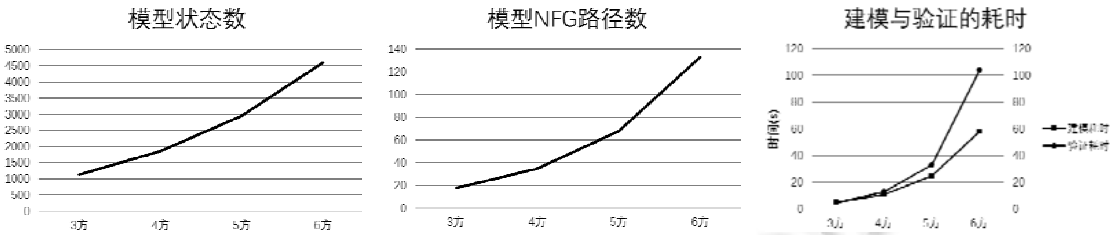

(a) (b) (c)

Fig.9 Four different modeling and verification situations

图 9 4 种不同建模和验证情况

6 相关工作

目前,大多数时序逻辑编程语言,如前文提到过的 METATEM,XYZ/E 和 Tempura,也支持基于消息传递的通信机制,用于描述并发和分布式系统中的通信,但都存在一定的不足.METATEM 代理之间通过广播或多播消息传递来相互通信,且由于 METATEM 代理的组件互相独立,所以对于同步和异步系统都适用[23].虽然从逻辑的角度来看这是个合理模型,但这种方法代价大并且不适合表示非扁平化和结构化系统.XYZ/E 中用一个变量表示通道,这个通道被视为一次存储一条信息的单缓冲区,基于消息传递的通信机制的实现依赖于两个通道:一个用于进程输出数据的写通道,一个用于进程读入数据的读通道[10].这种方法虽然灵活,但当一个通道同时被多个进程访问时,就会产生冲突[15].而 Tempura 中通过引入一个带端口的流包来对并行进程之间的同步通信进行建模,相关文献[11]中也给出了相应的通信语句和简单示例,但具体的实现细节在文献中并没有提及.在经典进程代数中,如 CCS[24]、π-演算[25]和 CSP[19],只支持同步通信,没有消息缓冲区或通道来连接通信代理,但是异步通信可以通过在两个通信实体之间引入缓冲代理进行建模.本文实现的 MSVL 通信机制同样基于消息传递,但是与上述方法不同,采用先进先出队列表示通道,引入面包店算法解决互斥问题,并给出了通道结构、通信语句和进程结构的形式化定义,适用于同步系统和异步系统的建模与验证.

7 结 论

为了更好地对分布式并发系统进行建模与验证,给 MSVL 增加了消息传递的通信机制,给出了通信的形式化定义,包括通道结构、面包店算法、通信语句和进程结构.通道被定义为一个存储消息的有界 FIFO 队列.面包店算法及通信语句用于对通道进行加锁及访问,解决了互斥问题.进程定义为 MSVL 的组合语句,用来描述系统的行为模式.研究了消息传递的通信机制在 MSV 平台中的实现机制.在 MSV 平台中,对多方电子合同签名协议进行建模与验证,表明该通信机制是有效的.验证了该协议的公平性与乐观性,验证了一个不可满足的测试性质并给出了反例.将来的研究工作包括将具有通信机制的 MSVL 应用到更多实际的通信系统中,如社交网络.

References:

[1] Leeuwen JV. Handbook of Theoretical, Computer Science, Vol.B: Formal Models and Semantics. London: The MIT Press, 1994. 298−306. [doi: 10.1016/0167-6423(95)90009-8]

[2] Baier C, Katoen J. Principles of Model Checking. London: The MIT Press, 2008.

[3] Tian C, Duan ZH. Expressiveness of propositional projection temporal logic with star. Theoretical Computer Science, 2011,412: 1729−1744. [doi: 10.1016/j.tcs.2010.12.047]

[4] Fisher M. An Introdution to Practical Formal Methods Using Temporal Logic. Wiley Publishing, 2011.

