软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2021,32(6):1818−1829 [doi: 10.13328/j.cnki.jos.006251]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

面向数据流的 ROS2 数据分发服务形式建模与分析*

芦 倩[1,2], 李晓娟[1,2], 关 永[1,3], 王 瑞[1,4], 施智平[1,4]

[1](首都师范大学 信息工程学院,北京 100048)

[2](高可靠嵌入式系统技术北京市工程研究中心(首都师范大学),北京 100048)

[3](北京成像理论与技术高精尖创新中心(首都师范大学),北京 100048)

[4](轻型工业机器人与安全验证北京市重点实验室(首都师范大学),北京 100048)

通讯作者: 李晓娟, E-mail: lixj@cnu.edu.cn

摘 要: 机器人操作系统(robot operating system,简称 ROS)是一种开源的元操作系统,能够在异种计算簇上提供基于消息机制的结构化通信层.为改善 ROS1 中存在的数据分发实时性、可靠性问题,ROS2 提出了面向数据流的数据分发服务机制.采用概率模型检验的方法,分析、验证 ROS2 系统数据分发机制的实时性和可靠性.首先,提出一种面向数据流的 ROS2 数据分发服务的形式化验证框架,并对通信系统模块建立概率时间自动机模型;其次,运用概率模型检测器,通过数据丢失率和系统响应时间等参数分析、验证 ROS2 面向数据流的数据分发服务的实时性、可靠性;最后,基于重传机制、服务质量(quality of service,简称 QoS)策略分析,通过设置和调整服务质量参数,实现不同的数据需求和传输方式的量化性能分析,为 ROS2 应用的设计人员以及基于数据流的分布式数据分发服务的形式化建模、验证和量化性能分析提供参考.

关键词: ROS2;数据分发服务;QoS;概率时间自动机;PRISM;形式化建模与分析

中图法分类号: TP311

中文引用格式: 芦倩,李晓娟,关永,王瑞,施智平.面向数据流的 ROS2 数据分发服务形式建模与分析.软件学报,2021,32(6):1818−1829. http://www.jos.org.cn/1000-9825/6251.htm

英文引用格式: Lu Q, Li XJ, Guan Y, Wang R, Shi ZP. Modeling and analysis of ROS2 data distribution service for data flow. Ruan Jian Xue Bao/Journal of Software, 2021,32(6):1818−1829 (in Chinese). http://www.jos.org.cn/1000-9825/6251.htm

Modeling and Analysis of ROS2 Data Distribution Service for Data Flow

LU Qian[1,2], LI Xiao-Juan[1,2], GUAN Yong[1,3], WANG Rui[1,4], SHI Zhi-Ping[1,4]

[1](College of Information Engineering, Capital Normal University, Beijing 100048, China)

[2](Beijing Engineering Research Center of High Reliable Embedded System (Capital Normal University), Beijing 100048, China)

[3](Beijing Advanced Innovation Center for Imaging Theory and Technology (Capital Normal University), Beijing 100048, China)

[4](Beijing Key Laboratory of Light Industrial Robot and Safety Verification (Capital Normal University), Beijing 100048, China)

Abstract: Robot operating system (ROS) is an open source meta-operating system, which can provide a structured communication layer based on message mechanism on heterogeneous computing clusters. In order to improve the real-time and reliability problems of data distribution in ROS1, ROS2 is proposed with data flow oriented data distribution service mechanism. This study adopts the method of

* 基金项目: 国家重点研发计划(2019YFB1309900); 国家自然科学基金(61876111); 科技创新服务能力建设-基本科研业务费(00620530290073); 首都师范大学交叉科学研究项目(0062155087)

Foundation item: National key Research and development program (2019YFB1309900); National Natural Science Foundation of China (61876111); Capacity Building for Sci-Tech Innovation-Fundamental Scientific Research Funds (00620530290073); Research Fund from Academy for Multidisciplinary Studies of Capital Normal University (0062155087)

本文由“形式化方法与应用”专题特约编辑邓玉欣教授推荐.

收稿时间: 2020-08-30; 修改时间: 2020-10-26; 采用时间: 2020-12-19; jos 在线出版时间: 2021-02-07

probability model test and analysis, validates real-time and reliability of the ROS2 system. Firstly, a data flow oriented ROS2 data distribution service system of communication formal validation framework is put forward, and the communication system module probabilistic timed automata model is set up. Secondly, probabilistic model detector PRISM is used to verify the real-time and reliability of ROS2 data flow oriented data distribution service through parameter analysis of data loss rate and system response time. Finally, based on retransmission mechanism, quality of service (QoS) strategy analysis, through the set up and adjust service quality parameters, different data requirements and quantitative performance analysis of transmission mode are achieved, providing the reference for application designers based on ROS2 and distributed data distribution service based on the data flow of formal modeling, validation, and quantitative performance analysis.

Key words: ROS2; data distribution service; QoS; probabilistic timed automata; PRISM; formal modeling and analysis

ROS 是开源的元操作系统,已广泛用于机器人软件研发.随着机器人相关技术的日益普及,对机器人应用的要求也在相应地提高,因此需要对机器人操作系统进行分析,使系统对外界的信号等信息及时地作出相应的动作.但是,ROS 机器人操作系统存在两个主要问题:通信延迟高和可靠性差.ROS 的性能受到其高延迟序列化方法和与 TCP/UDP 的套接字通信的限制,在消息传递过程中会带来多次内存复制[1].因此,ROS 系统实时性不高,不能直接应用于实时控制和关键任务应用.并且 ROS1 的通信系统基于 TCPROS/UDPROS,强依赖于主节点的处理,一旦主节点出现故障,系统可靠性将会受到很大的影响,在一定程度上限制了 ROS 的实际应用.

