第33卷第8期
2016年8月

控制理论与应用
Control Theory & Applications

Vol. 33 No. 8
Aug. 2016

DOI: 10.7641/CTA.2016.50767

工控网络安全态势感知算法实现

陆耿虹, 冯冬芹†

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

摘要: 为了探知工控系统的网络安全态势, 准确判断系统运行状况, 提出了安全态势感知方法. 针对已有的完整性攻击研究, 建立基于拜占庭将军问题的工控网络安全态势感知模型以及相应的安全态势感知算法. 本文提出的算法主要通过三个部分实现: 首先对控制回路内的各节点信息进行采集与处理, 得到系统中各节点状态; 然后, 利用所得节点状态, 执行算法流程, 确定系统内存在的恶意节点; 最终获取准确的工控网络安全态势. 实验结果表明: 该态势感知模型与算法能准确提炼系统中的恶意节点并判断当前系统安全态势.

关键词: 工业控制系统; 拜占庭将军问题; 完整性攻击; 网络安全态势感知

中图分类号: TP393　　**文献标识码:** A

Industrial control system network security situation awareness modeling and algorithm implementation

LU Geng-hong, FENG Dong-qin†

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

Abstract: In order to explore network security situation of industrial control system, and find out how exactly the industrial control system performs, a method based on security situation awareness is proposed. According to the current studies of integrity attacks, this paper presents an industrial control network security situation awareness model with Byzantine generals problem being taken into accounts and also security situation awareness algorithm. The algorithm proposed in this paper can be implemented by three major steps: firstly, acquiring the current nodes' states by the data which is collected from every nodes in the control loop of the industrial control system, and the data is preprocessed as well; Secondly, implementing the algorithm with the data obtained, the malicious node in the control industrial system can then be identified; At last, the accurate industrial control network security situation awareness is procured. The result of simulation indicates the validity of the proposed model and corresponding algorithm, which can be used for identifying the malicious node and then estimating the current industrial control network security situation.

Key words: industrial control system; Byzantine generals problem; integrity attacks; network security situation awareness (NSSA)

1 引言(Introduction)

在工业化与信息化高度融合的今天, 对应用于众多国家基础安全设施的工业控制系统(industrial control system, ICS)的智能化要求也在不断提升. 然而, 不同于传统IT系统, 工控系统网络的安全一旦受到威胁, 将会产生灾难性的严峻后果. 1996年, 南卡罗来纳州的油管系统受到完整性攻击, 造成爆裂, 导致了周边环境的严重污染及巨额财产损失[1]. 近年来, 类似的恶意攻击事件不断增多[2], 因此对工控系统的网络安全进行研究, 及时采取适当措施, 从而避免类似灾难性事故的发生, 成为当务之急.

当前工业控制系统网络安全研究多集中于状态监测、故障诊断[3]等手段, 大多数的研究都是在基于解析模型的方法上开展的[4]. Aubrun等人[5]通过构造状态观测器作为残差发生器, 分别研究了时延和丢包情况下网络化控制系统的故障诊断问题; Mao等人[6]利用Euler逼近的方法, 对控制系统进行建模, 并对容错控制问题进行了分析. 尽管这类方法能快速进行故障检测, 但其准确度在很大程度上受到模型精确度的影响. 此外, 文献[7]也指出异常检测对于人为攻击表现

收稿日期: 2015−09−19; 录用日期: 2016−05−13.
†通信作者. E-mail: dqfeng@iipc.zju.edu.cn; Tel.: +86 571-87974993.
本文责任编委: 陈增强.
国家自然科学基金项目(61223004)资助.
Supported by National Natural Science Foundation of China (61223004).

出较高漏检和误判率. 而过程工业具有规模庞大、变量众多的特点, 因此在面对海量系统过程信息时, 引入态势感知的思想, 将有助于改善当前“数据爆炸, 信息匮乏”[8]的局面.

对网络安全态势的研究, 具体而言, 即是对网络中运行的设备、网络行为以及用户行为等基本网络因素进行研究, 可获取整个网络安全状态和变化趋势. 网络态势感知(cyber situation awareness, CSA)是1999年 Tim Bass[9]首次提出的, 该理论是在对 ATC (air traffic control)态势感知成熟理论研究基础上提出的. 由于态势感知是一个动态且互相协作的过程, 通过将数据与基于计算机的智能技术相结合, 可以获取有效的态势感知方法[10]. Lu等人[11]开发了基于支持向量机的评估方法, 能对系统态势产生必要的警告. Brannon等人[12]提出了基于神经网络的态势评估模型, 为决策者提供了有效的决策支持. 但上述模型需要大量合适的训练数据, 因此这些模型在实际中的应用仍存在局限. 由于贝叶斯网络能对不确定的任意过程建模, 能优化系统态势感知, 例如, chai等人[13]提出了基于贝叶斯网络的层次化态势评估模型, 该模型包含了决策融合层与数据处理层; Naderpour等人[14]提出了一个结合神经网络的性能与专家系统的态势评估方法, 用以对态势进行感知与预测; 然而, 由于缺乏异常态势的数据, 无法运用到真实世界中.

