Australian National University

On Scheduling of Fuzzing Tests

Hongbo Zhang ANU

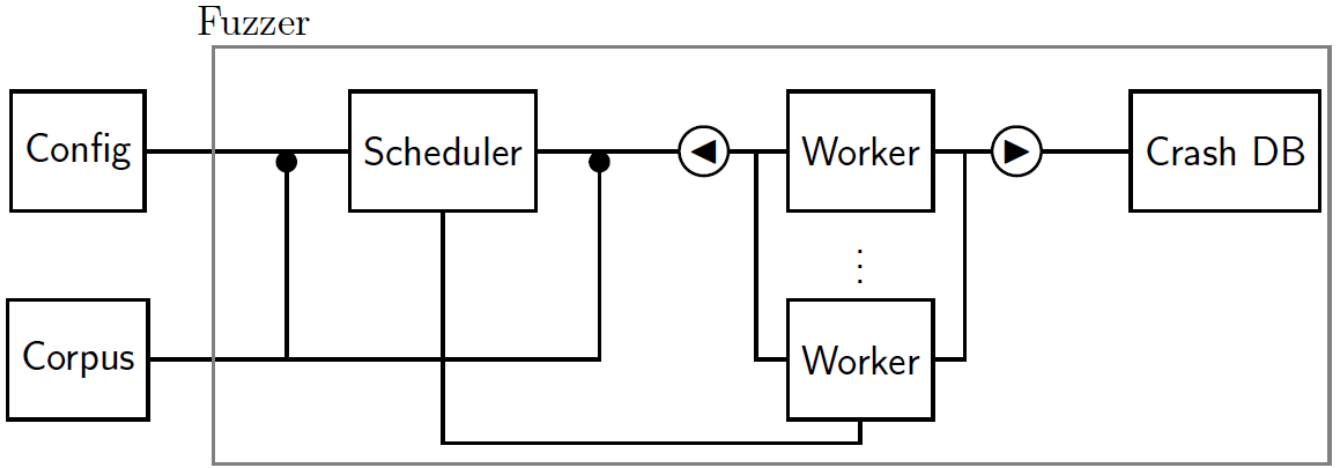
Supervisors: Steve Blackburn, Tony Hosking, Shane Magrath

Feb 13 2017
Sydney

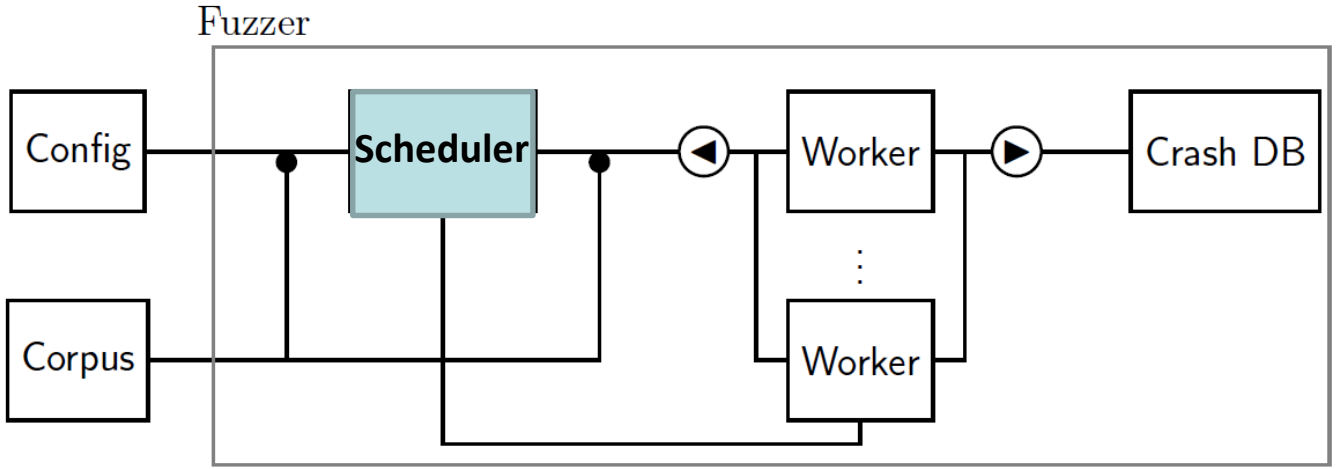
Overview

- Problem
- Models
- Results
- Conclusion

