On Scheduling of Fuzzing Test

Hongbo Zhang ANU

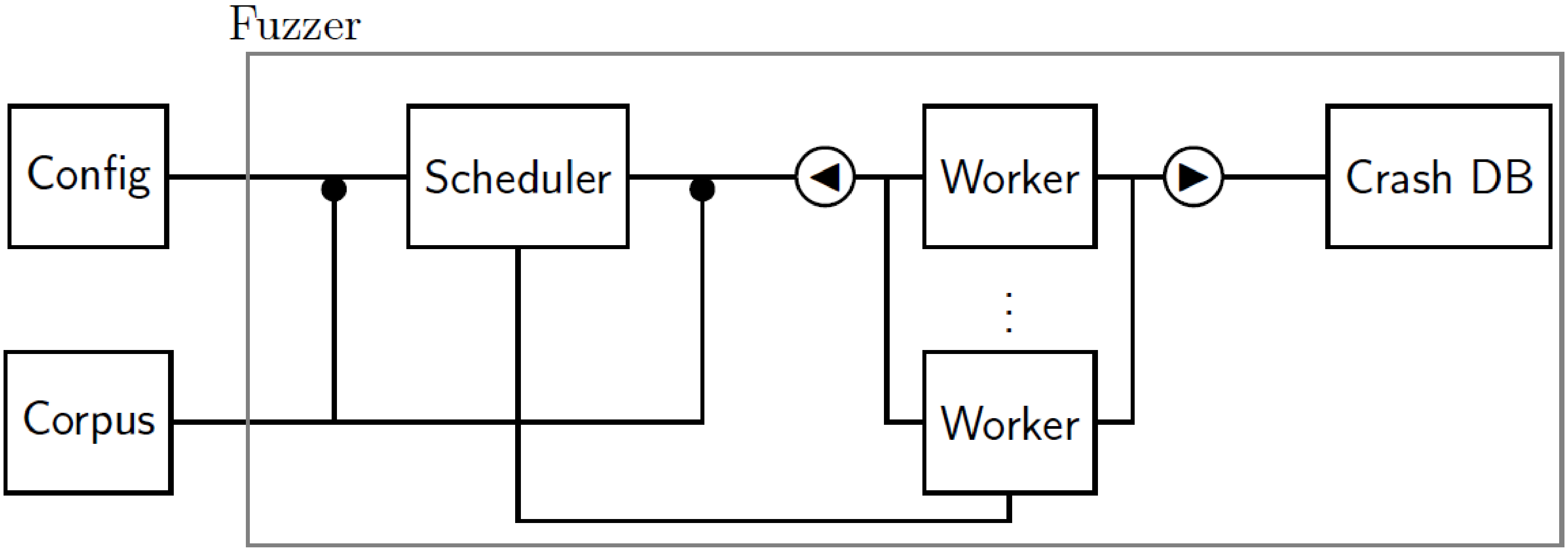
Superadvisors: Steve Blackburn, Tony Hosking, Shane Magrath