[5] Wang M, Duan ZH, Tian C. Simulation and verification of the virtual memory management system with MSVL. In: Hou JL, Trappey AJC, eds. Proc. of the CSCWD 2014. Danvers: IEEE, 2014. 360−365. [doi: 10.1109/cscwd.2014.6846870]

[6] Zhang P, Duan ZH, Tian C. Simulation of CTCS-3 protocol with temporal logic programming. In: Shen WM, Li WD, eds. Proc. of the CSCWD 2013. Piscataway: IEEE, 2013. 72−77. [doi: 10.1109/cscwd.2013.6580942]

[7] Yu Y, Duan ZH, Tian C, Yang MF. Model checking C programs with MSVL. In: Liu SY, ed. Proc. of the SOFL 2012. LNCS 7787. London: Springer-Verlag, 2013. 87−103. [doi: 10.1007/978-3-642-39277-1_7]

[8] Duan ZH, Tian C. A unified model checking approach with projection temporal logic. In: Liu SY, Maibaum T, Araki K, eds. Proc. of the ICFEM 2008. LNCS 5256. London: Springer-Verlag, 2008. 167−186. [doi: 10.1007/978-3-540-88194-0_12]

[9] Scott ML. Programming Language Pragmatics. 3rd ed. San Francisco: Morgan Kaufmann Publishers, 2009. [doi: 10.1016/b978-0-12-374514-9.x0001-8]

[10] Ma HD, Liu SQ. Multimedia data modeling based on temporal logic and XYZ system. Journal of Computer Science and Technology, 1999,14(2):188−193. [doi: 10.1007/bf02946527]

[11] Moszkowski B. Executing Temporal Logic Programs. New York: Cambridge University Press, 1986. [doi: 10.1017/s0022481200029169]

[12] Lee EA. The problem with threads. IEEE Computer, 2006,39(5):33-42. [doi: 10.1109/mc.2006.180]

[13] Herlihy M, Shavit N. The Art of Multiprocessor Programming. San Francisco: Morgan Kaufmann Publishers, 2012. [doi: 10.1145/1146381.1146382]

[14] Baum-Waidner B. Optimistic asynchronous multi-party contract signing with reduced number of rounds. In: Orejas F, Spirakis PG, Leeuwen JV, eds. Proc. of the ICALP 2001. LNCS 2076. London: Springer-Verlag, 2001. 898−911. [doi: 10.1007/3-540-48224-5_73]

[15] Mo DP, Wang XB, Duan ZH. Asynchronous communication in MSVL. In: Qin S, Qiu Z, eds. Proc. of the ICFEM 2011. LNCS 6991. London: Springer-Verlag, 2011. 82−97. [doi: 10.1007/978-3-642-24559-6_8]

[16] Duan ZH, Yang XX, Koutny M. Framed temporal logic programming. Science of Computer Programming, 2008,70(1):31−61. [doi: 10.1016/j.scico.2007.09.001]

[17] Charronbost B, Mattern F, Tel G. Synchronous, asynchronous, and causally ordered communication. Distributed Computing, 1996, 9(4):173−191. [doi: 10.1007/s004460050018]

[18] Cormen T, Leiserson C, Rivest R. Introduction to Algorithms. 3rd ed., London: The MIT Press, 2009.

[19] Hoare CAR. Communicating Sequential Processes. Upper Saddle River: Prentice-Hall, 1985. [doi: 10.1007/978-3-662-09507-2_19]

[20] Yang XX, Duan ZH. Operational semantics of framed tempura. The Journal of Logic and Algebraic Programming, 2008,78(1): 22−51. [doi: 10.1016/j.jlap.2008.08.001]

[21] Duan ZH. Temporal Logic and Temporal Logic Programming. Beijing: Science Press, 2006.

[22] Luo L, Duan ZH, Tian C, Wang XB. A structural transformation from $p-\pi$ to MSVL. Journal of Combinatorial Optimization, 2015, 29(1):308−329. [doi: 10.1007/s10878-014-9779-0]

[23] Fisher M. MetateM: The story so far. In: Bordinni RH, ed. Proc. of the ProMAS 2005. LNAI 3862. London: Springer-Verlag, 2005. 3−22. [doi: 10.1007/11678823_1]

[24] Milner R. A Calculus of Communicating Systems. New York: Springer-Verlag, 1980. [doi: 10.1007/3-540-10235-3]

[25] Milner R. Communicating and Mobile Systems: The π-calculus. New York: Cambridge University Press, 1999. [doi: 10.1016/s0167-6423(00)00008-3]

王小兵(1979－),男,湖北武汉人,博士,副教授,CCF 高级会员,主要研究领域为形式化方法,时序逻辑程序设计.

郭文轩(1994－),男,硕士,主要研究领域为形式化方法,时序逻辑程序设计.

段振华(1948－),男,博士,教授,博士生导师,CCF 杰出会员,主要研究领域为网络计算,高可信软件理论和技术.