Journal of System Simulation

Volume 36 | Issue 7 Article 15

7-15-2024

Modeling and Verification of Cooperative Vehicle Infrastructure System at Unsignalized Intersection Based on Time Automata

Wei Liu
School of Traffic and Transportation, Chongqing Jiaotong University, Chongqing 400074, China,
neway119@qq.com

Qirui Xiao
School of Traffic and Transportation, Chongqing Jiaotong University, Chongqing 400074, China,
m15215190891@163.com

Xinhai Chen
Chongqing Vehicle Test & Research Institute Co.,Ltd, Chongqing Engineering Research Center of Research and Testing for Automated Driving System and Intelligent Connected Vehicle, Chongqing 401122, China

Chang Rao
School of Traffic and Transportation, Chongqing Jiaotong University, Chongqing 400074, China

See next page for additional authors

Modeling and Verification of Cooperative Vehicle Infrastructure System at Unsignalized Intersection Based on Time Automata

Abstract

Abstract: Cooperative vehicle infrastructure system (CVIS) is one of the advanced solutions to enhance intersection vehicle passage safety. Due to the lack of clear specifications and standards regarding the dynamic timing and transition processes of system object state interaction in existing CVIS technologies, ensuring the safety of passage control logic is challenging. This study utilizes formal language to describe the functional logic of CVIS in unsignalized intersections, verifying the safety of system object state interaction and control logic to improve vehicle passage safety at unsignalized intersections. Simulations are conducted for scenarios including single-vehicle non-conflict, dual-vehicle conflict, and multi-vehicle conflict to identify state interactions and enable transition paths. By integrating tools and requirement specification statements for system safety attribute verification, the reliability and safety of control logic are demonstrated, providing a credible basis for developing high-security architecture for CVIS.

Keywords

urban traffic, formal language, cooperative vehicle infrastructure system (CVIS), time automata, control logic, credible verification

Authors

Wei Liu, Qirui Xiao, Xinhai Chen, Chang Rao, Yu Zhang, and Bosi Wang

Recommended Citation

Liu Wei, Xiao Qirui, Chen Xinhai, et al. Modeling and Verification of Cooperative Vehicle Infrastructure System at Unsignalized Intersection Based on Time Automata[J]. Journal of System Simulation, 2024, 36(7): 1682-1698.

第 36 卷第 7 期 系统仿真学报© Vol. 36 No. 7
2024 年 7 月 Journal of System Simulation Jul. 2024

基于时间自动机的无信号交叉口车路协同系统建模与验证

刘伟[1]，肖七瑞[1*]，陈新海[2]，饶畅[1]，张宇[1]，王博思[2]

(1. 重庆交通大学 交通运输学院，重庆 400074；
2. 重庆车辆检测研究院有限公司 自动驾驶系统及智能网联汽车技术研发与测试应用重庆市工程研究中心，重庆 401122)

摘要：车路协同系统(cooperative vehicle infrastructure system, CVIS)是提高交叉口车辆通行安全的重要解决方案之一。针对CVIS现有技术规范和标准未明确系统对象状态交互的动态时序及迁移过程，无法有效保障系统的通行控制逻辑安全问题，*采用形式化语言对无信号交叉口车路协同系统功能逻辑进行描述，验证系统对象的状态交互和控制逻辑安全，提高无信号交叉口的车辆通行安全性。*以单车无冲突、双车冲突和多车冲突场景分别进行仿真，明确状态交互和使能迁移路径；结合工具和需求规范语句进行系统安全属性验证，证明了控制逻辑的可靠性和安全性，为研发高安全架构的车路协同系统提供了可信依据。

关键词：城市交通；形式化语言；车路协同系统；时间自动机；控制逻辑；可信验证

中图分类号：TP391.9；U495　　文献标志码：A　　文章编号：1004-731X(2024)07-1682-17

DOI: 10.16182/j.issn1004731x.joss.23-0456

引用格式: 刘伟, 肖七瑞, 陈新海, 等. 基于时间自动机的无信号交叉口车路协同系统建模与验证[J]. 系统仿真学报, 2024, 36(7): 1682-1698.

Reference format: Liu Wei, Xiao Qirui, Chen Xinhai, et al. Modeling and Verification of Cooperative Vehicle Infrastructure System at Unsignalized Intersection Based on Time Automata[J]. Journal of System Simulation, 2024, 36(7): 1682-1698.

Modeling and Verification of Cooperative Vehicle Infrastructure System at Unsignalized Intersection Based on Time Automata

Liu Wei[1], *Xiao Qirui*[1*], *Chen Xinhai*[2], *Rao Chang*[1], *Zhang Yu*[1], *Wang Bosi*[2]

(1. School of Traffic and Transportation, Chongqing Jiaotong University, Chongqing 400074, China;
2. Chongqing Vehicle Test & Research Institute Co.,Ltd, Chongqing Engineering Research Center of Research and Testing for Automated Driving System and Intelligent Connected Vehicle, Chongqing 401122, China)

Abstract: Cooperative vehicle infrastructure system (CVIS) is one of the advanced solutions to enhance intersection vehicle passage safety. Due to the lack of clear specifications and standards regarding the dynamic timing and transition processes of system object state interaction in existing CVIS technologies, ensuring the safety of passage control logic is challenging. *This study utilizes formal language to describe the functional logic of CVIS in unsignalized intersections, verifying the safety of system object state interaction and control logic to improve vehicle passage safety at unsignalized intersections*. Simulations are conducted for scenarios including single-vehicle non-conflict, dual-vehicle conflict, and multi-vehicle conflict to identify state interactions and enable transition paths. By integrating tools and requirement specification statements for system safety attribute verification, the reliability and safety of control logic

收稿日期：2023-04-18　　修回日期：2023-05-31

基金项目：自动驾驶系统及智能网联汽车技术研发与测试应用重庆市工程研究中心课题(21AKC43)；重庆市交通规划研究院交通运输工程研究生联合培养基金(JDLHPYJD2018004)

第一作者：刘伟(1978-)，男，教授，博士，研究方向为交通工程、道路交通安全。E-mail：neway119@qq.com

通讯作者：肖七瑞(1998-)，男，硕士生，研究方向为交通运输规划与管理。E-mail：m15215190891@163.com

are demonstrated, providing a credible basis for developing high-security architecture for CVIS.

Keywords: urban traffic; formal language; cooperative vehicle infrastructure system (CVIS); time automata; control logic; credible verification

0 引言

无信号交叉口是一种常见的交叉口管理形式，受限于占地规模、通视距离和让行规则，其交通流常以无序状态通行，导致无信号交叉口事故频发[1]。面对随机动态的交通流，依靠传统标志控制和让行规则无法有效降低无信号交叉口的事故发生率，但随着车路协同系统应用推广，为降低无信号交叉口的事故率提供有效的解决方案。车路协同系统(cooperative vehicle infrastructure system, CVIS)作为智能交通系统(intelligent transportation system, ITS)的组成部分。在交叉口应用层面，路侧设备通过获取当前交叉路口范围内的车辆信息计算车辆路权，并下发路权或驾驶建议给车辆，优化无信号交叉口的交通[2]。CVIS 作为智能实时决策系统，在完成复杂功能时各子系统间和子系统内部需要遵守一定的事件时序逻辑顺序进行交互响应，满足通行过程中复杂逻辑和实时性能的安全需求，否则一旦系统逻辑发生紊乱失效，将会严重危及交叉口通行安全[3-6]。

从基于数据驱动的智能决策系统相关研究发现，训练数据的隐私性和质量敏感性往往会对结果造成不可预测的影响[7]，这表明相关智能决策系统安全性质保障仅仅依靠该类方法是不够的。形式化语言采用数学(逻辑)证明方法对系统及其内部要素进行建模、规约分析、推理和验证，在系统正确性与安全性保障层面具有广泛的应用[8]，其建模方式主要采用将自然语言[9]、半形式化语言[10]和领域特定语言[11]转换为形式化模型并进行形式化分析，如文献[12]以自动驾驶队列驾驶决策控制器为对象，将空间逻辑语言转换时间自动机网络模型，在UPPAAL 工具上实现并验证系统安全属性，形式化语言系统对象按特征可分为顺序系统、反应式系统等 6 种系统[13]；文献[14]提出将 B 方法与通信顺序进程(CSP)集成的形式化方法；文献[15]引入IS-DSL 特定语言来描述具体的联锁系统的参数，提出了基于随机混成自动机的形式化模型并进行安全分析；文献[16]提出一种基于标记随机 Petri 网故障模式诊断的形式化方法，对时间离散的事故系统故障进行诊断性分析并证明该方法的有效性。

