网络、通信与安全

并发系统的安全性与活性的验证方法

李 杨[1],程建华[2],房鼎益[1],陈晓江[1],冯 健[1]

1.西北大学 信息科学与技术学院，西安 710127
2.九江学院 信息科学与技术学院，江西 九江 332005

摘要　　网络环境下的分布式系统是典型的并发系统。安全性和活性是并发系统最为关注和需要保证的两个主要性质。然而在并发系统建模和形式化验证时，面临着描述繁琐、复杂和难以理解的问题，特别是当并发系统的规模（并发进程数目）较大时其性质验证时的效率问题更是严重阻碍了并发系统模型检测与验证技术的应用。将组合可达性分析和标号迁移系统的模块化思想与模型验证技术相结合，提出了一套有效的性质验证方法。论证、分析了三个并发系统安全性和活性验证定理，据此导出了并发系统的安全性与活性验证的有效算法。并通过一个简单实例，对算法有效性进行了初步验证。

关键词　　并发系统　安全性　活性　组合可达性　标号迁移系统

分类号

Verification of safety and liveness property based on concurrent system

LI Yang[1],CHENG Jian-hua[2],FANG Ding-yi[1],CHEN Xiao-jiang[1],FENG Jian[1]

1.College of Information Science and Technology,Northwest University，Xi'an 710127，China
2.College of Information Science and Technology,Jiujiang University，Jiujiang，Jiangxi 332005，China

Abstract

　Distributed system is one type of typical concurrent systems.In concurrent system，safety and liveness are the two main characteristics which should be most concerned and ensured in its application.However，we have to face the problems，in concurrent system modeling and formal verification，such as tedious description，complex and difficult understanding，and it is more serious because of the low efficiency in model checking when it is much large（with a great number of the processes）.Combining the features of good modularity in Compositional Reachability Analysis（CRA） and high efficiency in Labeled Transition System（LTS），an efficient model verification method is proposed.Three theorems for safety and liveness verification of concurrent systems are proved，and the relevant effective verification algorithms are derived.The feasibility of the algorithms is indicated through a simplified example.

Key words　concurrent system　safety　liveness　compositional reachability analysis　labeled transition system

DOI: