第41卷 第6A期
2014年6月

计 算 机 科 学
Computer Science

Vol. 41 No. 6A
June 2014

一种基于 LHPN 的信息物理融合系统模型验证方法

丘 威
(嘉应学院计算机学院 梅州 514015)

摘 要 由于信息物理融合系统(CPS)的硬件集成度和软件参与度不断提高,大量软件与硬件间异构连通并相互控制,使得CPS的分析设计、建模与验证也愈加困难,由此引起模型的状态空间膨胀问题。提出利用带标记混合Petri网方法对CPS进行建模和验证研究,在CPS中采用模型检测和定理证明相结合的形式化方法,对试图解决系统验证时状态空间膨胀问题供理论依据。提出一种自动抽取及其简化模型的方法,在容错温度传感器系统中的初步实验结果表明该方法是可行的,通过一个实例原型的应用说明了该方法的有效性。

关键词 带标记混合Petri网,信息物理融合系统,建模,验证
中图法分类号 TP391.4 **文献标识码** A

Method for Verification of LHPN-based Cyber Physical System

QIU Wei
(School of Computer Science, Jiaying University, Meizhou 514015, China)

Abstract Because the cyber-physical system(CPS) hardware integration and software involvement in degree rise ceaselessly, many software and hardware have heterogeneous connectivity and mutual control. The analysis design, modeling of CPS have become more and more difficult. In this paper, a safety verification method based on labeled hybrid Petri net and differential-algebraic dynamic logic was proposed. The method firstly transforms LHPN model to differential-algebraic program, then realizas the specification of system safety using differential-algebraic program, and finally the cyber physical systems safety is verified according to differential-algebraic program reasoning rules. It is effectiveness for the method through an instance of the prototype application.

Keywords Labeled hybrid Petri net, Cyber physical system, Modeling, Verification

1 引言

信息物理融合系统(Cyber-Physical System,简称CPS)融入了先进的计算机、通信以及控制技术[1]。CPS将改变人与物理世界交互的方式并广泛应用于重要基础设施,如智能家居与机器人辅助、智能手机系统、环境监控与医疗保健和智能交通等诸多领域[2]。由于信息物理融合系统(CPS)的硬件集成度和软件参与度不断提高,大量软件与硬件间异构连通并相互控制,使得CPS的建模验证与能量控制也愈加困难,由此引起模型的状态空间膨胀问题。CPS的模型包含了硬件、软件和物理环境的各种细节以及不同系统的异构性,导致了状态空间膨胀(State Space Explosion),为系统验证带来了巨大的挑战,极大地增加了验证过程的能量成本。因此对CPS的形式化建模与验证显得非常重要。迄今为止,CPS的形式化方法的建模与验证研究成果还是较为缺乏,如布伦瑞克技术大学控制与自动化工程学院以ERTMS/ETCS规范为基础提出了一种形式化模型,选择Petri网作为一种系统设计全过程的统一的描述方法[3]。印度学者采用Z语言对ATO进行形式化建模[4]。同济大学采用Z语言对计算机联锁系统进行建模[5]。Vicaire采用形式化方法验证系统设计的正确性,提出一个控制系统的形式化模型和安全约束集,对控制算法的安全性进行了验证[11]。尽管形式化方法在不同系统中得到了很多应用,但是形式化方法在CPS中仍然有很多问题亟待解决:(1)形式化描述模型和CPS系统需求的一致性问题;(2)模型检验方法中的状态膨胀可预防可验证问题;(3)CPS时间动态验证的连续性问题。

CPS的模型包含了硬件、软件和物理环境的各种细节以及不同系统的异构性,导致了状态空间膨胀(State Space Explosion),为系统验证带来了巨大的挑战,极大地增加了验证过程的能量成本[7]。因此对CPS的形式化建模与验证显得非常重要。本文提出利用带标记混合Petri网方法对CPS进行建模和验证研究,在CPS中采用模型检测和定理证明相结合的形式化方法,对试图解决系统验证时状态空间膨胀问题提供理论依据。

2 带标记混合Petri网

混合自动机是信息物理融合系统的一个候选模型[8,9],但它们使用的变量产生了更高层次的繁琐描述。混合Petri网是另一种选择[5],但是它们使用的离散连续空间和转换导致模型生成困难。标记混合Petri网(Labeled Hybrid Petri