从无信号交叉口控制策略层面上来看，现有的技术规范《基于车路协同的高等级自动驾驶数据交互内容》(YD/T3978-2021)[17]定义了车路协同无信号交叉口通行场景信息交互框架，但没有细化场景中信息交互的具体实现过程。文献[18]面向区域路网下无信号交叉口场景，提出一种基于时延 Petri 网建模的优化控制方法并设计两种实验分别验证该方法的有效性；文献[19]研究了混合交通的控制方法，并根据快慢变量伺服协同原理，提出一种基于逻辑的交叉口信号与车辆轨迹协同控制方法，该方法有效降低了信号绿灯启动损失时间；文献[20]根据交叉口的车路端的实时信息，建立辅助决策模型，根据判断结果对黄灯状态进行控制，缩短了保守驾驶行为造成的车辆启动延迟时间。

可以看出，当前车路协同交叉口控制策略的研究已较为深入，主要从交叉口的交通参数、车辆的行驶特性等角度进行了探究，如通行效率与行驶稳定性等。然而，现有研究鲜有从系统安全性角度考虑交叉口场景下整个车路协同系统的逻辑安全，未能针对 CVIS 无信号交叉口的控制逻辑进行探究，难以满足系统实时并发交互和安全需求。为了探究车路协同无信号交叉口场景下车辆随机到达时的系统实时控制逻辑，本文通过规范和形式化建模方法明确交叉口功能、信息交互过程和安全性质，利用 UPPAAL 工具进行仿真并验证系统安全属性，为开发车路协同系统核心控制逻辑提供可信依据。

DOI: 10.16182/j.issn1004731x.joss.23-0456

1 研究基础

1.1 无信号交叉口车路协同系统及通行场景

车路协同系统实现了将交通参与者、运载工具及交通基础设施间实时的信息交互[21]，主要包括路侧子系统(road side sub-system, RSS)、车载子系统(vehilce sub-system, VSS)以及通信技术。

RSS 指在车路协同环境下，根据交通信息和相关优化模型及算法，以安全行车为目标，制定车辆控制策略；VSS 指在车路协同环境下，通过采集车辆状态信息，使用无线通讯技术与 RSS 进行通信，实时接收 RSS 传递的车辆控制策略，实现实时调整车辆运动状态的目标[22]，工作流程如图 1 所示。

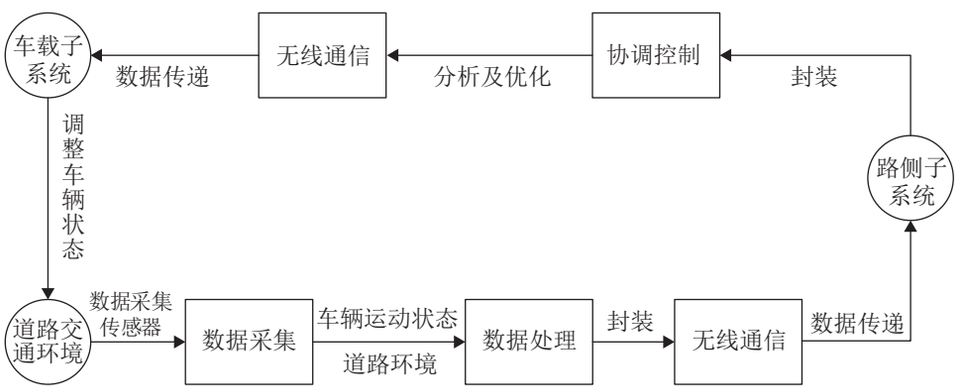


图 1 工作流程图
Fig. 1 Workflow

搭建无信号控制十字交叉口的车辆通行场景，将无信号交叉口范围的控制区域划分为接近、路权申请、进口道控制和冲突通行区域。通行权按先到先行原则分配，不同进口道路权一致；车辆遵循控制逻辑和决策规划，能及时进行减速以及停车至停车线前，如图 2 所示。

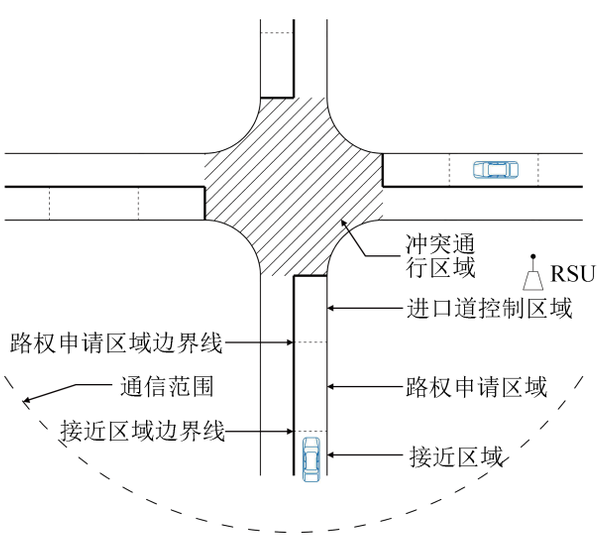


图 2 交叉口划分
Fig. 2 Intersection division

场景内控制过程：一定时段内交叉口车辆进入接近区域，进入通信范围触发环境通信，数据采集设备将车辆行驶信息实时发送给 RSS；RSS 接受并融合车辆信息后，给出当前时段车辆通行冲突情况并依照路权分配原则生成通行决策，实时通信车辆 VSS；VSS 按照通行决策进行行为控制，通行后将反馈信号给 RSS，然后对其余车辆进行上述逻辑控制，反复至该时段内所有车辆通行。

1.2 统一建模语言 UML

统一建模语言(unified modeling language, UML)专注于对事物性质、结构、状态以及事物之间的关系和状态的变化过程进行描述，具有规范化、可视化、结构化等特点，适用于从多角度对实际的系统和不同开发阶段的系统状态进行描述[23]。

UML 结合面向对象对现实系统建模，将现实中某个事物映射成对象，在计算机中利用对象和类的概念实现计算机逻辑。利用系统不同视图表

达系统的需求，该方式能提升系统的描述精度，但也使模型验证困难。由于没有严格数学(逻辑)定义，所以对于半形式化语言UML，无法进行形式化验证，为检验其正确性，可将半形式化语言进行形式化建模再通过验证工具或定理进行模型正确性验证[24]。

1.3 时间自动机理论与验证

时间自动机(timed automaton, TA)作为实时系统形式化描述和建模语言，包含时钟变量的有限状态自动机，其数学模型为[25]

$$A=<L,L_0,C,X,I,E> \tag{1}$$

式中：L为位置的集合；L_0为系统的初始位置集合；C为通道集合；X为时钟变量集合；I为每个位置上的时钟约束；E为状态转移路径$<s,a,\delta,\lambda,x>$，其中：s为初始位置，x为转移后的位置状态，a为转换触发事件，δ为使能转移条件，λ为转移后的状态集合。

UPPAAL[26]是常用的基于TA的系统建模、仿真、验证工具，常用于描述非确定的并行过程的控制系统，其构成及功能见表1。

表1 UPPAAL工具的构成及功能
Table 1 Composition and function of UPPAAL tool

主要构成	主要功能
系统编辑器	创建和编辑实时系统模型
模拟器	模拟系统模型状态迁移情况等
验证器	验证模型的功能属性

UPPAAL使用的时序逻辑公式，所属于时间分支序列逻辑(time computational tree Logic, TCTL)[27]，其规范验证语言BNF为

$$\begin{aligned}\text{Prop}::=&\text{A[ ]exp}|\text{E}<>\text{exp}|\text{E[ ]exp}|\text{A}<>\\&\text{exp}|\text{exp}\rightarrow\varphi\end{aligned} \tag{2}$$

式中：字符A表示给定的性质对于所有路径均满足；exp和φ为描述待可信验证的系统属性逻辑表达式；字符E表示给定的性质至少有一条路径满足；[]表示给定的性质对于路径上的所有状态均满足；<>表示给定的性质在路径上至少有一个状态满足，其具体逻辑BNF语法见表2。

表2 BNF语法
Table 2 BNF grammar

BNF语法	含义
E<>exp	存在路径，exp在该路径的某状态为真
E[ ]exp	存在路径，exp在该路径的所有状态为真
A[ ]exp	对于所有路径，exp在任一路径的所有状态为真
A<>exp	对于所有路径，exp在任一路径的某状态为真
exp→φ	对于所有路径，exp在任一路径的某状态为真，φ必然为真

