基于粒子滤波的工业控制网络态势感知建模

陆耿虹 [1] 冯冬芹 [1]

摘 要 粒子滤波 (Particle filtering, PF) 算法能有效地对工控系统这一类非线性、非高斯噪声系统进行状态估计, 但在实际采用经典粒子滤波状态估计检测攻击时, 实验结果显示该方法存在很高的漏检率, 无法保障系统安全. 因此改进经典算法, 提出了基于粒子滤波输入估计的态势理解算法. 该算法在考虑系统输入与输出关系的同时, 结合蒙特卡洛思想, 提取工控系统态势特征, 计算态势指标, 最终实现态势理解. 实验结果表明, 该算法能有效地感知持续性攻击, 并判断系统态势.

关键词 工控系统, 态势感知, 粒子滤波, 态势理解

引用格式 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. 自动化学报, 2018, **44**(8): 1405−1412

DOI 10.16383/j.aas.2017.c160830

Modeling of Industrial Control Network Situation Awareness With Particle Filtering

LU Geng-Hong[1] FENG Dong-Qin[1]

Abstract Particle filtering (PF) algorithm can estimate the states of industrial control systems, which are non-linear and have non-Gaussian noises. However, when using classical particle filtering state estimation to detect continuous attacks, it is shown that the false negative rate is too high to ensure the security of the system. Therefore, a situation perception algorithm by means of particle filtering input estimation is proposed to improve the effectiveness of the classical algorithm. Considering the relationship between system input and output and combining Monte-Carlo simulation, the proposed algorithm can extract industrial control system situation features, calculate situation metrics and realize the situation perception. Experimental results indicate that the proposed algorithm can recognize continuous attacks and judge the system situation effectively.

Key words Industrial control system, situation awareness, particle filtering (PF), situation perception

Citation Lu Geng-Hong, Feng Dong-Qin. Modeling of industrial control network situation awareness with particle filtering. *Acta Automatica Sinica*, 2018, **44**(8): 1405−1412

工控网络处于快速发展阶段, 由于工业通信协议中存在不可避免的漏洞, 工控网络容易遭受攻击者的恶意攻击, 给工控网络的安全带来巨大威胁[1], 例如伊朗的震网病毒事件[2], 就是攻击者借助 Stuxnet 病毒对可编程逻辑控制器 (Programmable logic controller, PLC) 代码进行篡改, 实现攻击, 从而达到破坏离心机正常运行的恶意目的, 并造成不可逆转的严重事故. 此外, 由于工控网络自身存在的复杂性增加了攻击判断与检测的难度, 尤其当管理员处于高压紧张的环境下, 更容易发生判断失误[3].

因此, 如何提高对工控系统网络整体态势的准确判断成为当务之急. 1999 年, Bass[4] 首次将态势感知 (Situation awareness, SA) 与网络安全技术相结合, 以期能准确全面地掌握系统的安全状态, 预防事故发生, 为安全管理员提供可靠有效的决策依据. Naderpour 等[5] 提出新型异常态势模型 (Abnormal situation modeling, ASM), 构建贝叶斯网络对多种态势进行分析, 该方法针对安全性要求极高的系统, 利用风险指标判断系统在出现异常态势 (Abnormal situation) 情况下的危险态势 (Hazardous situation) 风险等级, 以此确定系统态势. Kim 等[6] 提出一个基于贝叶斯推论的核电厂态势评估解析模型, 该方法是对核电厂操作员在面对事故发生时的态势评估思考模型 (Mental model) 建模.

以上两种方法, 均是在系统出现异常或事故的情况下对系统态势进行分析, 其前提是异常或事故

收稿日期 2016-12-19 录用日期 2017-05-22
Manuscript received December 19, 2016; accepted May 22, 2017
国家自然科学基金 (61433006) 资助
Supported by National Natural Science Foundation of China (61433006)
本文责任编委 高会军
Recommended by Associate Editor GAO Hui-Jun
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

报警为可信的; 但是, 若系统遭受到欺骗性攻击 (例如假数据注入攻击[7]), 由于系统内的报警系统被攻击者蒙蔽, 此类态势感知技术将无法对系统真实态势进行感知.

针对以上问题, 结合系统在遭受到攻击的情况下系统内部状态值会发生相应改变, 本文提出基于粒子滤波的工业控制网络态势感知建模方法. 粒子滤波 (Particle filtering, PF)[8−9] 是采用蒙特卡罗仿真完成递推贝叶斯滤波过程, 核心是采用一组粒子近似表示系统的后验概率分布, 然后使用近似表示估计非线性系统的状态[10]. Arulampalam 等[11] 对 PF 的非线性/非高斯噪声系统状态的估计性能进行了考察, 并将其与扩展卡尔曼滤波进行比较, 证明 PF 能有效解决非线性/非高斯噪声系统的状态估计问题.