针对上述问题, 本文将拜占庭将军问题理论与网络安全态势感知的研究相结合, 通过采集系统节点原始数据, 将实际(节点间实际存在的数据传输关系)与本质(节点状态变化的一致性)两个方面结合起来, 充分分析各节点设备在遭受完整性攻击时的性状, 给出工控系统网络安全态势感知模型与算法, 该模型能判断出系统状态及系统中存在的恶意节点, 为决策者在攻击存在的情况下, 提供可靠的决策依据. 本文最后对系统进行了仿真实验, 从而证明提出模型与算法的有效性和可靠性.

2 工控系统中的拜占庭将军问题模型 (Byzantine generals problem model for ICS)

拜占庭将军问题的研究起源于对计算机系统的可靠性理解以及冲突信息造成的系统故障的思考[15-16]. 该问题描述的是, 当拜占庭将军在进行作战指挥时, 他会通过信使与其他军官联系并共同决定是进行攻击还是撤退. 如果信使是叛徒, 他可能会更改信息内容, 使得接收者和发送者的信息不一致. 而每个接收到信息的军官则是通过比较其从相邻军官处接收到的信息来做出决定. 这样一来, 错误信息的出现, 最终可能会更改战争走向. 图1为拜占庭将军问题的示意图.

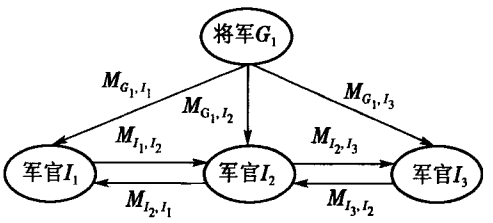


图 1 拜占庭将军问题

Fig. 1 Byzantine generals problem

定义 1　拜占庭将军问题 (Byzantine generals problem), B:

$$B = (\text{node}, \text{rec}_\text{M}, \text{result}). \tag{1}$$

B用一个三元组进行描述, 其中:

1) node为当前将要进行决策的节点;

2) rec_M(recieve message)为节点node接收到的来自其余节点的信息

$$\text{rec}_\text{M} = (M_{s_1,r_\text{node}}, M_{s_2,r_\text{node}}, M_{s_3,r_\text{node}}), \tag{2}$$

$M_{s_i,r_\text{node}}, i = 1,2,3$为节点node接收到来自节点$i$的作战信息, 其中: s_i为发送信息的节点, r_node为接收信息的节点. M_{s_i,r_node}只有两种信号, 攻击A或撤退R.

3) result为节点node进行判断处理后获取的结果.

$$\text{result} = (\text{Atc}_\text{node}, \text{Send}_\text{M}), \tag{3}$$

其中: Atc_node为节点node判断的背叛节点, Send_M为对当前作战态势进行的判断, 即是否存在背叛者.

本文将拜占庭将军问题理论运用到工控系统, 如图2所示: 最底层的实物图为现场层; Pi节点为PLC等设备, 对物理层节点进行控制; S节点所处的是态势感知层, 以实现态势感知的目标.

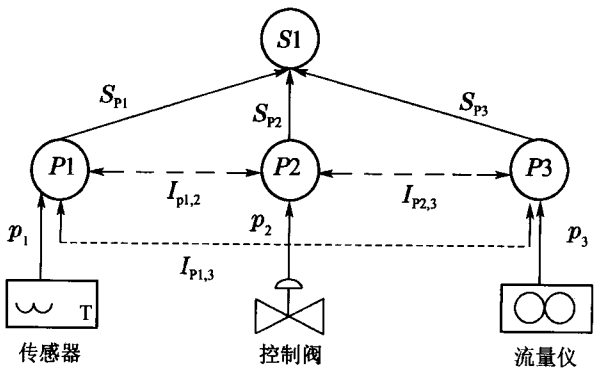


图 2 拜占庭将军问题的工控系统示意图

Fig. 2 Byzantine generals problem of ICS

定义 2　拜占庭将军问题−工控系统表示B_ICS:

$$B_\text{ICS} = (\text{raw}_\text{data}, \text{node}, \text{rec}_\text{M}, \text{result}). \tag{4}$$

不同于B, 结合工控系统的特点, 用一个四元组对B_ICS进行描述.