2 车路协同系统控制逻辑建模

利用UML对车路协同无信号交叉口控制过程和时空逻辑建模描述，如图3所示，从系统控制逻辑角度进行建模验证。

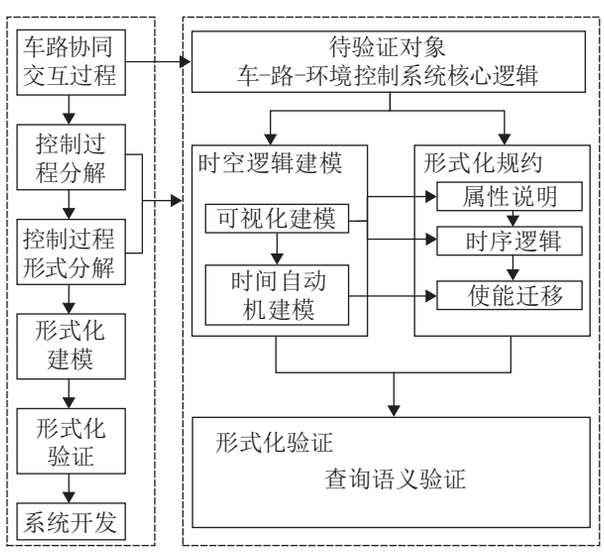


图3 控制逻辑建模总体流程
Fig. 3 Overall process of control logic modeling

根据标准YD/T3978-2021，基于车路协同的无信号交叉口通行应用场景中车路协同的车辆级别通行，进行时空逻辑可视化和时间自动机建模，其中可视化建模利用UML半形式化语言通过用例图明确系统控制逻辑框架、时序图明确系统时序交互顺序、状态图明确系统对象功能及状态；利用时间自动机建模，将半形式化语言转化为形式化模型，从而进行形式化表达，用数学逻辑描述。

DOI: 10.16182/j.issn1004731x.joss.23-0456

第 36 卷第 7 期 系统仿真学报 Vol. 36 No. 7
2024 年 7 月 Journal of System Simulation Jul. 2024

2.1 状态及交互可视化建模

采用统一建模语言，分解车辆随机到达下基于车路协同无信号交叉口通行场景，用例图明确系统控制信息，辨识系统主要信息交互内容；时序图体现系统对象之间的信息交互时间顺序；状态图界定在交互顺序中各个系统对象的功能及其状态。

2.1.1 控制信息辨识

用例图主要是用于描述系统的静态使用情况，通过分析系统外部与交互的人或物(参与者)，确定系统的对象、用例信息。描述车路协同无信号交叉口中VSS和RSS的调用关系，定义参与者和用例信息，参与者为VSS和RSS，用例信息为感知交通状况、发送车辆行驶信息、冲突判断，决策生成、运行控制、反馈控制等，如图4所示。