由上述文献的研究结果可知, 传统的 PF 状态估计, 可以预测非线性非高斯系统的态势变化. 但是在实际应用 PF 状态估计算法对工控系统受到的持续攻击进行检测时, 实验结果显示漏检率高达 96 %, 这是因为在控制器的作用下, 系统从临界状态趋于稳态, 此时, 由于 PF 状态估计算法自身的跟踪能力可跟踪到系统的攻击状态导致无法检测出异常, 从而使得该算法在检测持续性攻击时, 存在较高的漏检率, 这一不足也为工控系统安全带来威胁.

因此, 为了实现对持续性攻击的检测, 降低 PF 状态估计算法对该类攻击的漏检率, 本文将工控系统内在特征与攻击特征相结合, 提出基于 PF 输入估计的态势理解算法. 该方法考虑了工控系统遭受到网络攻击时 (以传感器参数篡改为例), 虚假的传感器参数导致系统的输入值与输出值之间的非线性关系发生变化, 利用这一特点, 结合 Monte-Carlo 思想, 对系统输入的先验概率进行随机取样, 依据相似性对样本粒子分配权值, 并获取系统输入的估计值将估计值与实际值之间的差值, 作为系统态势特征, 判断工控系统是否处于危险态势, 避免了由于 PF 状态估计引起的漏检, 为针对工控系统网络的持续性攻击检测提出新思路. 在本文最后, 对经典 PF 状态估计算法和态势理解算法进行仿真验证. 需要说明, 不同于文献 [12] 对网络安全态势预测算法的精度进行考察 (算法精度越高, 对复杂网络环境的预测结果越准确), 本文考虑到工控系统遭受攻击的后果严重性, 系统中出现的漏报与误报将会误导操作员对工控系统的态势判断, 从而引发灾难, 因此参考 Salerno 等[13] 提出的态势指标, 对本文提出算法报警结果的漏检率与错误率进行分析, 而不再考虑算法精度. 实验结果表明, 本文提出的算法能有效感知系统中的不同态势 (正常态势及危险态势), 漏检率与错误率均处于较低水平.

1 工控网络态势感知模型

1.1 网络安全态势感知模型简介

Endsley[14] 在 1988 年提出了态势感知的定义: 在一定的时空条件下, 对环境因素的获取、理解以及对未来状态的预测.

网络安全态势感知 (Network security situation awareness, NSSA) 模型分为三个层次, 通过对来自系统的数据进行处理后, 获取系统当前态势, 并对未来态势进行预测. 从下至上依次为 (如图 1 所示):

1) 态势要素获取: 态势要素获取层是 NSSA 模型的基础, 主要包括对数据的预处理和特征提取. 其目的主要在于对工控系统中的海量数据进行缩减, 保留关键信息, 并从中提取特征.

2) 态势理解: 对获取的特征进行进一步处理, 包括数据关联、特征检测、识别与分类, 并对多个分类结果进行决策融合, 获取最终决策即整体系统态势.

3) 态势预测: 利用预测算法对工控网络态势的趋势进行预测.

1.2 工控网络态势

出于保护工控系统安全的目的, 将工控网络态势分为安全态势和危险态势[15]. 安全态势指系统中的过程参数均处于系统既定的安全值范围内; 危险态势指系统遭受到攻击, 过程参数超出安全临界值 δ 的工控系统状态.

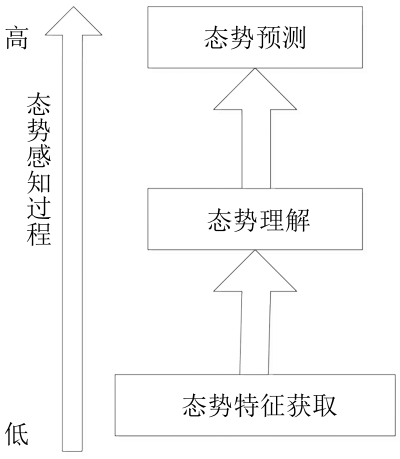


图 1 态势感知模型

Fig. 1 Situation awareness model

一般的 PLC 系统如图 2 所示, 传感器在将传感数据发送至 PLC 的过程中, 可能会遭受到攻击者的攻击, 真实传感数据被篡改[16], 导致控制系统不稳定. 本文假定系统的危险态势是由攻击者施加的假数据注入攻击[17] 产生.