1) $\mathrm{raw_{data}}$为物理层节点接收到的来自现场层设备的原始数据:

$$\mathrm{raw_{data}} = (p_1, p_2, p_3), \tag{5}$$

其中$p_i(i = 1, 2, 3)$代表的是经过处理的节点原始数据, 包括平均值和方差;

2) node指定为图中S节点, 用于对系统态势进行判断, 它并非工控系统物理层节点;

3) 接收节点信息$\mathrm{rec_M}$

$$\mathrm{rec_M} = (S_{P1}, S_{P2}, S_{P3}), \tag{6}$$

S_{Pi}为节点Pi的单个节点信息, 作为节点node的接收值;

4) 态势感知结果reslut

$$\mathrm{result} = (\mathrm{Atc_{node}}, S_{\mathrm{sec}}), \tag{7}$$

其中: $\mathrm{Atc_{node}}$用于判断系统内是否遭受到完整性攻击; S_{sec}为当前系统态势.

3 完整性攻击下的工控系统 (ICS under the integrity attacks)

基于拜占庭将军问题对工控系统遭受攻击的情况进行分析, 由第2节的介绍可知, 物理层各节点在进行数据处理与分析时, 具有相似性, 因此在本节中, 以传感器受到完整性攻击为例, 对完整性攻击下的工控系统进行说明与介绍.

3.1 单回路控制系统定义(Definition of the single loop control system)

图3为单回路控制系统, 该图展示了控制系统的基本组成, 传感器用于检测控制对象的状况, 并将该检测值传递给控制器; 控制器根据接收到的传感器检测值, 对执行器产生控制信号, 以使得控制对象处于稳定状态.

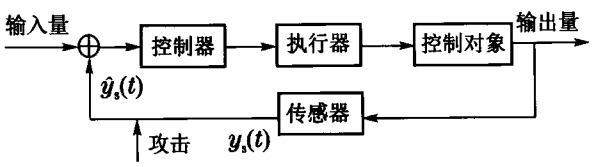


图 3 单回路控制系统

Fig. 3 Single loop control system

定义 3 时间t, T: t为传感器、控制器发送或获取数据的时间点, T意味着工控系统的整个运行过程: $T = [t_{\mathrm{start}}, t_{\mathrm{end}}]$, 其中: t_{start}为工控系统开始运行的时间, t_{end} 为工控系统运行结束的时间.

定义 4 传感器检测值$y_s(t)$: $y_s(t)$为传感器s在时间t对控制对象进行检测获得的检测值, 且$y_s(t) \in Y_s$; $Y_s = [y_s^{\min}, y_s^{\max}]$, 其中: $y_s^{\min}$, $y_s^{\max}$分别为传感器能检测到的最小及最大值, 该值与传感器的自身性能有关.

定义 5 控制器接收值$\hat{y}_s(t)$: $\hat{y}_s(t)$为控制器在时间t接收到的来自传感器的值, 且$\hat{y}_s(t) \in Y_s$.

当$y_s(t)$与$\hat{y}_s(t)$存在一个不为0的偏差$r(t)$时, 说明系统工况出现异常, 此时系统可能出现攻击或内部故障, 两者特点如下:

攻击: 攻击者采用某种攻击策略, 使某一传感器信号在一段攻击时间$T_{\mathrm{atc}}(T_{\mathrm{atc}} \in T)$内产生偏差$r(t)$, 该值为受到攻击者操控的任意不同值$c(t)$.

$$r(t) = \hat{y}_s(t) - y_s(t) = \begin{cases} c(t), & t \in T_{\mathrm{atc}}, \\ 0, & t \notin T_{\mathrm{atc}}, \end{cases} \tag{8}$$

故障: 传感器在k时刻产生突发故障[17], 即出现偏差$r(t)$, 其值为常数c, 并在此之后的所有时刻维持这个偏差.

$$r(t) = \begin{cases} c, & t \geqslant k, \\ 0, & t < k. \end{cases} \tag{9}$$

由攻击与故障的特点, 可知二者之间的区别:

1) 由于攻击者的攻击目的不同, 攻击产生的偏差值是动态变化的; 而故障发生后往往是不可恢复的, 其偏差维持在某一定值.

2) 攻击的发生往往遵循某种攻击策略而具有一定规律, 如几何攻击; 而故障的发生是随机的.

对于上述问题的分析, 将在之后的研究中开展, 本文考虑的是在完整性攻击这一攻击场景下, 利用拜占庭将军问题理论, 对工控系统安全进行态势感知, 并判断系统内存在的恶意节点.

3.2 攻击模型(Attack model)

完整性攻击是指攻击者通过妥协节点, 改变节点真实值, 从而使控制过程发生变化, 如图3中所示: 攻击者通过妥协传感器节点, 改变传感器实际值$y_s(t)$, 并把攻击信号$\tilde{y}_s(t)$作为传感器检测值输出到控制器, 最终达到使工控系统偏离稳定状态或处于危险状态的目的.

