的评价值距离最小向量越近.

$$S_i^* = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^*\right)^2} \tag{19}$$

$$S_i^- = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^-\right)^2} \tag{20}$$

根据各个设备求出的指标向量值到最大向量 v^* 和最小向量 v^- 的欧几里得距离 S_i^* 和 S_i^-, 可以利用式 (21) 得到第 i 个设备与最大最小向量的相对接近度 C_i, C_i 越大, 表示设备 i 的评价值距离最小向量越远, 距离最大向量越近, 即距离最安全情况越远, 距离最具威胁性情况越近, 即受攻击后的危害越大.

$$C_i = \frac{S_i^-}{S_i^- + S_i^*}, \quad i = 1, \cdots, m, \ 0 \le C_i \le 1 \tag{21}$$

3) 根据每个设备的相对接近度 C_i, 可以根据式 (22) 计算出每个设备受攻击的可能性 p_i.

$$p_i = \frac{C_i}{\sum_{i=1}^{m} C_i} \tag{22}$$

3 实验与计算

本文以 TE 过程为例, 对 TE 过程中的反应炉控制系统的各个设备实施几何攻击, 采用 PCA 作为异常检测算法, 观察各个设备受攻击后反应炉压力与温度的变化情况以及 PCA 检测异常的时间, 量化计算出各个设备受攻击的可能性.

3.1 仿真实验平台

田纳西 – 伊斯曼过程 (Tennessee-Eastman process, TEP) 是一个现实的工业过程[12], 被广泛应用于多变量控制、最优化、自适应控制、非线性控制和故障诊断等领域. 该过程有 5 个主要单元: 反应器、冷凝器、压缩机、分离器和汽提塔; 包括了 8 种成分: A, B, C, D, E, F, G 和 H; 能够同时监测 41 个测量变量和 12 个操作变量, 满足多变量、多数据的采集. 它反映了现实中在闭环控制下运行的过程, 如图 2 所示, 这个控制结构的详细描述可以查看文献 [13−14].

由于 TEP 是根据实际化工过程进行仿真的模型, 因此, 在实际的化工过程中, 对过程指标存在约束, 包括反应炉的压力、液位、温度等指标. 具体的参数与要求见表 2[12].

表 2 过程操作限制

Table 2 Process operating constraints

过程变量	正常操作限制		停机操作限制	
	下限	上限	下限	上限
反应炉压力 (kPa)	无	2 895	无	3 000
反应炉液位 (m^3)	50 % (11.8)	100 % (21.3)	2.0	(24.0)
反应炉温度 (°C)	无	150	无	175
分离器液位 (m^3)	30 % (3.3)	100 % (9.0)	11.8	12.0
汽提塔基准液位 (m^3)	30 % (3.5)	100 % (6.6)	1.0	8.0

在本文的量化评估计算中, 需要在设备受攻击后将敏感工艺指标的变化情况作为评估标准, 根据文献 [12] 提供的 TEP 过程中的操作限制, 同时考虑到实际生产过程中最易造成破坏的工艺参数, 本文选取反应炉的压力与温度作为评估标准.

3.2 实验计算

根据选定的工艺指标, 查看与压力温度相关的控制变量. 本文选取的攻击点为各回路的传感器与控制器的输出值.

