形式化方法与CPS自适应性

学习报告

白 洋

2017.05.05

相关论文

- [1]Towards Self-Adaptation in Real-time, Networked Systems: Efficient Solving of System Constraints for Automotive Embedded Systems (TMU,德国,后续项目为SafeAdapt)

- [2]Bersani M M, GarcA-Valls M. The Cost of Formal Verification in Adaptive CPS. An Example of a Virtualized Server Node[C]// IEEE High Assurance Systems Engineering. IEEE, 2016:39-46.（Italy，Spain）

- [3]Alur R, Henzinger T A, Vardi M Y. Theory in practice for system design and verification[M]. ACM, 2015.（Rajeev Alur）

[1][2]cps adaption问题：形式化方法 两种角度

[1]Towards Self-Adaptation in Real-time, Networked Systems: Efficient Solving of System Constraints for Automotive Embedded Systems (TMU,德国,后续项目为SafeAdapt)

解决运行时配置的问题
=>形式化建模=>转化为约束求解问题

[2]Bersani M M, GarcA-Valls M. The Cost of Formal Verification in Adaptive CPS. An Example of a Virtualized Server Node[C]// IEEE High Assurance Systems Engineering. IEEE, 2016:39-46.（Italy，Spain）

测评了formal tools 在支持在线验证方面对利弊

［1］［2］均用形式化方法，但两种角度研究cps adaption的问题。

[3]关于形式化方法

- 好的设计方法学和设计工具能够辅助开发者、使其以合理的成本/代价构建出高可信的软硬件。

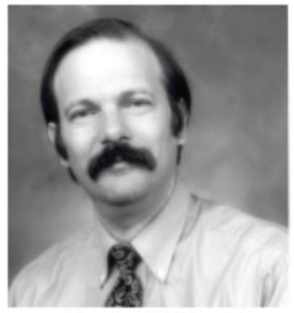
- 对设计方法学和设计工具的研究一直是计算机科学的中心主题之一。

实践中的理论 *for* 系统设计及验证 简版

ACM SIGLOG News 46 January 2015, Vol. 2, No. 1 （白洋 译 简化版）

Rajeev Alur
Univ. of Pennsylvania

Thomas A. Henzinger
IST Austria



Moshe Y. Vardi
Rice University

为此, 形式化方法(formal methods)研究关注两个互补的目标:
1)提供数学抽象以对设计的复杂性进行管理；
2)研发分析工具 (analysis tools)，用以检验系统的实现 (implementation) 是否可按照设计需求正确地工作。

[1][2]cps adaption问题：形式化方法 两种角度

[1]Bersani M M, GarcA-Valls M. The Cost of Formal Verification in Adaptive CPS. An Example of a Virtualized Server Node[C]// IEEE High Assurance Systems Engineering. IEEE, 2016:39-46.（Italy，Spain）

通过实验，测评了formal tools 在支持在线验证方面对利弊（以一个松耦合的cps系统为例）

[2]Towards Self-Adaptation in Real-time, Networked Systems: Efficient Solving of System Constraints for Automotive Embedded Systems (TMU,德国,后续项目为SafeAdapt)

解决运行时配置的问题=>形式化建模=>转化为约束求解问题

［1］的主要贡献在于形式化建模；。。。？一个点

［2］的主要工作在于对形式化工具在支持在线验证方面的利弊测评，是一整套的实验，包括系统概念模型，自适应性建模、验证、测评。。。一整套 practical

这两个文献中讨论的CPS adaption问题：就是**计算资源在线分配的问题**

文献[1]合理形式化建模以快速求解约束问题

- This is the first paper to show an efficient computation of system constraints (in a few seconds) for realistic embedded, networked systems
- 快速计算有效放置（某软件组件->放置在某个ECU上）
- 约束：内存和硬件限制、任务调度和时间依赖性
- 一个模型（使得问题简化）+两种方法（求解不难）
  - 真实的汽车功能数据

将问题转化为一个可解决的形式
利用**SAT求解器**

Model

- 简化却不简单（说明本文的工作量工作难度）
  - 相比那些专一考虑一种约束的模型，我们的模型是简化的
  - 简化是为了快速计算
  - 但我们模型同时考虑所有约束，
  - 即使这样仍然有超过2milion的变量以及126k个方程。

并不是严格意义上系统建模或系统性质建模，只是利用了其概念 工具

因实时嵌入式系统有自己的特殊需求，故已有自适应研究不适用。在这些约束中，我们考虑了内存和硬件限制，也考虑了任务调度和时间依赖性。
目标：有效地找到软件组件的一种正确放置，即使这些单独约束中的大多数都是高度难解决的(NP完全问题)。
这个问题的解决是运行时自适应的先决条件，可用作系统优化、扩展、错误处理。