定义 6 攻击时间T_{atc}: T_{atc}意味着系统遭受到攻击的时间, $T_{\mathrm{atc}} = [t_{\mathrm{atc_s}}, t_{\mathrm{atc_e}}]$, 且$T_{\mathrm{atc}} \subset T$, 其中, $t_{\mathrm{atc_s}}$, $t_{\mathrm{atc_e}}$分别为攻击开始及结束时间.

定义 7 攻击信号$\tilde{y}_{x_i}(t)$: $\tilde{y}_{x_i}(t)$意味着攻击者在进行攻击时, 节点x_i在时间t的传感器输出值.

$$\tilde{y}_{x_i}(t) = \alpha(t) y_{x_i} + \beta(t), \ t \in T_{\mathrm{atc}}, \tag{10}$$

其中: $\alpha(t)$, $\beta(t)$可视为攻击者在进行攻击时的调节函数, 用以实现不同类型的攻击, 依据文献[18], 通过设定不同的调节函数, 可以建立不同类型的完整性攻击模型.

4 工控网络安全态势感知算法(Industrial control network security situation awareness algorithm)

4.1 相关概念定义(Definition of related concepts)

本文提出的算法通过对系统内节点参数的分析与处理, 结合拜占庭将军问题的思想, 从而获取系统整体态势, 首先对算法内的相关函数进行定义与描述.

定义 8 STATE函数:

$\mathrm{STATE}=(\mathrm{state}_{p_1},\mathrm{state}_{p_2},\mathrm{state}_{p_3})$获得系统节点序列, state_{p_i}为节点i的状态值, 当其值超过稳定运行时的正常值$\bar{Y}_i^{\mathrm{normal}}$时, state_{p_i}为1; 若小于, 则为0, 其表达式如下:

$$\mathrm{state}_{p_i}=\begin{cases}0, & \bar{Y}_i<\bar{Y}_i^{\mathrm{normal}},\\ 1, & \bar{Y}_i>\bar{Y}_i^{\mathrm{normal}},\end{cases}\tag{11}$$

其中: $\bar{Y}_i^{\mathrm{normal}}$为节点$i$稳定运行时均值; $\bar{Y}_i$为节点i状态变化后均值$\bar{Y}_i=\dfrac{\sum Y_i}{T}$;

定义 9 Attack函数: 该函数用以确定恶意节点.

在给出Attack函数前, 需要首先考虑各节点间的状态一致性关系$f_{i,j}(i\neq j)$, $f_{i,j}$是提炼恶意节点的判据, 其思想与原始拜占庭将军问题理论中确定“背叛节点”的思想一致, $f_{i,j}$ 体现的是将拜占庭将军问题理论应用于工控系统时, 节点之间存在的逻辑关系, 并分两种情况进行讨论(普遍情况):

1) 对于具有负响应关系的两个节点, 将其节点状态进行同或运算.

例如, 当温度传感器接收到温度上升的信号时($\mathrm{state}_{p_1}=1$), 控制阀门开度将减小($\mathrm{state}_{p_1}=0$):

$$f_{1,2}(\mathrm{state}_{p_1},\mathrm{state}_{p_2})=\mathrm{state}_{p_1}\odot\mathrm{state}_{p_2}.\tag{12}$$

2) 对于具有正响应关系的两个节点, 将其节点状态进行异或运算. 例如, 当控制阀门开度减小($\mathrm{state}_{p_1}=0$)时, 流量仪流量也变小($\mathrm{state}_{p_3}=0$):

$$f_{2,3}(\mathrm{state}_{p_2},\mathrm{state}_{p_3})=\mathrm{state}_{p_2}\oplus\mathrm{state}_{p_3}.\tag{13}$$

如式(14)所示的Attack函数是针对本文的研究对象, 即单回路系统, 给出的表达形式并能对恶意节点进行判断:

$$\mathrm{rec_M}=\begin{cases}(s_{p_1},s_{p_2},s_{p_3}), & \mathrm{Atc_{node}}=1,\\ (0,0,0), & \mathrm{Atc_{node}}\neq 1,\end{cases}\tag{14}$$

$$\mathrm{Atc_{node}}=s_{p_1}+s_{p_2}+s_{p_3},\tag{15}$$

其中s_{p_i}为节点p_i与其余节点状态之间的一致性判值:

$$s_{p_i}=f_{i,j}\odot f_{i,k},\ i\neq j\neq k.\tag{16}$$

若$\mathrm{Atc_{node}}=1$, 则表示系统受到完整性攻击, 且$\mathrm{rec_M}$中状态显示为1的节点, 为系统中的恶意节点; 否则, 系统正常, 即$\mathrm{rec_M}$中, 3个节点显示值均为0.

4.2 算法(Algorithm)

图4所示为工控网络安全态势感知的算法流程图.