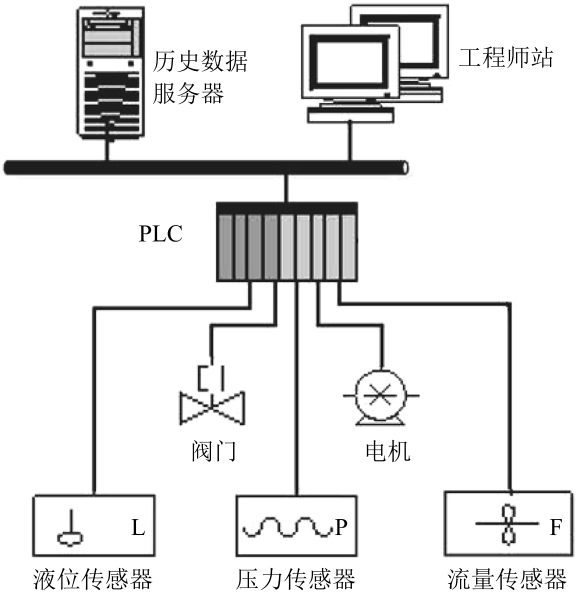


图 2　PLC 系统示意图

Fig. 2　A diagram of PLC implementation

$$\widetilde{y}(t) = y(t) + \alpha(t), \quad t \in T_{\text{atc}} \tag{1}$$

其中, $y(t)$ 和 $\widetilde{y}(t)$ 分别是在安全态势和危险态势下, PLC 接收到的数值. $\alpha(t)$ 为攻击者施加的攻击参数, $T_{\text{atc}} = [t_{\text{atc}_s}, t_{\text{atc}_e}]$ 为从攻击开始 t_{atc_s} 到攻击结束 t_{atc_e} 的攻击时间.

1.3　工控网络态势感知建模

态势理解层作为态势感知过程中承下启上的中心环节, 利用态势要素对获取的数据进行态势理解, 并将数据处理结果输送至态势预测层. 态势理解的优劣, 将直接影响态势感知的结果以及态势预测的性能. 因此高效准确的态势理解过程在态势感知中, 显得尤为重要.

本文创新性地提出了工控网络态势感知模型, 如图 3 所示, 该模型从下至上共包含三个部分: 态势要素获取层、态势理解层以及后续态势感知过程, 本文主要对底部两层进行研究与分析.

1) 态势要素获取层: 采集来自各传感器节点的数据, 将其存储在数据集 D 中.

2) 态势理解层: 利用 PF 算法估计系统输出, 并提取特征, 使用态势指标对要素理解的效果进行衡量, 最后将态势理解结果输出至态势评估与预测中.

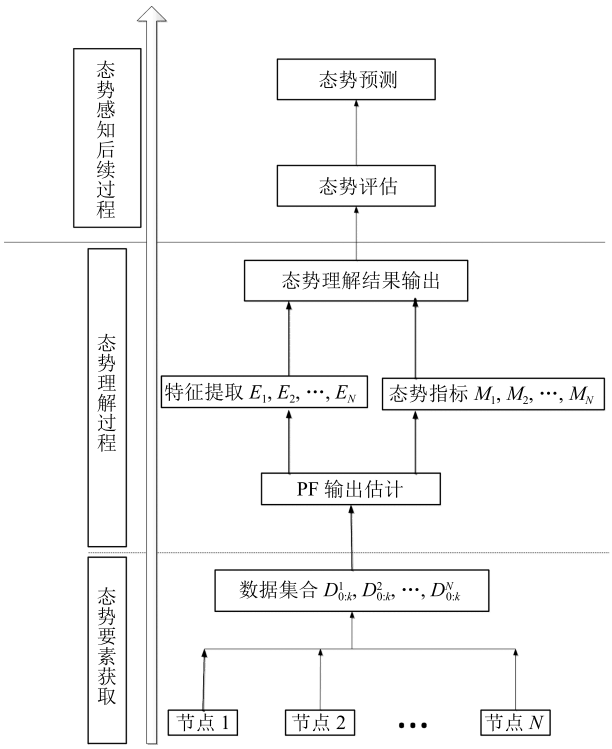


图 3　工控网络态势感知模型

Fig. 3　Industrial control network situation awareness model

定义 1. 数据集合 $D^i_{0:k} = \{d_j, j = 0, \cdots, k\}$ 表示从 $0 \sim k$ 时刻, 第 i 个节点采集的数据集合.

定义 2. 特征提取 E 作为 PF 输入估计的结果之一, 记录 PF 输入估计算法的输出结果, 是数据集 $D^i_{0:k}$ 在经 PF 输入估计算法处理后, 得到的特征序列.

$$E = \{e^i_{\text{atc}} \mid i = 1, \cdots, m\} \tag{2}$$

定义 3. 态势指标 $M = \{MR, FR\}$ 包含两个元素. 表示在进行 PF 状态估计时出现的错误率和漏检率.

$$MR = \frac{\sum\limits_{j=1}^{k} I(m_j)}{\sum\limits_{j=1}^{k} S(m_j)} \tag{3}$$

$$FR = 1 - \frac{\sum\limits_{j=1}^{k} C(m_j)}{\sum\limits_{j=1}^{k} W(m_j)} \tag{4}$$

其中, I 为误测特征个数, S 为测得特征个数, C 为正确测得的危险态势特征个数, W 为期望得到的危险态势特征个数.

由于在特征提取过程中, 可能存在感知错误、遗漏等情况, 因此提出对态势特征获取过程中 PF 出现的错误特征数量和丢失的特征数量进行衡量.

本文提出的态势感知模型中的态势理解层不仅能对来自工控系统众多节点的海量数据进行简化, 给出系统态势特征, 而且可以利用态势指标对态势理解过程的质量进行计算, 为后续阶段的态势感知结果可靠性提供依据.

