

基于关联图模型的信息物理融合系统感知数据可信性分析

汤巍* 景博 黄以锋

(空军工程大学航空航天工程学院 西安 710038)

摘要: 针对信息物理融合系统(CPS)感知层数据的不确定性与随机性, 该文提出一种 CPS 中感知数据的可信性分析框架。摒弃以往以传感器为中心的建模思路, 该文充分考虑被监测对象因素, 建立传感器-目标关联图模型, 以此为基础设计了传感数据可信性推理算法。同时, 为提高算法的实时性, 减少传感器-目标关联图的搜索空间与时间, 设计了基于可信目标筛选的改进推理算法。通过实例验证表明, 该算法能实时、有效地滤掉 CPS 中感知数据中的虚假信息, 极大提高感知数据的可信性。

关键词: 信息物理融合系统; 感知数据; 可信性分析; 关联图

中图分类号: TP301; TP212

文献标识码: A

文章编号: 1009-5896(2015)03-0679-07

DOI: 10.11999/JEIT140437

Credibility Analysis of Sensor Data in the Cyber-physical System Based on the Relationship Diagram Model

Tang Wei Jing Bo Huang Yi-feng

(Aeronautics and Astronautics Engineering College, Air Force Engineering University, Xi'an 710038, China)

Abstract: The high uncertainty and randomness are the characteristics of the sensor data in the Cyber-Physical Systems (CPS), which make the data unreliable. A credibility analysis framework is proposed to solve those problems. Abandoning the idea that the sensor is the center in modeling, the theory takes monitoring targets into consideration and constructs the sensor-target relationship diagram, which is the base of the credibility reasoning algorithm. Meanwhile, in order to reduce the space and time of searching the relationship diagram, an improving reasoning method basing on filtering the incredible targets is designed. The examples demonstrate that the proposed algorithm can filter out the false message in the sensor data and enhances the credibility of the data in CPS.

Key words: Cyber-Physical System (CPS); Sensor data; Credibility analysis; Relationship diagram

1 引言

信息物理融合系统(Cyber-Physical System, CPS)是一个集成物理设备和信息组件的智能分析系统, 能够对物理世界中的动态变化做出实时响应^[1]。CPS 通过部署的传感器网络获取大规模的物理世界数据, 并针对不同的应用领域, 将这些数据用于实时分析、控制。CPS 的前景被广泛看好, 可以应用于智能交通^[2]、智能医疗^[3]、智能电网^[4]和战场监视^[5]等领域。所以, CPS 研究得到了美国、欧洲、日本、中国等许多国家的专家学者的广泛关注^[6-8]。

目前, 虽然众多学者关于 CPS 的准确概念与内

涵还有分歧, 但是都认为 CPS 是计算、通信、控制与物理系统融合的产物, 且应该具有可靠性、分布性、实时性、自治性等共有特征^[9]。一个可靠的 CPS 必须具有很高的可信度。然而由于传感系统本身故障及可能出现的突发事件使 CPS 所获取的传感数据具有较大的随机性和不确定性, CPS 获得的海量数据既包含所需要的可信数据也混杂着可能引发虚警的虚假数据。因此, 数据的可信性问题已经成为制约 CPS 应用的主要瓶颈问题之一。总结起来其面临的困难主要有以下几个方面:

(1)数据规模巨大。一个 CPS 的感知层可能包含成百上千个传感器的异构传感器网, 会产生海量的数据。CPS 的数据处理系统需要在实时、高效处理大量的数据。

(2)传感数据混杂噪声。在传感器数据采集过程中可能会出现各种形式的故障, 而且故障模式大多

2014-04-03 收到, 2014-08-05 改回

国家自然科学基金(51201182)和航空科学基金(20101996012)资助课题

*通信作者: 汤巍 rk1019@163.com

是不可预测的。文献[10]指出,加州大学伯克利分校部署在大鸭岛上用于生态环境监测的传感器系统大约有 60%的数据是错误的。文献[11]指出,传感器采集的数据只有少于 49%的信息是有效的。不可靠的噪声数据是制约 CPS 应用的主要因素之一。