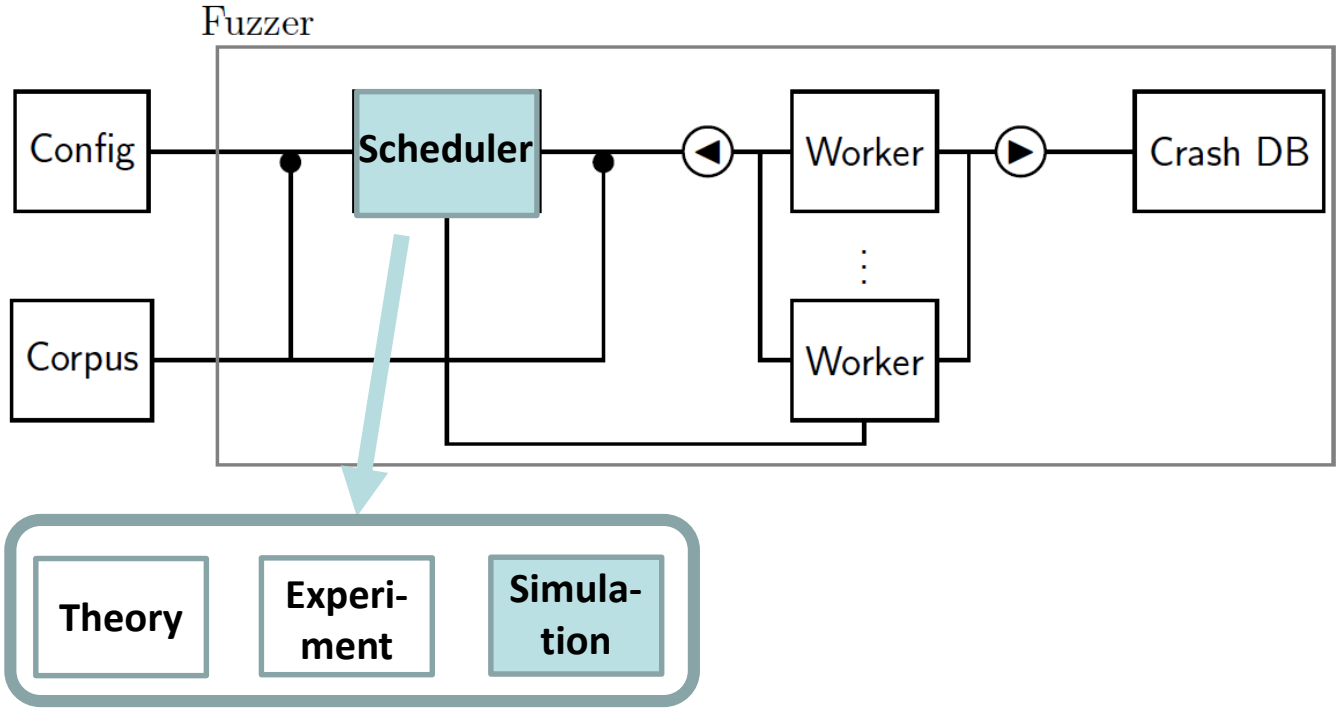
Fuzzing Tests



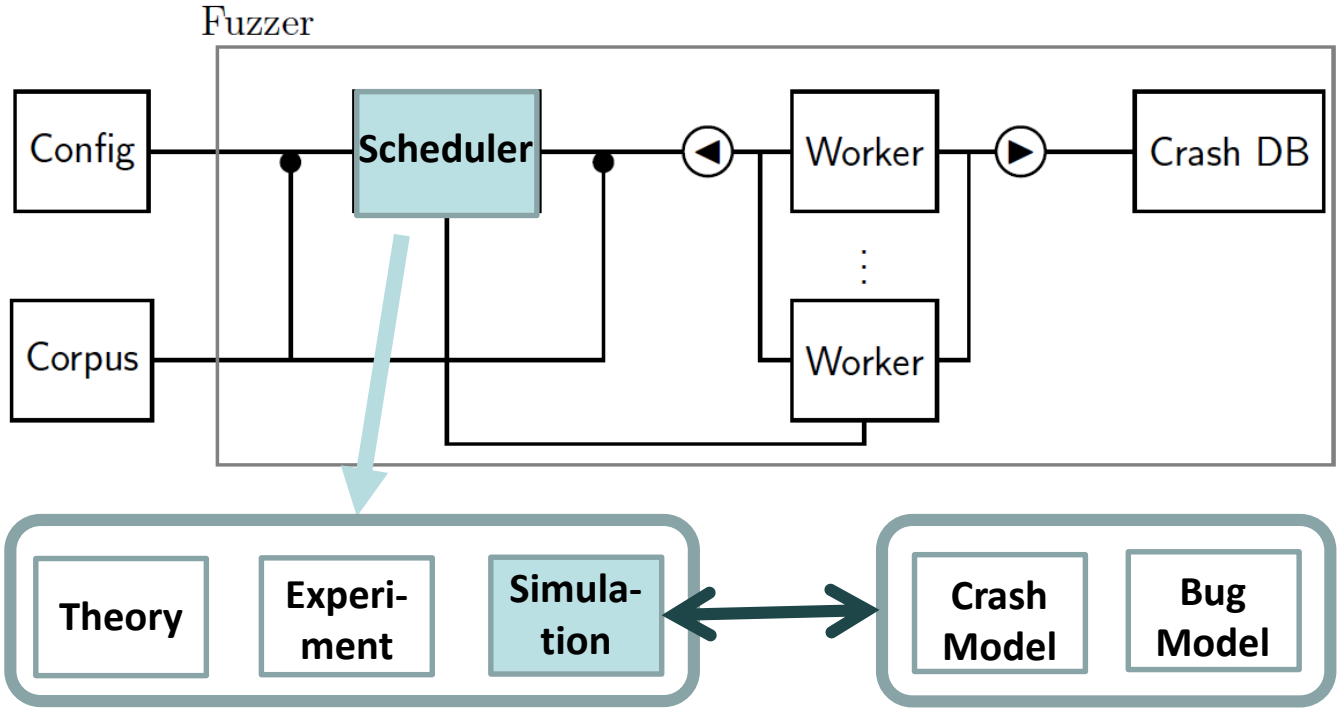
Fuzzing Tests