1.3.1 粒子滤波状态估计

为了获取非线性、非高斯噪声的工控系统状态特征, 采用 PF 算法进行状态估计, 是一种很有效的非线性滤波技术[18], 适用于任何能用状态空间模型表示的非高斯背景的非线性随机系统, 精度可以逼近最优估计. 该算法的实质是由粒子及其权重组成的离散随机测度近似相关的概率分布, 并根据算法递推更新离散随机测度[19].

对于一个非线性、非高斯过程建模如下:

$$x_k = g(x_{k-1}, w_k) \tag{5}$$

$$y_k = h(x_k, v_k) \tag{6}$$

其中, x_k 为待估计的状态量, 假设状态 x_k 的先验分布 $p(x_0)$ 已知; y_k 为已知的观测量; $g(\cdot)$ 为状态转移方程, $h(\cdot)$ 为观测方程; w_k 和 v_k 都为独立的噪声, 分别称为状态噪声和观测噪声.

步骤 1. 初始化. 设 $k = 0$, 采样: $x_0^i \sim p(x_0)$, 根据 $p(x_0)$ 分布采样得到 N 个 x_0^i, $i = 1, 2, \cdots, N$.

步骤 2. 重要性权值计算. 采样 $x_k^i \sim q(x_k|x_{0:k-1}^i, y_{0:k})$, $i = 1, 2, \cdots, N$, 利用下式计算重要性权值.

$$w_k^i = w_{k-1}^i p(y_k|x_{k-1}^i) = w_{k-1}^i \frac{p(y_k|x_k^i)p(x_k|x_{k-1}^i)}{q(x_k|x_{0:k-1}^i, y_k)} \tag{7}$$

其中, $p(y_k|x_k^i)$ 为似然函数概率密度.

$$p(y_k|x_k^i) = p_{e_k}(y_k - h(x_k^i)) \tag{8}$$

式 (7) 中的 $q(x_k|x_{0:k-1}^i, y_k)$ 是重要性概率密度, 在本算法中, 选取使权系数方差最小的最优重要密度函数.

$$q(x_k|x_{0:k-1}^i, y_k) = p(x_k|x_{k-1}^i) \tag{9}$$

在计算重要性权值后, 进行归一化.

$$\bar{w}_k^i = \frac{w_k^i}{\sum_{i=1}^N w_k^i} \tag{10}$$

步骤 3. 重采样. 设定有效样本数 $N_{\text{threshold}}$, 并计算退化因子 N_{eff}

$$N_{\text{eff}} = \frac{1}{\sum_{i=1}^N (\bar{w}_k^i)^2} \tag{11}$$

N_{eff} 越小, 意味着退化现象越严重.

若 $N_{\text{eff}} < N_{\text{threshold}}$, 则进行重采样, 将原来的带权样本 $\{x_{0:k}^i, \bar{w}_k^i\}_{i=1}^N$ 映射为等权样本 $\{\tilde{x}_{0:k}^i, 1/N\}_{i=1}^N$. 其中, $\tilde{x}_{0:k}^i$ 为重采样后的粒子.

步骤 4. 预测. 获取状态预测 $\hat{x}_k$, 据此计算观测值估计 $\hat{y}_k$, 并计算估计值与真实值的偏差 e_k (特征).

$$\hat{x}_k = \sum_{i=1}^N \bar{w}_k^i \tilde{x}_k^i \tag{12}$$

$$\hat{y}_k = h(\hat{x}_k, v_k) \tag{13}$$

$$e_k = y_k - \hat{y}_k \tag{14}$$

步骤 5. 输出. 将 e_k 与安全阈值 δ 进行比较, 当 $|e_k| > \delta$ 时, 记录系统第 i 次出现危险态势的时刻 k_{atc}^i 以及对应偏差 e_k^i.

1.3.2 基于粒子滤波输入估计的态势理解算法

在实际应用 PF 状态估计对系统受到的攻击进行检测时, 实验结果显示, 对于系统中施加持续时间为 100 小时的攻击, PF 状态估计算法可以在系统被攻击 (即状态值发生突然变化) 后的 10 分钟内检测到攻击, 即偏差值 e 将会超出阈值; 但是由于 PF 估计算法自身具备的状态变化跟踪能力, 在系统遭受到攻击的 2 小时后, 系统状态将趋于稳定, 即此时的偏差值 e 将会接近于零, 从而导致 PF 状态估计算法无法持续检测出系统受到的攻击.

考虑到对于输入输出之间存在函数关系 $y = f(u)$ 的系统, 在遭受到攻击时, 系统的输入 u 也会发生变化, 因此, 本文提出基于 PF 输入估计的态势感知算法, 以实现对长时间持续攻击的态势感知, 降低系统漏报率.

基于 PF 输入估计的态势感知算法, 不再考虑状态的估计, 利用输出残差进行报警; 而是利用 Monte-Carlo 思想, 在已获得的输出 y_k 基础上, 估计输入 $\hat{u}$. 利用实际输入 (控制器输出) u 与 $\hat{u}$ 的差值, 对系统态势进行感知.