Towards Self-Adaptation in Real-time, Networked Systems: Efficient Solving of System Constraints for Automotive Embedded Systems

有效解决 汽车嵌入式系统的系统约束

Marc Zeller, Christian Prehofer, Gereon Weiss, Dirk Eilers, Rudi Knorr
Fraunhofer Institute for Communication Systems ESK
Munich, Germany
{marc.zeller, christian.prehofer, gereon.weiss, dirk.eilers, rudi.knorr}@esk.fraunhofer.de

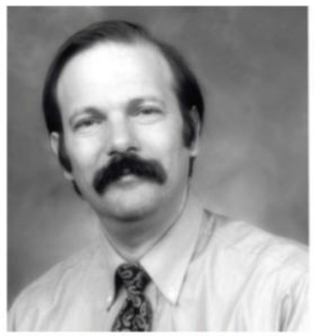
[3]关于形式化方法

- [3]Alur R, Henzinger T A, Vardi M Y. Theory in practice for system design and verification[M]. ACM, 2015.（Rajeev Alur）

Theory in Practice for System Design and Verification

Rajeev Alur
Univ. of Pennsylvania

Thomas A. Henzinger
IST Austria



Moshe Y. Vardi
Rice University

- 介绍了形式化方法在工业上的成功案例：源于学术研究且根植于理论基础的一些*ideas*是如何发展为工业界及其他领域的成熟的工具和方法学的

- 总结了形式化方法未来研究方向

Published in:
SIGLOG · Newsletter
ACM SIGLOG News archive
Volume 2 Issue 1, January 2015
Pages 46-51
ACM New York, NY, USA
table of contents doi>10.1145/2728816.2728827

[3]关于形式化方法

- 成功案例：

- **约束求解器（Constraint Solvers）**

- **硬件设计自动化（Hardware Design Automation）**

- **时序逻辑模型检验（Temporal Logic Model Checking）**

- **软件分析（software analysis）**

- **CPS系统形式化建模CPS(Formal Models for Cyber-Physical Systems)**

2.1 约束求解器（Constraint Solvers）

命题可满足性问题（propositional satisfiability problem）是众所周知的NP完全问题，在过去的四十年里，理解它的结构已经成为复杂性理论的中心议题之一。**在验证领域，一项并行的研究成果即是有效的SAT求解器的研发。**得益于核心算法、数据结构、决策启发（decision heuristics）的持续创新以及对当前处理器架构的充分利用带来的性能提高，目前的SAT求解器能够求解具有几千个变量的实例（instances)[12]。

逻辑可满足性问题有一个更具挑战性的形式，就是确定由命题及其他类型的变量所得出的逻辑公式的真假。比如，在线性实数运算中，输入公式由命题及实数、逻辑连接词、线性运算操作符组成。对结合不同判定程序的一般方法的理论上的理解（在线性实数运算中，将命题满足性求解器与线性不等式合取的一致性检验求解器进行集成）为SMT求解器(Satisfiability Modulo Theories,可满足性模理论)的研发铺平了道路，现在的SMT求解器已经可以在丰富的类型上`解决约束满足性问题。

现今的分析和验证工具根据源语言、验证方法学以及自动化程度的不同分为很多种，但它们均依赖于重复调用SAT或SMT求解器以进行核心的计算任务，如检验一个验证条件的正确性以及自动生成一个候选的不变量（见［3］中的判定程序和程序验证的介绍). 由于其强大的可扩展性和成熟度，**SAT和SMT求解器也被用于很多其他的方面，如规划和优化**（见［7］及smt-lib.org）。

[2]探讨工具对在线验证的支持程度

2016 IEEE 17th International Symposium on High Assurance Systems Engineering

The cost of formal verification in adaptive CPS. An example of a virtualized server node

Marcello M. Bersani
Dipartamento di Elettronica, Informazione e Bioingegneria
Politecnico di Milano
Milano, Italy
marcellomaria.bersani@polimi.it

Marisol García-Valls
Departament of Telematic Engineering
Universidad Carlos III de Madrid
Leganés (Madrid), Spain
mvalls@it.uc3m.es

- 针对一类特定的松耦合的cps。根据mobile客户端的请求，模型会change，然后验证这些备选的新模型的正确性。正确则执行 不正确则拒绝
- cps必须online地适应new situations且保持 **correct operation**
- practical exercise
- 例子：virtualized sever node　松耦合CPS