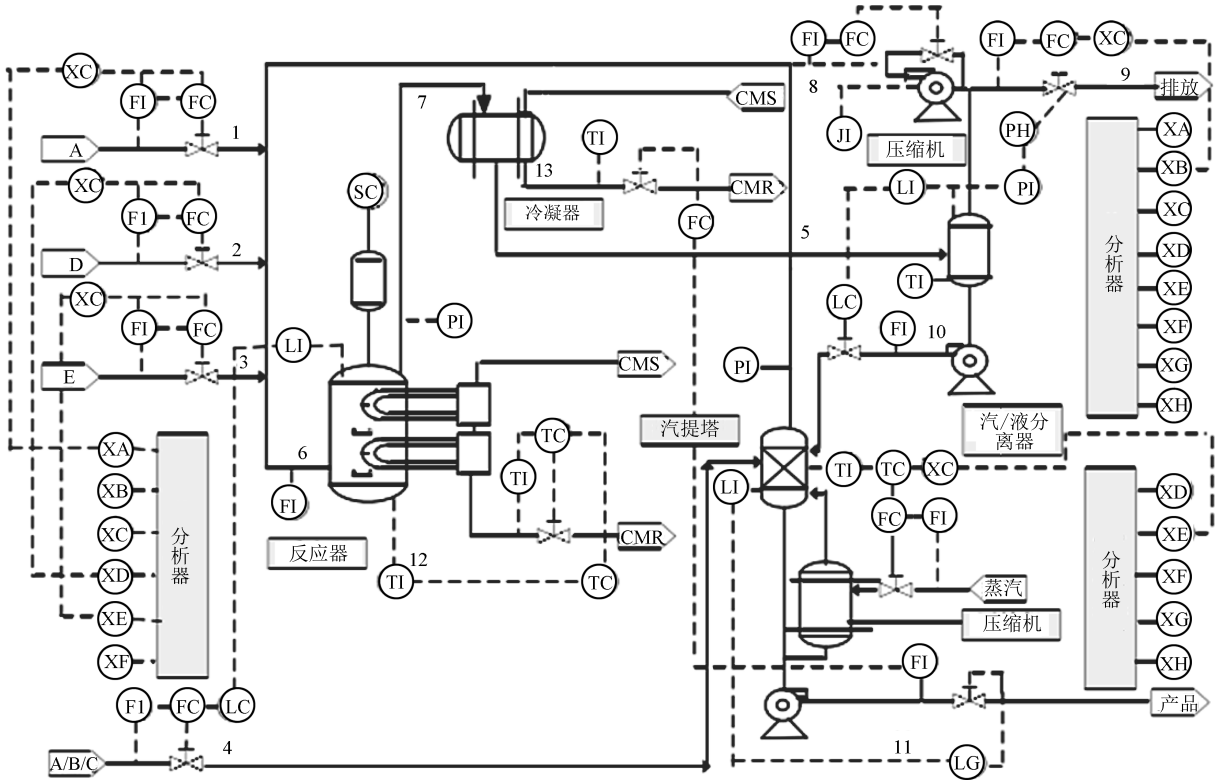


图 2　TE 过程工艺流程图

Fig. 2　Reactor control system

在 $t = 5\,\mathrm{h}$ 的时候加入附加攻击的几何攻击形式 $a(k)$, 如式 (23) 所示, 取几何攻击为指数型的攻击信号, 若为负反馈部分, 则取负指数.

$$a(k) = \begin{cases} 0, & t < 5\,\mathrm{h} \\ \pm \mathrm{e}^{t}, & t \geq 5\,\mathrm{h} \end{cases} \tag{23}$$

首先, 在没有攻击的情况下, 运行 TEP 仿真系统, 得到正常情况下的数据集, 作为 PCA 检测的训练集. 然后, 分别对压力控制系统的主回路控制器、副回路控制器、主回路传感器、副回路传感器和温度控制系统的控制器、传感器共 6 个设备进行攻击, 攻击其中一个设备时, 另外 5 个设备不受攻击. 以攻击压力控制系统副回路的传感器为例, 得到如图 3 和图 4 所示的结果. 图 3 表示反应率压力与温度的变化情况, 图 4 表示 PCA 检测的结果, 横坐标每 100 个采样点表示 1 h, 虚线为设定的控制限, 统计值超过虚线的部分表示系统异常, 受到了攻击.

根据量化评判表的内容对 6 个设备攻击下的数据进行记录. 得到如表 3 所示的实验结果. 反应炉压力控制系统的副回路控制器、传感器、主回路控制器、传感器、反应炉温度控制系统控制器、传感器分别为 A_1、A_2、A_3、A_4、A_5、A_6.

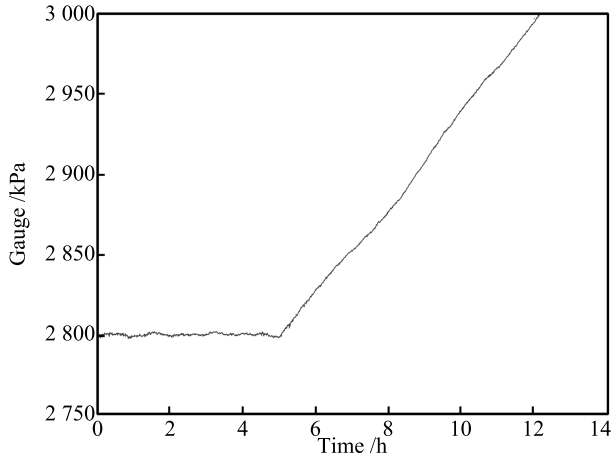
表 3 中, 压力、温度均记录最大值. 对于 T^2 统计量和 SPE 统计量, 若无法检测, 则记为 "–", 归一化后取 1; 能检测出的按检测时刻来衡量, 每 100 个采样点为 1 h. 根据权重量化计算方法中的说明, 我们根据表 3 可以得到决策矩阵 R.