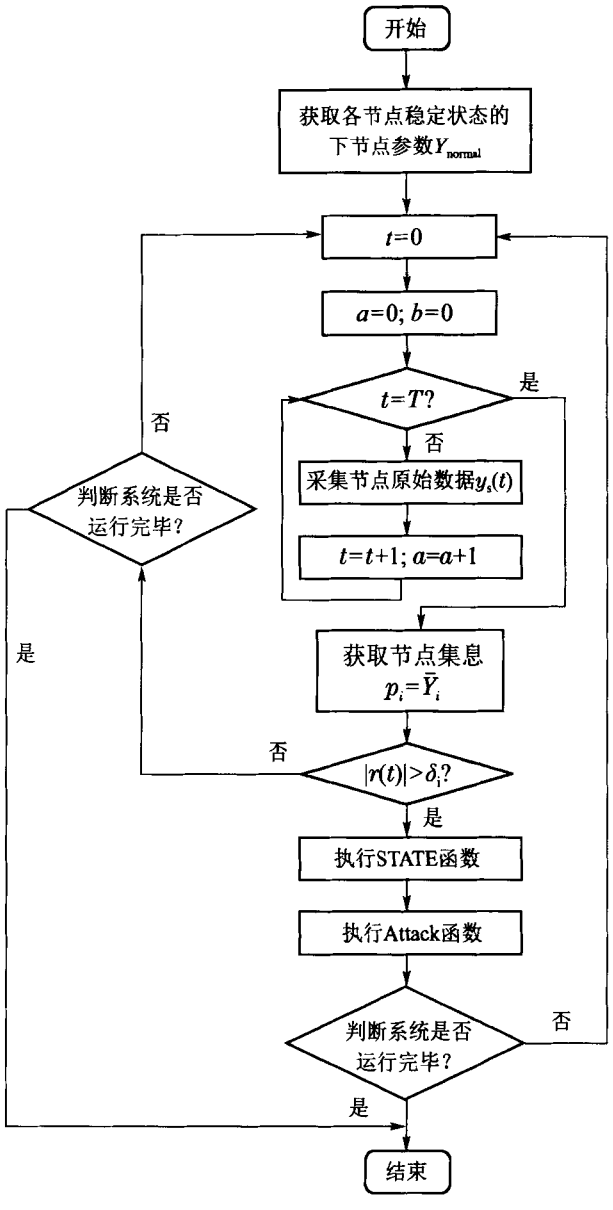


图 4 算法流程图

Fig. 4 Algorithm flow chart

本文算法的基本思想如下:

1) 信息预处理: 获取系统在稳定、无攻击运行状态下的各节点参数$\bar{Y}_{\mathrm{normal}}$, 该值为系统稳定运行时各节点的均值;

2) 在整个工控系统运行过程中, 以周期T'为单位, 对系统中的每个节点的原始数据进行处理, 获取节点信息$Pi=\bar{Y}_i$;

3) 判断此时的节点参数是否偏离稳定值, 若是, 则系统可能出现扰动或异常, 则执行步骤5), 否则, 系统正常, 执行下一步;

4) 判断系统是否执行完毕, 若是, 则结束算法; 否

则返回步骤2), 继续对接收到的新数据进行判断;

5) 执行STATE函数, 对接收到的节点信息进行二次处理, 并将值输出给Attack函数;

6) 执行Attack函数, 判断系统内是否存在攻击, 并确定恶意节点;

7) 判断系统运行是否全部完成, 若是, 则结束算法, 否则, 返回步骤2), 继续执行循环.

5 MATLAB 仿真实验 (MATLAB simulation experiments)

5.1 仿 真 模 型 搭 建 (Construction of simulation models)

某精馏塔提馏段温度单回路控制方案[19], 如图5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: 粗实线部分表示工艺管线, 细实线部分表示信号线. 图中各标记含义: Q代表蒸汽流量, 用于表征控制阀开度; P_{v}代表蒸汽控制阀阀前压力; P为蒸汽控制阀阀后压力; F是进料量; B为塔底产品馏出液.

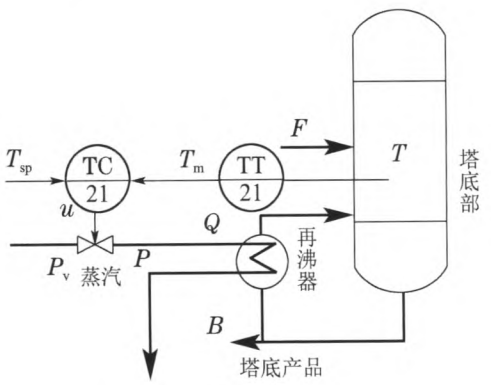


图 5 提馏段温度单回路控制方案

Fig. 5 Temperature single loop control scheme of distillation

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f_{V}处于0%~100%之间, 即控制阀完全关闭或完全打开. 在仿真过程中, 对传感器温度参数T_{m}, 控制阀参数f_{V}, 流量参数Q进行检测.