[2]探讨工具对在线验证的支持程度

Our approach is the first developed attempt, based on a dense time temporal logic, that experiments on the support of adaptation of CPS exemplified for a virtualized server design, taking a practical step to research the applicability of pure logical models in practice, for correct construction of dynamic CPS and on-line verification. It also points out the need of ad-

[2]探讨工具对在线验证的支持程度

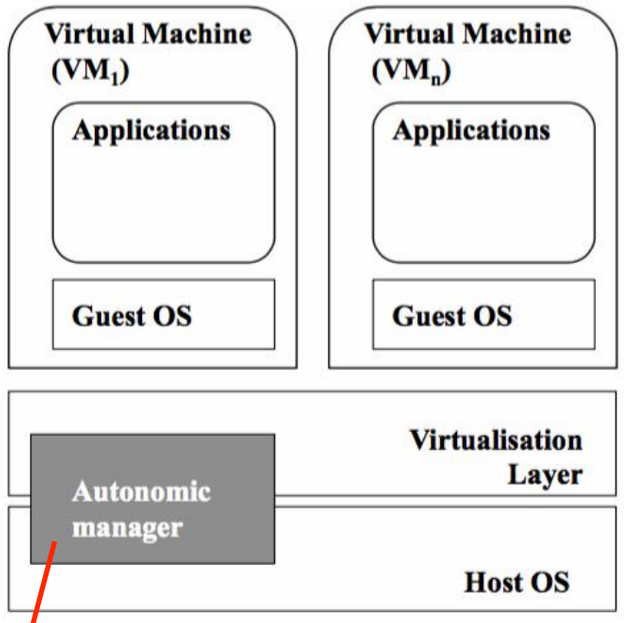


Fig. 1. *Software design of an adaptive virtualized server*

IBM提出的MAPE-K[18]自治计算模型

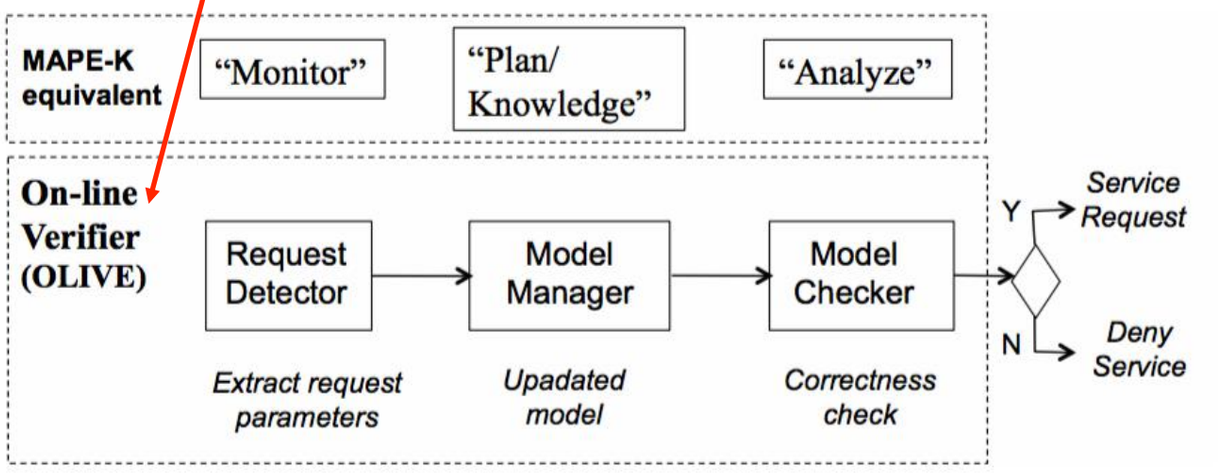


Fig. 2. *Mapping of OLIVE components to MAPE-K entities.*