$$R = \begin{bmatrix} 0.4115 & 0.3888 & 0.6079 & 0.5062 \\ 0.4115 & 0.3888 & 1.0000 & 0.4342 \\ 0.4115 & 0.3888 & 1.0000 & 0.3618 \\ 0.4115 & 0.3888 & 0.6296 & 0.4993 \\ 0.4184 & 0.4462 & 0.3126 & 0.2750 \\ 0.3841 & 0.4430 & 0.3691 & 0.3148 \end{bmatrix}$$

表 3　实验结果

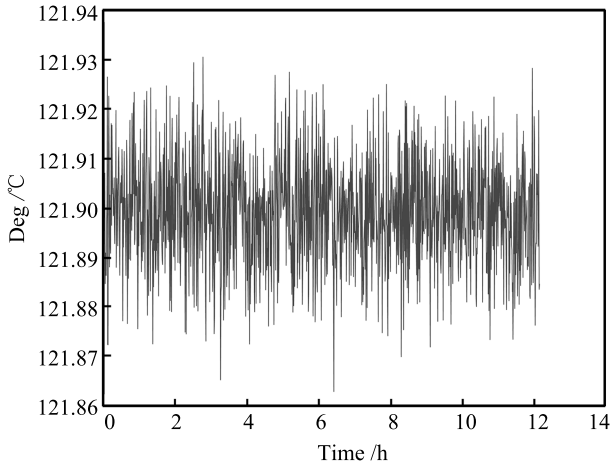
Table 3　Experiment results

设备	反应炉压力 (kPa)	反应炉温度 (°C)	检测时间 T^2 异常	检测时间 SPE 异常
A_1	3 000	122	1 400	1 400
A_2	3 000	122	–	1 200
A_3	3 000	122	–	1 000
A_4	3 000	122	1 450	1 380
A_5	3 050	140	720	760
A_6	2 800	139	850	870



(a) 反应炉压力

(a) Pressure of reactor

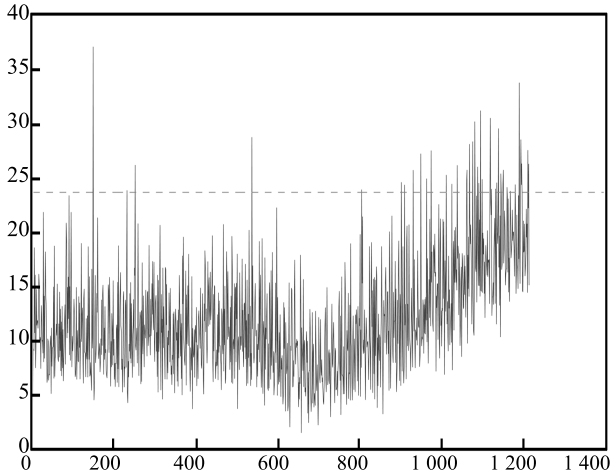


(b) 反应炉温度

(b) Temperature of reactor

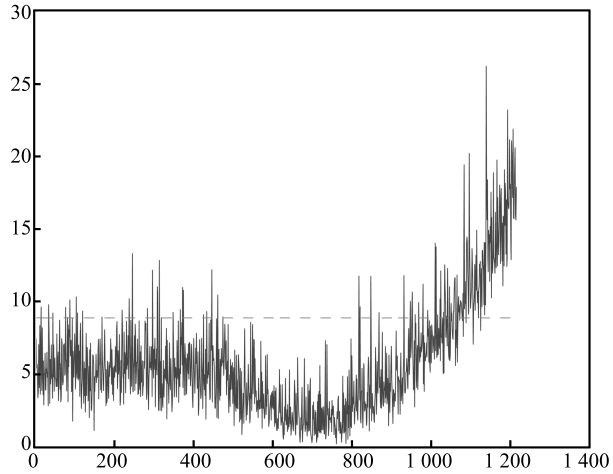
图 3 受攻击后反应炉压力温度变化

Fig. 3 Pressure and temperature condition of reactor



(a) T^2 统计值

(a) T^2 statistical value



(b) SPE 统计值

(b) SPE statistical value

图 4 SPE 和 T^2 统计值 TE 过程工艺流程图

Fig. 4 SPE and T^2 statistical value

考虑反应炉控制系统中压力、温度和异常检测时间这三者的重要性关系. 首先, 压力过大是最易引起爆炸等重大破坏的原因, 因此压力的变化情况是最重要的评判指标. 其次, 对于温度指标而言, 由于 TEP 反应炉本身没有高温条件, 整体温度并不高, 温度的变化情况并不会造成特别严重的破坏, 因此, 温度的变化情况是三者中最不重要的评判指标. 综上, 本文对三者的重要性赋值为 W.