ROS2 在 ROS 的基础上改进应用了众多新技术,带来了整体架构的颠覆.为了改善 ROS1 实时性、可靠性问题,ROS2 采用面向数据流的数据分发服务(data distribution service,简称 DDS)作为其通信机制.DDS 是对象管理组织提出的一种以数据为中心的新一代分布式系统数据规范,它允许使用发布-订阅机制进行可靠和实时的数据收集和交付,支持节点的动态发现、基于主题的数据分发和数据流的时空解耦.因此,该数据规范保证了数据分发的实时性与可靠性,并且由于其灵活的配置方法和其可扩展性而广泛应用于实时分布式系统中.与其他发布订阅中间件相比,DDS 的一个主要特征是具有极其丰富的 QoS 支持[2].QoS 策略提供了数据传输的保证[3].系统设计者可以根据这些 QoS 参数,基于特定的要求和可用性来构建分布式应用.面向数据流的 ROS2 数据分发服务机制相对于以主节点为中心的基于消息的数据分发机制,能较好地满足分布式节点间数据通信的实时性、提高数据传输效率,因此擅长处理数量庞大和复杂多变的数据.通过控制 QoS 参数,可以将对更新速率、可靠性和带宽控制等有不同要求的模块很好地集成到系统中.但是随着系统内部数据交互频繁,同时,随着系统规模的扩大,系统中发送者和订阅者的数量、数据类型和 QoS 需求也随之增加,系统性能会急剧下降,并且不同的应用对 DDS 性能的要求有不同的差别.这些问题都会给数据分发带来严峻的考验,给设计造成隐患.所以在系统开发早期应该对其进行分析,但是使用传统的测试和仿真方法,无法对系统模型进行完备的验证.形式化方法运用数学和逻辑的方法描述和验证系统.形式化验证[4]与传统的验证方法相比,以形式化方法为基础的工具进行辅助设计和验证,对提高系统的可信度有很大帮助.并且能够对指定描述的所有可能的情况进行验证,有效地克服了模拟验证的不足.概率模型检测结合了概率分析和通用的模型检测技术,适用于验证非确定的系统,并可实现量化分析.因此,我们使用形式化验证中的概率模型检测的方法分析系统的正确性,基于形式化模型进一步对系统性能进行参数化分析,从而给系统设计人员和 ROS 程序开发人员提供有价值的参考.

已有学者对有关 DDS 的形式化验证问题进行了研究.He 等人[5]最先基于概率时间自动机对发布订阅系统进行了形式化建模.Liu 等人[6]验证了 DDS 在 ROS2 中的活性.Yin 等人[7]使用通信顺序进程(CSP)对实时发布订阅协议(RTPS)中的多个模块中组件进行了建模,通过使用模型检测工具 PAT 验证了不发散性、确认机制、数据一致性等属性.上述工作都对数据分发机制进行了形式化建模,但大多数是对基于消息的数据分发机制进行建模,没有对 QoS 策略进行形式描述,缺少对系统的性能的分析.QoS 是控制了各方面与底层的通信机制,是用于解决延迟和阻塞的传输控制策略.在关键和分布式系统运行时,需要保证可靠性并且满足所需的性能.调整 QoS 参数可以满足不同场景的数据应用需求,对系统实时性可靠性有至关重要的影响.而对系统 QoS 服务质量分析的国内外研究中,Maruyama 等人[8]阐明了 ROS1 和 ROS2 在各种情况下的数据传输性能.从延迟、吞吐量、线程数和内存消耗对比 ROS1 与 ROS2 的性能.QoS 自适应方法是基于发布/订阅中间件开发实时系统的一种有效的方法,在动态环境中开发大型实时分布式系统时,其重要性日益提高.当在众多异构实体之间传播大量数据时,

需要严格的服务质量策略约束.Inglés-Romero 等人[9]提出一种可以在基于 DDS 的中间件中安全、自动和透明地调整 QoS 属性的方法,从而在提供的可用资源内,以最佳的性能运行.在此基础上, Casini 等人[10]提出一种在动态环境下的实时系统中自动调整 QoS 策略,以实现 QoS 自适应控制的新方法,通过降低其计算能力来改善实时系统的性能并使其更稳定.上述工作虽然都对 QoS 服务质量进行了描述分析,但大多数是采用测试、模拟和仿真的方法,鲜有文献从形式化验证的角度对 ROS2 通信系统的 QoS 参数量化分析其性能.

在本文中,我们对 ROS2 面向数据流的数据分发机制进行形式化建模,将数据流形式表达成由多个数据块组成的数据序列,并对 ROS2 中相关 QoS 策略 DEADLINE,RELIABLITY,DURABILITY,HISTORY 进行形式描述,建立概率时间自动机模型,并在模型中考虑到数据流通信特点、数据重传机制、确认机制以及环境因素不确定性,最后通过调整服务质量参数量化分析其系统性能,验证 ROS2 通信系统的可靠性和实时性,从而给系统设计和 ROS 程序开发人员提供有价值的参考,使 ROS2 系统更加安全可靠.

本文第 1 节描述 ROS2 的数据分发机制,并构建基于 DDS 的 ROS2 通信系统的抽象模型.第 2 节将通信系统抽象模型分为各个子模块,并对每个子模块建立概率时间自动机模型.第 3 节用 PRISM 概率模型检测器验证验证 ROS2 通信系统的实时性、可靠性,对机器人通信过程进行关键属性的验证和分析.结合 ROS2 系统间的通信特点,通过加入 QoS 策略进行量化分析,通过设置和调整服务质量参数,实现不同的数据需求和传输方式,并在特定的通信环境下能够保证通信的质量.第 4 节总结与展望,总结了本文的主要工作与创新点,并对下一步的研究提出建议.

1 系统描述

在机器人操作系统中,ROS1 的通信系统是基于 TCPROS 和 UDPROS 的,而此通信方式依赖于主节点,一旦主节点出现问题,将会影响整个通信系统.ROS2[11]的通信系统则是基于 DDS 的,在系统内部提供了 DDS 抽象层的实现,用户不需要知道 DDS 的 API,并允许 ROS2 使用高级配置选项来优化 DDS 的使用.此外,ROS2 通信系统不需要主节点,真正成为了去中心化的分布式系统,使得 ROS2 比 ROS1 具备更强大的容错能力.ROS2 支持构建在 Linux、Windows、Mac、实时操作系统上.ROS2 系统框架如图 1 所示.

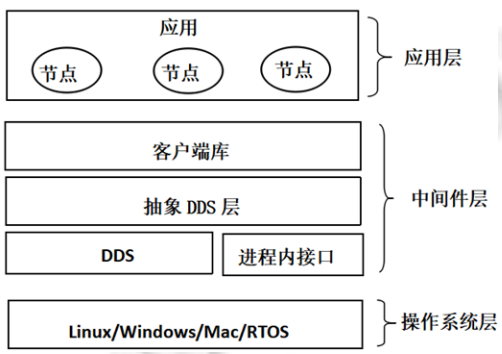

Fig.1 ROS2 system framework

图 1 ROS2 系统框架

DDS 是由以数据为中心的发布订阅层(data centered publish subscribe,简称 DCPS)和数据本地重构层(data local reconstrution layer,简称 DLRL)组成的[12,13].DLRL 是 DDS 规范的上层,它使分布式数据可以为本地和远程对象所共享.DCPS 是 DDS 规范的核心和底层,负责数据传输和 QOS 控制保证,可以将来自发布者的数据高效地交付给给订阅者,保证了数据传输的可靠性.DDS 则是面向数据流的通信范式,以数据为中心通信可以在每个数据的基础上添加各种参数,其中包括发布速率、订阅速率、数据有效的时间以及许多其他参数.这些服务质量参数允许系统设计者根据每个特定数据的要求和可用性构建分布式应用程序.DDS 关键的抽象概念是全局数据空间(global data space,简称 GDS).DDS 规范要求通信模型中的 GDS 以完全分布式的形式实现,这使得对需要

获取 GDS 内的数据的应用程序都可以在任何时刻动态地加入或者离开该系统,当单个节点上的应用程序出现故障时,并不会导致整个系统崩溃[14].因此在时间和空间上保证了系统的松耦合性,系统的灵活性和扩展性也大大提高了.