算法 1. 基于 PF 输入估计的态势感知算法

步骤 1. 获取 $t = 0, \cdots, k$ 时刻的输出 y_k;

步骤 2. 初始化. 设 $k = 0$, 在 $[u_{\min}, u_{\max}]$ 内随机采样 N 次, 获得 N 个随机样本 (粒子), 构成序列 $\{u_k^*(i)|i = 1, \cdots, N\}$;

步骤 3. 权值分配. 对每个粒子 $u_k^*(i)$ 分配相应的权重 $q_k^*(i)$, $i = 1, \cdots, N$, 计算方式如下:

$$q_k^*(i) = \frac{p(y_k|u_k^*(i))}{\sum_{j=1}^{N} p(y_k|u_k^*(j))} \tag{15}$$

其中, $p(y_k|u_k^*(i))$ 为相似性, 即

$$p(y_k|u_k^*(i)) = p_{e_k^*}(y_k - f(u_k^*(i))) \tag{16}$$

步骤 4. 重采样. 采用多项式重采样法, 将原来的带权样本 $\{u_{0:k}^*(i), q_k^*(i)\}_{i=1}^N$ 映射为等权样本 $\{\tilde{u}_{0:k}^*, 1/N\}_{i=1}^N$. 其中, $\tilde{u}_{0:k}^*(i)$ 为重采样后的粒子, 获得新粒子样本.

步骤 5. 输出估计. 获取输出估计值预测 $\hat{u}_k$, 并计算估计值与真实值的偏差 e_k^* (特征).

$$\hat{u}_k = \sum_{i=1}^{N} q_k^*(i)\tilde{u}_k^*(i) \tag{17}$$

$$e_k^* = u_k - \hat{u}_k \tag{18}$$

步骤 6. 计算态势特征. 将 e_k^* 与安全阈值 δ 进行比较, 当 $|e_k^*| > \delta$ 时, 记录系统第 j 次出现危险态势的时刻 $k_{\text{atc}}^*(j)$ 以及对应偏差 $e_k^*(j)$.

步骤 7. 计算态势指标. 利用式 (3) 和式 (4) 计算该系统的态势指标, 态势指标 $M = \{MR, FR\}$.

步骤 8. 态势理解结果输出. 依据步骤 6 和步骤 7 的计算结果, 整理得到态势理解结果并作为算法输出 E, M.

2　实验验证

2.1　仿真对象

某精馏塔提馏段温度单回路控制方案[20] 如图 4 所示, 蒸馏塔提馏段某块板的温度为主变量, 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, 温度传感器 TT 21 能对提馏段的温度 y 进行检测 (系统输出), y_{sp} 为设定值.

2.2　仿真过程

对 PF 状态估计算法和态势理解算法进行仿真, 通过计算两种算法的漏报率, 对算法有效性进行分析.

阶段 1. 仿真模型建立. 依据图 4 的控制方案, 建立相应的控制系统方框图, 如图 5 所示. 对图 5 中各环节进行参数设置: G_{Tm} 为温度测量环节, $G_{Tm} = 1/(s+1)$; 控制阀 G_v 为近似线性阀, $G_v = 1$; 蒸汽流量对象 $G_{p2} = 0.1/(1.5s+1)$; 提馏段温度对象的控制通道与扰动通道动态特性的参数设置分别为 $G_{p1} = 5/(4s^2+5s+1)$, $G_d = -0.5/(3s+1)$; 单回路控制器 TC 的 PID 参数 $K_c = 2.4$, $T_i = 8.8$, $T_d = 2.2$.

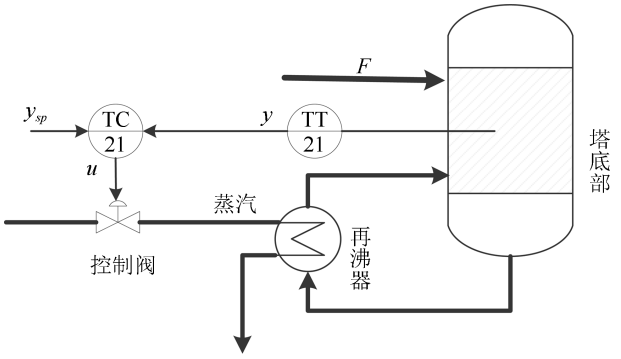


图 4　提馏段温度单回路控制方案

Fig. 4　Temperature single loop control scheme of distillation

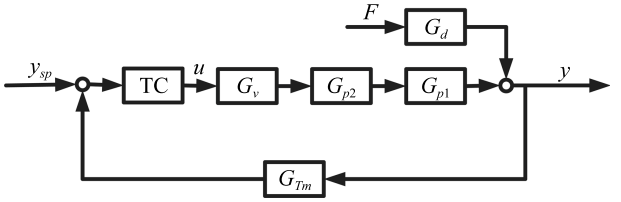


图 5　提馏段温度单回路控制系统方框图

Fig. 5　Block diagram of temperature single loop control scheme of distillation

阶段 2. 态势设置. 对安全态势及遭受不同时长攻击的两种危险态势进行仿真, 设定系统运行总时长 $T_{\text{run}} = 500$.