Feb 13 2017
Sydney

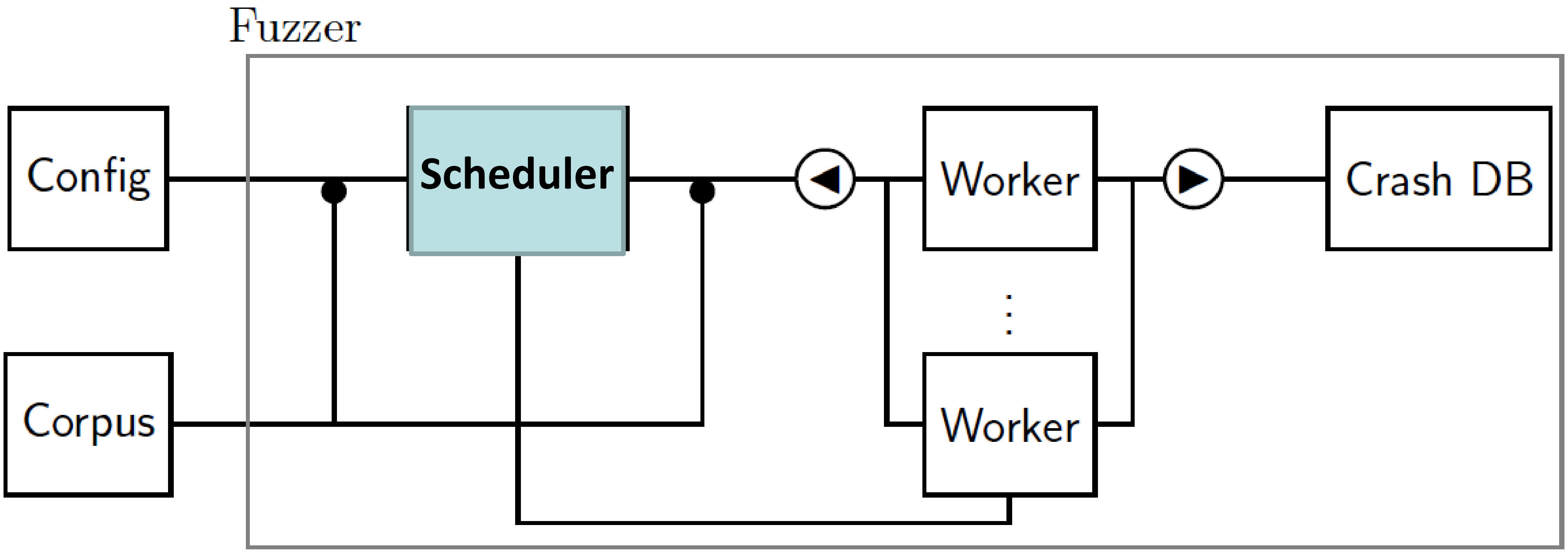
Overview

- Problem
- Model
- Result
- Discussion

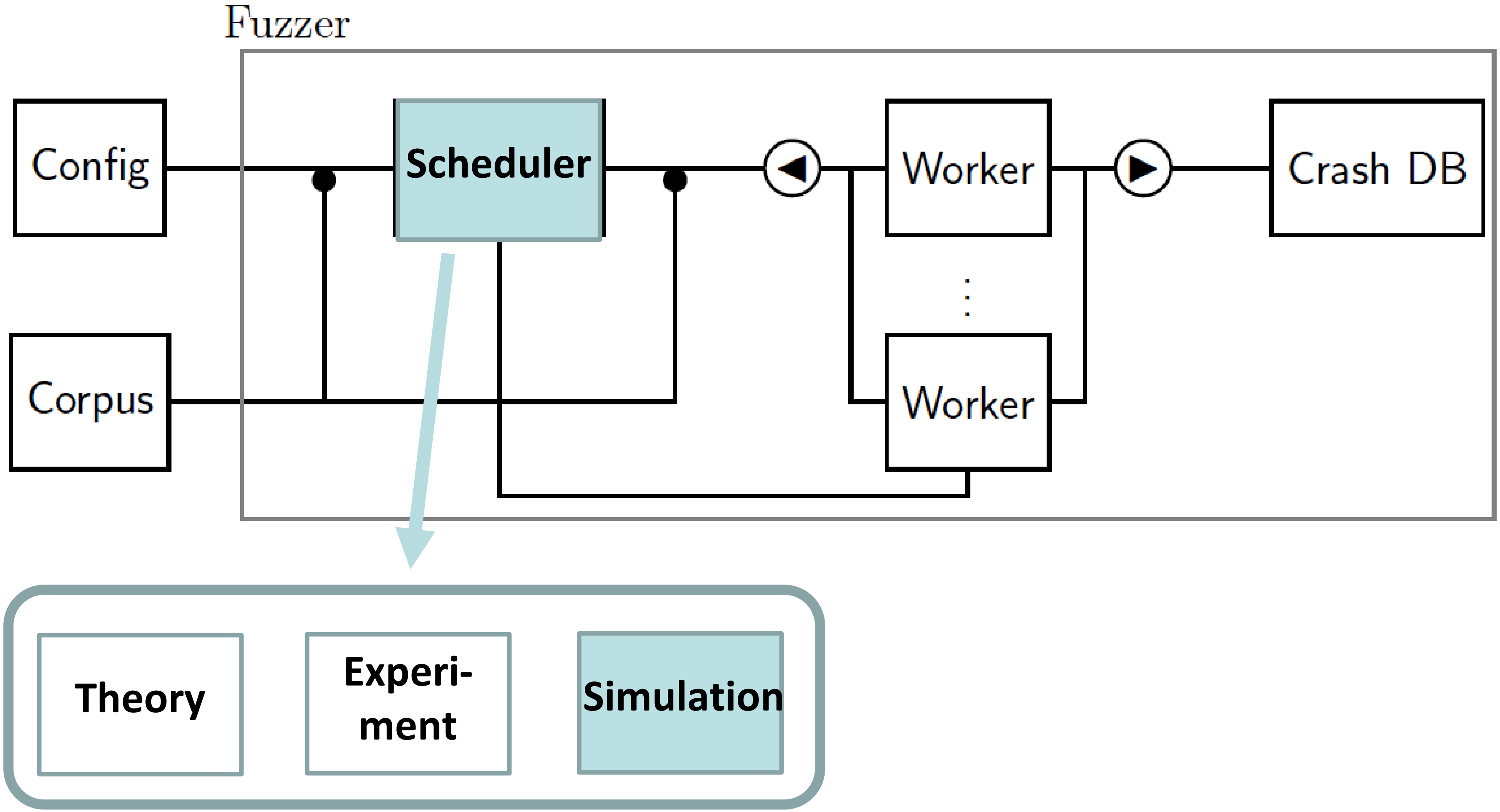
Fuzzing Test