在 DDS 通信模型中,每个 DDS 实体都有一套 QoS 策略,通过控制 QoS 策略,数据传输的性能可以被动态调整,从而满足系统对数据传输的多样性要求.如图 2 所示为 ROS2 通信系统的服务质量策略,在 ROS2 中有以下 4 种服务质量策略[8]:

1. DEADLINE:该服务质量策略要求数据写入者和数据读取者必须在每个截止时间内更新一次数据;
2. HISTORY:该服务质量策略控制着数据传输是只传递最新值,还是传递所有中间值,还是传递介于两者之间的值,可以通过设置队列深度设置存储样本的深度;
3. RELIABLITY:DDS 可靠性通信模式中,分为 Best_Effort(高效传输模式)和 Reliable(可靠传输模式)两种通信模式:Best_Effort 高效通信模式要求尽可能快地发送数据,但有可能存在数据丢失;在 Reliable 可靠通信模式时,丢失的数据会重新传输,因此数据传输是有保证的;
4. DURABILITY:该服务质量策略规定发布者是否为未加入的节点保存未接收的数据.DURABILITY 策略分为 Transient_local,Volatile 两个属性:Transient_local 属性规定,发送者会为未加入的节点保存未接收的数据;Volatile 属性规定,发布者不会特意保存样本数据.

在基于 DDS 的 ROS2 通信系统中,可以加入不同的 QoS 策略量化分析,通过设置和调整服务质量参数,可以实现不同的数据需求和传输方式,并在特定的通信环境下,能够保证通信的质量.

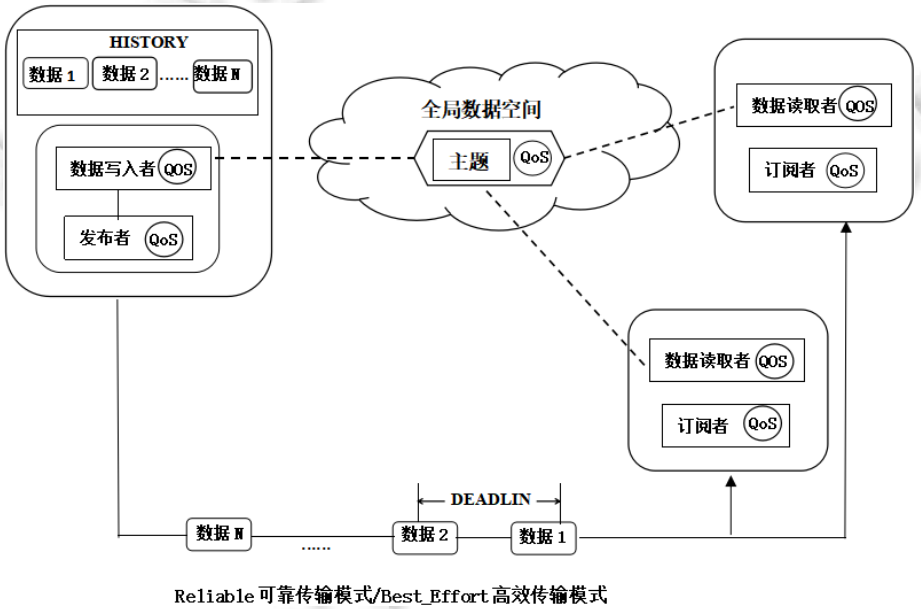

Fig.2 Quality of service policy for ROS2 communication system

图 2 ROS2 通信系统的服务质量策略

ROS2 中,DDS 发布订阅模型主要由发布者、订阅者、数据写入者、数据读取者和全局数据空间构成,实现主题的发布订阅和数据分发功能[15].我们可将其分为发布模块、订阅模块、全局数据空间模块、通信信道模块:

- 发布模块:发布者首先要创建数据写入者 DW_i,DW_i 将所需要发布的数据的主题 T_i 以及可提供的 QoS 发布到全局数据空间中.若发布成功,DW_i 将进入阻塞等待状态.同时,将 DW_i 的发布记录同步计入同一 DDS 域中每一个节点的发布主题表.当有匹配成功的订阅信息时,DW_i 等待状态被激活,查看发布主题表内与 T_i 相对应的 QoS 中 *Durability* 属性的值:若其取值为 1 时,需在发布缓冲区添加数据,以便

后续的订阅者可顺利接收到此数据;否则,将数据发送给订阅者之后,将该数据删除;

- 订阅模块:订阅者首先需要创建一个数据读取者 DR_j,DR_j 在它的全局数据空间的发布主题表中查询相匹配的发布者,将订阅主题 T_j 及 QoS 发送至该发布者的全局数据空间上;随后,DR_j 变为阻塞状态.当该发布者接收到 DR_j 的订阅消息时,需将其订阅记录添加至全局数据空间的订阅主题表内,并查询发布主题表中 T_j 相对应的 *Durablity* 值:若其取值为 0,表示数据没有存入到发布数据缓冲区中,则表示此次订阅失败;若 *Durablity* 取值为 1 时,说明在发布数据缓冲区中存有满足订阅条件的数据信息,然后激活 DW_i,将所有符合条件的数据按照对应的 QoS 策略传输给订阅者;
- 全局数据空间模块:在全局数据空间模块中,包含发布主题表、订阅主题表、订阅失败表、发布数据缓冲区.其中:发布主题表内保存了同一 DDS 域中所有节点的发布主题信息;订阅主题表保存了订阅该节点的订阅信息.发布模块中的数据写入者和订阅模块中的数据读取者之间的联系通过主题实现,并通过将名称、数据类型、与数据本身相关的 QoS 联系到一起,完成发布订阅之间的连接.订阅失败表保存本节点订阅失败的历史记录,发布数据缓冲区保存了发布者发布且需要长期保存的数据.DDS 发布订阅模型将发布者可提供的数据资源状况及订阅者对数据资源的期待程度用 QoS 参数来描述.DDS 中间件通过这些参数选择最符合通信双方 QoS 要求的传输方式来分发数据,既实现了数据传输的实时性,也增加了通信的灵活性.以数据流作为整个平台的触发点和导向,实现数据的实时分发;
- 通信信道模块:通信信道负责数据发布者和数据订阅者之间的数据传输功能.在通信信道中,数据以数据流的形式进行传输,数据流可以被视为一组有顺序、有起止和终止的数据序列.在数据传输中,由于通信信道是不可靠的,可能会发生数据的丢失.为满足不同的通信需求,通过选择一定的 QoS 策略,数据传输的性能可以被动态调整.

