ISCAS 中国科学院软件研究所学术年会’2023
暨计算机科学国家重点实验室开放周

学术论文

模型检查制导的分布式系统测试方法

Model Checking Guided Testing for Distributed Systems

王栋，窦文生，高钰，吴陈傲，魏峻，黄涛

In Proceedings of the 18th European Conference on Computer Systems,
EuroSys 2022.

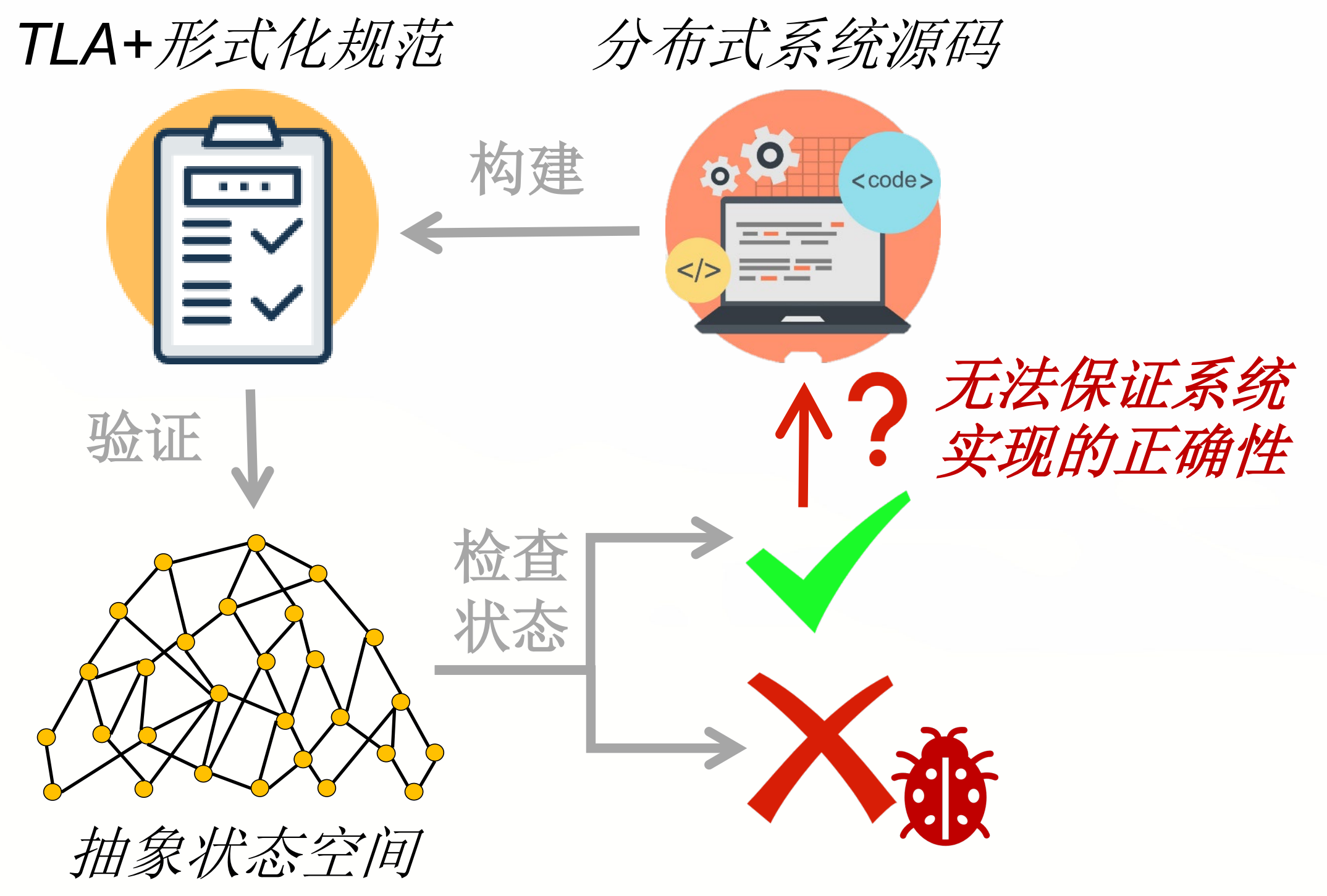
联系人：王栋, wangdong18@otcaix.iscas.ac.cn

研究背景

近年来有很多研究者和开发者利用形式化方法如**TLA+**对各类分布式系统进行验证，但形式化方法***无法保证分布式系统实现的正确性！***

mongoDB TiDB
elasticsearch
Microsoft Azure amazon

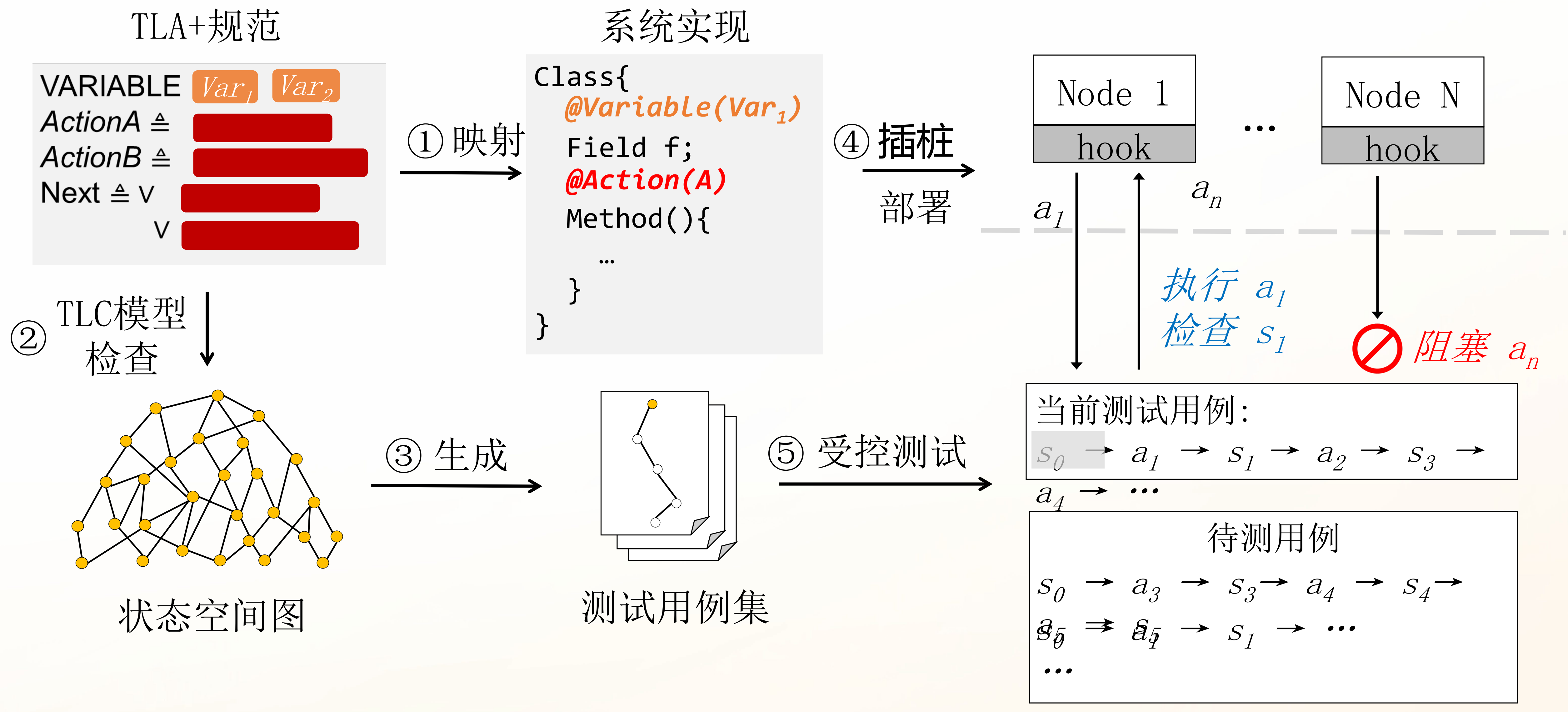
部分使用TLA+进行形式化验证的分布式系统及企业



方法概述

利用TLA+形式化规约定义的抽象状态空间指导分布式系统的测试过程

- 对分布式系统展开高精度、系统化的测试
- 检测系统测试过程中与状态空间不一致的动作和状态
- 支持对节点宕机、消息丢失等不确定性故障场景进行测试



```
Class{
  @Variable(Var1)
  Field f;
  @Action(A)
  Method(){
    …
  }
}
```

- 基于Java标注实现的映射框架
- 基于图遍历的测试用例生成算法
- 基于ASM实现的自动化实时插桩控制

应用效果

分布式共识协议Raft

- 使用Raft官方TLA+规约，并根据不同系统特性进行微调；
- 针对两个Raft系统Xraft和Raft-java展开测试

被测系统	ZooKeeper	Xraft	Raft-java
系统源码行数	1,6530	1,5895	1,5017
TLA+规约行数	841	1053	809
状态数量	10,5054	9,1532	2,3911
测试用例数量	4,4361	3,9047	9829
测试用时	123小时	75小时	13小时
发现缺陷数量	2	3	2

分布式协调系统ZooKeeper

- 根据系统源码开发了新的TLA+规约

在Xraft中找到的缺陷示例：节点重启故障导致同一集群中的Node 1/4都成为了领导者