Fuzzing Test



Fuzzing Test



Fuzzer

Config

Scheduler

Worker

Crash DB

Corpus

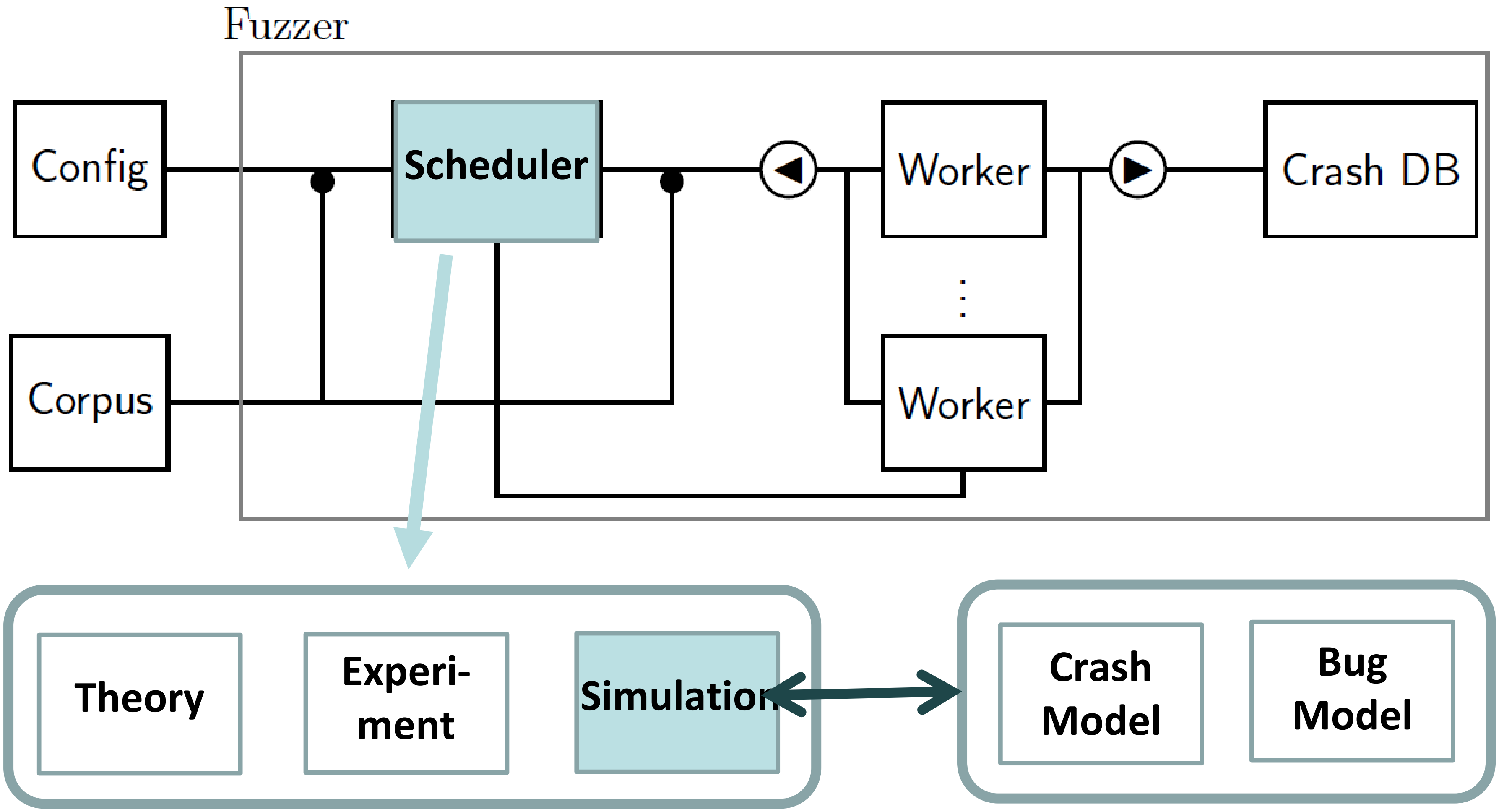
Worker

Theory

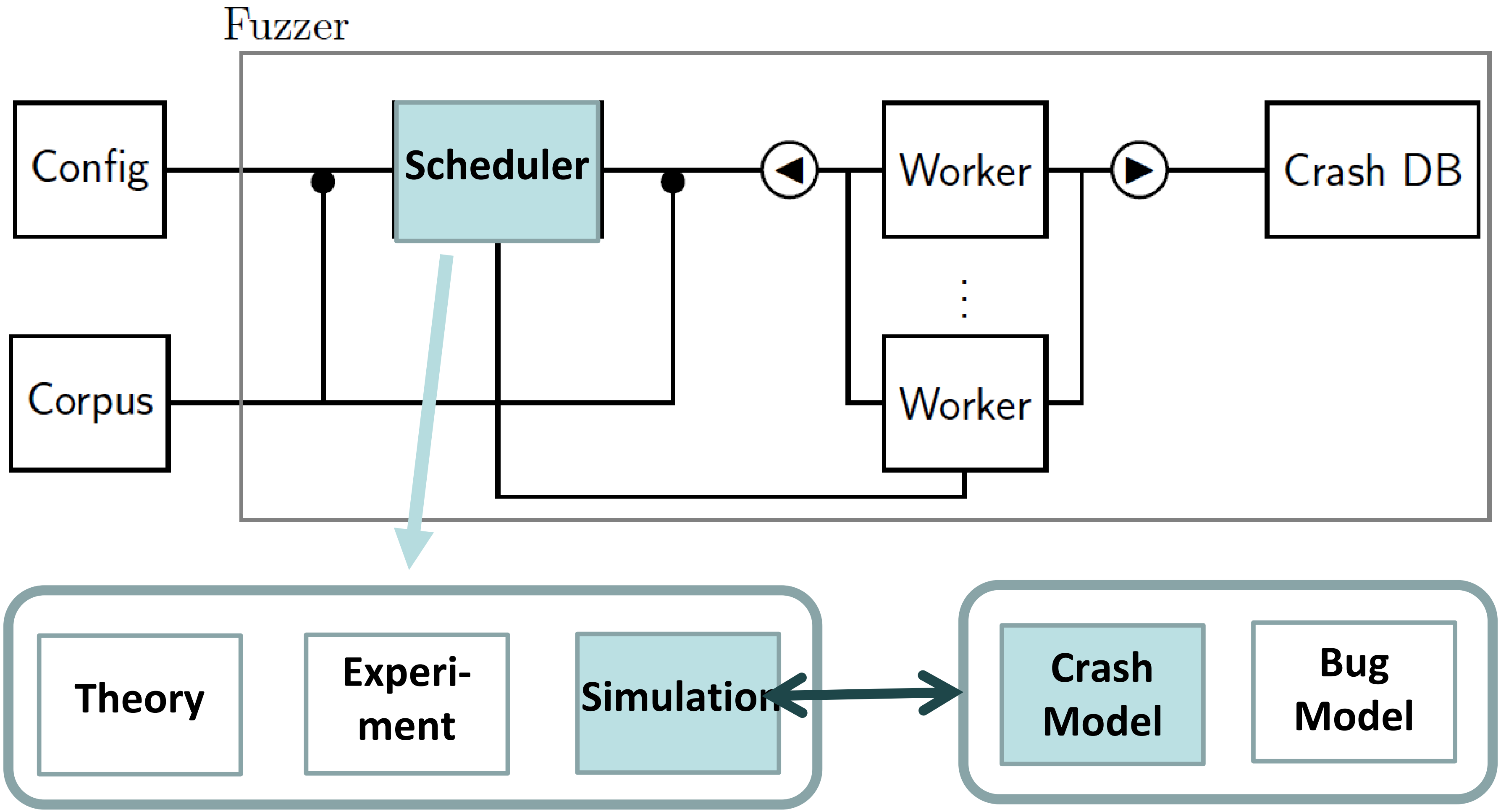