(3)传感数据之间的相悖。一个可靠的 CPS 感知层应有合理的冗余度。例如,每个监测区域至少被 k 个传感器覆盖^[12]。当其中一个或几个传感器出现故障时,故障传感器提供的信息会与其他可靠传感器提供的信息发生矛盾。由于用户并不知道哪个传感器的数据是可信的,所以系统从矛盾的数据中推断出正确的结果是很困难的。

(4)缺乏有效的训练数据。传统的数据分析方法大多是基于有监督学习的方式进行的,即需要大量的训练数据,而这种方法在 CPS 中实现起来非常困难且由于大量的随机因素很容易产生错误。

(5)目标的不确定性。由于硬件条件的限制,大部分传感器只能采集 CPS 中目标的部分信息或某一方面的信息,不可能提供 CPS 所需的完备信息,因此系统需要通过整合从多种传感器获取的各种信息来估计目标的整体信息,这大大增加了传感数据的不确定性。

在传感器网络和过程控制领域,已有关于传感器故障数据检测方面的研究。但是 CPS 不同于传统的传感器网络。首先,CPS 通常包括更多的传感器,监测的领域更大,这些传感器通过各种异构无线网络连接,会产生更多的随机因素。而且传统传感器网络的输入通常是定义好的并且是可控的。而 CPS 中的传感器是用来感知物理世界的自然现象或者监测人类的行为。由于监测目标的不确定,导致传感器行为和数据故障建模中存在较高的不确定性。近年来,一些学者提出用数据挖掘理论解决该问题。比较有代表性的方法是基于邻域相似性假设条件^[13],即一个传感器的数据应与其临近的 k 个传感器数据相似。但是有时被监测目标并不处于邻域传感器的监测范围,因此这种假设会导致一定程度的系统误判。

针对上述 CPS 中数据可信性问题,本文摒弃以往以传感器为中心的建模思路,提出了一种新的 CPS 中传感数据可信性分析框架,充分考虑被监测目标因素,建立传感器-目标关联图模型,以此为基础设计了数据可信性推理算法。同时,为提高算法的实时性,减少搜索传感器-目标关联图的空间与时间,设计了基于可信目标筛选的改进推理算法,极大地提高了 CPS 中传感数据可信性分析效率。

2 问题分析与定义

一个 CPS 会根据任务不同在区域内部署各种传感器,例如红外传感器、超声传感器、表面波传感器等,尽管它们的传感机理与测量方法不同,统一用函数 $R(s,t)$ 来表示传感器 s 在时刻 t 检测到的信号强度,显然, $R(s,t)$ 是关于目标与传感器距离和传感器类型的函数^[14], $R(s,t) = f(\text{dist}(s,o),\Omega(o))$ 。

令 $R = \{R(s_1,t_1),R(s_2,t_2),\dots,R(s_m,t_n)\}$ 为传感器网络产生的数据集。设置安全阈值为 δ_s ,当 $R(s,t) > \delta_s$ 时,传感器会发出告警信息,用 $R_a(s,t)$ 表示。显然,在 CPS 中传感器产生的 R_a 数据集是整个感知层采集到的数据集 R 的一个子集,即 $R_a \subset R$,相比于 R 中的正常样本数据, R_a 是用户重点关注的传感数据集,这也是本文的研究对象。但由于受到外界干扰因素或传感器系统本身故障的影响, R_a 中也必然存在大量导致虚警的虚假信息。

定义 1 在 R_a 数据集中,定义传感数据的可信度为将 $R_a(s,t)$ 表示正确信息的概率,用 $\tau(R_a(s,t))$ 表示。

CPS 中的传感器不可能提供目标的完备信息,通常情况下,传感器的检测范围是一个以传感器为中心的圆。一些特殊的传感器可以缩小目标位置的范围,比如距离传感器可以估计与目标之间的大致距离,方位传感器可以估计目标的大致方向。如果将几种传感器结合起来可以使目标定位的精度会有所提高,但是在 CPS 中同时部署距离传感器和方位传感器会消耗系统的大量能源,使经济成本显著增加,系统的整体可靠性降低,而且它们也会受到噪声干扰,应用性不强。因此,本文研究的数据可信性分析方法是基于普通传感器设计实现的,可以扩展到其他特殊传感器。