本文受广东省自然科学基金(S2013010013307),广东省高等学校学科专业建设专项资金(2013KJCX0171)资助。
丘 威(1974—),男,硕士,副教授,主要研究方向为软件工程、信息处理,E-mail:qiuwei@jyu.edu.cn。

Net,LHPN)模型已经被开发和应用于模拟/混合信号电路系统模型的验证,而且编译器从 VHDL-AMS 和 SPICE 中被开发出来并仿真数据[10],该模型既包括代表数字电路的布尔变量,也包括代表模拟电路的连续变量。在文献[11]中,LHPN 模型被扩展到支持离散变量,以通过描述软件变量及其表达式来检测和修改模型。这些扩展允许在一个单独的模型及其连续物理环境中表达硬件和软件。在文献[12]中已经开发了一个编译器和模型检测器,用于支持信息物理融合系统的验证的模型。

由于会产生状态膨胀问题,对信息物理融合系统的所有细节的 LHPN 模型进行验证是不可能的。本文提出了一种简化这些 LHPN 模型的自动抽取技术,基本思路是应用 LHPN 转换移除哪些与模型描述无关的细节。这些转换是通过对普通 Petri 网和时间 Petri 网的转换来激发的[5],他们也激发了用于编译器的各种静态分析技术[1],其他相关工作包括对时间化和混合自动机的减除技术[6,7,10]。

一个 LHPN 是一个 Petri 网模型,最初被开发用于表达模拟/混合信号(AMS)电路[8],最近已扩大到描述软件[12,13]。LHPN 模型是通过混合 Petri 网和混合自动机两者来激发的[3]。本文中的模型当然可以使用传统的形式化方法来描述,我们发现用这些形式化表达来开发一个自动编译器是极其困难的。因此,LHPN 模型开发制定的目标是容易生成对各类型的较高水准的信息物理融合系统的描述。一个 LHPN 是一个元组 $N=\langle P,T,Tf,B,X,V,\Delta,F,L,M0,S0,Y0,Q0,R0\rangle$:$P$ 是一个空间有限集合,T 是一个有限的变换集,$Tf\subseteq T$ 是一个有限的出错变换集,B 是一个布尔变量的有限集合,X 是一个离散的整数变量的有限集合,V 是一个连续变量的有限集合,Δ:是一个速度(频率)变量的有限集合,$V:V\rightarrow\Delta$ 是其速度(频率)的变量的映射,$F\subseteq(P\times T)\cup(T\times P)$ 是流程的关系,L 是下面定义的标签的元组,$M0\subseteq P$ 是最初标记空间的集合,$S0:B\rightarrow\{0,1,\perp\}$ 是每个布尔初值的有限集,$Y0:X\rightarrow(Z\cup\{-\infty\})\times(Z\cup\{\infty\})$ 是每个离散变量的初始值范围,$Q0:V\rightarrow(Q\cup\{-\infty\})\times(Q\cup\{\infty\})$ 是每个连续变量的初始值范围,$R0:\Delta\rightarrow(Q\cup\{-\infty\})\times(Q\cup\{\infty\})$ 是每个连续变量的速度(频率)的初始范围。

LHPNs 的特性验证和分析会导致状态空间膨胀,这种膨胀因 LHPNs 典型地有无限多个状态的因素而复杂化。因此,对 LHPNs 上的状态空间膨胀的处理,就是对这种无限多个状态必须由一个具有有限多个凸状态的等价类(称为状态集)来表达。特别是,这种状态集应用区域的描述采用差异边界矩阵(difference bound matrices,DBMs)。状态的搜索处理作为一个深度优先搜索的状态空间,它的终止不是所有的状态集被发现,就是一个故障转换被发射了。然而,应当指出,为 LHPNs 的状态空间搜索是不可判定的,所以它实际上可能不会终止。有关状态搜索的方法的详细资料已在较早的文献[8,12]中探讨过。由手工构造 LHPN 模型是相当繁琐乏味的。为了解决这个问题,我们已经开发了一个从高级别描述映射到低级别 LHPN 模型的编译器。一个信息物理融合系统的一个 LHPN 模型由 3 部分组成:硬件(模拟和数字)、软件和物理环境。硬件和物理环境模型趋向于更稳定和更可复用性。例如,一个微控制器可以被复用在任何使用该微控制器的系统中。另一方面,软件在任一系统中是独特的,可能被更新,也可能轻易被修改等等。在一些高级语言上开发软件,然后将其编译成微处理器的汇编语言或直接编译成微处理器执行的指令。精确的时序分析对信息物理融合系统的正确处理往往是至关重要的。在软件开发中这种信息使用高级语言是不可靠的,因此我们的分析必须集中在单个指令时序被理解的汇编语言水平上。然而,高级语言的编译器是利用汇编语言输入到我们的编译器来处理的。我们的编译器作为输入一个语言的定义来定义每个指令如何映射到 LHPN 结构和如何使用这个语言来处理的一个描述。语言的定义只需要为每个类型的处理构造一次。使用这个定义,编译器直接把每个指令转换成 LHPN 的一部分,然后封装在一起成为一个完整过程的模型。已经开发了这些结构来表达子程序、中断和线程,使用这些建模方法和细节参考文献[13]。