2.1.2 控制逻辑时序

车辆协同无信号交叉口场景下控制系统是实时动态变化的，需进行明确车辆随机到达系统对象间信息交互的时间顺序，如图5所示。

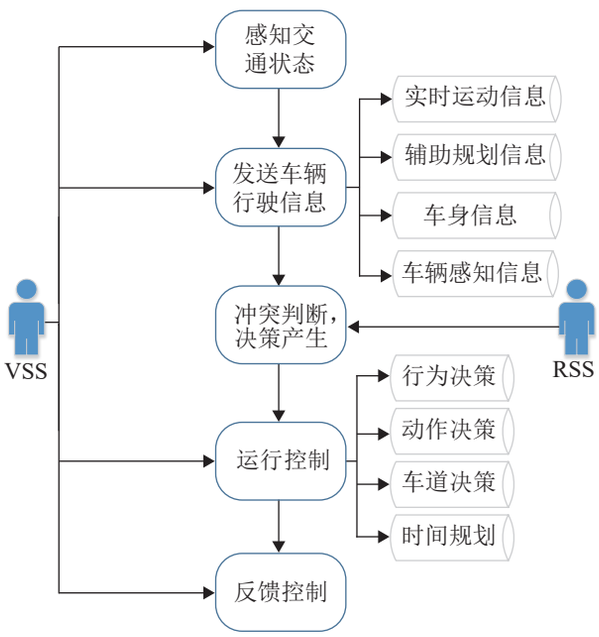


图4 系统用例图
Fig. 4 System use case

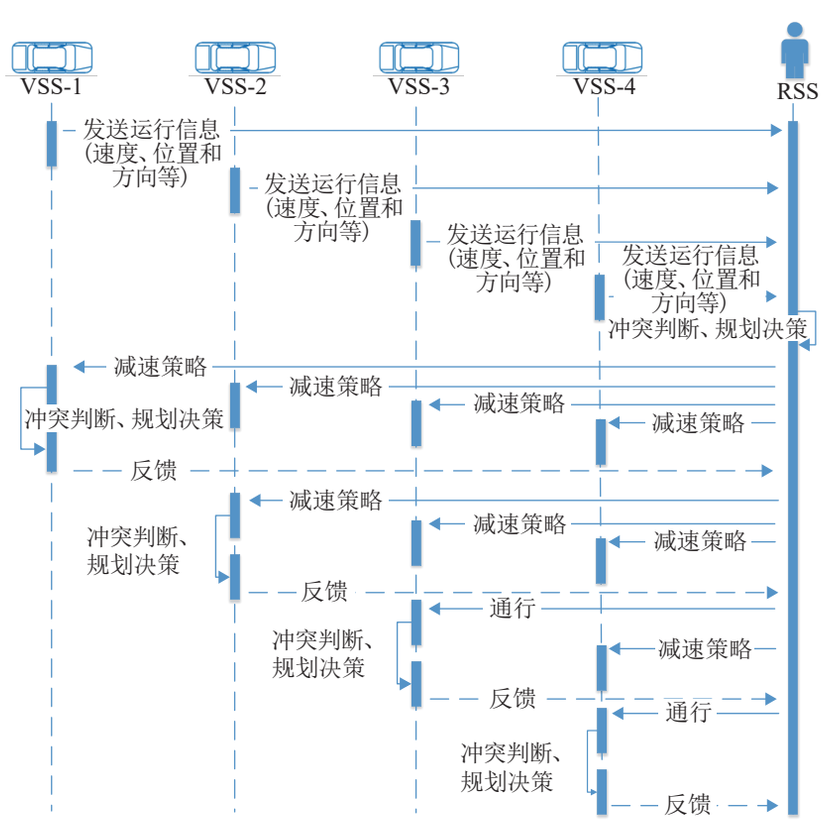


图5 系统时序图
Fig. 5 System sequence

2.1.3 对象功能及状态

当车辆 V_0 进入车路协同下的无信号交叉口，针对 VSS 和 RSS 所有状态以及存在的对象行为建立对应的状态机模型。

(1) 将 VSS 系统状态划分为安全行驶、减速行驶、减速策略和安全通行 4 个状态，如图 6 所示。

1) 安全行驶状态。执行统一速度命令。

2) 减速行驶状态。输入接收环境命令信息，执行减速和发送请求通行命令，退出发送减速策略或车辆通行命令信号。

3) 减速策略状态。输入接收减速策略命令信息，执行减速策略命令，退出加速或统一速度命令。

4) 安全通行状态。输入接收车辆通行命令信息，执行速度保持或加速命令，退出发送车辆离开命令信息。

(2) 将 RSS 系统状态划分为冲突车辆控制和无冲突通行，如图 7 所示。

1) 冲突车辆控制。输入接收车辆冲突命令信息，执行车辆通行和减速策略、接收车辆离开和离开后剩余车辆控制命令信息，退出发送剩余车辆队列命令信息。

2) 无冲突通行。输入接收车辆无冲突命令信息，执行车辆请求通行和接收车辆离开命令信息，退出发送车辆离开命令信息。

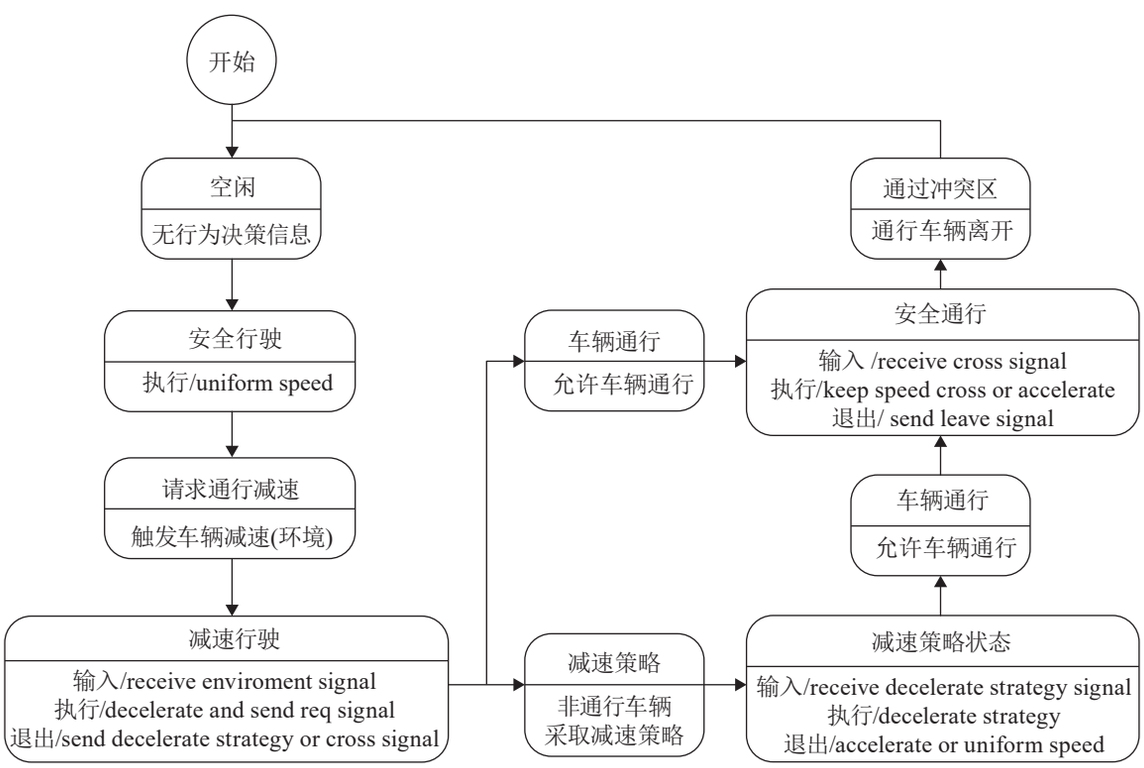


图 6 VSS 状态图
Fig. 6 VSS state

https://dc-china-simulation.researchcommons.org/journal/vol36/iss7/15
DOI: 10.16182/j.issn1004731x.joss.23-0456

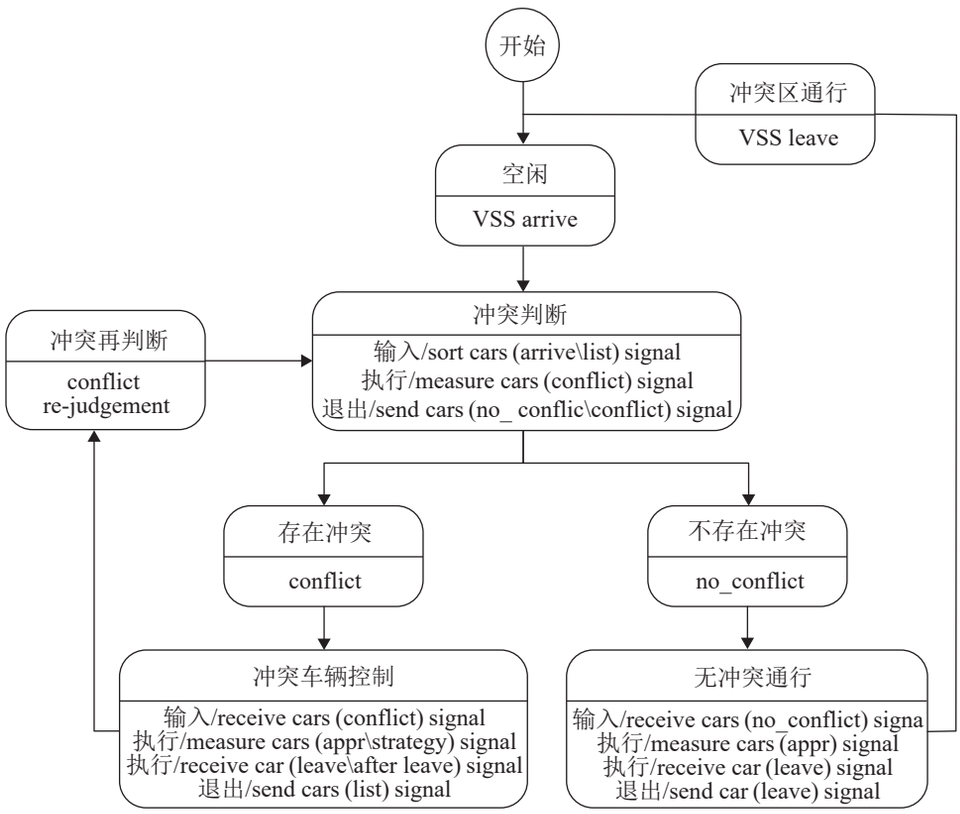


图7 RSS状态图
Fig. 7 RSS state

2.2 基于时间自动机的数学逻辑描述

基于半形式化语言对系统对象信息交互内容、时间顺序和功能及状态的界定，利用形式化语言进行转化建模，以信息交互时间顺序为通道、功能及状态为通道节点和交互内容为通道转移条件与变量，结合时间自动机语义对系统对象进行形式化规约描述建立子时间自动机，并利用UPPAAL进行数学逻辑可视化，组成时间自动机网络。

时间自动机网络主要由VSS(Carcontrol)、RSS(Roadcontrol)和环境(Envircontrol)为节点，各个通道和全局变量为路径组成，如图8所示。

2.2.1 VSS建模

当车辆进入无信号交叉口的接近区段，VSS向环境发送请求通行命令，环境受到VSS办理命令后，向RSS发送应答命令，然后RSS对VSS进行通行控制，此时检测无信号交叉口命令控制条件是否满足，根据车辆的各个状态和转移条件得到时间自动机模型Carcontrol，如图9所示。

从而得到无信号交叉口车辆控制的时间自动机六元组模型为

$$A_1 = < L, L_0, C, X, I, E > \tag{3}$$

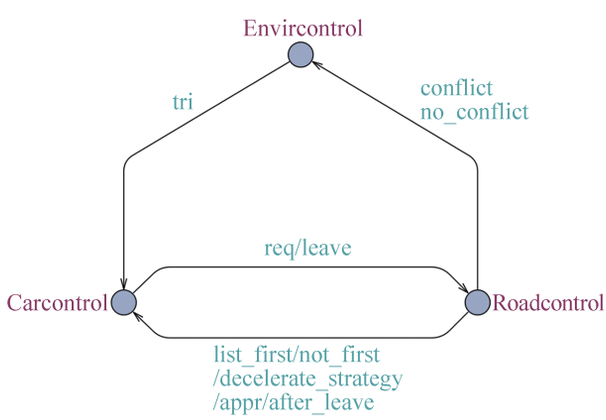


图8 时间自动机网络
Fig. 8 Time automata network

表 3 和图 9 所示为 VSS 模型的位置、通道说明。其中 clock_time 是对某些状态加以时钟约束，表示时间条件符合前提下才能进行状态迁移。

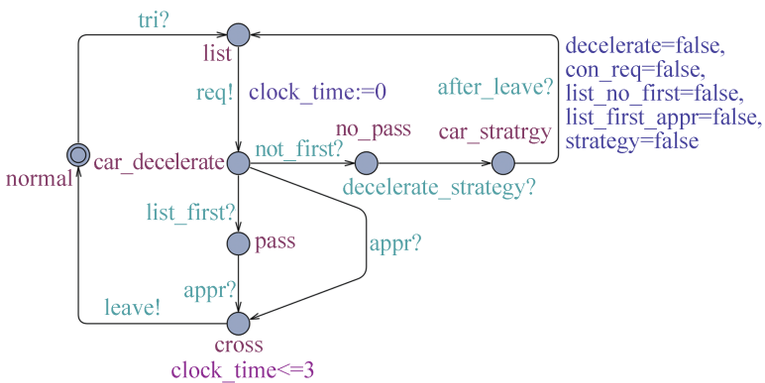


图 9 VSS 时间自动机模型

Fig. 9 VSS time automata model

表 3 模型 Car 位置、通道说明

Table 3 Model car location and channel description

名称	定义	状态
位置集合 L	normal	初始状态
	list	同时段接近区段车辆编队
	car_decelerate	请求减速状态
	car_stratrgy	减速策略状态
	pass	冲突下头车可通行状态
	no_pass	冲突下非头车可通行状态
	cross	通过冲突区段
初始位 L_0	normal	初始状态
通道集合 C	tri	车辆通信命令
	req	请求通行权命令
	list_first	冲突下队列头车
	not_first	冲突下队列非头车
	appr	允许车辆通行命令
	decelerate_stratrgy	通行减速策略
	leave	离开信号反馈
	after_leave	冲突头车通行后剩余车辆控制命令
时钟集合 X	clock_time	
状态时钟约束 I	cross:clock_time<=4	
状态转移路径 E	{<normal, tri, list>, <list, req, clock_time: = 0, car_decelerate>, <car_decelerate, list_first, pass>, <car_decelerate, appr, cross>, <car_decelerate, not_first, no_pass>, <no_pass, decelerate_strategy, car_strategy>, <car_strategy, after,(decelerate = false, con_req = false, list_no_first = false, list_first_appr = false, strategy = false), list>, <pass, appr, cross>, <cross, leave, normal>};	