定义 2 定义目标可信性为对用户来说有价值目标 o 真实存在的概率,用 $\tau(o)$ 表示。值得注意的是,这里定义的可信目标必须是对用户来说有价值的目标。

定义 3 定义一个传感器所检测到的目标集为 O_s ,显然 $O_s = \{o \mid o \in O, \text{dist}(s,o) < d_s\}$ 。其中, d_s 表示传感器 s 的检测范围, $\text{dist}(s,o)$ 表示传感器 s 与目标 o 之间的距离。

同理,定义检测到目标 o 的传感器集为 S_o ,则 $S_o = \{s \mid s \in S, \text{dist}(s,o) < d_s\}$ 。

3 传感数据可信性分析框架

3.1 传感器-目标关联图模型

在 CPS 中,传感器的类型和检测范围是已知的。通过分析可知,一个传感器的数据可能与多个

目标有关，同时一个目标可能被多个传感器检测到。因此，可以构建传感器与目标的关联关系图，在传感器-目标关联图上，一组节点表示传感器及其数据，另一组节点表示目标，两者的连线表示检测关系，其权重表示由该目标引起相应传感器告警的可能性，即条件可信概率 $\tau(R_u(s_i, t) | o)$ 。

根据现有的工艺水平，解决传感器网络的目标定位问题普遍应用的是基于采样理论的方法，即设一个传感器的检测范围包含 N 个点，采样率为 l ，根据采样算法则有 $n = l \times N$ 个可能的目标位置^[15]。图 1 显示了某仓库监视网络的拓扑图，该监测网络包含 34 个传感器，其中 6 个传感器发出了告警信息。图中虚线标注了告警传感器的检测范围，以及确定的 10 个可能目标位置。

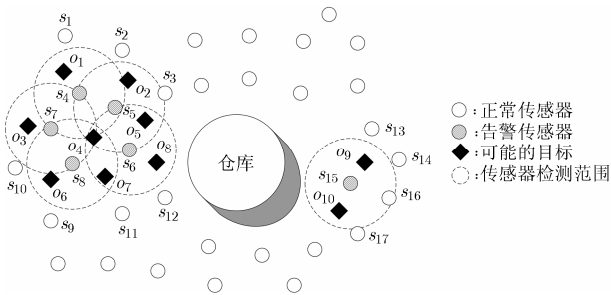


图 1 某仓库监视网络的拓扑图

将该监测网络抽象成传感器-目标关联图模型如图 2 所示。

图 2(a) 图表示各目标及其传感器集，其中带左斜线的圆形节点表示产生告警信息的传感器，其他圆形节点表示产生正常信息的传感器，菱形节点表示可能的目标。传感器-目标关联图如图 2(b) 图所

示，图中虚线代表和目标相关的正常传感器信息，实线代表与目标相关的告警传感器信息。例如，可能目标 o_9 的传感器集为 $S_{o_9} = \{s_{13}, s_{14}, s_{15}, s_{16}\}$ ，其中 s_{15} 产生了告警信息 $R_u(s_{15}, t)$ ；同时由于 s_{15} 传感器的目标集为 $O_{s_{15}} = \{o_9, o_{10}\}$ ，即 $R_u(s_{15}, t)$ 不仅与 o_9 有关，也与 o_{10} 有关。

3.2 可信性推理算法

分析传感器-目标关联图，确定目标可信性推理算法为：

步骤 1 根据传感器-目标关联图，确定与每一个可能目标相关的传感器集 S_o 。传感器集中包含两类传感器，一类是告警传感器，一类是正常传感器。

步骤 2 对各个传感器集中发出的告警信息数据进行一致性检验，即计算与目标 o 相关的传感器集中其他传感器如果处于告警传感器位置时所产生的数据与告警传感器产生的数据之间的差异。当两者的差异较小时，则说明该传感器发出的告警信息可信性较高。

以声传感器为例， $R(s, t)$ 可以表示成^[16]

$$R(s, t) = \begin{cases} \alpha \cdot \Omega(o) + b, & o \in \text{Area}(s) \\ b, & o \notin \text{Area}(s) \end{cases} \quad (1)$$