$$W=\begin{bmatrix} 0.4 & 0 & 0 & 0 \\ 0 & 0.1 & 0 & 0 \\ 0 & 0 & 0.25 & 0 \\ 0 & 0 & 0 & 0.25 \end{bmatrix}$$

根据式 (12) 可以得到加权规范化矩阵 V 为

$$V=\begin{bmatrix} 0.1646 & 0.0389 & 0.1520 & 0.1266 \\ 0.1646 & 0.0389 & 0.2500 & 0.1086 \\ 0.1646 & 0.0389 & 0.2500 & 0.0905 \\ 0.1646 & 0.0389 & 0.1574 & 0.1248 \\ 0.1674 & 0.0446 & 0.0782 & 0.0688 \\ 0.1536 & 0.0443 & 0.0923 & 0.0787 \end{bmatrix}$$

从矩阵 V 中选取各项指标最大值组成 v^*, 选取各项指标最小值组成 v^-.

$$v^*=(0.1674, 0.0446, 0.25, 0.1266)$$

$$v^-=(0.1536, 0.0389, 0.0782, 0.0688)$$

根据式 (19) 和式 (20) , 我们可以计算出各个设备到最大向量和最小向量的欧几里得距离 s_i^* 和 s_i^-. 可以由向量 S^* 和 S_i^- 表示.

$$S^* = (0.0982, 0.0191, 0.0367, 0.0928, 0.1813, 0.1654)^{\mathrm{T}}$$

$$S^- = (0.0944, 0.1767, 0.1735, 0.0976, 0.0149, 0.0180)^{\mathrm{T}}$$

根据式 (21), 可以计算出各个设备与最大最小向量的相对接近度, 可以由向量 C 表示.

$$C = (0.4900, 0.9023, 0.8254, 0.5126, 0.0759, 0.0983)^{\mathrm{T}}$$

最后, 利用式 (22) 可以计算出各个设备受攻击的可能性 P.

$$P = (0.1687, 0.3106, 0.2842, 0.1765, 0.0261, 0.0338)^{\mathrm{T}}$$

3.3 实验结果分析

从各个设备受攻击的可能性 P 来看, 压力控制系统副回路的传感器与主回路的控制器在 6 个设备中受攻击的可能性较高, 而温度控制系统的传感器与控制器在 6 个设备中受攻击的可能性较低.

结合实际的 TEP 系统来看, 由于反应炉压力控制系统采用的是串级控制, 因此, 副回路在受到攻击后, 参数的变化不易被检测出来, 因此, 它在实际的控制系统中, 受攻击的可能性较大. 其次, 由于 TEP 系统的反应炉不是高温条件, 因此温度的变化对反应炉并不会造成太大的破坏. 因此, 温度控制系统的传感器和控制器在控制系统中受攻击的可能性较低. 这都说明了本文提出的设备受攻击可能性的量化计算方法是符合实际情况的, 并能得到一个相对客观的量化计算结果.

最后, 从实验的结果与计算结果来看, 如果在本文的量化计算方法中, 采用不同的攻击方法、不同的异常检测算法, 并应用于不同控制策略的控制系统中, 那么它的结果都将大不相同. 而这也正是符合实际情况的. 在判断工控系统设备受攻击可能性的时候, 必须要结合实际的控制系统, 考虑控制系统的工艺情况与控制策略, 在不同工艺情况与控制策略下, 相同的设备受攻击的可能性是完全不同的.

4 总结与展望

本文对系统设备受攻击的可能性进行了量化分析、计算, 利用系统设备受攻击后引起的工控系统敏感参数变化情况和异常检测算法检测异常的时间这两类指标, 提出了一种基于多目标决策的量化计算方法. 最后, 利用 TE 过程, 对该方法进行了验证计算.

本文的量化计算方法改进了过去系统安全量化评估过程中, 利用专家经验对系统设备受攻击可能性赋值的主观性问题, 提出了一种较为客观的量化计算方法. 可以应用于系统安全评估的层次分析法、贝叶斯网络等方法中的系统设备受攻击可能性的赋值中.