DOI: 10.16182/j.issn1004731x.joss.23-0456

第 36 卷第 7 期 系统仿真学报 Vol. 36 No. 7
2024 年 7 月 Journal of System Simulation Jul. 2024

2.2.2 RSS 建模

RSS 负责车路协同无信号交叉口车辆通行冲突与控制通行时序判断，由 VSS 和 RSS 状态图并根据各个状态和转移条件得到时间自动机模型 Roadcontrol，如图 10 所示。

从而得到无信号交叉口车辆控制的时间自动机六元组模型为

$$A_2 = < L, L_0, C, X, I, E > \tag{4}$$

表 4 和图 10 为 RSS 模型的主要位置、通道和相关变量。T_number 表示时段内车辆通信数量，con 表示车辆队列冲突判断，no_con 表示车辆队列非冲突判断，trigger 表示环境触发车辆通信命令，con_list_first 表示冲突状态下头车判断，list_no_first 冲突状态下队列存在头车，b_count 表示冲突状态下队列车辆请求通行数量，list_first_appr 表示冲突状态下头车允许通行，strategy 表示冲突状态下队列非头车采取减速控制策略，c_count 表示冲突状态下队列车辆采取减速策略的数量，no_r_number 表示不冲突状态下队列车辆请求通行数量，con_req 表示冲突状态下车辆请求通行，no_a_number 表示不冲突状态下允许队列车辆通行数量。

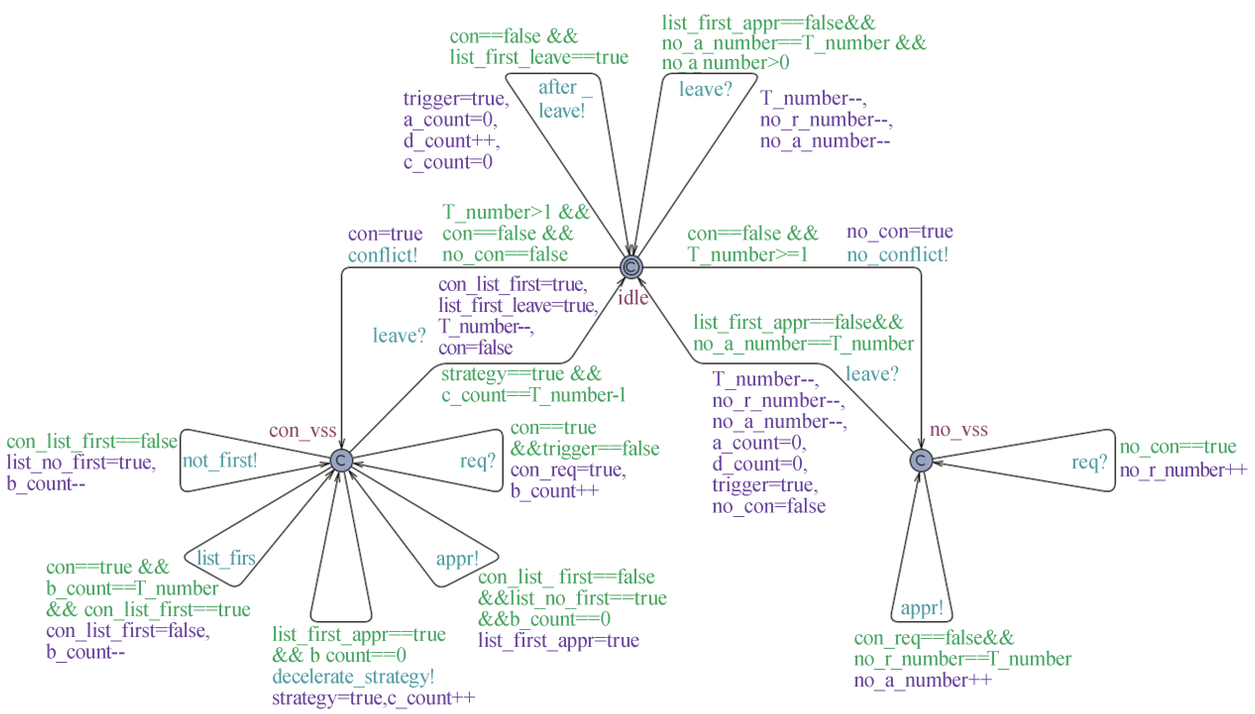


图 10 RSS 时间自动机模型

Fig. 10 RSS time automata model

表4 模型rss位置、通道说明

Table 4 Model RSS location and channel description

名称	定义	状态
位置集合L	idel	初始状态
	con_vss	冲突判断
	no_vss	非冲突判断
初始位L_0	idel	初始状态
通道集合C	conflict	车辆冲突命令
	no_conflict	车辆非冲突命令
	req	请求通行权命令
	not_first	冲突下队列非头车
	list_first	冲突下队列头车
	decelerate_stratrgy	通行减速策略
	appr	允许车辆通行命令
	after_leave	冲突头车通行后剩余车辆控制命令
	leave	离开信号反馈
时钟集合X	—	
状态时钟约束I	—	
状态转移路径E	{< idle, conflict, con = true, con_vss >, < idle, no_conflict, no_con = true, no_vss > < idle, after_leave,(trigger = true, a_count = 0, d_count ++, c_count = 0), idle >, < idle, leave,(T_number −−, no_r_number −−, no_a_number −−), idle >, < con_vss, req,(con_req = true, b_count ++), con_vss >, < con_vss, appr, list_first_appr = true, con_vss >, < con_vss, decelerate_strategy,(strategy = true, c_count ++), con_vss >, < con_vss, list_first,(con_list_first = false, b_count −−), con_vss >, < con_vss, not_first,(list_no_first = true, b_count −−), con_vss >, < con_vss, leave,(con_list_first = true, list_first_leave = true, T_number −−, con = false), idle >, < no_vss, req, no_r_number ++, no_vss >, < no_vss, appr, no_a_number ++, no_vss >, < no_vss, leave,(T_number −−, no_r_number −−, no_a_number −−, a_count = 0, d_count = 0, trigger = true, no_con = false), idle >}	

2.2.3 交叉口环境建模

无信号交叉口的环境(高精地图、进口车辆队列等)作为车–路–环境控制系统的触发，主要触发车辆进入交叉口通信范围减速和可安全通行状态判定，发送信号给RSS系统并接收其反馈信号，根据各个状态和转移条件得到时间自动机模型Envircontrol，如图11所示。

从而得到无信号交叉口车辆控制的时间自动机六元组模型为

$$A_3 = < L, L_0, C, X, I, E > \tag{5}$$

表5和图11为环境模型的主要位置、通道和相关变量，decelerate表示车辆处于请求通行减速状态，a_count表示队列车辆同阶段逻辑控制数量，d_count表示冲突头车通行后队列剩余车辆数量，其余变量与前文释义一致。

DOI: 10.16182/j.issn1004731x.joss.23-0456

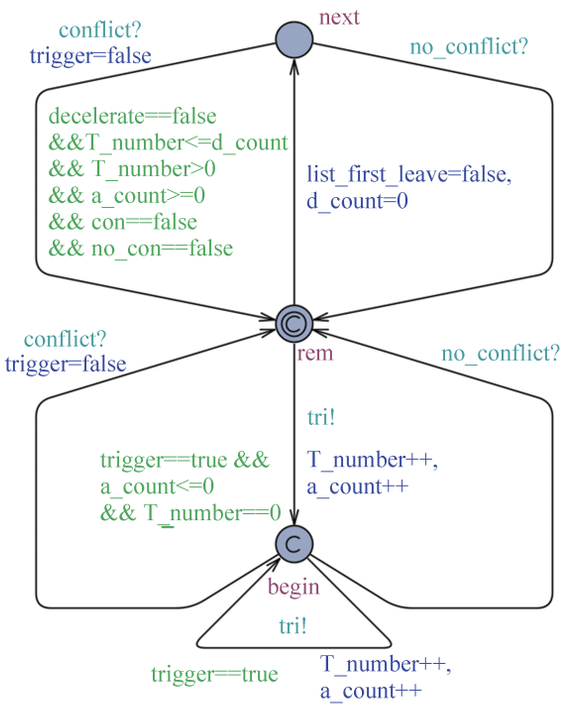


图 11 环境时间自动机模型

Fig. 11 Environmental time automata model

3 案例实现与仿真验证分析

在上述车路协同控制逻辑建模完成后，探究车路协同无信号交叉口环境下通行过程的 3 种情况：①单车无冲突；②双车冲突；③多车冲突。其中，对于双车和多车均无冲突的情况，等同于多个单车无冲突情况的叠加，因而这里不单独进行过程分析。