Experiment

Simulation

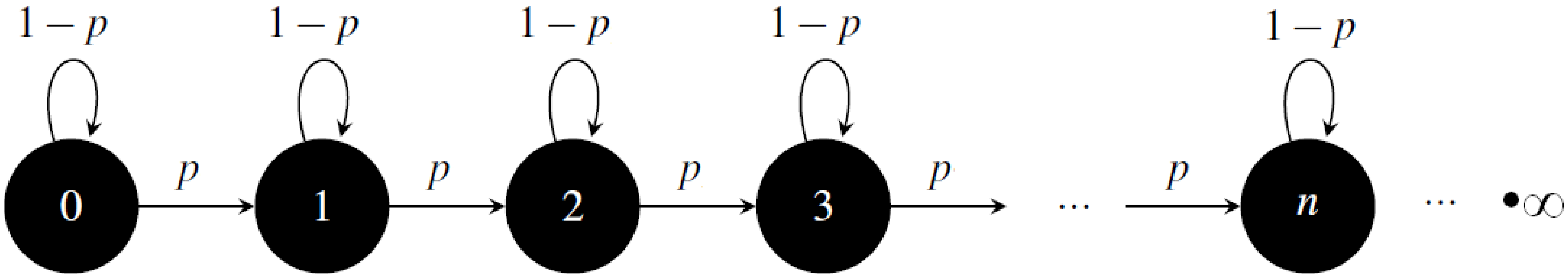
Fuzzing Test



Fuzzing Test

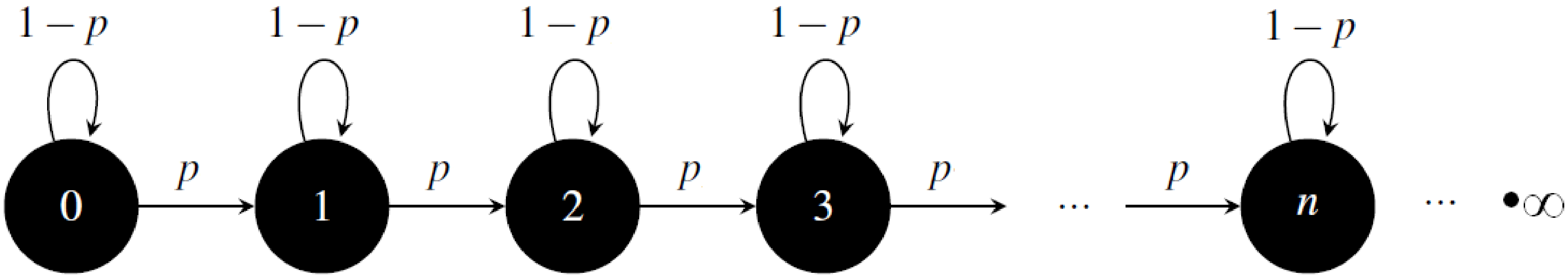


Model