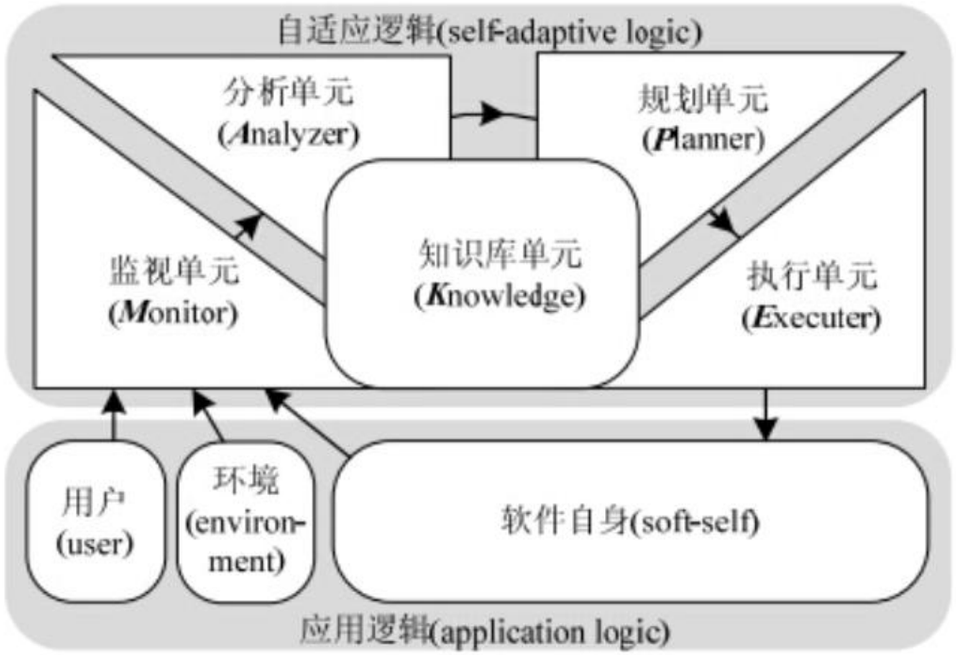


Fig. 2 Modified MAPE-K model

图 2 改进的MAPE-K模型

· 监视单元.主要关注从应用逻辑抽取属性或状态信息.

· 分析单元.主要判定系统中的错误和异常,如某一系统属性是否越限等.

· 规划单元.主要侧重于当发现系统出现问题时决定采用何种动作.

· 执行单元.关注于执行规划阶段所选择的自适应动作,对软件自身施加影响以应对变化

[2]探讨工具对在线验证的支持程度

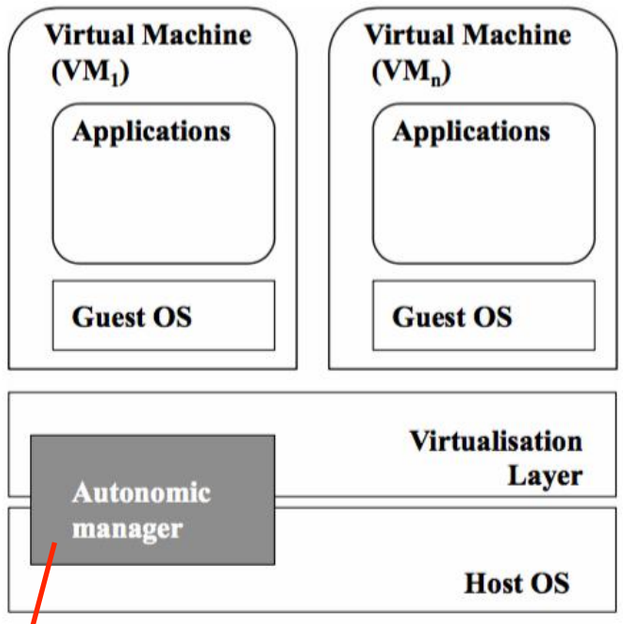


Fig. 1. *Software design of an adaptive virtualized server*

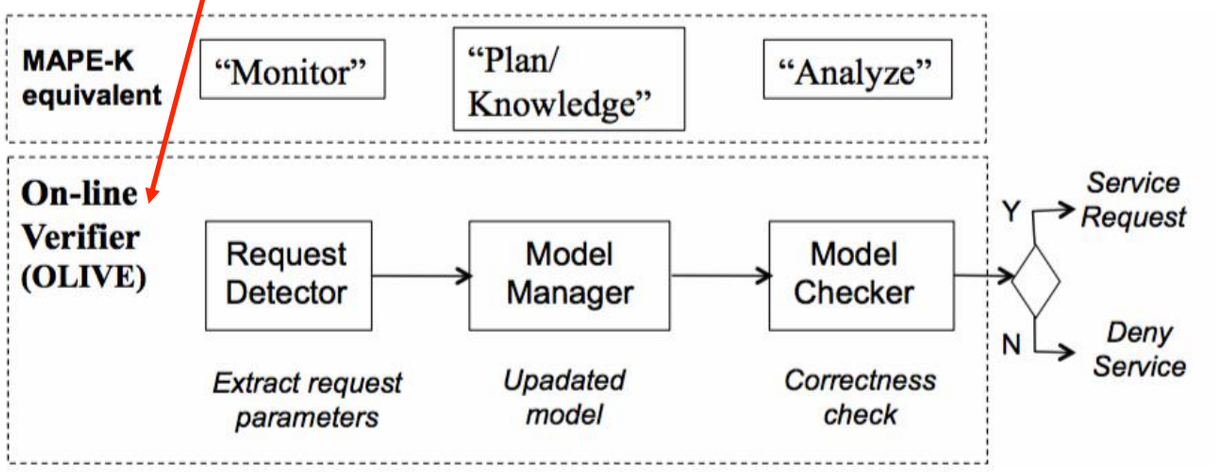


Fig. 2. *Mapping of OLIVE components to MAPE-K entities.*

等价 时间自动机

- The manager uses **CLTLoc** with dense-time clocks to model the server (an off-line model or a tentative on-line model) and the properties.