3.1 过程仿真分析

(1) 时段内单车无冲突通行过程分析

模拟序列为时段内单车通行冲突区无冲突点情况，如图 12 所示，过程步骤如下：

1) 车辆到达接近区段(图 12(b))，受到环境 tri 触发命令(图 12(a))，车辆进入 *list* 状态，同时 RSS 发出 no_conflict 命令，判断出当前时段通行不存在冲突点。

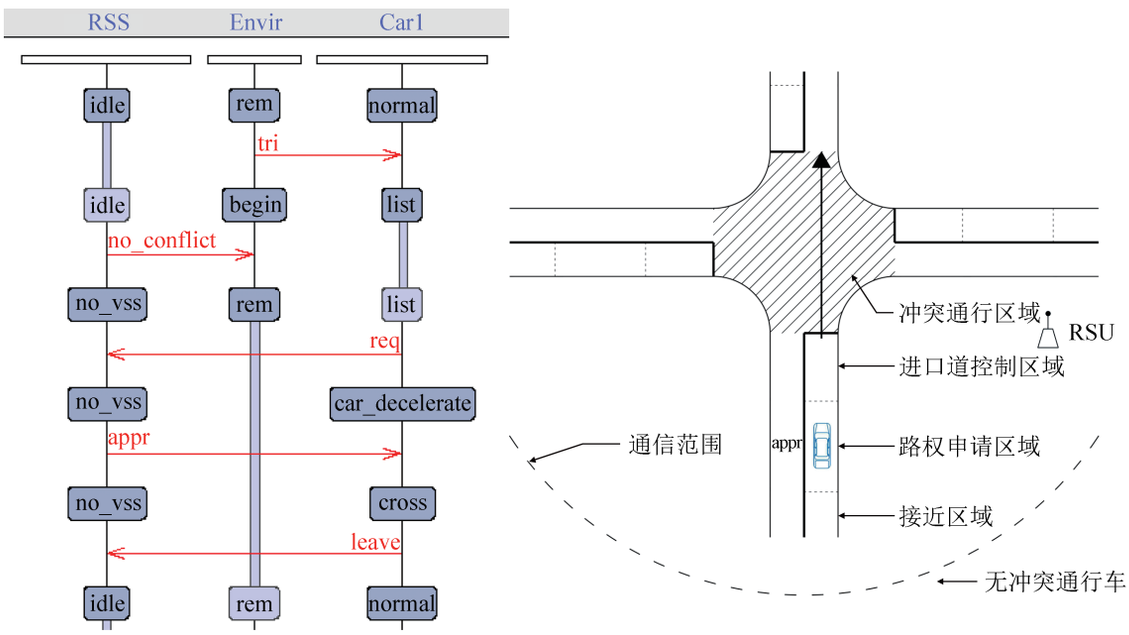
2)车辆发出 req，进行请求路口通行，同时进入 car_decelerate 状态，RSS 发出 *appr* 命令(如图 12(b))，允许车辆通行。

3) 车辆进入 cross 状态(图 12(a))车辆通过冲突区后向 RSS 发送 leave 信号，当前进口道方向冲突区可通行，环境进入 rem 初始状态。

表 5 模型 Envir 位置、通道说明

Table 5 Model Envir location and channel description

名称	定义	状态
位置集合 L	rem	初始状态
	begin	车辆通信阶段判断
	next	剩余车辆再判断
初始位 L_0	rem	初始状态
通道集合 C	tri	请求通行权命令
	conflict	车辆冲突命令
	no_conflict	车辆非冲突命令
时钟集合 X	—	
状态时钟约束 I	—	
状态转移路径 E	{< rem, tri,(T_number ++, a_count ++), begin >, < rem,(list_first_leave = false, d_count = 0), next >, < begin, tri,(T_number ++, a_count ++), begin >, < begin, conflict, trigger = false, rem >, < begin, no_conflict, rem >, < next, no_conflict, rem >, < next, conflict, trigger = false, rem >}	



(a) 模型使能迁移　　(b) 单车无冲突交叉口示意

图 12　单车无冲突通行
Fig. 12　Non-conflict traffic of single vehicle

(2) 时段内双车冲突通行过程分析

模拟序列为时段内双车通行冲突区存在冲突点情况，如图 13 所示，过程步骤如下：

1) 车辆队列到达接近区段(图 13(c))，受到环境 *tri* 触发命令(图 13(a))，车辆进入 list 状态，同时 RSS 发出 conflict 命令，判断出当前时段通行队列存在冲突点。

2) 车辆队列发出 req 进行请求路口通行，RSS 进行冲突通行和非通行车判断(list_first 和 not_first)，对通行车 appr 命令允许通行，同时非通行车进入 car_decelerate 状态(图 13(b))。

3) 冲突头车进入 cross 状态(图 13(c))，车辆通过冲突区后向 RSS 发送 leave 信号(图 13(b))，RSS 向冲突非通行发送 after_leave 命令，显示已通过冲突区。

4) 冲突非通行车按时段内单车通行冲突区无冲突点情况进行逻辑控制。

(3) 时段内多车冲突通行

模拟序列为时段内三车无信号交叉口存在冲突点通行情况，如图 14 所示。

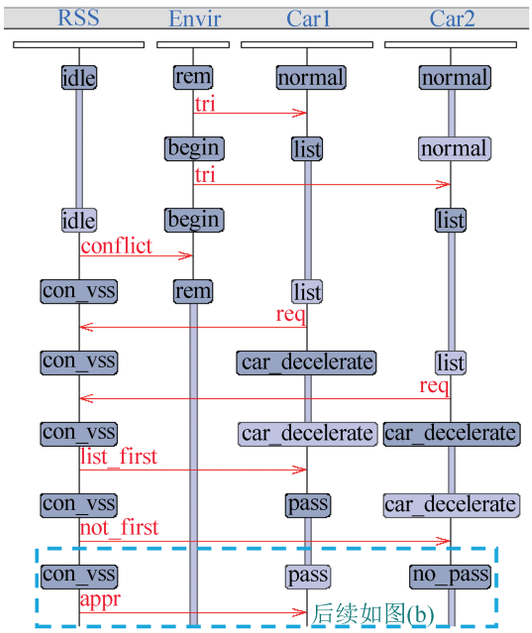
1) 车辆队列到达接近区段(图 14(d))，受到环境 *tri* 触发命令(图 14(a))，车辆进入 list 状态，同时 RSS 发出 conflict 命令，判断出当前时段通行队列存在冲突点。

2) 车辆队列发出 req 进行请求路口通行，RSS 进行冲突通行和非通行车判断(list_first 和 not_first)(图 14(b))，对通行车 appr 命令允许通行，同时非通行车进入 car_decelerate 状态。

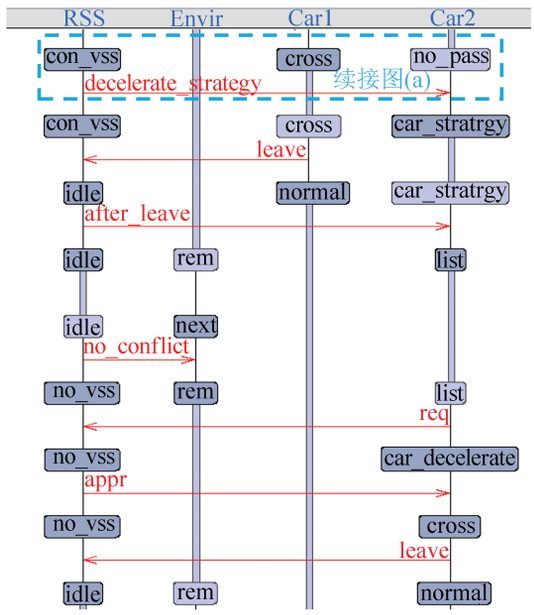
3) 冲突头车进入 cross 状态(图 14(d))，车辆通过冲突区后向 RSS 发送 leave 信号，RSS 向冲突非通行车发送 after_leave 命令，显示已通过冲突区。这存在两种情况(图 14(c))：①剩余冲突非通行车存在冲突点，按时段内双车通行冲突区存在冲突点情况进行逻辑控制；②剩余冲突非通行车不存在冲突点，按时段内单车通行冲突区无冲突点情况进行逻辑控制，以先到先行原则分配路权。