Bernoulli Model

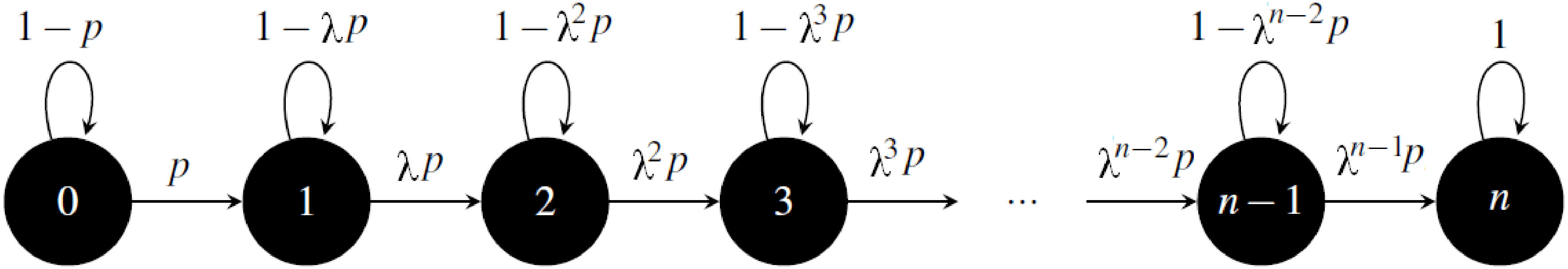
Crash Model



Bernoulli Model

- Infinite is impossible
- Probability to find a new unique crash should be decrease.