其中， α 是信号衰减速率，与距离的平方成反比； $\Omega(o)$ 为目标 o 的信号强度； b 为背景噪声； $\text{Area}(s)$ 表示传感器 s 的覆盖范围。

则可得目标的信号强度函数

$$\Omega_j(o) = \frac{R(s_j, t) - b}{\alpha} \propto \text{dist}(s_j, t)^2 (R(s_j, t) - b) \quad (2)$$

假设 s_i 传感器为告警传感器，则 s_j 传感器处于 s_i 传感器的位置时 s_j 传感器的期望数据值为

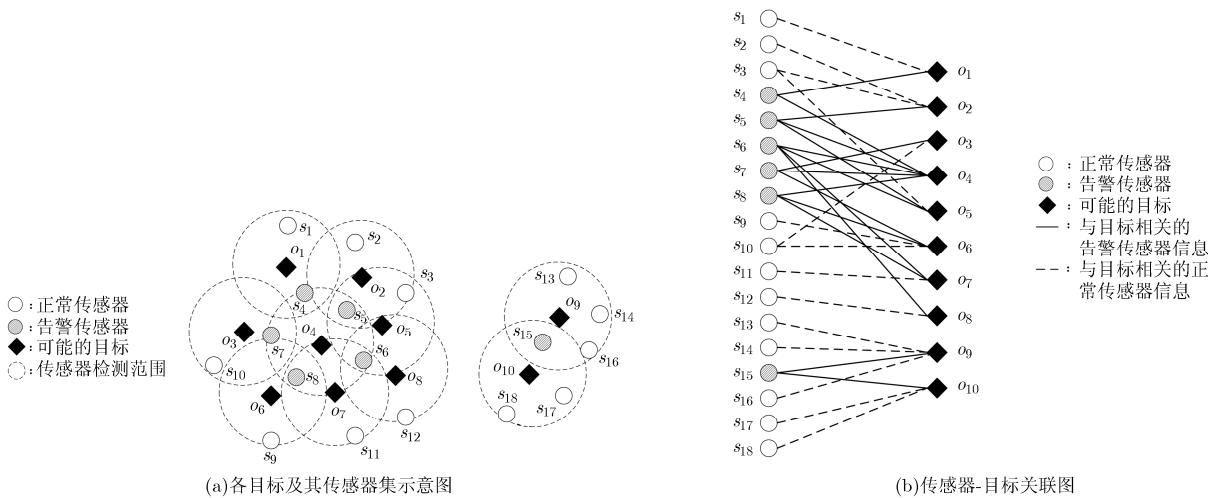


图 2 监测网的传感器-目标关联图模型

$$R'(s_j, t) = f(\text{dist}(s_i, o), \Omega_j(o)) = \frac{\text{dist}(s_j, t)^2}{\text{dist}(s_i, t)^2} (R(s_j, t) - b) \quad (3)$$

对 s_i 传感器实际数据值与期望数据值进行一致性检验:

$$\text{diff}(R', R) = |R'(s_j, t) - R_a(s_i, t)| \quad (4)$$

$$\text{coh}(R_a(s_i, t), R(s_j, t))$$

$$= \begin{cases} 1 - \frac{\text{diff}(R', R)}{\sigma}, & \text{diff}(R', R) < \sigma \\ 0, & \text{其它} \end{cases} \quad (5)$$

其中, σ 是传感器集中各传感器数据的标准差。

步骤 3 计算可能目标的条件可信概率 $\tau(R_a(s_i, t) | o)$ 和可信概率 $\tau(o)$ 。

$$\tau(R_a(s_i, t) | o) = \frac{\sum_{s_j \in R_a, s_i \neq s_j} \text{coh}(R_a(s_i, t), R(s_j, t))}{|S_o| - 1} \quad (6)$$