因此在无攻击情况下, 对系统加入一个扰动, 由于进料量F为温度环节的主要干扰量, 因此加入一个幅度为20的扰动; 在此情况下, 系统将进行正常控制, 图6所示为各节点输出状态, 表1为相应实验结果.

表 1 无攻击情况下, 实验结果统计表

Table 1 Experiment results under no attacks situation

	算法参数	实验结果
各节点状态	$\mathrm{STATE}=(1,0,0)$	
完整性攻击判断	$\mathrm{Atc}_{\mathrm{node}}=3$ $\mathrm{rec}_{\mathrm{M}}=(0,0,0)$	不存在完整性攻击无恶意节点

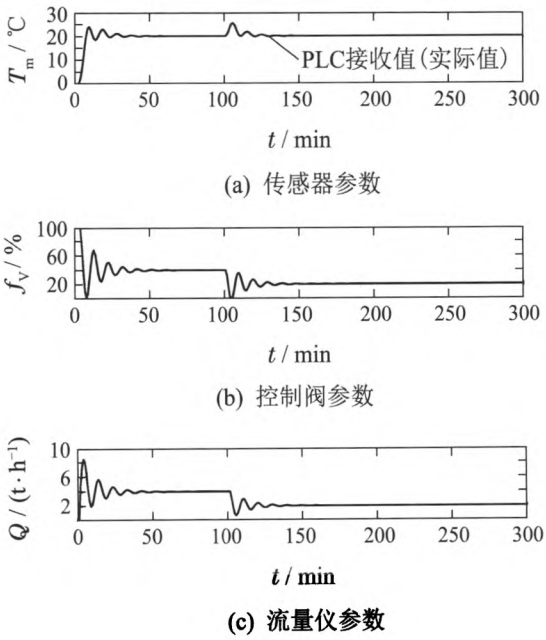


图 6 无攻击情况

Fig. 6 No attacks situation

5.2 实验验证(Verification)

利用MATLAB软件对系统进行仿真实验, 本文假定完整性攻击每次只作用在一个节点上, 且攻击是在系统运行处于稳定后发生. 仿真时间$T=[0,300]$, 攻击时间$\mathrm{Tatc}=[101,300]$.

1) 模拟温度传感器受到完整性攻击, 其中输入攻击信号:

$$\tilde{y}_{\mathrm{sensor}}(t)=y_{\mathrm{sensor}}(t)+\beta(t),\ \beta(t)=-15.$$

图7为各节点输出示意图, 表2为相应实验结果.

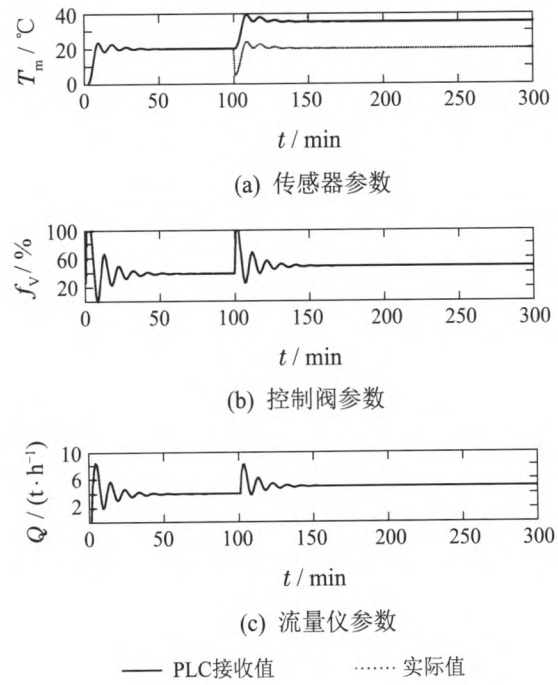


图 7 攻击温度传感器

Fig. 7 Attack the temperature sensor

表 2 攻击传感器时, 实验结果统计表

Table 2 Experiment results of attacking the sensor

	算法参数	实验结果
各节点状态	$\mathrm{STATE}=(1,1,1)$	
完整性攻击判断	$\mathrm{Atc_{node}}=1$ $\mathrm{rec_M}=(1,0,0)$	存在完整性攻击传感器为恶意节点

2) 模拟控制阀节点受到完整性攻击, 其中输入攻击信号:

$$\widetilde{y}_{\mathrm{valve}}(t)=y_{\mathrm{valve}}(t)+\beta(t),\beta(t)=40.$$

图8为各节点输出示意图, 表3为相应实验结果.