3 模型验证实例

一个典型的信息物理融合系统的示例是核反应堆的冷却系统,在这个示例中,对反应堆堆芯的温度进行检测,当温度过高时,两个控制棒中的一个被插入反应堆堆芯冷却。在我们的例子修改的版本中,有两个温度传感器用于增加容错。在每个温度传感器周期性采样中,如果在任何时候它们俩的温度变形之间的差异很大,这种情形假设成其中之一发生故障并关闭该反应堆。这是一个很有趣的例子,因为它包含了一个与物理环境(如温度及其传感器),混合信号组件(如模拟/数字转换器(ADC))、数字组件(如单片机,即微控制器)和嵌入式软件接口(如在微控制器上运行的程序)。这种情况存在的问题是,温度在匹配时有可能出现错误或温度传感器也可能在正常运行下发生匹配出错。对于第一个问题,通常只有一个 ADC 在一个微控制器上复用同一时刻来自每一个 ADC 的样品,这也就是温度传感器同时采样的温度不完全相同的问题,第二个问题是,既然结果的比较不是在相同的装配水准的单一原子指令下完成的,可能的结果甚至来自于相同采样周期。

温度传感器的建模需要三道工序。第一个是环境模型,第二是 ADC 硬件处理器,最后是软件。为了简化描述,只有部分与温度相关的传感器被表达。这里使用 set-rate 指令作为一个能动条件的操作,忽略了控制棒,反应堆的温度被简化建模成一个三角波。温度允许以单位时间内的两个温度单位的速度下降,直到达到 2200 的值。温度允许以时间单位内两个温度单位的速度上升,直到达到的值为 9800。此时,温度又开始下降。模型中的模拟电路(低通滤波器和放大器)被封装在这个模型中,temp 的变量被作为 ADC 子系统的输入。文献[3]由于空间的限制,省略了 ADC 子系统的描述。特别地,这个模型显示 10 个操作模式中的两个,其他的相类似。该模型实现初始化和冗余温度感应器的检测,但没有实现冷却棒控制回路。然后程序忙等待,直到它接收来自 ADC 子系统的 adc-ecf 标志,显示为读自 ADCTL 寄存器的高位标志。一旦完成一个完整的周期,程序就重复读取 ADR1 和 ADR2 的内容并比较它们的值,如果是在一个容许的范围,则重复循环,如果不是,对 PORTB 写入一个错误代码和程序,从而进入一个摊位循环。注意:@fail-set 标记为如下的转换,t36,作为一个失败的转换。

大多数系统模型太复杂,以致很难在低层次细节上进行

分析，但是过高的细节也不利于属性的验证。例如，在高级语言如 C 的程序验证就省略了时间信息，但是对汇编级别软件验证就迅速导致状态膨胀。本文简略介绍几个 LHPN 转换，可以通过消除不必要的细节来简化系统模型。LHPN 转换基本上把汇编语言程序转变成更高级别的表达，同时能保持关键操作的时序。

一个转换 t 表示读取一个变量 v，如果它包含任何参考 v 甚至包含自己空作业。形式化这个定义如下：

$$reads(t,v)\Leftrightarrow(v\in \sup(En(t)) \vee \exists v'\in AV.(\neg vac(t,v') \wedge v\in \sup(AA(t,v'))))$$

注意，该函数 $sup(e)$ 返回表达式 e 中出现的所有变量的集合。许多 LHPN 转换只能应用于本地进程的变量。形式上，一个变量 v 是本地的包含转换 t 的进程，其定义如下：

$$local(t,v)\Leftrightarrow(v\in(B\cup X)\wedge\forall t'\in(T-proc(\{t\})).(\neg reads(t',v)\wedge vac(t',v)))$$