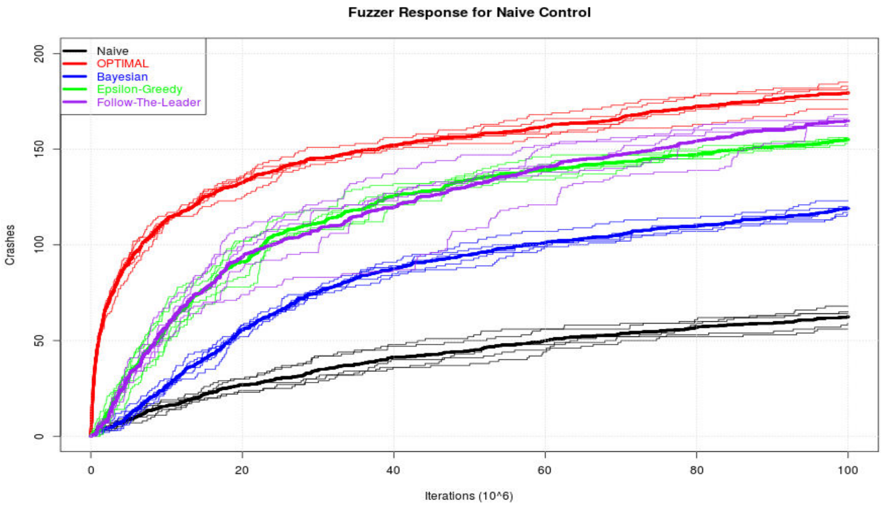
Crash Model



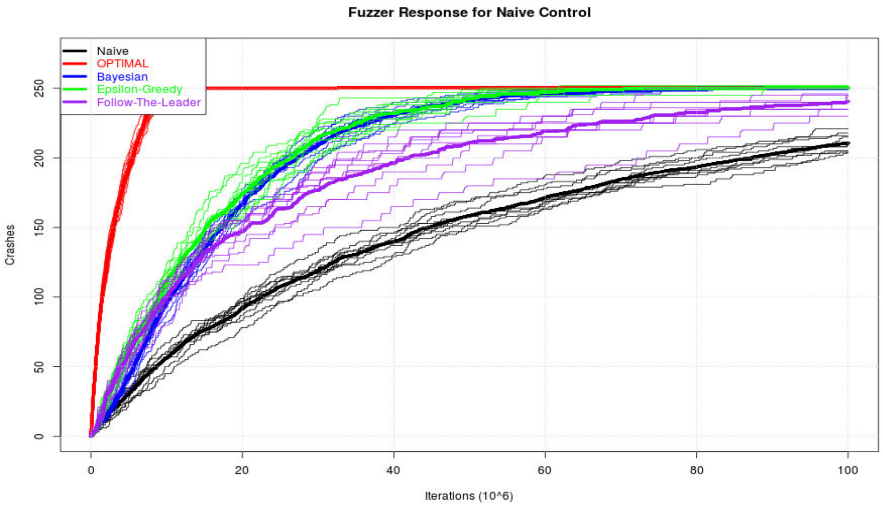
Limited Crashes Model

- λ is decay parameter
- n is unique crashes triggered by a seed potentially
- p is much smaller than 1.
- All of them are unknown as a priori.