面向数据流 ROS2 的 DDS 发布订阅模型的模型图如图 3 所示.

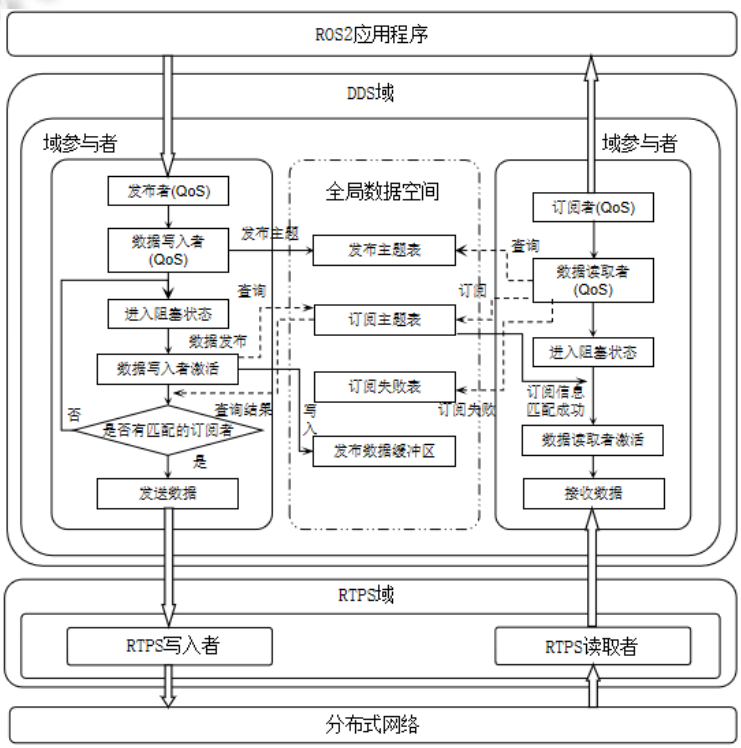

Fig.3 DDS publish subscribe model

图 3 DDS 发布订阅模型

在面向数据流的 ROS2 数据分发服务的通信系统中,它允许部署一个或多个 DDS 域.同一域内的域参与者通过匹配主题和 QoS 策略来发布订阅数据.在 DDS 通信系统中,发布者并不实际传输数据,而是通过创建和管理数据写入者 DW_i,DW_i 负责发布主题,并将数据发送给订阅该主题且 QoS 一致的订阅者.订阅者通过创建数据读取者 DR_j 订阅数据.ROS2 通信系统中,QoS 包括 DEADLINE,RELIABLITY,DURABILITY,HISTORY 策略.当 DW_i 发布的主题与 DR_j 订阅的主题且 QoS 策略一致时,就形成了数据发布订阅关系.若存在多个满足订阅主题的 DW_i,选择其中一个符合对应 QoS 策略的 DW_i 进行订阅,当 DW_i 失效时,则可订阅其他的数据写入者中的数据.因此,ROS2 通信系统解决了单点失效的问题.

2 基于 Prism 的系统建模

本文使用概率自动时间机来对 ROS2 面向数据流的数据分发服务进行形式建模.概率时间自动机是关于时间和概率的有限自动机的扩展,它同时表示时间和概率,因此适合于在此模型中表示损失概率和时间延迟.根据上节的系统描述,本节具体介绍系统中涉及到的主要模型形式化表示,并在 PRISM 概率模型检测器实现各模型的概率时间自动机模型.

2.1 概率模型检测工具PRISM

概率时间自动机[16]是在时间自动机的基础上进行概率扩展,为实时系统在概率环境下的建模提供了一套形式化的框架和机制.概率模型检测器 PRISM[17,18]是由牛津大学开发研究的一个检测概率模型是否满足给定时序逻辑属性的工具,它已被用于分析来自许多不同应用领域的系统,包括通信和多媒体协议、随机分布式算法、安全协议、生物系统和许多其他系统.PRISM 可以构建和分析几种类型的概率模型:离散时间马尔可夫链(DTMC)、连续时间马尔可夫链(CTMC)、马尔可夫决策过程(MDP)、概率自动机(PA)、概率时间自动机(PTA).PRISM 首先分析模型的描述;然后构建概率模型的内部表示,计算模型可达状态空间并丢弃所有的不可达状态,这意味着在建模系统中所有可能的组合集都可能会出现;接着解析逻辑规范,并通过归纳语法对模型应用适当的模型检测算法进行验证.

2.2 系统在PRISM中的实现

根据系统描述中对 ROS2 数据分发服务的通信系统进行抽象,我们将系统形式化建模为数据发布节点概率时间自动机模型、数据订阅节点概率时间自动机模型、全局数据空间概率时间自动机模型、通信信道模块概率时间自动机模型.为了构建 ROS2 数据分发服务的通信系统模型,我们需要考虑以下情况:传输信道不可靠,即数据在信道传输过程中可能会丢失,并且信道的数据丢包率为 P;数据传输时延不可忽略;数据被接受的次序与其被发送的次序一致;在缓冲区溢出的情况下,新来的数据信息将会被直接丢弃.

2.2.1 数据发布节点和数据订阅节点概率时间自动机模型

在 DDS 中,节点既可以是数据发布者,也可以是数据订阅者.建模中,我们将节点分为数据发布节点和数据订阅节点,分别建立概率时间自动机模型.图 4 所示为以数据流形式通信的发布节点概率时间自动机模型.DDS 作为 ROS2 的通信机制,通过数据流的方式进行数据的分发传输.数据流是一组有顺序、有起始和终止的字节的数据序列.在形式化模型中,我们可以将数据流看成是由多个数据块组成的数据序列,并用布尔类型的标记位对每个数据块标识:*fp* 用来指示当前发送的数据块是否是起始的数据块,*lp* 指示当前发送的数据块是否是终止的数据块,*flag* 用来判定数据块是否成功发送.*flag* 的初始值为 false,当数据块发送成功至订阅者,并收到来自订阅者的确认信息,标记位 *flag* 替换成 true,代表当前数据块传输成功.然后发送下一个数据块,但在数据块连续发送时,发布者在一段时间 *timeout* 内没有收到来自订阅者传来的确认信息,即 *flag* 值仍为 false,则中断连续数据块的发送.发布者首先将时钟变量 t 重新设置为 0,并重传相应的丢失数据块.每个数据块重传的次数是有界的,最大重传次数 *conut* 大小为 MAX.重传后,恢复连续发送.发布节点概率时间自动机模型的状态空间包含 8 个状态:S={*Idle*,*Pub_datablock*,*Waitack*,*Retransmit*,*Datablock_Succ*,*Success*,*Fail*,*Waitsync*}.当没有数据发送时,发布者的初始状态是空闲状态;当有数据需要发送时,将每一次通信的数据流划分成多个数据块,初始化 k 表示当前所