直观来说，这意味着既不是引用变量，也没有在任何其他进程中分配。某些转换只能应用于进程内写操作的本地变量。引用这些进程内的变量可以被调整，但必须保持作业时序。形式上，一个变量 v 是本地进程内写操作包含转换 t 的定义如下：

$$lw(t,v)\Leftrightarrow(v\in(B\cup X)\wedge\forall t'\in(T-proc(\{t\})).vac(t',v))$$

函数 $LW(T)=\{V\in AV|\ lw(t,v)\}$ 返回所有本地转换 t 的进程中写的变量的集合。作为一个编译和 LHPN 转换的手工制品，表达式往往被简化构造。函数 $simplify(e)$ 执行基本算术和逻辑简化，当所有操作数是常量或在某种情况下一个操作数是一个常数。当应用 LHPN 转换时，它是偶尔需要退换变量成一个表达式。函数 $replace(e,v,e')$ 退换表达式 e'，就是在表达式 e' 中产生每一个变量 v。然后应用 $simplify(e)$ 函数产生结果表达式。函数 $replace(t,v,e)$ 为所有在 AV 中的 v' 执行 $replace(En(t),v,e)$ 和 $replace(AA(t,v'),v,e)$。一个转换序列 $\rho=(t_0,t_1,\cdots,t_n)$ 定义成一个路径，如果 $\forall i\in\{0,1,\cdots,n\}((t_i\in T)\wedge((i=n)\vee(t_{i+1}\in t_i\cdot\cdot)))$，路径 $\Pi(N)$ 的集合是所有 ρ 由一个 LHPN 内流程相关的路径集合。注意，这不是一个表达式序列，而是一个图形连接定制的转换集合。本文提出的 LHPN 转换假设只适用于 LHPN 中每个进程可能有选择但无并发（如 $\forall t\in T.|t\cdot|=|\cdot t|=1$）情形。这个假设是合理的，因为编译生成的所有 LHPN 满足此性质。并发是通过通信进程的使用来实现的。

时序约束规范化方法是，本文的状态空间搜索发现状态集不是单独的状态。替换不规则的状态集是困难的。因此，它有利于用时间界限来封装一序列的行为。这可以采用时序约束规范化来延迟作业被扩大，其界限是一个给定的规范化因子 k 的倍数。然而，这是一个抽象的可达状态集，因为它引入了新的行为。可是，这是保守的没有假的发生的积极的验证结果。这个转换形式化定义如下：

（时序约束规范化），对于一个规范化因子 k，为每一个转换 t 调整延迟作业，定义如下：

1. $d_l=\lfloor d_l(t)/k\rfloor*k$

2. $d_u=\lceil d_u(t)/k\rceil*k$

在我们的例子中，$k=5$ 规范化表现良好。此值的选择，是因为它在环境转换上的延迟约束比多数在 LHPN 模型中的其他延迟偏小。

还有其他一些 LHPN 已开发的转换，但受篇幅所限这里没有相关细节。需要注意的是环境模型是不变的。

4 验证结果实验分析

实验采用更新了的 LEMA 验证工具，以支持自动编译、转换和信息物理融合系统的模型验证。在一个研究案例中，我们已经应用 LEMA 于容错温度传感器并取得几个参数值。在每种情况下，空间集数的建立、数秒内的执行（包括编译、转换和验证）、是否正确的验证等都会被报告。回想结果，由于温度传感器被假定在 LHPN 模型中完美，以致被验证的属性标明反应堆从未关闭过。

原 LHPN 验证不能超过 12 个小时且找到的状态集超过 100 万套。在 311 秒（约 5 分钟）减少 LHPN 模型及归并参数完成 35563 状态集后，取得正确的验证。一个没有经验的设计师可能会初始化 ADC 转换，并立即启动到主软件循环，LEMA 需要 0.52 秒并发现 5 个状态集以致认为这个设计是失败的。失败的原因是 ADR1 和 ADR2 采样前，它们已经从 ADC 中装载过，所以 regA 和 regB 加载了被初始化的复位值。假设一个新的微控制器被替换成一个成熟的从 8 位提高到 9 位解析度的 ADC 设计，在这种情况下没有提高解析度的误差是 ±7，影响稍大些，系统出现故障。LEMA 需要 0.79 秒，发现 945 个状态集并发现这个漏洞。不用假设，经过 32 个时钟周期获得一个转换就需要 64 周期。LEMA 在 0.38 秒内记录 38 个状态集并发现这个错误。新的实验数据能够判定温度 ±4 而不是 ±2 的变化率，适于存在的现有环境模型，读数之间的累积误差超过允许的 ±7，系统出现故障。LEMA 需要 0.41 秒和发现 32 个状态集并发现这种故障。作为最后的变动，考虑采用较低解析度的 ADC，试图纠正摆率较高的温度。这种组合被证明是成功的，需要 94.5 秒和 21787 套状态就能验证。这些结果标明，这种容错温度传感器对参数选择的正确性是相当敏感的。