Result: Limited Crashes Model

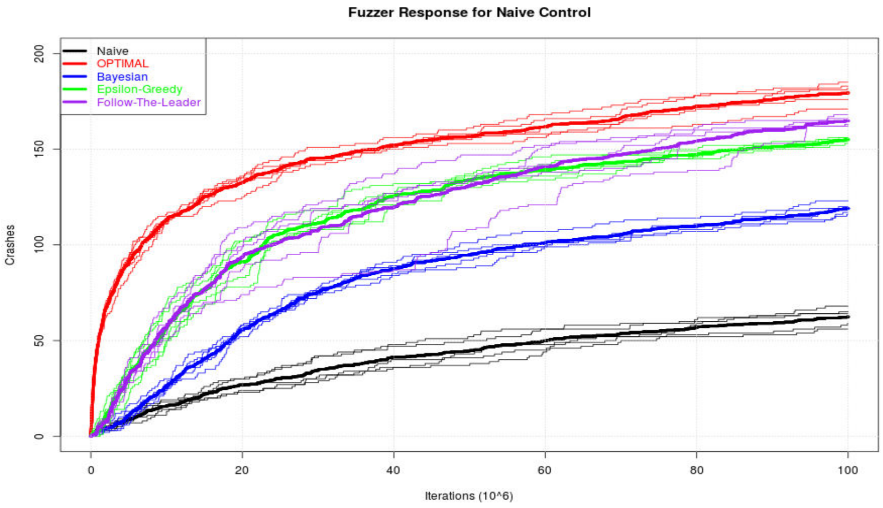


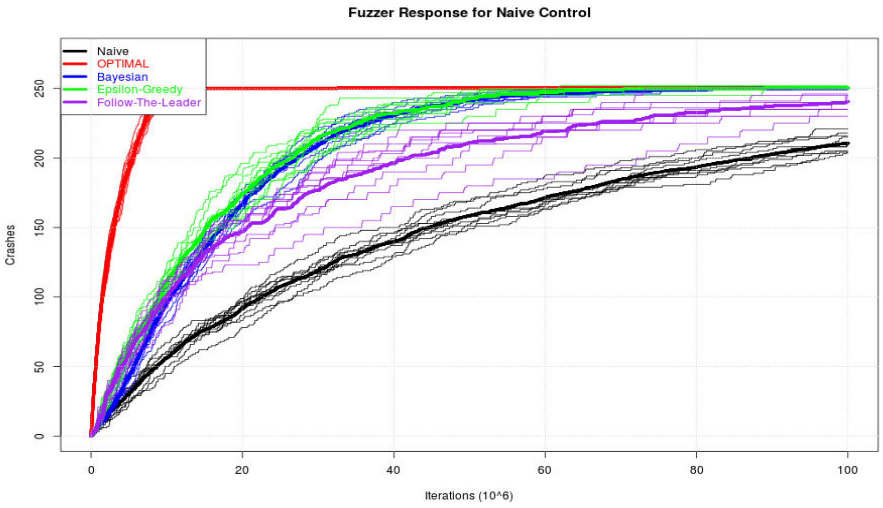
n -> ∞



n = 5

Result: Limited Crashes Model



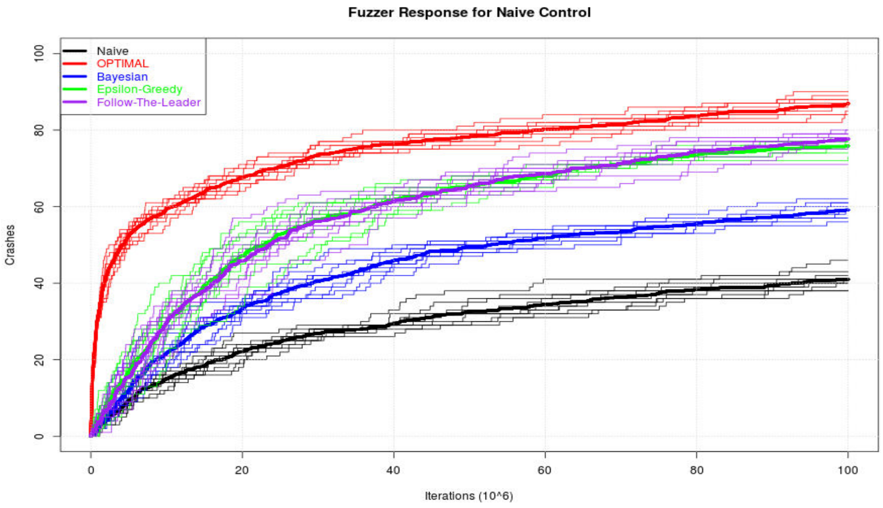


n -> ∞

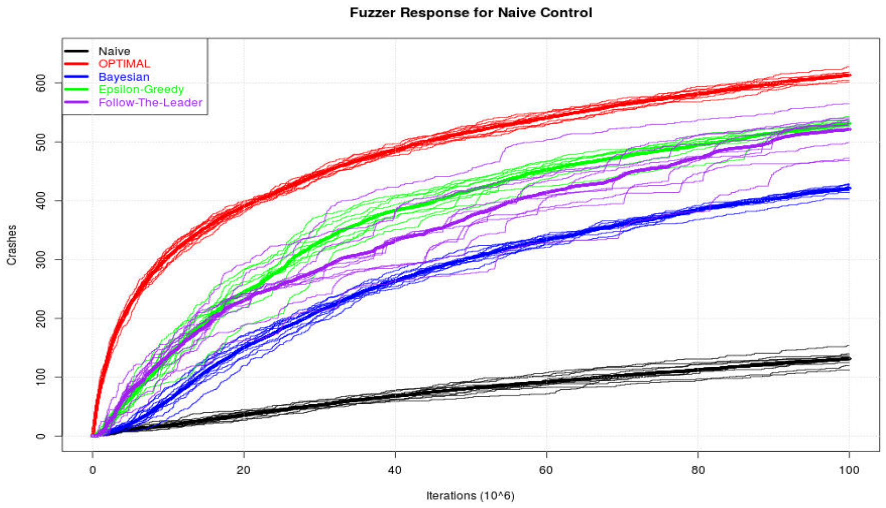
n = 5

- Exploration vs. Exploitation
- A critical number n*

Result: Decay factor



$\lambda = 0.3$

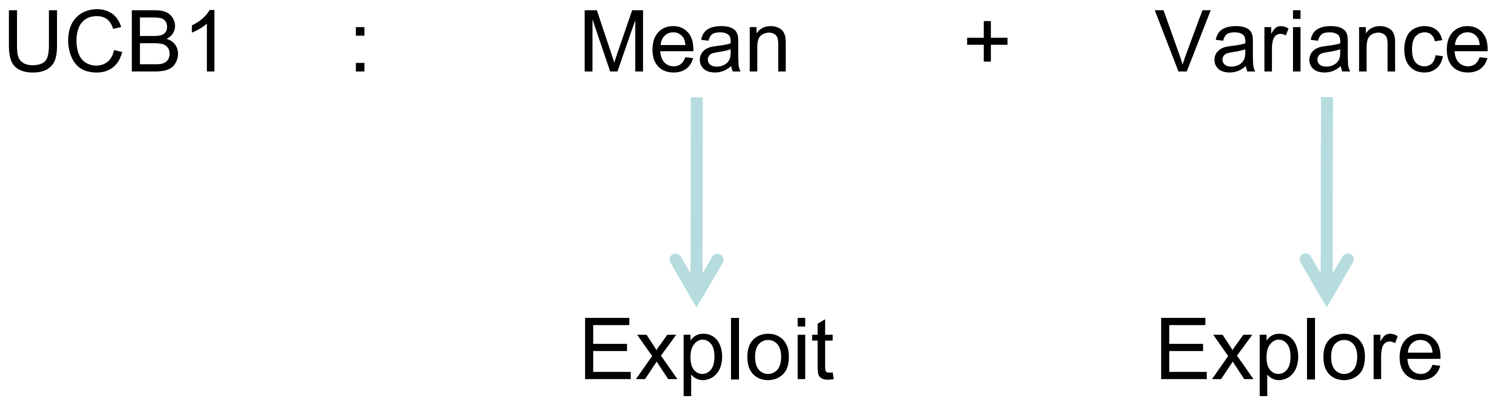


$\lambda = 0.9$

- n >> n*
- Crashes are expected to be found earlier for smaller λ, hence favor more exploration

Result: α-UCB1