发送的数据块是整个数据流中第 k 个数据块,并初始化 *count* 为最大重传次数,N 表示整个数据流中数据块的个数.此时,发布者由空闲状态转移到 *Pub_datablock* 发送数据块状态,并连续不断地发送之后的数据块.每个数据块发送出去后,需要等待来自订阅者的确认信息.若在时间 *timeout* 之内收到确认信息 *flag*=true,则状态转移到 *Datablock_Succ* 数据块传输成功状态.在 *Datablock_Succ* 状态时,需要判断当前所传数据块是否是整个数据流的终止数据块:若当前数据块为终止数据块,转换到 *Success* 成功状态,表示整个数据流传输成功,之后返回至 *Idle* 状态;否则,将回到 *Pub_datablock* 状态,接着发送下一个数据块.若在发送其中一个数据块时,在 *timeout* 时间内没有收到来自订阅者的确认信息,则进入 *Retransmit* 重传状态.在最大重传次数内,可以允许重传当前数据块,直到收到来自订阅者的确认信息.当重传次数用尽却没有发送完终止数据块或已经发送了终止数据块但没有收到来自订阅者确认信息,则状态转移到 *Fail* 状态,表示数据流传输失败.在 *Fail* 状态时,发布者进入 *Waitsync* 状态,初始化同步信号 *sync_signal* 为 false,等待与订阅者同步;当 *sync_signal* 为 true 时,表示发布者与订阅者状态同步,返回到 *Idle* 状态.

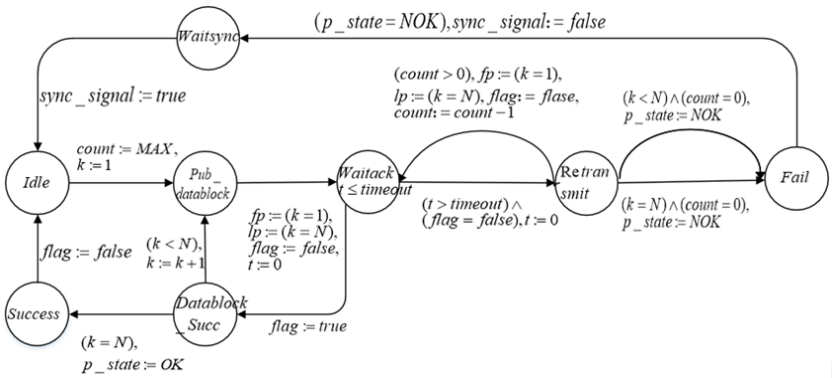

Fig.4 Probabilistic time automata model of data publish node

图 4 数据发布节点概率时间自动机模型

如图 5 所示为数据订阅节点的概率时间自动机模型.

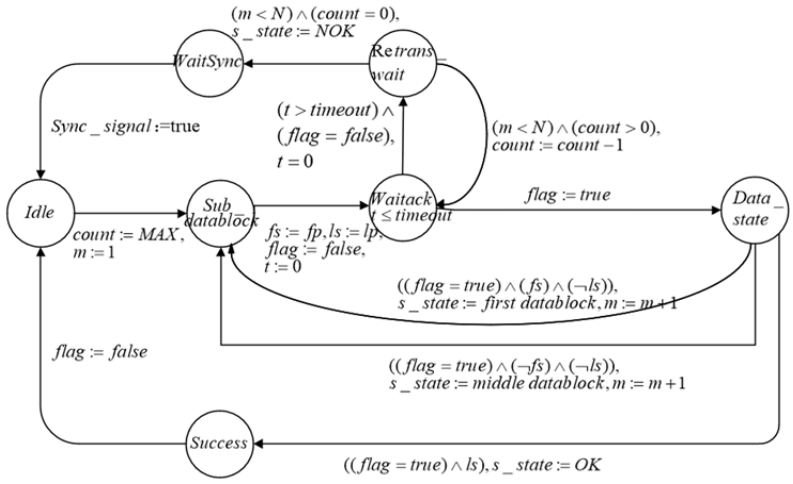

Fig.5 Probabilistic time automata model of data subscription node

图 5 数据订阅节点概率时间自动机模型

数据订阅节点模型的状态空间包含 7 个状态:S={*Idle*,*Sub_datablock*,*Waitack*,*Retrans_wait*,*WaitSync*, *Success*,*Data_state*}.订阅者将要订阅的数据信息与发布者发布表中的数据信息进行匹配:若匹配成功,则相应

的发布者将发布的数据传输到订阅者.当没有数据订阅时,订阅者的初始状态是空闲状态.一旦有新的数据块到达时,初始化 *m* 表示当前所要接收的数据块是整个数据流中第 *m* 个数据块,并初始化 *count* 为最大重传次数.此时,订阅者由空闲状态转移到 *Sub_datablock* 状态.在 *Sub_datablock* 状态时,订阅者等待接收数据块.每个数据块订阅成功后,订阅者将标记位 *flag* 取反,以返回确认信息至发布者.若在时间 *timeout* 之内,订阅者成功接收到数据块,则从 *Waitack* 状态转移到 *Data_state* 数据流传输情况状态.在 *Data_state* 状态时,需要判断当前所接收的数据块是否是所订阅数据流的终止数据块:若当前数据块为终止数据块,则代表整个数据流订阅成功,返回 *Idle* 状态;否则,将回到 *Sub_dataBlock* 等待接收下一个数据块.若在 *timeout* 时间内订阅者没有接收到数据块,则从 *Waitack* 状态转移至 *Retrans_wait* 等待重传状态,等待发布者重传当前没有收到的数据块.当重传次数不为 0 时,则等待订阅之前丢失的数据块;当发布者重传次数用尽时,订阅者仍有未接收的数据块,则订阅失败,状态转移到 *WaitSync* 状态.在 *WaitSync* 状态时,等待同步信号.当接收到同步信号 *sync_signal* 时,订阅者状态返回至 *Idle* 状态.