结束语　本文提出了一种基于 LHPN 的信息物理融合模型验证方法。该模型的描述使用一种由汇编代码启发和 C 语言的用户定义语言开发，它们能够被自动编译成容纳硬件、软件和单一形式化环境的 LHPN 模型。采用 LHPN 转换降低了模型的复杂度，在大多数情况下都不会改变验证的结果，并在最坏的情况下不会产生错误的消极结果。这种方法被应用到一个容错温度传感器的研究案例实践中。虽然初步结果是令人鼓舞的，但今后仍然有一些有趣的研究工作。特别是，有许多额外的 LHPN 转换可以开发。抽象求精也可以自动化。最后，对多种类型的模型验证案例应进行调查研究。

参 考 文 献

[1] Zhang Li-chen. Formal Methods for Aspect-Oriented Specification of Cyber Physical Systems[C]// Communications in Computer and Information Science. Springer, 2011, 215: 316-322

[2] Zhang Li-chen. QoS Specification for Cyber-physical Systems [C]// CCIS. Springer, 2011, 215: 329-334

[3] Thacker R A, Jones K R, Myers C J, et al. Automatic Abstraction for Verification of Cyber-Physical Systems[C]// Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems. 2010: 12-21

（下转第 86 页）

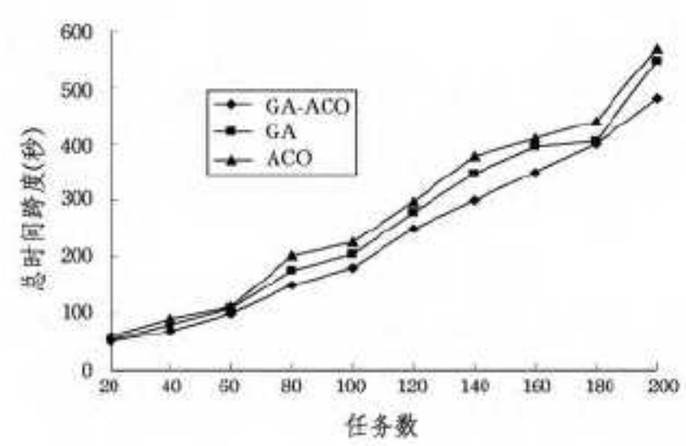

图 5　不同任务数量下的总时间跨度

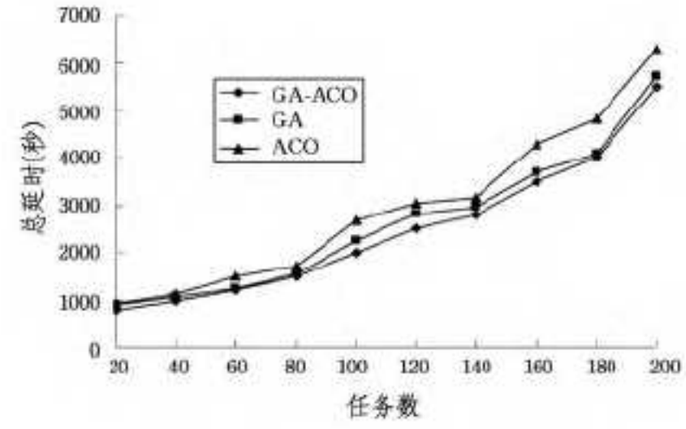

图 6　不同任务数下的总延时

从图 4—图 6 可以看出，单独使用 GA 或 ACO 进行云计算系统的任务调度问题求解，得到调度方案的任务执行总时间跨度大，用户等待的时间长，而且总费用相对较高，算法收敛效果不好。而 GA-ACO 集成了 GA 和 ACO 的优点，在寻优前期采用 GA 对云计算任务调度问题进行求解，可以较快地找到较优解，然后采用 ACO 对 GA 获得的解进行精细寻优，加快了收敛速度，获得了更加令人满意的云计算任务调度方案。