1) 安全态势: 系统正常运行, 温度设定值 $y_{sp} = 20$;

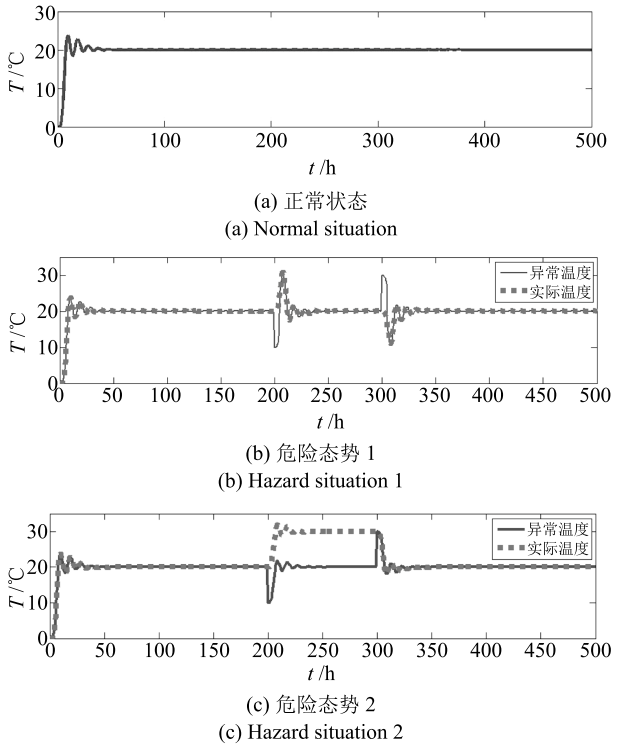
2) 危险态势 1: 在 $k_1 = 200$ 和 $k_2 = 300$ 时刻, 攻击者篡改温度传感器值, 分别施加攻击强度为 $\alpha(k_1) = 30$, $\alpha(k_2) = -30$ 的攻击, 每次攻击持续时长为 $T_{\text{atc}} = 5$;

3) 危险态势 2: 在 $k = 200$ 时, 攻击者开始篡改温度传感器值, 攻击强度为: $\alpha(k) = 30$, 攻击持续时长为 $T_{\text{atc}} = 100$.

图 6 为系统中可能出现的三种态势仿真结果示意图.

阶段 3. 算法验证. 算法验证部分选择 $t = 70$ 以后的数据进行分析, 即对系统处于稳定后的数据进行仿真处理.

1) PF 状态估计. 图 7 为利用 PF 状态估计对三种情况进行态势检测的结果, 假设安全阈值 $\delta = 2$.



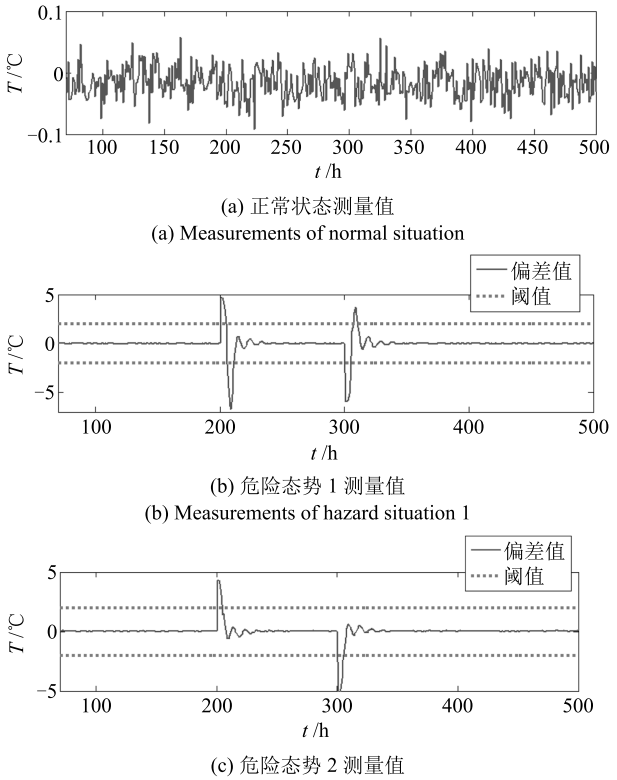
(a) 正常状态
(a) Normal situation

(b) 危险态势 1
(b) Hazard situation 1

(c) 危险态势 2
(c) Hazard situation 2

图 6 三种不同态势情况

Fig. 6 The three different situations



(a) 正常状态测量值
(a) Measurements of normal situation

(b) 危险态势 1 测量值
(b) Measurements of hazard situation 1

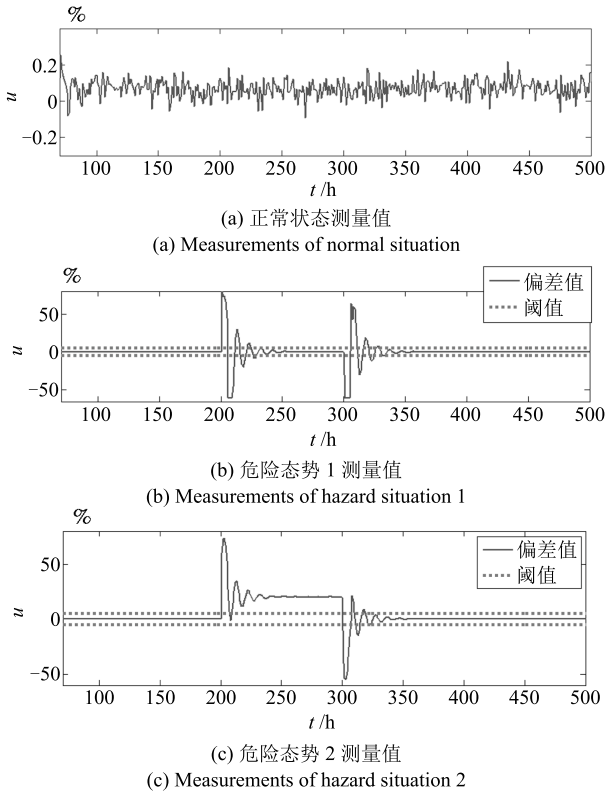
(c) 危险态势 2 测量值
(c) Measurements of hazard situation 2

图 7 PF 状态估计算法仿真结果

Fig. 7 The simulation results related to PF state estimation algorithm

从图 7 可以看出, a) $M_a = \{0, 0\}$, 此时算法没有检测到攻击, 判断系统处于正常运行状态; b) $M_b = \{0.0200, 0.1667\}$, 此时算法检测到两次攻击, 存在较低的错误率与漏检率; c) $M_c = \{0.2040, 0.9604\}$, 由态势指标可得, 该算法在面对持续时间较长的攻击时, 漏检率高达 0.9604. 但是能检测到攻击开始以及结束的时刻.

2) 基于 PF 输入估计的态势理解. 图 8 为利用态势理解算法对三种情况进行态势检测的结果, 假设安全阈值 $\delta = 5$. 从图 8 可以看出, a) $M_a = \{0, 0\}$, 此时算法没有检测到攻击, 判断系统处于正常运行状态; b) $M_b = \{0.0820, 0.1667\}$, 此时算法检测到两次攻击, 错误率与漏检率均较低; c) $M_c = \{0.048, 0.0396\}$; 检测到长持续时间下的攻击, 错误率与漏检率均低于 5 %.



(a) 正常状态测量值
(a) Measurements of normal situation

(b) 危险态势 1 测量值
(b) Measurements of hazard situation 1

(c) 危险态势 2 测量值
(c) Measurements of hazard situation 2

图 8 态势理解算法仿真结果

Fig. 8 The simulation results related to situation awareness algorithm

2.3 仿真结果分析

对比两种算法的仿真结果可知:

1) PF 状态估计算法

由 a) 和 b) 的检测结果可知, 当系统存在突然发生的变化时, 该算法能进行有效的检测, 特征值变

化明显, 检测的错误率与漏检率较低; 由 c) 的仿真结果可知, 该算法无法感知到系统中出现的长持续性攻击, 存在很高的漏报率, 对系统安全产生严重威胁.

2) 基于 PF 输入估计的态势理解算法

a) 和 b) 的仿真结果证明, 该算法能有效跟踪和预测输入的变化趋势, 两种算法的漏检率相同, 尽管态势理解算法的错误率相对 PF 状态估计算法偏高 6 %, 但是对于系统安全性能而言, 该算法依然有效检测出了 b) 的危险态势; 由 c) 的仿真结果可得, 态势理解算法能有效检测到系统中存在的长时间持续的攻击, 错误率与漏检率均小于 5 %, 远低于 PF 状态估计算法.

对比仿真结果可知, 本文提出的基于 PF 输入估计的态势理解算法能有效判断系统中出现的危险态势, 为工控网络安全态势感知提供可靠的感知判据.

3 结论

本文介绍了基于粒子滤波的工业控制网络态势感知建模, 将文中构造的态势感知模型中的态势理解层作为研究重点, 提出了基于 PF 输入估计的态势理解算法. 该算法是对经典 PF 状态估计的改进, 在 Monte-Carlo 思想的基础上, 考虑到系统输入与输出之间的联系, 通过输出值校准输入的估计值, 利用实际值与估计值之间存在的差值, 判断系统是处于安全态势还是危险态势. 该算法具有较好的输入值估计能力, 可准确获取系统态势特征, 给出态势指标, 对特征的可靠性进行定量衡量. 该算法可为后续的态势预测过程提供科学可靠的数据信息, 提升态势感知结果的准确性.

实验结果表明, 本文提出的态势理解算法, 能有效地利用数据源中的信息对系统内存在的危险态势进行感知. 仿真结果表明该算法具有较高的可靠性与准确性.