2.2.2 全局数据空间概率时间自动机模型

发布订阅的节点调度匹配过程的具体实现在全局数据空间模块中,该模块主要由发布主题表 *P_table*、订阅主题表 *S_table*、订阅失败表 *S_fail_table*、发布数据缓冲区 *data_pool* 和匹配标志 *pair* 变量组成.在全局数据空间模块中:处理发布数据信息的最小时间为 *TPL*,最大时间为 *TPH*;处理订阅数据信息的最小时间为 *TSL*,最大时间为 *TSH*.图 6 表示全局数据空间的概率时间自动机模型,全局数据空间模型的状态空间包含 5 个状态:

$$S=\{Idle,PUB,P\_match,S\_match,SUB\}.$$

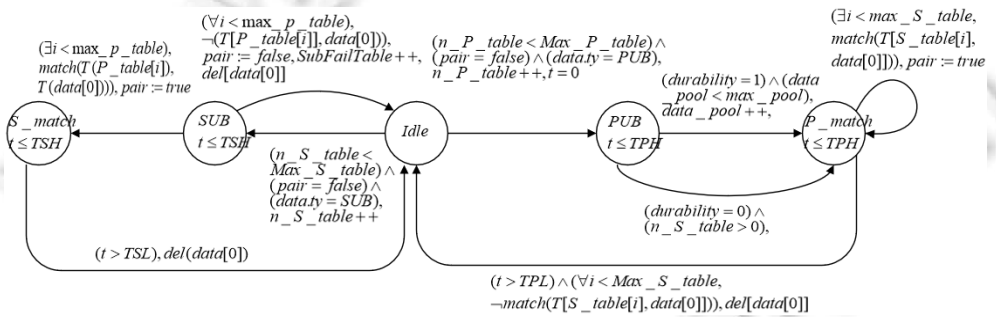

Fig.6 Probabilistic time automata module of global data space

图 6 全局数据空间概率时间自动机模型

当全局数据空间中发布节点的缓冲区非空时,取出缓冲区第 1 条数据信息并判断其类型.如果是发布信息,则判断发布节点的发布主题表 *P_table* 有没有满:若不满,则将要发布数据的主题信息和所对应的 QoS 参数信息添加到该节点的发布表中.发布者变更发布主题表,并将该发布信息同步计入同一 DDS 域中每一个节点的发布主题表中,以保持发布主题表的全局一致性.此时,全局数据空间状态转移至 *PUB* 状态.在 *PUB* 状态时,需要判断发布主题信息及所对应的 *durability* 属性的值:若 *durablity*=1,则将要发布的数据保存在 *data_pool* 中,以便之后新加入的节点订阅;若 *durabilty* 值为 0,则不需要将发布数据保存.在全局数据空间中,当状态转移至 *P_match* 状态时,将要发布数据的节点与订阅表中的订阅节点进行匹配:若要发布数据节点的主题信息及对应的 QoS 参数信息与订阅表中的订阅节点一致,则匹配成功,发布者将要发布的数据发送给对应的订阅者;若匹配失败,则返回空闲状态.其中,*match* 是一个布尔函数,它的参数分别为发布数据信息和订阅表内的一条订阅数据信息.若两者匹配,系统根据函数返回值以及匹配节点的 QoS 策略,选择需要发布或者订阅的节点进行通信,当匹配成功时,会赋值 *pair* 变量为 true.

如果是订阅信息,则判断订阅者的订阅表有没有满:如果订阅表已满,根据溢出处理策略,丢弃该条订阅消息;若不满,则将要订阅数据的主题和所对应的 QoS 参数信息添加至该订阅节点所对应的订阅表中.此时,全局数据空间状态转移至 *SUB* 状态.在 *SUB* 状态时,需要将要订阅者与发布主题表中的发布者进行匹配.在发布主题

表中,若存在主题信息及其对应的 QoS 参数信息一致的发布者,则匹配成功.若有多个发布者满足条件,则按照一定策略选取一个作为订阅的对象.若不存在主题信息与 QoS 参数一致的发布者,则订阅失败,将订阅失败记录添加到订阅失败表 *Sub_fail_table* 中.

2.2.3 通信信道概率时间自动机模型

通信信道模块主要用于发布者订阅者之间的数据传输,在数据流传输过程中,由于信道是不可靠的,可能会发生数据丢失,丢包率为 $p[i]$,在此概率下,数据会发生重传;数据成功传输的概率为 $1-p[i]$,变量 N 为整个数据流中数据块的数量,k 表示数据发布者当前正在传输的数据块是数据流中的第 k 个数据块,m 表示数据订阅者当前正在接收的数据块是数据流中的第 m 个数据块.图 7 表示通信信道模块概率时间自动机模型.通信信道模型的状态空间包含 4 个状态:$S=\{Idle,Transmit,Success,Fail\}$.当发布订阅节点匹配成功后,数据发布者将会将数据发送给主题信息与 QoS 参数一致的订阅者.当发送的数据块没有达到 N 时,说明仍有没有发送的数据块,则通信信道由空闲状态转移到 *Transmit* 状态,发送当前的数据块.如果在时钟变量 *timeout* 内,订阅者收到来自发布者发送的数据块以及发布者收到来自订阅者的确认信息 *flag*=true,则说明当前数据块传输成功,然后状态转移到 *Idle*,等待传输下一个数据块;否则说明数据传输失败,状态转移至 *Fail* 状态,重置时钟变量,回到 *Idle* 状态等待该数据块的重传.

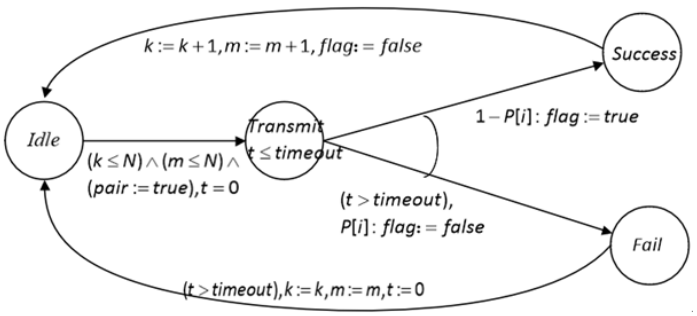

Fig.7 Probabilistic time automata moduleof communication channel

图 7 通信信道概率时间自动机

3 属性抽象与形式化表达

为了验证系统功能的正确性,本文抽取 3 个关键属性.属性的抽象表示如下:

(1) 安全性

对于面向数据流的 ROS2 通信系统,如果系统在某个时刻进入死锁状态,则系统不能正常运行.在 PRISM 中,验证系统无死锁的属性可以表示为:“*init*”=>$P\geqslant 1$[true & !“*deadlock*”].

(2) 可靠性

不同的应用对 DDS 性能的要求不同.DDS 提供了 Best-Effort(高效传输),Reliable(可靠传输)两种传输方式,以满足不同应用的需要.通过 QoS 属性的配置,可以对数据传输方式进行选择.可靠传输模式对于 DDS 来说,它应该在不同的条件下完成规定大小数据的分发.