结束语　云计算具有规模大、可动态伸缩等特点，任务调度十分复杂，针对当前云计算任务调度算法存在的不足，基于组合优化理论，提出一种多群智能算法的云计算任务调度策略，仿真实验验证了 GA-ACO 在云计算任务调度求解中的有效性和正确性。

参 考 文 献

[1] 张建勋，古志民，郑超. 云计算研究进展综述[J]. 计算机应用研究，2010，27(2)：429-433

[2] 陈全，邓倩妮. 云计算及其关键技术[J]. 计算机应用，2009，29(9)：562-2568

[3] Iosup A，Ostermann S，Yigitbasi M N. Performance Analysis of cloud computing services for many-tasks scientific computing [J]. IEEE Trans. on Parallel and Distributed System，2011，22(6)：931-945

[4] Jeffrey D，Sanjay G. Map/Reduce：simplified data processing on large clusters[J]. Communications of the ACM，2008，51(1)：107-113

[5] 左利云，左利锋. 云计算中基于预先分类的调度优化算法[J]. 计算机工程与设计，2012，33 (4)：1357-1361

[6] Rochwerger B，Breitgand D，Levy E，et al. The reservoir model and architecture for open federated cloud computing [J]. IBM Journal of Research and Development，2009，53(4)：1-17

[7] 张春艳，刘清林，孟珂. 基于蚁群优化算法的云计算任务分配[J]. 计算机应用，2012，32(5)：1418-1420

[8] 李建锋，彭舰. 云计算环境下基于改进遗传算法任务调度算法[J]. 计算机应用，2011，31(1)：184-186

[9] 刘万军，张孟华，郭文越. 基于 MPSO 算法的云计算资源调度策略[J]. 计算机工程，2011，37(11)：43-48

[10] 申丽君，刘丽，陆锐. 基于改进免疫进化算法的云计算任务调度[J]. 计算机工程，2012，38(9)：208-210

(上接第 66 页)

[4] Zhang Li-chen. MDA Approach for Non-functional Characteristics of Cyber Physical Systems Based on Aspect-Oriented Method[C]// Communications in Computer and Information Science. Springer，2011，215：323-328

[5] 黎作鹏，张天驰，张菁. 信息物理融合系统(CPS)研究综述[J]. 计算机科学，2011(9)：25-31

[6] Yun H，Liang Wu-po，Rahmaniheris M，et al. A Reduced Complexity Design Pattern for Distributed Hierarchical Command and Control System[C]// Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems. 2010：42-49

[7] Parolini L，Tolia N，Sinopoli B，et al. A Cyber-Physical Systems Approach to Energy Management in Data Centers[C]// ICCPS'10. Stockholm，Sweden，2010：168-177

[8] Tan Ying，Vuran M C，Goddard S，et al. A Concept Lattice-based Event Model for Cyber-Physical Systems[C]// Proceedings of the 1 st ACM/IEEE International Conference of Cyber Physical Systems. 2010：50-60

[9] Chun I，Park J，Kim W，et al. Autonomic Computing Technologies for Cyber-Physical Systems[C]// Proceedings of the International Conference on Advanced Communication Technology. 2010：1009-1014

[10] Woo H，Yi Jiang-liang，Browne J C. Design and Development Methodology for Resilient Cyber-Physical Systems[C]// Proceedings of the 28 th International Conference on Distributed Computing Systems Workshops. 2008：525-528

[11] Vicaire P A，Hoque E，Xie Zhi-heng，et al. Bundle：A Group Based Programming Abstraction for Cyber Physical[C]// Proceedings of the 1st ACM/IEEE International Conference of Cyber-Physical Systems. 2010：32-41

[12] Ahmadi H，Abdelzaher T F，Gupta I. Congestion control for spatiotemporal data in cyber-physical systems[C]// Proceedings of the 1st International Conference on Cyber-physical Systeam(ICCPS'10). New York，NY，USA：ACM，2010：89-98

[13] Tan Ying，Vuran M C，Goddard S，et al. A Concept Lattice-based Event Model for Cyber-Physical Systems[C]// Proceedings of the 1st ACM/IEEE International Conference on Cyber Physical Systems. 2010：50-60