当条件可信概率较小时, 则说明可能有两种情况: (1) $R_a(s_i, t)$ 是一个虚假信息; (2) $R_a(s_i, t)$ 所反映的告警信息是真实的, 但并不是由目标 o 引起的。用均值法来计算可能目标的可信概率。

$$\tau(o) = \frac{\sum \tau(R_a(s_i, t) | o)}{|S_o|} \quad (7)$$

步骤 4 计算传感数据的可信概率 $\tau(R_a(s, t))$ 。一个传感器可能与多个目标发生联系, 因此也可能产生多个条件可信概率。在实际应用中, 即便仅有一个真实目标则与之联系的传感器告警信息也应该是可信的, 因此, 选择条件可信概率的最大值作为该传感器数据的可信概率值。

$$\tau(R_a(s, t)) = \max_{o \in O_s} (\tau(R_a(s, t) | o)) \quad (8)$$

可信性推理算法流程图如图 3 所示。通过分析可以发现, 设置合适的可信阈值 δ_i 是确定可信目标和可信数据的重要保证。当可信阈值设置很小(如 $\delta_i < 0.10$)时, 一些虚警信息会被误认为是真实的; 同理当可信阈值设置很大(如 $\delta_i > 0.95$)时, 一些真实信息也会被认为是虚警。设置合适的可信阈值有两种方法: 一是基于大量的历史数据, 根据数据计算结果的统计规律, 结合经验确定, 这也是比较准确的方法; 二是当没有大量历史数据时, 则根据通过阈值处理后的数据集间的方差最大原则设置阈值。一般 δ_i 的取值范围在 0.55~0.75 之间。

3.3 基于可信筛选的改进推理算法

CPS 的一个重要特征就是实时性, 因此有必要对算法的效率进行分析。推理算法是以目标为首要考虑因素的, 因此, 算法所消耗的时间也主要与目标的多少有关。可以预见的是, 当 CPS 中存在较多

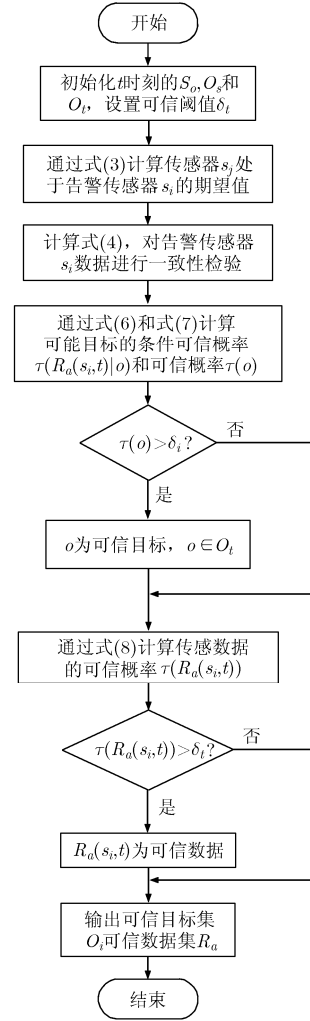


图 3 可信性推理算法流程图

且对用户来说无意义的目标时, 将严重影响算法的效率。如果能事先去掉一些可信度极低的虚假目标信息, 则算法是运算速度会明显提高。

设 S_o 为与目标 o 相关的传感器集, R_{ao} 为与目标 o 相关的告警传感器集, 由于目标 o 的可信概率范围为 $[0, 1]$, 且条件可信概率 $\tau(R_a(s, t) | o) < 1$, 推出

$$\tau(o) = \frac{\sum \tau(R_a(s_i, t) | o)}{|S_o|} < \frac{|R_{ao}|}{|S_o|} \quad (9)$$

可以确定目标 o 可信概率的上阈界为 $\tau_{\text{upp}}(o) = |R_{ao}| / |S_o|$ 。

基于以上推理, 可以改进可信推理算法。首先计算目标可信概率 o 的上阈界, 对可能的目标进行可信性筛选, 去掉可信概率的上阈界明显低于设置的可信阈值的目标, 然后再进行可信性推理。当然如果目标的筛选率为 0 时, 改进算法的复杂度与原始推理算法相同。但由于在实际应用中, CPS 感知层中存在大量低可信度的信息, 可信性筛选可以过

滤掉很多无意义的目标，将使算法的效率大大提高，具有很强的实用性。

4 实例数据分析

以前文提到的某仓库监测网络为例，首先根据图 2(b)中的传感器-目标关联图，基于可能目标传感器集数据，利用原始可信推理算法计算传感数据的可信性。和可能目标相关的原始数据如表 1 所示。