DOI: 10.16182/j.issn1004731x.joss.23-0456

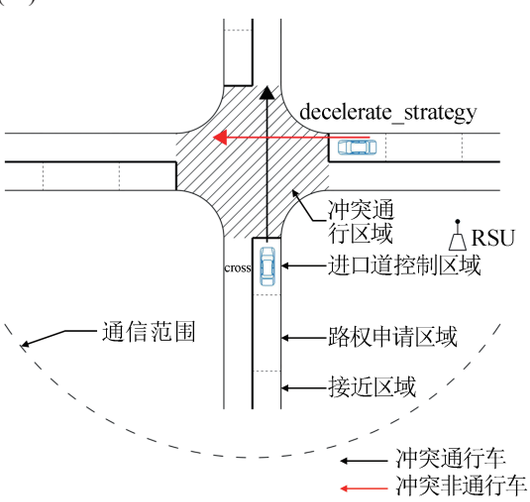
第 36 卷第 7 期
2024 年 7 月
系统仿真学报
Journal of System Simulation
Vol. 36 No. 7
Jul. 2024



(a) 使能迁移(一)



(b) 使能迁移(二)



(c) 两车冲突交叉口示意

图 13　两车冲突通行

Fig. 13　Dual vehicle conflict traffic

3.2 模型性质验证

通过对车路协同无信号交叉口系统控制流程的仿真建模，得到系统各对象、进程间交互的时序与使能迁移路径，并在此基础上利用 UPPAAL 工具和安全属性需求规范语言进行建模和可信验证，保障无信号交叉口车路协同系统的安全属性。

表 6 为系统待验证属性的逻辑表达式，对应着相应的需求规范语言，各序列及其含义如下：

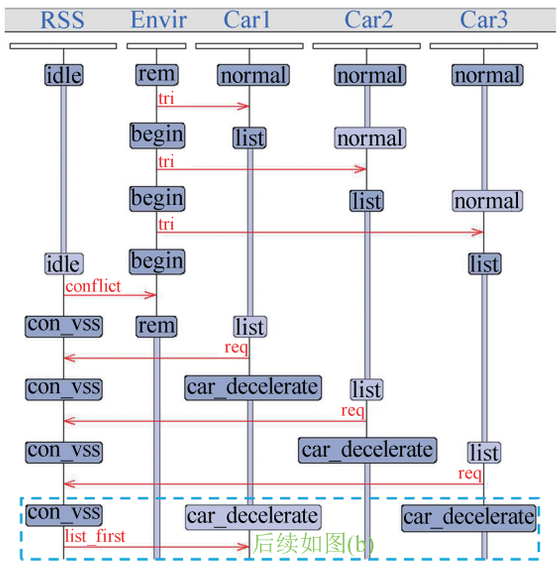
P1：系统死锁验证。车、路、环境三个系统间的信息交互和控制逻辑正确，无死锁状态。

P2：系统内部死锁验证。各个系统控制逻辑无死锁状态。

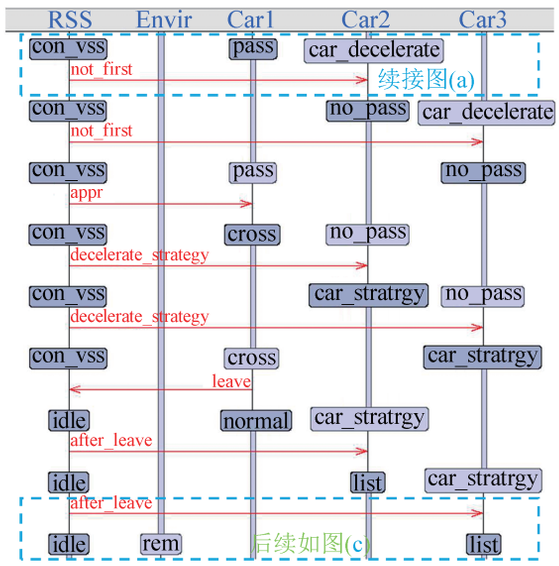
P3：状态时序性验证。同时段冲突状态下车辆时序状态正确性验证，当冲突通行车正常通行时，非通行车应处于减速策略状态。

P4：可达性验证。车辆系统各个状态均可达。

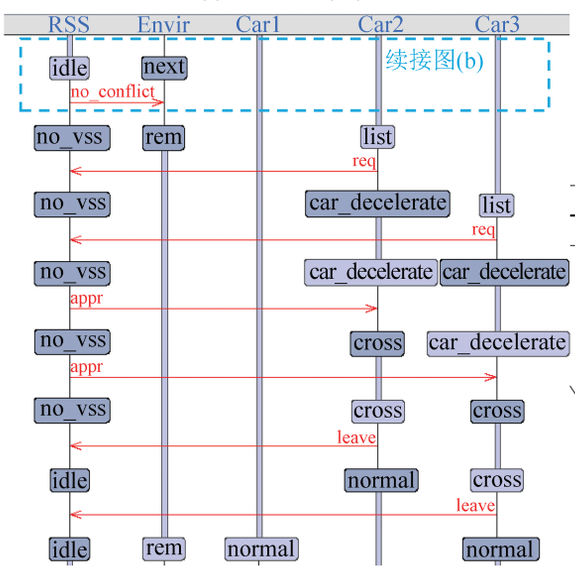
P5：正确性验证。同时段冲突区域内同一冲突点仅有单车能通过。



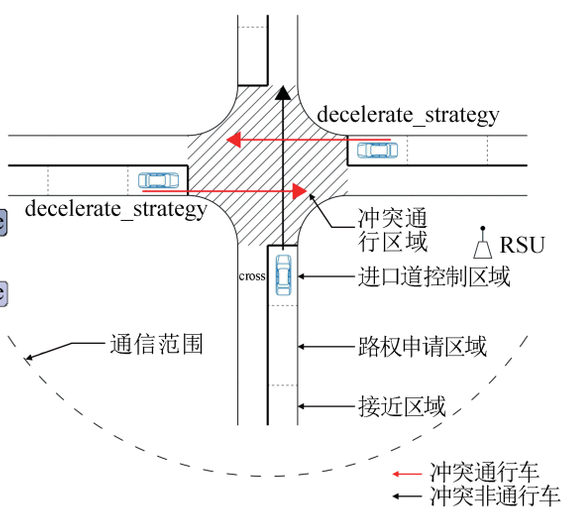
(a) 使能迁移(一)



(b) 使能迁移(二)



(c) 使能迁移(三)



(d) 多车冲突交叉口示意

图 14　多车冲突通行

Fig. 14　Multi-vehicle conflict traffic

表 6　安全属性需求规范

Table 6　Security attribute requirement specification

序列	性质
P1	A[]not deadlock
P2	A[](deadlock imply(Car1.normal and Car2.normal and Car3.normal and rss.idle and Envir.rem)))
P3	E>Car1.cross and Car2.car_stratrgy and Car3.car_stratrgy
P4	E<>Car1.cross or Car2.cross or Car3.cross
P5	A>Car1.cross+Car2.cross+Car3.cross<=1
P6	A[](Car1.cross imply(Car1.clock_time<=4)))

DOI: 10.16182/j.issn1004731x.joss.23-0456

P6：时序验证，车辆在规定时间通过状态完成并返回结果。

在UPPAAL工具中，编辑器用于在一个项目里进行建模，每个项目有一个全局声明，用来声明全局变量(所有模板及其实例都可见)，可添加若干Template(进程模板)，在模型声明中对进程模板进行例化，对整个系统的组织进行描述。模拟器里可对所建立的模型选择转换进行单步模拟执行，模拟器也用于性质验证不通过时候给出反例，可从上到下把整个Trace重放一遍，每个实例状态机上当前所处的状态会标红。语法检查通过后，在验证器里分别验证各个性质，得到上述逻辑表达式验证如图15所示。

实验结果表明：在确定车路协同无信号交叉口系统交互时序和使能迁移路径的情况下，给出时间自动机模型的转换规则并对系统安全属性可满足性的验证，确保系统安全运行，满足系统的安全性需求，从而验证系统策略核心控制逻辑的正确性。

图15 验证结果
Fig. 15 Verification results

4 结论

车路协同无信号交叉口控制系统作为智能实时决策系统，明确逻辑状态合理交互过程对于车辆安全高效通过具有重要意义。

本文为探究车路协同无信号交叉口场景下车路随机到达的系统实时控制逻辑。在相关现有标准和规范要求基础上，利用UML进一步明确系统控制过程中系统对象功能及状态、交互内容和顺序；基于时间自动机转化UML进行形式化建模，明确系统对象时间自动机模型六元组和其变量条件；进行仿真与验证，给出单车无冲突、双车冲突和多车冲突下状态交互和使能迁移路径，结合需求规范语句进行系统逻辑安全属性验证。

未来研究中，可考虑车载和路侧子系统内各软硬件设施的信息流交互过程，结合通信传输协议进行延时设定；考虑其他无信号控制和信号控制的交叉口场景，研究不同场景的控制逻辑差异；进一步以驾驶决策特征为基础，从人工驾驶和智能网联车辆的特性出发，提出交叉口车路协同系统混合车辆的诱导机理，分析系统中车辆控制的数学约束内容和工况逻辑，构建复杂的车路协同系统控制模型，从而进一步细化完善车路协同交叉口控制系统的实时控制逻辑。

参考文献：

[1] Chen Xiaolong, Hu Manjiang, Xu Biao, et al. Improved Reservation-based Method with Controllable Gap Strategy for Vehicle Coordination at Non-signalized Intersections[J]. Physica A: Statistical Mechanics and Its Applications, 2022, 604: 127953.