属性 $R=?[C\leqslant t]$ 为 PRISM 中的累计奖励公式,主要是计算在时间 t 内,数据发布订阅成功传输的累计数据量.在实验中,我们使用计算时间 t 内数据成功传输的数据量的属性,验证在 QoS 为可靠传输时的数据传输情况.在模型中使用了两个参数 N,P,分别表示传输数据的数据量、信道的数据丢包率,如图 8 所示.实验中设置整个数据流中数据块块数 N 为 20,验证在不同数据丢包率 P 的情况下,完成数据传输所对应的不同的奖励期望值 R 是多少.从实验结果可以看出:在 QoS 为可靠传输方式的情况下,随着数据丢包率的变化,每个曲线都很接近,并最终显示都可以完成规定数据流大小的数据传输,即奖励期望值 R 与数据块块数 N 相等都为 20.验证了 DDS 在 QoS 为可靠传输下数据传输的可靠性.这表明:DDS 在可靠传输模式时,因其较好的数据重传机制,发送数据成

功率不会受到数据丢包率的影响.因此,系统在可靠传输模式下具有高可靠性.

在图 9 中,我们验证了在 Best-Effort 高效传输时数据流传输的情况.数据发布订阅成功的概率属性表示为:

lable "*PubSub_Success*"=(*p_state*=1) & (*s_state*=1); *P*=?[*F* "*PubSub_Success*"].

其中,*p_state*=1 表示发布者成功发布数据,*s_state*=1 表示订阅者成功订阅数据.实验中,*M* 表示数据流大小,设置不同的数据丢包率 *p*,从实验结果可以看出:在信道数据丢包率一定的情况下,数据传输随着数据流字节数的增大,数据流在高效传输模式下数据传输成功的概率降低;在数据流大小一定的情况下,数据丢包率增大,数据流传输成功的概率减小,可靠性降低.

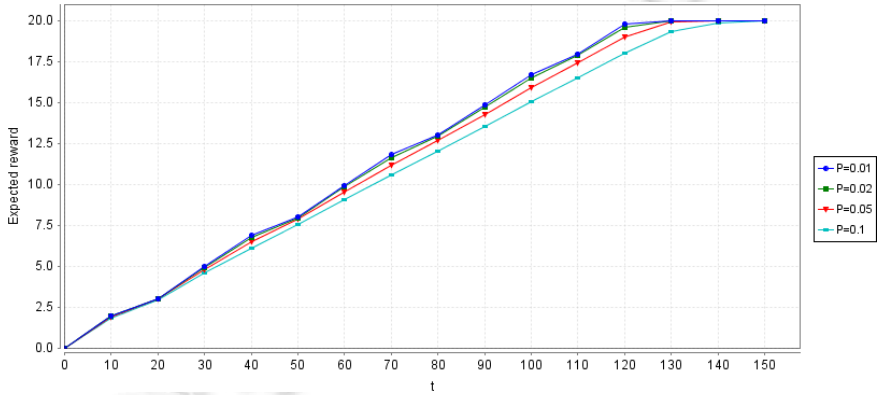

Fig.8 System reliability in Reliable communication mode

图 8 Reliable 通信模式下系统的可靠性

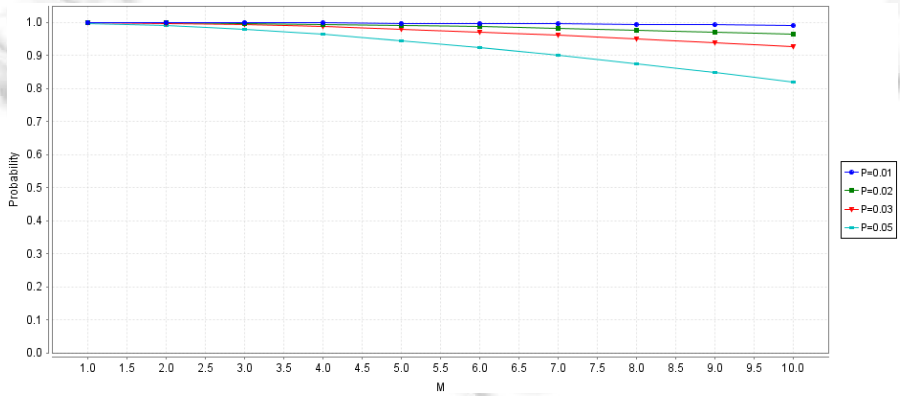

Fig.9 System reliability in Best-effort communication mode

图 9 Best-effort 通信模式下系统的可靠性

(3) 实时性

在计算系统运行时间时,可采用 PRISM 中的奖励结构来计算发布者和订阅者之间完成数据通信所需要的时间.*rewards* 结构为:

rewards "*time*"

[*data_transmit*] true: *responsetime*;

[*retrans*] true: *responsetime*;

endrewards

使用属性 *R*{"*time*"}=?[*F* "*PubSub_Success*"]分析验证不同的数据丢包率下,DDS 两种传输模式传输数据时系统响应时间的情况.在实验中,我们对数据发布者和数据订阅者之间进行数据流通信的每个过程奖励一个常

量 *response time*.在完成通信时,统计奖励值,依此标志节点通信所需要的响应时间.实验中,我们设置数据流大小 *M* 为 10;设置 Reliable1 和 Best-Effort1 策略下数据丢包率相同,均为 0.05;Reliable2 和 Best-Effort2 策略下的数据丢包率相同,均为 0.1.如图 10 所示,实验中,我们验证了两种 DDS 策略在不同传输方式下的响应时间.可以看出:在数据丢包率相同时,可靠传输模式因其良好的重传确认机制,系统响应时间比高效传输方式响应时间久;在数据丢包率不同时,在相同的数据传输策略下,丢包率越大,系统响应时间越久.

