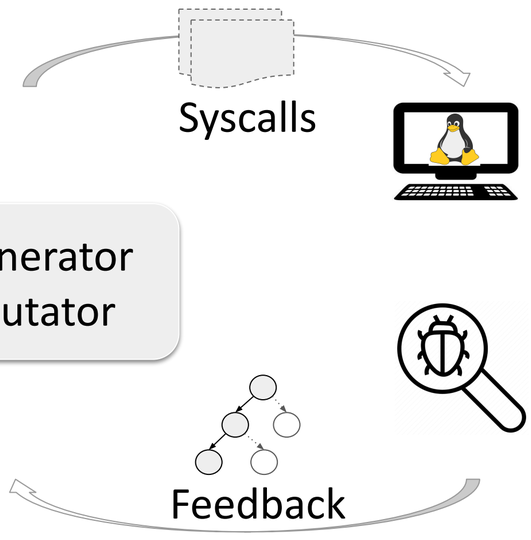
Monarch: A Fuzzing Framework for Distributed File Systems

Tao Lyu Liyi Zhang* Zhiyao Feng Yueyang Pan Yujie Ren
Meng Xu* Mathias Payer Sanidhya Kashyap

EPFL * UNIVERSITY OF WATERLOO

Fuzzing Background



Single-node in-kernel LFSes

Crash consistency (*CC*) + memory (*Mem*) bug checker

Motivation

Current LFS fuzzers are not applicable for DFSes

- Single-node kernel FS
- Syscalls
- Single-kernel state representation
- CC + Mem check

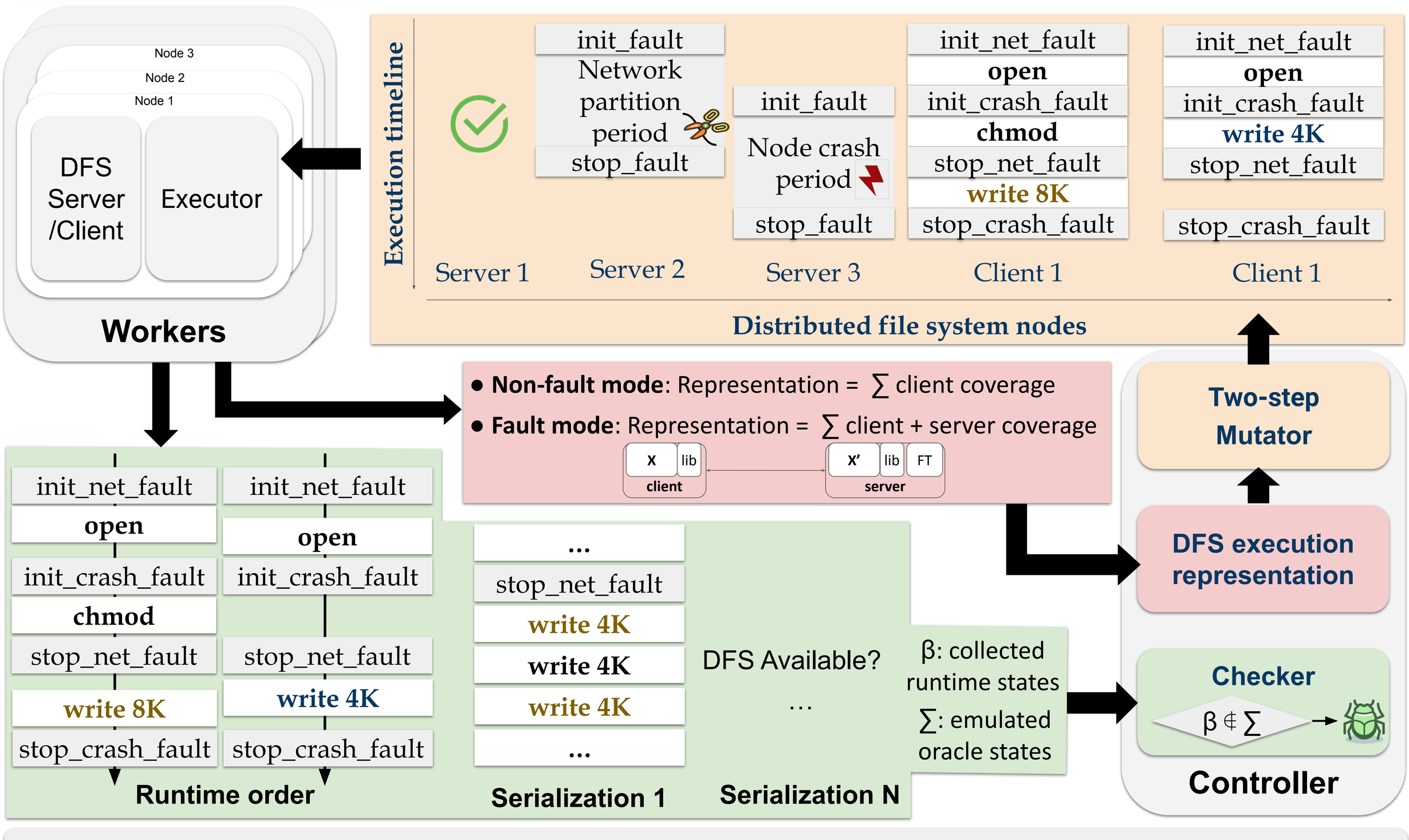
Multi-node cross-kernel (K)/ Userspace (U) fuzzing architecture

Faults as a testing input space

Representation of cross-node and cross-K/U execution states

A systematic DFS semantic checker

Monarch Design



Evaluation

DFS	Memory bugs	Semantic bugs
Lustre	8	0
GlusterFS	17	5
OrangeFS	3	0
BeeGFS	0	2
CephFS	4	1
NFS	8	0
Total	**40**	**8**

Faults play a critical role in exposing these bugs

→ 14/40 memory bugs and 3/8 semantic bugs are exposed under faults

Vulnerable code is scattered in both server and client

→ 17 bugs (servers) vs 31 bugs (clients)
→ Root causes of semantics bugs are mostly in DFS servers

Bug exposure might depend on specific DFS configurations