[2] Dey K C, Rayamajhi A, Chowdhury M, et al. Vehicle-to-vehicle (V2V) and Vehicle-to-infrastructure (V2I) Communication in a Heterogeneous Wireless Network-performance Evaluation[J]. Transportation Research Part C: Emerging Technologies, 2016, 68: 168-184.

[3] Grembek O, Kurzhanskiy A, Medury A, et al. Making Intersections Safer with I2V Communication[J]. Transportation Research Part C: Emerging Technologies, 2019, 102: 396-410.

[4] Banks V A, Plant K L, Stanton N A. Driver Error or Designer Error: Using the Perceptual Cycle Model to Explore the Circumstances Surrounding the Fatal Tesla Crash on 7th May 2016[J]. Safety Science, 2018, 108: 278-285.

[5] 易振国. 车路协同实验测试系统及安全控制技术研究[D]. 长春: 吉林大学, 2011.
Yi Zhenguo. Vehicle Infrastructure Integration Experimental Testing System and Safety Control Technology[D]. Changchun: Jilin University, 2011.

[6] 上官伟, 李鑫, 柴琳果, 等. 车路协同环境下混合交通群体智能仿真与测试研究综述[J]. 交通运输工程学报, 2022, 22(3): 19-40.
Shangguan Wei, Li Xin, Chai Linguo, et al. Research Review on Simulation and Test of Mixed Traffic Swarm in Vehicle-infrastructure Cooperative Environment[J]. Journal of Traffic and Transportation Engineering, 2022, 22(3): 19-40.

[7] Elsayed G F, Shankar S, Cheung B, et al. Adversarial Examples that Fool Both Computer Vision and Time-limited Humans[C]//Proceedings of the 32nd International Conference on Neural Information Processing Systems. Red Hook, NY, USA: Curran Associates Inc., 2018: 3914-3924.

[8] Gleirscher M, Foster S, Woodcock J. New Opportunities for Integrated Formal Methods[J]. ACM Computing Surveys, 2020, 52(6): 117.

[9] Aryldo G Russo, Lukas Ladenberger. A Formal Approach to Safety Verification of Railway Signaling Systems[C]// 2012 Proceedings Annual Reliability and Maintainability Symposium. Piscataway, NJ, USA: IEEE, 2012: 1-4.

[10] Steve Jeffrey Tueno Fotso, Marc Frappier, Régine Laleau, et al. Modeling the Hybrid ERTMS/ETCS Level 3 Standard Using a Formal Requirements Engineering Approach[J]. International Journal on Software Tools for Technology Transfer, 2020, 22(3): 349-363.

[11] Muhammed Ali O Z, Ozgur Turay Kaymakci. An Automatic Formal Model Generation and Verification Method for Railway Interlocking Systems[J]. Gazi University Journal of Science, 2017, 30(2): 133-147.

[12] Xu Bingqing, Li Qin, Guo Tong, et al. A Scenario-based Approach for Formal Modelling and Verification of Safety Properties in Automated Driving[J]. IEEE Access, 2019, 7: 140566-140587.

[13] 王淑灵, 詹博华, 盛欢欢, 等. 可信系统性质的分类和形式化研究综述[J]. 软件学报, 2022, 33(7): 2367-2410.
Wang Shuling, Zhan Bohua, Sheng Huanhuan, et al. Survey on Requirements Classification and Formalization of Trustworthy Systems[J]. Journal of Software, 2022, 33(7): 2367-2410.

[14] 王鲲. 基于通信顺序进程与B方法的CBTC计算机联锁系统的形式化建模与验证[J]. 中国铁道科学, 2018, 39(3): 101-109.
Wang Kun. Formal Modeling and Verification of CBTC Computer Interlocking System Based on Communication Sequential Process and B Method[J]. China Railway Science, 2018, 39(3): 101-109.

[15] 赵梦瑶, 陈小红, 孙海英, 等. 轨道交通联锁领域特定语言的形式化[J]. 软件学报, 2020, 31(6): 1638-1653.
Zhao Mengyao, Chen Xiaohong, Sun Haiying, et al. Formalizing Railway Interlocking Domain Specific Language[J]. Journal of Software, 2020, 31(6): 1638-1653.

[16] Dimitri Lefebvre, Christoforos N Hadjicostis. Diagnosability of Fault Patterns with Labeled Stochastic Petri nets[J]. Information Sciences, 2022, 593: 341-363.

[17] 中华人民共和国工业和信息化部. 基于车路协同的高等级自动驾驶数据交互内容: YD/T 3978-2021[S].

Ministry of Industry and Information Technology of the People's Republic of China. Data Exchange Standard for High Level Automated Driving Vehicle Based on Cooperative Intelligent Transportation System: YD/T 3978-2021[S].

[18] 崔晓丹. 基于车路协同的区域化无信号交叉口控制方法研究[D]. 北京: 北京交通大学, 2017.
Cui Xiaodan. Research on Regional Unsignalized-intersection Control Method Based on Cooperative Vehicle Infrastructure System[D]. Beijing: Beijing Jiaotong University, 2017.

[19] 孙伟, 张梦雅, 马成元, 等. 新型混合交通交叉口信号与车辆轨迹协同控制方法[J]. 交通运输系统工程与信息, 2023, 23(1): 97-105.
Sun Wei, Zhang Mengya, Ma Chengyuan, et al. Coordination of Signal and Vehicle Trajectory at Intersections for Mixed Traffic Flow[J]. Journal of Transportation Systems Engineering and Information Technology, 2023, 23(1): 97-105.

[20] Qu Dayi, Zhao Zixu, Song Hui, et al. Design of Vehicle-road Cooperative Assistant Decision System for Active Safety at Intersections[J]. Journal of Transportation Engineering, Part A: Systems, 2022, 148(5): 04022022.

[21] 张毅, 姚丹亚, 李力, 等. 智能车路协同系统关键技术与应用[J]. 交通运输系统工程与信息, 2021, 21(5): 40-51.
Zhang Yi, Yao Danya, Li Li, et al. Technologies and Applications for Intelligent Vehicle-infrastructure Cooperation Systems[J]. Journal of Transportation Systems Engineering and Information Technology, 2021, 21(5): 40-51.

[22] Wang Yang, Ning Wei, Zhang Shengyu, et al. Architecture and Key Terminal Technologies of 5G-based Internet of Vehicles[J]. Computers and Electrical Engineering, 2021, 95: 107430.

[23] Rumbaugh J, Jacobson I, Booch G. The Unified Modeling Language Reference Manual[M]. 2nd ed. Boston: Addison-Wesley, 2005.

[24] 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.
Han Deshuai, Yang Qiliang, Xing Jianchun. UML-based Modeling and Formal Verification for Software Self-adaptation[J]. Journal of Software, 2015, 26(4): 730-746.

[25] Johan Bengtsson, Kim Larsen, Fredrik Larsson, et al. UPPAAL-a tool Suite for Automatic Verification of Real-time Systems[C]//Hybrid Systems III. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996: 232-243.

[26] Alur R, Dill D L. A Theory of Timed Automata[J]. Theoretical Computer Science, 1994, 126(2): 183-235.

[27] Frank Ortmeier, Wolfgang Reif, Gerhard Schellhorn. Formal Safety Analysis of a Radio-based Railroad Crossing Using Deductive Cause-consequence Analysis (DCCA) [C]//Dependable Computing-EDCC 5. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 210-224.