- It translates the **CLTLoc** input formula through the reduction in [4] and [5],
- and it **verifies** the satisfiability of the outcome by invoking an external **SMT-solver** (Microsoft Z3, github.com/Z3Prover/z3).

Constraint LTL over clocks (CLTLoc)
linear-time temporal logic(LTL)

[2]探讨工具对在线验证的支持程度

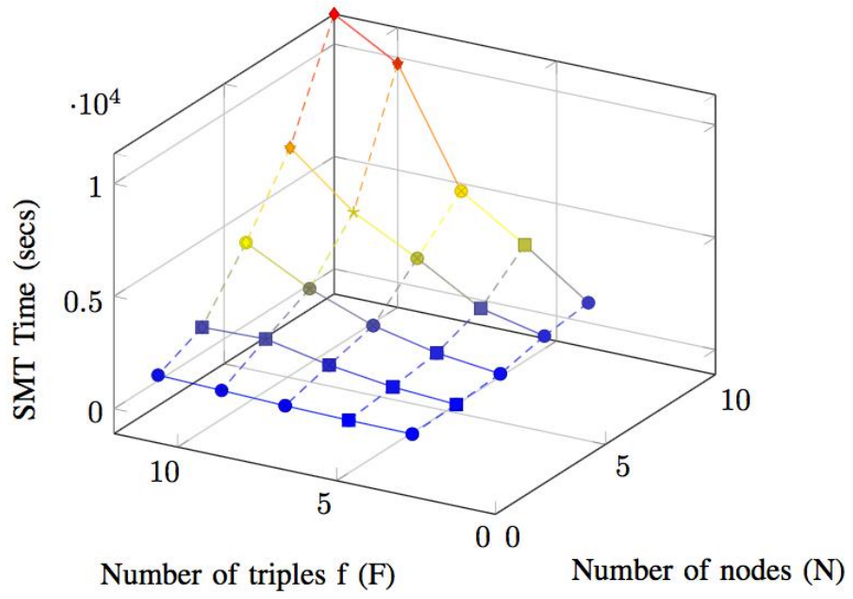


Fig. 4. SMT time (secs) w.r.t. number of nodes (N) and features f (F).

不同系统规模/问题规模VS求解时间

比较和讨论

这两个文献中讨论的CPS adaption问题：都是计算资源在线分配的问题

- ［1］如何进行形式化，使得便于在线验证
  - 基本脱离系统设计验证的流程、工具，只抽出来一点问题，手动建模
  - 将问题转化成约束求解问题
  - 依靠实验室现有的研究积累可以模仿的
- ［2］设计一个具有adaption性质的软件架构（添），用已有的形式化工具对这个自适应功能进行建模、用已有的验证工具进行验证，**测评已有的工具对adaptive 性能（时间）**的支持，
  - 纯从软件系统设计与验证的流程、角度
  - 下一步要那建模方法说事儿了？
  - 更适合松耦合cps？无标准 可发挥；不太适合汽车cps
  - 需要学习形式化理论、工具等，目前实验室积累不多

参考文献

- [1]Towards Self-Adaptation in Real-time, Networked Systems: Efficient Solving of System Constraints for Automotive Embedded Systems (TMU,德国,后续项目为SafeAdapt)
- [2]Bersani M M, GarcA-Valls M. The Cost of Formal Verification in Adaptive CPS. An Example of a Virtualized Server Node[C]// IEEE High Assurance Systems Engineering. IEEE, 2016:39-46.（Italy，Spain）
- [3]Alur R, Henzinger T A, Vardi M Y. Theory in practice for system design and verification[M]. ACM, 2015.（Rajeev Alur）
- [4]韩德帅, 杨启亮, 邢建春. 一种软件自适应UML建模及其形式化验证方法[J]. 软件学报, 2015, 26(4):730-746.
- [5]王婷. 基于自动机理论的高效模型检验算法研究[D]. 浙江大学, 2015.