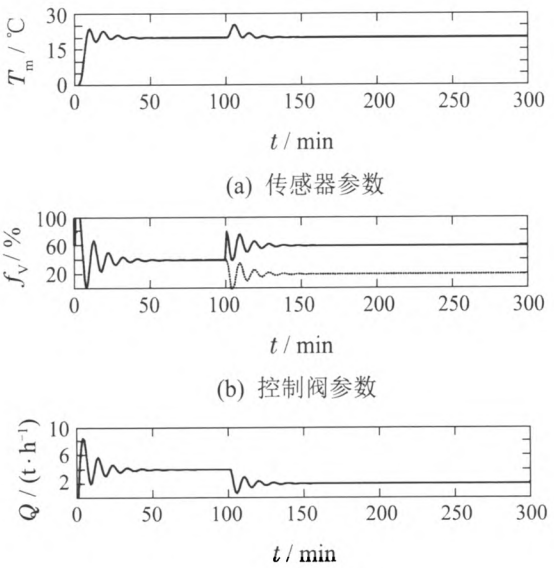


图 8 攻击控制阀节点

Fig. 8 Attack the valve

表 3 攻击控制阀时, 实验结果统计表

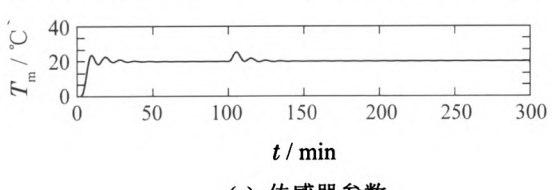
Table 3 Experiment results of attacking the valve

	算法参数	实验结果
各节点状态	$\mathrm{STATE}=(1,1,0)$	
完整性攻击判断	$\mathrm{Atc_{node}}=1$ $\mathrm{rec_M}=(0,1,0)$	存在完整性攻击控制阀为恶意节点

3) 模拟流量仪受到完整性攻击, 其中输入攻击信号:

$$\widetilde{y}_{\mathrm{meter}}(t)=y_{\mathrm{meter}}(t)+\beta(t),\beta(t)=5.$$

图9为各节点输出示意图, 表4为相应实验结果.



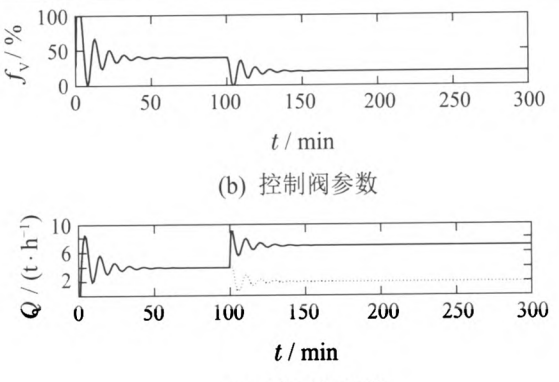


图 9 攻击流量仪

Fig. 9 Attack the meter

表 4 攻击流量仪时, 实验结果统计表

Table 4 Experiment results of attacking the meter

	算法参数	实验结果
各节点状态	$\mathrm{STATE}=(1,0,1)$	
完整性攻击判断	$\mathrm{Atc_{node}}=1$ $\mathrm{rec_M}=(0,0,1)$	存在完整性攻击控制阀为恶意节点

5.3 仿真结果分析(Analysis of simulation results)

通过实验, 可以明确节点状态与恶意节点之间的关系, 如表5所示.

在工控系统运行的过程中, 无法避免地将受到外部扰动的影响, 因此, 各节点输出数据无法始终维持在某一稳定值, 但由于控制目标不变, 各节点的变化趋势总是一致的, 因此当$\mathrm{STATE}=(1,0,0)$时, 也就意味着温度传感器接收到温度上升的信号, 控制阀阀门关小, 流量也相应减小, 系统正常; 然而当各节点输出参数无法维持变化趋势一致时, 即可知当前系统内已出现完整性攻击, 并能够判断出恶意节点.

表 5 节点状态与恶意节点关系

Table 5 Relationships between nodes' states and malicious nodes

STATE	恶意节点
(0, 0, 0)	传感器
(0, 0, 1)	控制阀
(0, 1, 0)	流量仪
(1, 0, 0)	无
(1, 1, 1)	传感器
(1, 1, 0)	控制阀
(1, 0, 1)	流量仪
(0, 1, 1)	无

6 结语(Conclusions)

本文以拜占庭将军问题为理论基础, 设计了一个工控网络安全态势感知模型, 利用所提出的算法对系

统中存在的完整性攻击进行检测, 并对系统安全态势进行感知, 给出当前网络态势, 另外, 在检测到系统中存在攻击的基础上, 能对网络中的恶意节点进行判断.