To see “explore vs. exploit” more clearly

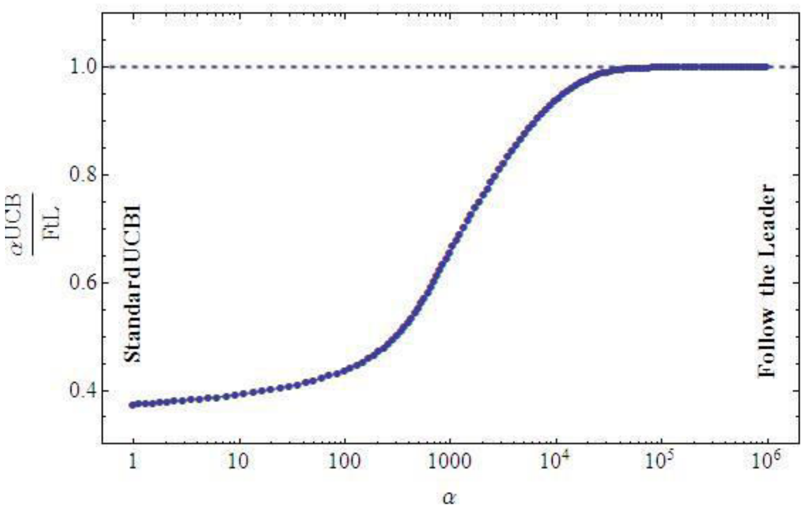


UCB1 : Mean + Variance

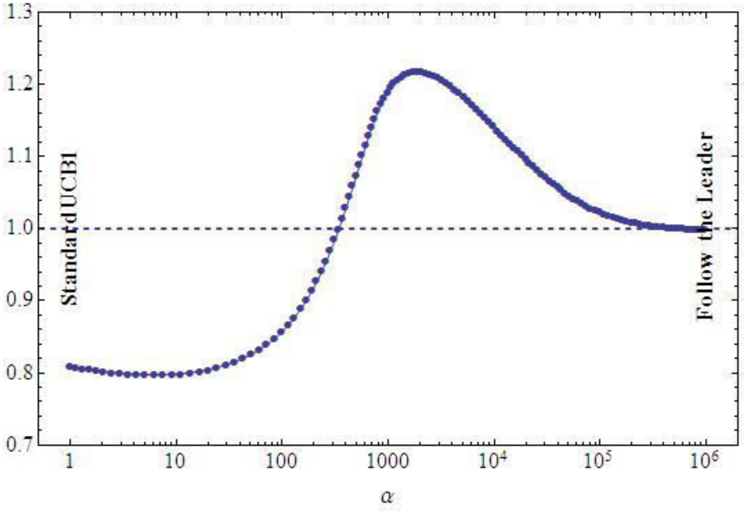
Exploit Explore

α -UCB1 : α×Mean + Variance

Result: α-UCB1



n -> ∞



n = 5

Discussion

- Exploration vs. Exploitation
- Accurate crash modeling is essential in designing a scheduling policy.
- Mortal multi-arm bandits
- Bug model

THANKS

Appendix

- n*

$$\frac{a}{\lambda_0} \times \frac{\gamma^{n+1} - 1}{\gamma^{n+1} - \gamma^n} \approx m = t \times c \times w$$