传感数据的可信性计算结果如表 2 所示。

根据仓库的历史数据规律设置可信阈值 δ_t 为 0.60，则根据计算结果可以确定， o_4 为可信目标，传感器 $s_4 \sim s_8$ 的数据为可信数据，传感器 s_{15} 的数据传递的为虚警信息，实验结论与真实情况相符，实际中，传感器 s_{15} 为阵风引起的虚警。

根据改进可信推理算法，计算各目标可信概率的上阕界，对目标进行可信性筛选，计算结果如表 3 所示。

经过筛选后，只有 o_4, o_5 和 o_7 3 个可能目标保留下来，对应的传感器-目标关联图如图 4 所示。

可以发现，图中的传感器由原来的 14 个减少到 7 个，接着利用原始推理算法可以得出 $\tau(o_4) = 0.86$ ， $\tau(o_5) = 0.32$ ， $\tau(o_7) = 0.15$ 。虽然可能目标 o_5, o_7 经过计算推理仍可确定其为不可信目标，但这已经使算法的复杂度大大降低。

经过可信筛选后，推理算法的计算时间大大缩短，由原来的 0.257 s 降至 0.017 s，极大地提高了

表 1 传感数据表

传感器(s)	相关目标(o)	传感数据
s_1	o_1	$R(s_1, t) = 2$
s_2	o_2	$R(s_2, t) = 4$
s_3	o_2, o_5	$R(s_3, t) = 3$
s_4	o_1, o_4	$R(s_4, t) = 66$
s_5	o_2, o_4, o_5	$R(s_5, t) = 67$
s_6	o_4, o_5, o_8	$R(s_6, t) = 65$
s_7	o_3, o_6	$R(s_7, t) = 90$
s_8	o_4, o_6, o_7	$R(s_8, t) = 99$
s_9	o_6	$R(s_9, t) = 4$
s_{10}	o_3, o_6	$R(s_{10}, t) = 2$
s_{11}	o_7	$R(s_{11}, t) = 4$
s_{12}	o_8	$R(s_{12}, t) = 2$
s_{13}	o_9	$R(s_{13}, t) = 3$
s_{14}	o_9	$R(s_{14}, t) = 6$
s_{15}	o_9, o_{10}	$R(s_{15}, t) = 93$
s_{16}	o_9	$R(s_{16}, t) = 9$
s_{17}	o_{10}	$R(s_{17}, t) = 2$
s_{18}	o_{10}	$R(s_{18}, t) = 5$

表 2 传感数据可信概率表

条件可信概率(目标)	目标的可信概率	条件可信概率(传感器)	传感数据的可信概率
$\tau(R_a(s_4, t) o_1) = 0.31$	$\tau(o_1) = 0.15$	$\tau(R_a(s_4, t) o_1) = 0.31$	$\tau(R_a(s_4, t)) = 0.90$
$\tau(R_a(s_5, t) o_2) = 0.21$	$\tau(o_2) = 0.07$	$\tau(R_a(s_4, t) o_4) = 0.90$	
$\tau(R_a(s_7, t) o_3) = 0.08$	$\tau(o_3) = 0.04$	$\tau(R_a(s_5, t) o_2) = 0.21$	$\tau(R_a(s_5, t)) = 0.88$
$\tau(R_a(s_4, t) o_4) = 0.90$	$\tau(o_4) = 0.86$	$\tau(R_a(s_5, t) o_5) = 0.42$	
$\tau(R_a(s_5, t) o_4) = 0.88$		$\tau(R_a(s_5, t) o_4) = 0.88$	
$\tau(R_a(s_6, t) o_4) = 0.91$		$\tau(R_a(s_6, t) o_4) = 0.91$	
$\tau(R_a(s_7, t) o_4) = 0.84$		$\tau(R_a(s_6, t) o_5) = 0.54$	
$\tau(R_a(s_8, t) o_4) = 0.79$	$\tau(o_5) = 0.32$	$\tau(R_a(s_6, t) o_7) = 0.29$	$\tau(R_a(s_6, t)) = 0.91$
$\tau(R_a(s_5, t) o_5) = 0.42$		$\tau(R_a(s_6, t) o_8) = 0.33$	
$\tau(R_a(s_6, t) o_5) = 0.54$		$\tau(R_a(s_7, t) o_3) = 0.08$	
$\tau(R_a(s_7, t) o_6) = 0.31$	$\tau(o_6) = 0.19$	$\tau(R_a(s_7, t) o_4) = 0.84$	$\tau(R_a(s_7, t)) = 0.84$
$\tau(R_a(s_8, t) o_6) = 0.26$		$\tau(R_a(s_7, t) o_6) = 0.31$	
$\tau(R_a(s_6, t) o_7) = 0.29$	$\tau(o_7) = 0.15$	$\tau(R_a(s_8, t) o_4) = 0.79$	$\tau(R_a(s_8, t)) = 0.79$
$\tau(R_a(s_8, t) o_7) = 0.17$		$\tau(R_a(s_8, t) o_6) = 0.26$	
$\tau(R_a(s_6, t) o_8) = 0.33$		$\tau(R_a(s_8, t) o_7) = 0.17$	
$\tau(R_a(s_{15}, t) o_9) = 0.12$	$\tau(o_9) = 0.03$	$\tau(R_a(s_{15}, t) o_9) = 0.12$	$\tau(R_a(s_{15}, t)) = 0.12$
$\tau(R_a(s_{15}, t) o_{10}) = 0.07$	$\tau(o_{10}) = 0.02$	$\tau(R_a(s_{15}, t) o_{10}) = 0.07$	