References

1 Illiashenko O, Kharchenko V, Ahtyamov M. Security assessment and green issues of FPGA-based information and control systems. In: Proceedings of the 2013 International Conference on Digital Technologies (DT). Zilina, Slovakia: IEEE, 2013. 185−190

2 Papakonstantinou N, Sierla S, Charitoudi K, O′Halloran B, Karhela T, Vyatkin V, Turner I. Security impact assessment of industrial automation systems using genetic algorithm and simulation. In: Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA). Barcelona, Spain: IEEE, 2014. 1−8

3 Leszczyna R, Fovino I N, Masera M. Approach to security assessment of critical infrastructures′ information systems. *IET Information Security*, 2011, **5**(3): 135−144

4 Wang L J, Wang B, Peng Y J. Research the information security risk assessment technique based on Bayesian network. In: Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). Chengdu, China: IEEE, 2010. V3-600−V3-604

5 Bian N Y, Wang X Y, Mao L. Network security situational assessment model based on improved AHP_FCE. In: Proceedings of the 6th International Conference on Advanced Computational Intelligence (ICACI). Hangzhou, China: IEEE, 2013. 200−205

6 Lu Hui-Kang, Chen Dong-Qing, Peng Yong, Wang Hua-Zhong. Quantitative research on risk assessment for information security of industrial control system. *Process Automation Instrumentation*, 2014, **35**(10): 21−25
(卢慧康, 陈冬青, 彭勇, 王华忠. 工业控制系统信息安全风险评估量化研究. 自动化仪表, 2014, **35**(10): 21−25)

7 Sasirekha V, Ilanzkumaran M. Heterogeneous wireless network selection using FAHP integrated with TOPSIS and VIKOR. In: Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME). Salem, India: IEEE, 2013. 399−407

8 Mohyeddin M A, Gharaee H. FAHP-TOPSIS risks ranking models in ISMS. In: Proceedings of the 7th International Symposium on Telecommunications (IST). Tehran, Iran: IEEE, 2014. 879−882

9 Cárdenas A A, Amin S, Lin Z S, Huang Y L, Huang C Y, Sastry S. Attacks against process control systems: risk, assessment, detection, and response. In: Proceedings of the 6th ACM Symposium on Information. Computer and Communication Security. New York, USA: ACM Press, 2011. 355−366

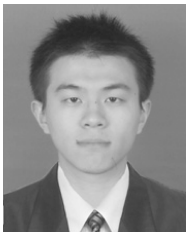
10 Nziga J P, Cannady J. Minimal dataset for network intrusion detection systems via MID-PCA: a hybrid approach. In: Proceedings of the 6th International Conference Intelligent Systems (IS). Sofia, Bulgaria: IEEE, 2012. 453−460

11 Livani M A, Abadi M. A PCA-based distributed approach for intrusion detection in wireless sensor networks. In: Proceedings of the 2011 International Symposium on Computer Networks and Distributed Systems (CNDS). Tehran, Iran: IEEE, 2011. 55−60

12 Downs J J, Vogel E F. A plant-wide industrial process control problem. *Computers and Chemical Engineering*, 1993, **17**(3): 245−255

13 Lyman P R, Georgakis C. Plant-wide control of the Tennessee Eastman problem. *Computers and Chemical Engineering*, 1995, **19**(3): 321−331

14 McAvoy T J. A methodology for screening level control structures in plantwide control systems. *Computers and Chemical Engineering*, 1998, **22**(11): 1543−1552



贾驰千 浙江大学智能系统与控制研究所硕士研究生. 2014 年获得浙江大学控制学院工学学士学位. 主要研究方向为工业控制系统安全.
E-mail: cqjay2010@163.com
(**JIA Chi-Qian** Master student at the Institute of Cyber-Systems and Control, Zhejiang University. He received his bachelor degree from Zhejiang University in 2014. His research interest covers security of industrial control system.)

冯冬芹 浙江大学工业控制技术国家重点实验室、浙江大学智能系统与控制研究所教授. 主要研究方向为现场总线, 实时以太网, 工业无线通信技术, 工业控制系统安全以及网络控制系统的研发与标准化工作. 本文通信作者.
E-mail: dqfeng@iipc.zju.edu.cn
(**FENG Dong-Qin** Professor at the State Key Laboratory of Industrial Control Technology, Institute of Cyber-Systems and Control, Zhejiang University. His research interest covers field bus, real-time ethernet, industrial wireless communication technology, security of industrial control system, and network control system. Corresponding author of this paper.)