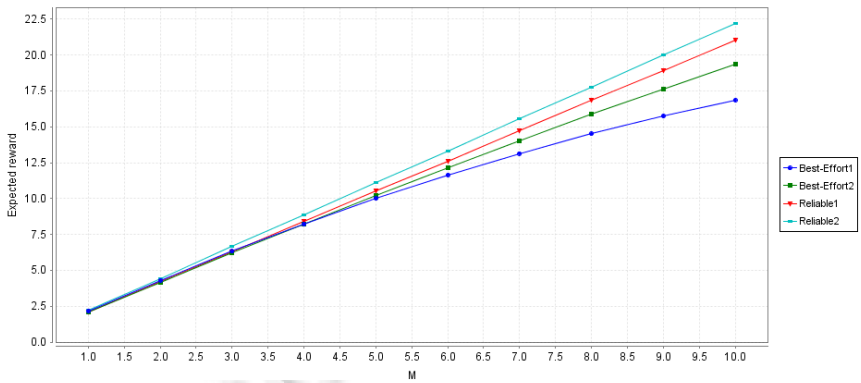

Fig.10 Influence of QoS policy on system responsetime

图 10 QoS 策略对系统响应时间的影响

在数据分发服务的数据传输中,为满足不同的通信需求,每个传输数据的过程以及数据写入者、数据读取者、发布者和订阅者等实体对象都配有相应的 QoS 策略.在系统可靠性与实时性上,ROS2 的不同节点在通信时采用了适当的服务质量策略,其通信服务可以选择可靠传输服务,也可以选择尽可能快速的数据传输服务.但如果在某些特定的网络环境对数据分发的性能有相关需求,则可以自定义相关的 QoS 策略.通过对以上的属性提取与实验验证,可以针对不同的服务需求与网络环境更改相应的 QoS 策略.当处于网络环境较差的条件下,即上述实验中当丢包率较大时,可调节 QoS 策略中的 RELIABLITY 属性,即增加系统数据流方式传输中的重传次数,以实现系统较高的稳定性;在相同网络环境下,为保证系统数据的实时传输,即减少上述实验的响应时间,可选择 BEST-EFFORT 服务质量策略,即系统要求尽可能速度快的方式交付与处理数据,则需要调整数据传输过程中的数据块大小以及重传次数等相应的参数,以尽可能实现较高的实时性.

4 总 结

本文提出了一种基于 DDS 的 ROS2 通信系统的抽象模型的形式化验证框架,应用概率模型检测器 PRISM 通过分析数据丢失率和系统响应时间,从而验证 ROS2 通信系统的实时性、可靠性.并通过加入重传机制、QoS 策略量化分析,实现不同的数据需求和传输方式.本文的形式化建模框架为面向数据流的分布式数据分发服务的形式化建模、验证和量化性能分析提供参考.基于本文的工作,下一步我们将基于本文所提出的框架,针对不同应用领域分布式众节点之间通信的数据分发服务进行层次化的建模与性能分析,为实现性能优良的应用系统设计提供参考.

References:

[1] Jiang Z, Gong Y, Zhai J, *et al*. Message passing optimization in robot operating system. Int'l Journal of Parallel Programming, 2019,48(1):119−136.

[2] Pardo-Castellote G, Farabaugh B, Warren R. An introduction to DDS and data-centric communications. RTI, 2005.

[3] García-Valls M, Domínguez-Poblete J, Touahria IE. Using DDS middleware in distributed partitioned systems. ACM SIGBED Review, 2018,14(4):14−20.

[4] Dong W, Wang J, Qi ZC. Model checking for concurrent and real-time systems. Computer Research and Development, 2001, 38(6):698−705 (in Chinese with English abstract).

[5] He F, Baresi L, Ghezzi C, *et al*. Formal analysis of publish-subscribe systems by probabilistic timed automata. In: Proc. of the Int'l Conf. on Formal Techniques for Networked and Distributed Systems. Berlin, Heidelberg: Springer, 2007. 247−262.
[6] Liu Y, Guan Y, Li X, *et al*. Formal analysis and verification of DDS in ROS2. In: Proc. of the 2018 16th ACM/IEEE Int'l Conf. on Formal Methods and Models for System Design (MEMOCODE). IEEE, 2018. 1−5.
[7] Yin J, Zhu H, Fei Y, *et al*. Formalization and verification of RTPS StatefulWriter module using CSP. In: Proc. of the 31st Int'l Conf. on Software Engineering and Knowledge Engineering. 2019.
[8] Maruyama Y, Kato S, Azumi T. Exploring the performance of ROS2. In: Proc. of the 13th Int'l Conf. on Embedded Software. ACM, 2016. 5.
[9] Inglés-Romero JF, Romero-Garcés A, Vicente-Chicote C, *et al*. A model-driven approach to enable adaptive QoS in DDS-based middleware. IEEE Trans. on Emerging Topics in Computational Intelligence, 2017,1(3):176−187.
[10] Casini D, Blaß T, Lütkebohle I, *et al*. Response-Time analysis of ROS 2 processing chains under reservation-based scheduling. In: Proc. of the 31st Euromicro Conf. on Real-Time Systems (ECRTS 2019). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019.
[11] Kim J, Smereka JM, Cheung C, *et al*. Security and performance considerations in ROS 2: A balancing act. 2018.
[12] Schlesselman JM, Pardo-Castellote G, Farabaugh B. OMG data-distribution service (DDS): Architectural update. In: Proc. of the IEEE MILCOM 2004 Military Communications Conf. IEEE, 2004. 961−967.
[13] Guesmi T, Rekik R, Hasnaoui S, *et al*. Design and performance of DDS-based middleware for real-time control systems. IJCSNS, 2007,7(12):188−200.
[14] Corsaro A, Schmidt DC. The data distribution service—The communication middleware fabric for scalable and extensible systems-of-systems. System of Systems, 2012.
[15] Chen C. Design and implementation of data distribution system based on DDS [Master. Thesis]. Shamghai: Fudan University, 2008 (in Chinese with English abstract).
[16] Norman G, Parker D, Sproston J. Model checking for probabilistic timed automata. Formal Methods in System Design, 2013,43(2): 164−190.
[17] Kwiatkowska M, Norman G, Parker D. PRISM: Probabilistic symbolic model checker. In: Proc. of the Int'l Conf. on Modelling Techniques and Tools for Computer Performance Evaluation. Berlin, Heidelberg: Springer, 2002. 200−204.
[18] Kwiatkowska M, Norman G, Parker D. PRISM: Probabilistic model checking for performance and reliability analysis. ACM SIGMETRICS Performance Evaluation Review, 2009,36(4):40−45.

附中文参考文献:

[4] 董威,王戟,齐治昌.并发和实时系统的模型检验技术.计算机研究与发展,2001,38(6):698−705.
[15] 陈春甫.基于 DDS 的数据分发系统的设计与实现[硕士学位论文].上海:复旦大学,2008.

芦倩(1993－),女,硕士,主要研究领域为嵌入式系统形式建模与验证,网络协议分析.

王瑞(1981－),女,博士,教授,博士生导师,主要研究领域为形式化方法,软件安全验证.

李晓娟(1968－),女,博士,教授,博士生导师,主要研究领域为嵌入式系统形式建模与验证,网络协议分析.

施智平(1974－),男,博士,教授,博士生导师,主要研究领域为形式化方法,人工智能.

关永(1966－),男,博士,教授,博士生导师,主要研究领域为形式化验证,高可靠嵌入式系统,机器人.