实验结果表明, 本文给出的工控网络安全态势感知模型和算法, 能对系统内存在的攻击进行有效判断, 并给出恶意节点, 为安全管理人员评估网络态势及采取有效措施提供了决策依据.

参考文献(References):

[1] National Transportation Safety Board, Pipeline Accident Report. *Pipeline Rupture and Release of Fuel Oil into the Reedy River at Fork Shoals, South Carolina* [Z]. Washington, DC, Report PB98-916502/NTSB/PAR-98-01, 1996.

[2] CHEMINOD M, DURANTE L, VALENZ ANO A. Review of security issues in industrial networks [J]. *IEEE Transactions on Industrial Informatics*, 2013, 9(1): 277 – 293.

[3] WANG Yongqiang, YE Hao, WANG Guizeng. Recent development of fault detection techniques for networked control systems [J]. *Control Theory & Applications*, 2009, 26(4): 400 – 409.
(王永强, 叶昊, 王桂增. 网络化控制系统故障检测技术的最新进展 [J]. 控制理论与应用, 2009, 26(4): 400 – 409)

[4] FANG H J, YE H, ZHONG M Y. Fault diagnosis of networked control systems [J]. *Annual Reviews in Control*, 2007, 31(1): 55 – 68.

[5] AUBRUN C, SAUTER D, YAME J. Fault diagnosis of networked control systems [J]. *International Journal of Applied Mathematics and Computer Science*, 2008, 18(4): 525 – 538.

[6] MAO Z H, JIANG B, DING S X. A fault-tolerant control framework for a class of nonlinear networked control systems[J]. *International Journal of Systems Science*, 2009, 40(5): 449 – 460.

[7] WANG Yanan. *Deceptive attack and information security protection of process control system* [D]. Shanghai: East China University of Science and Technology, 2014.
(王亚楠. 过程控制系统欺骗攻击与信息安全防护 [D]. 上海: 华东理工大学, 2014.)

[8] GUO Ming. *Researches on performance monitoring and fault diagnosis for process industry based on data-driven technique* [D]. Hangzhou: Zhejiang University, 2004.
(郭明. 基于数据驱动的流程工业性能监控与故障诊断研究 [D]. 杭州: 浙江大学, 2004.)

[9] BASS T, GRUBER D. A glimpse into the future of id[EB/OL]. http://www.usenix.org/publications/login/1999-9/features/future.html, 1999.

[10] NADERPOUR M, LU J, ZHANG G Q. An intelligent situation awareness support system for safety-critical environments [J]. *Decision Support Systems*, 2014, 59: 325 – 340.

[11] LU J, LIU B, ZHANG G, et al. A situation assessment approach using support vector machines as a learning tool [J]. *International Journal of Knowledge Management Studies*, 2008, 3(1): 82 – 97.

[12] BRANNON N G, SEIFFERTT J E, DRAELOS T J, et al. Coordinated machine learning and decision support for situation awareness [J]. *Neural Network World*, 2009, 22(3): 316 – 325.

[13] CHAI H, WANG B. A hierarchical situation assessment model based on fuzzy Bayesian network [C] *//Artificial Intelligence and Computational Intelligence (AICI)*. Taiyuan, China: Springer-Verlag, 2011: 444 – 454.

[14] NADERPOUR M, LU J. A fuzzy dual expert system for managing situation awareness in a safety supervisory system [C] *//The 21st IEEE International Conference on Fuzzy Systems*. Brisbane, Australia: IEEE, 2012: 715 – 721.

[15] CARDENAS A A, AMIN S, LIN Z S. Attacks against process control systems: risk assessment, detection, and response [C] *//Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*. Hong Kong, China: ACM, 2011: 355 – 366.

[16] ARNOLD C, BUTTS J, THIRUNARAYAN K. Detecting integrity attacks on industrial control systems [J]. *IFIP Advances in Information and Communication Technology*, 2014, 441: 3 – 13.

[17] YANG C K, ALEMI A, LANGARI R. Sensor fault detection and isolation using phase space reconstruction [C] *//American Control Conference (ACC)*. Chicago, IL, USA: IEEE, 2015: 892 – 899.

[18] HUANG Y L, CARDENAS A A, AMIN S, et al. Understanding the physical and economic consequences of attacks on control systems [J]. *International Journal of Critical Infrastructure Protection*, 2009, 3(2): 73 – 83.

[19] DAI Liankui, YU Ling, TIAN Xuemin, et al. *Process Control Engineering* [M]. Beijing: Chemical Industry Press, 2012.
(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.)

作者简介:

陆耿虹 (1992–), 女, 博士研究生, 目前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;

冯冬芹 (1968–), 男, 教授, 目前主要研究方向为现场总线、实时以太网、工业控制系统安全以及网络控制系统的研发与标准化, E-mail: dqfeng@iipc.zju.edu.cn.