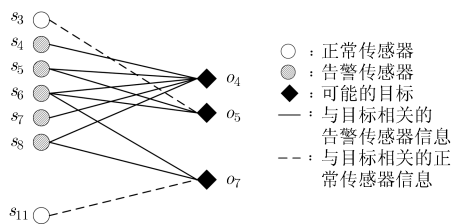


图 4 筛选后的传感器-目标关联图

表 3 可信性筛选表

可能目标(o)	可信概率上界限 ($\tau_{\text{upp}}(o)$)	保留与否	可信概率($\tau(o)$)
o_1	0.50	×	-
o_2	0.33	×	-
o_3	0.50	×	-
o_4	1.00	√	0.86
o_5	0.66	√	0.32
o_6	0.50	×	-
o_7	0.66	√	0.15
o_8	0.50	×	-
o_9	0.25	×	-
o_{10}	0.33	×	-

算法的实时性。这在传感器网络复杂、资源有限而实时性要求很高的 CPS 应用中是非常有价值的。

为进一步评估算法性能，基于某监控区内分布的 3 个传感器网络数据对算法进行验证。3 个传感网内分布的传感器数目分别为 515, 800 和 1200，监测时间为 1.5~3.0 h，传感器发送数据的频率为 0.1 Hz，同时用原始推理算法和改进推理算法对数据进行处理，计算结果如表 4 所示，计算效率如图 5 所示。可以发现，数据量最大的 D_3 中的 13920 次报警中包含高达 66% 的虚警信息，这与真实的调查结果 72% 接近。

5 结束语

本文研究了信息物理融合系统中传感数据的可信性问题，提出了传感数据可信性分析框架，构建了传感器-目标关联图模型，以关联图模型为基础设

表 4 试验数据计算结果

数据集序号	传感器数目	监测时间(h)	频率(Hz)	告警次数(次)	可信概率(%) ($\tau(R_a(s, t))$)
D_1	515	1.5	0.1	2986	66
D_2	800	2.5	0.1	6237	48
D_3	1200	3.0	0.1	13920	34

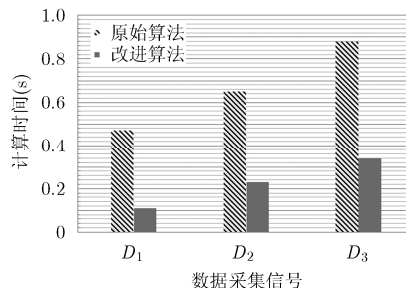


图 5 不同数据集的计算效率

计了 CPS 中传感数据可信性推理算法，并根据 CPS 实时性要求，增加可信筛选环节，对可信推理算法进行了改进，实例分析证明了该算法的正确性与有效性，为 CPS 中传感数据可信性分析提供了一种较为简单易行的解决方案。