References

1 Huang Jia-Hui, Feng Dong-Qin, Wang Hong-Jian. A method for quantifying vulnerability of industrial control system based on attack graph. *Acta Automatica Sinica*, 2016, **42**(5): 792−798
(黄家辉, 冯冬芹, 王虹鉴. 基于攻击图的工控系统脆弱性量化方法. 自动化学报, 2016, **42**(5): 792−798)

2 Genge B, Nai Fovino I, Siaterlis C, Masera M. Analyzing cyber-physical attacks on networked industrial control systems. *Critical Infrastructure Protection V*. Berlin Heidelberg, Germany: Springer, 2011. 167−183

3 Lu J, Yang X W, Zhang G Q. Support vector machine-based multi-source multi-attribute information integration for situation assessment. *Expert Systems with Applications*, 2008, **34**(2): 1333−1340

4 Bass T. Multisensor data fusion for next generation distributed intrusion detection systems. In: Proceedings of the 1999 IRIS National Symposium on Sensor and Data Fusion. Washington, USA: IRIS, 1999. 24−27

5 Naderpour M, Lu J, Zhang G Q. An abnormal situation modeling method to assist operators in safety-critical systems. *Reliability Engineering and System Safety*, 2015, **133**: 33−47

6 Kim M C, Seong P H. An analytic model for situation assessment of nuclear power plant operators based on Bayesian inference. *Reliability Engineering and System Safety*, 2006, **91**(3): 270−282

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

8 Doucet A, de Freitas N, Gordon N. *Sequential Monte Carlo Methods in Practice*. New York, USA: Springer, 2001.

9 Carpenter J, Clifford P, Fearnhead P. Improved particle filter for nonlinear problems. *IEE Proceedings — Radar, Sonar and Navigation*, 1999, **146**(1): 2−7

10 Kadirkamanathan V, Li P, Jaward M H, Fabri S G. Particle filtering-based fault detection in non-linear stochastic systems. *International Journal of Systems Science*, 2002, **33**(4): 259−265

11 Arulampalam S, Maskell S, Gordon N, Clapp T. A tutorial on particle filters for online nonlinear/non-Gaussian Bayesian tracking. *IEEE Transactions on Signal Processing*, 2002, **50**(2): 174−188

12 Tang Yong-Li, Li Wei-Jie, Yu Jin-Xia, Yan Xi-Xi. Research on a prediction method of network security situation based on particle filter. *Computer Applications and Software*, 2017, **34**(1): 293−297
(汤永利, 李伟杰, 于金霞, 闫玺玺. 基于粒子滤波的网络安全态势预测方法研究. 计算机应用与软件, 2017, **34**(1): 293−297)

13 Salerno J J, Blasch E P, Hinman M, Boulware D M. Evaluating algorithmic techniques in supporting situation awareness. In: Proceedings of the 2005 Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications. Orlando, Florida, USA: SPIE, 2005. 96−104

14 Endsley M R. Design and evaluation for situation awareness enhancement. In: Proceedings of the 32nd Human Factors Society Annual Meeting. Santa Monica, USA: SAGE, 1988. 97−101

15 Naderpour M, Lu J, Zhang G Q. A situation risk awareness approach for process systems safety. *Safety Science*, 2014, **64**: 173−189

16 Gonzalez C A, Hinton A. Detecting malicious software execution in programmable logic controllers using power fingerprinting. *Critical Infrastructure Protection VIII*. Berlin Heidelberg, Germany: Springer, 2014. 15−27

17 Lu Geng-Hong, Feng Dong-Qin. Industrial control system network security situation awareness modeling and algorithm implementation. *Control Theory and Applications*, 2016, **33**(8): 1054−1060
(陆耿虹, 冯冬芹. 工控网络安全态势感知算法实现. 控制理论与应用, 2016, **33**(8): 1054−1060)

18 Cheng Q, Varshney P K, Michels J, Belcastro C M. Distributed fault detection via particle filtering and decision fusion. In: Proceedings of the 8th International Conference on Information Fusion. Philadelphia, PA, USA: IEEE, 2005. 1239−1246

19 Li Tian-Cheng, Fan Hong-Qi, Sun Shu-Dong. Particle filtering: theory, approach, and application for multitarget tracking. *Acta Automatica Sinica*, 2015, **41**(12): 1981−2002
(李天成, 范红旗, 孙树栋. 粒子滤波理论、方法及其在多目标跟踪中的应用. 自动化学报, 2015, **41**(12): 1981−2002)

20 Dai Lian-Kui, Yu Ling, Tian Xue-Min, Wang Shu-Qing. *Process Control Engineering* (3rd edition). Beijing: Chemical Industry Press, 2012.
(戴连奎, 于玲, 田学民, 王树青. 过程控制工程 (第 3 版). 北京: 化学工业出版社, 2012.)

陆耿虹 浙江大学智能系统与控制研究所博士研究生. 主要研究方向为工业控制系统网络安全态势感知.
E-mail: olivialu@zju.edu.cn
(**LU Geng-Hong** Ph. D. candidate at the Institute of Cyber-Systems and Control, Zhejiang University. Her research interest covers industrial control system network security situation awareness.)

冯冬芹 浙江大学工业控制技术国家重点实验室和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: dongqinfeng@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.)