参考文献

- [1] Barsocchi P, Chessa S, Martinovic I, et al. A cyber-physical approach to secret key generation in smart environments[J]. *Journal of Ambient Intelligence and Humanized Computing*, 2013, 4(1): 1-16.
- [2] Lukasiewicz M, Steinhorst S, Sagstetter F, et al. Cyber-physical systems design for electric vehicles[C]. Proceedings of the 2012 15th Euromicro Conference on Digital System Design, Izmir, Turkey, 2012: 477-484.
- [3] Shah A H and Syed M A. False alarm detection in cyber-physical systems for healthcare application[C]. Proceedings of the 2013 AASRI Conference on Parallel and Distributed Computing System, Bucharest, Romania, 2013: 54-61.
- [4] Adam H, Aditya A, Siddharth S, et al. Cyber-physical security testbeds: architecture, application, and evaluation for smart grid[J]. *IEEE Transactions on Smart Grid*, 2013, 4(2): 847-855.
- [5] Volkan C and Lance M. Acoustic sensor network design for position estimation[J]. *ACM Transactions on Sensor Networks*, 2009, 5(3): 21-27.
- [6] Zhenkai Z, Emeka E, and Xenofon K. A co-simulation framework for design of time-triggered automotive cyber physical systems[J]. *Simulation Modelling Practice and Theory*, 2014, 43(4): 16-33.
- [7] Mackowski A W and Williamson C H K. Developing a cyber-physical fluid dynamics facility for fluid-structure interaction studies[J]. *Journal of Fluids and Structures*, 2011, 27(5): 748-757.
- [8] 赵俊华, 文福拴, 薛禹胜, 等. 电力 CPS 的架构及其实现技术与挑战[J]. *电力系统自动化*, 2010, 34(16): 1-7.
Zhao Jun-hua, Wen Fu-shuan, Xu Yu-sheng, et al. Cyber physical power systems: architecture, implementation

- techniques and challenges[J]. *Automation of Electric Power Systems*, 2010, 34(16): 1-7.
- [9] Wu F J, Kao Y F, and Tseng Y C. From wireless sensor networks towards cyber physical systems[J]. *Pervasive and Mobile Computing*, 2011, 7(4): 397-413.
- [10] Szewczyk R, Polastre J, Mainwaring A, *et al.* Lessons from a Sensor Network Expedition[M]. *Wireless Sensor Networks*, Springer Berlin Heidelberg, 2004: 307-322.
- [11] Tolle G, Polastre J, Szewczyk R, *et al.* A microscope in the redwoods[C]. *Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems*, San Diego, USA, 2005: 51-63.
- [12] Gupta H, Zhou Z, Das S R, *et al.* Connected sensor cover: self-organization of sensor networks for efficient query execution[J]. *IEEE/ACM Transactions on Networking*, 2006, 14(1): 55-67.
- [13] Xiao X Y, Peng W C, Hung C C, *et al.* Using sensor ranks for in-network detection of faulty readings in wireless sensor networks[C]. *Proceedings of the 6th ACM International Workshop on Data Engineering for Wireless and Mobile Access*. Beijing, China, 2007: 1-8.
- [14] Tang L A, Yu X, Kim S, *et al.* Trustworthiness analysis of sensor data in cyber-physical systems[J]. *Journal of Computer and System Sciences*, 2013, 79(3): 383-401.
- [15] Isler V, Kannan S, and Daniilidis K. Sampling based sensor-network deployment[C]. *IEEE/RSJ International Conference on Intelligent Robots and Systems*, Sendai, Japan, 2004: 1780-1785.
- [16] Baumgartner K, Ferrari S, and Wettergren T A. Robust deployment of dynamic sensor networks for cooperative track detection[J]. *IEEE Sensors Journal*, 2009, 9(9): 1029-1048.
- 汤 巍: 男, 1987年生, 博士生, 研究方向为无线传感器网络、信息物理融合系统.
- 景 博: 女, 1965年生, 博士生导师, 教授, 研究方向为无线传感器网络、实时信息处理、信息物理融合系统.
- 黄以锋: 男, 1982年生, 博士, 讲师, 研究方向为无线传感器网络、信息物理融合系统.