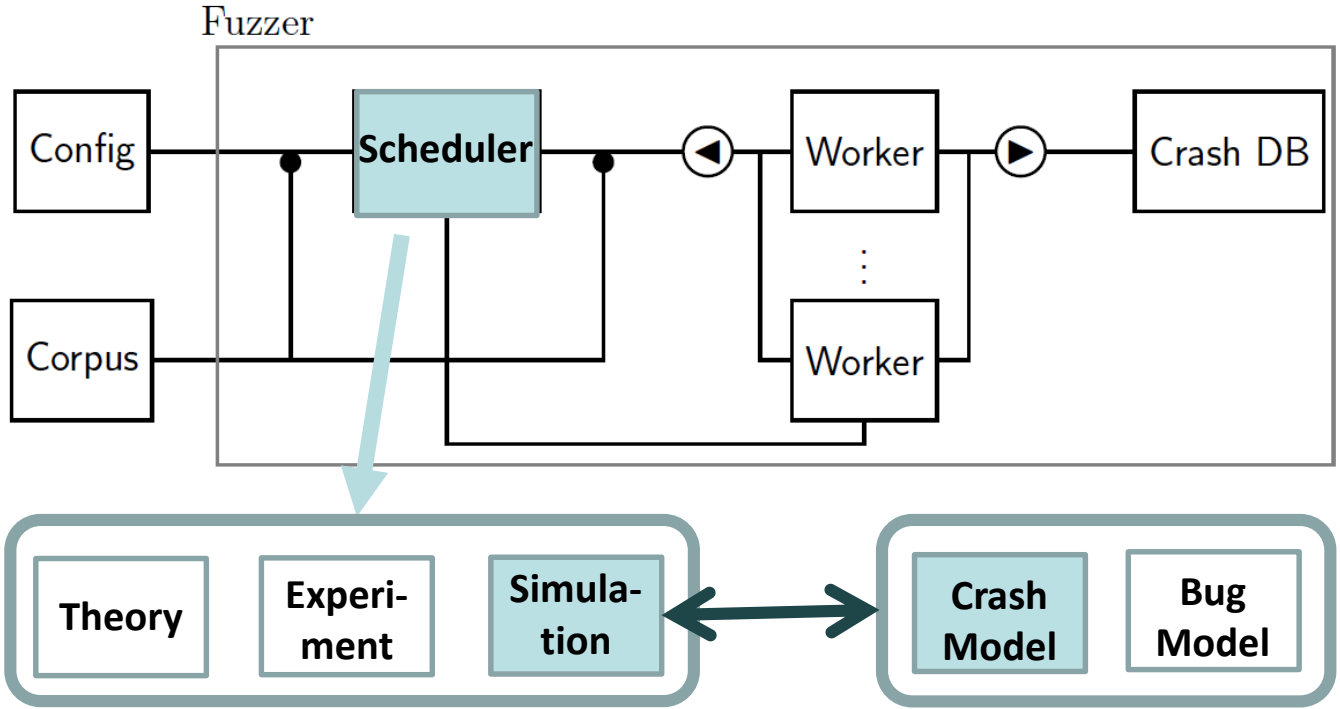
Fuzzing Tests



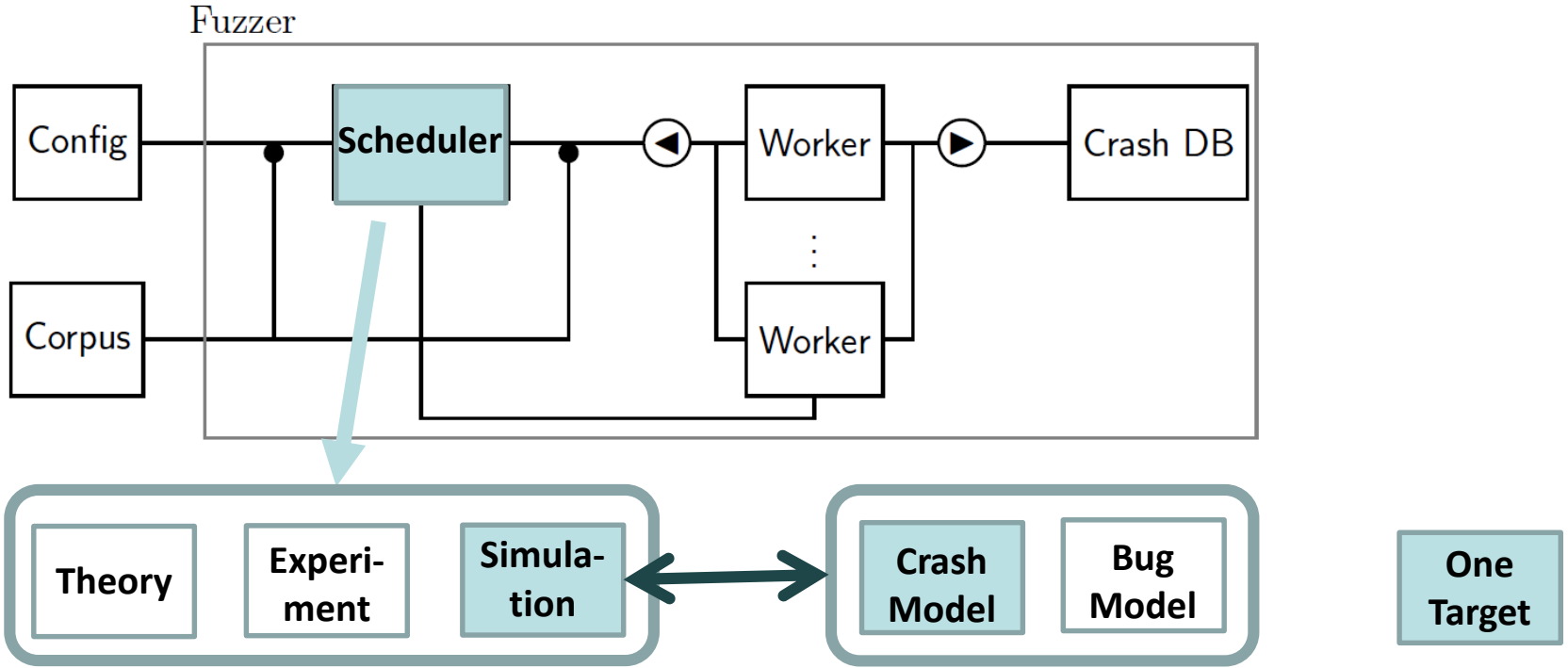
Fuzzing Tests



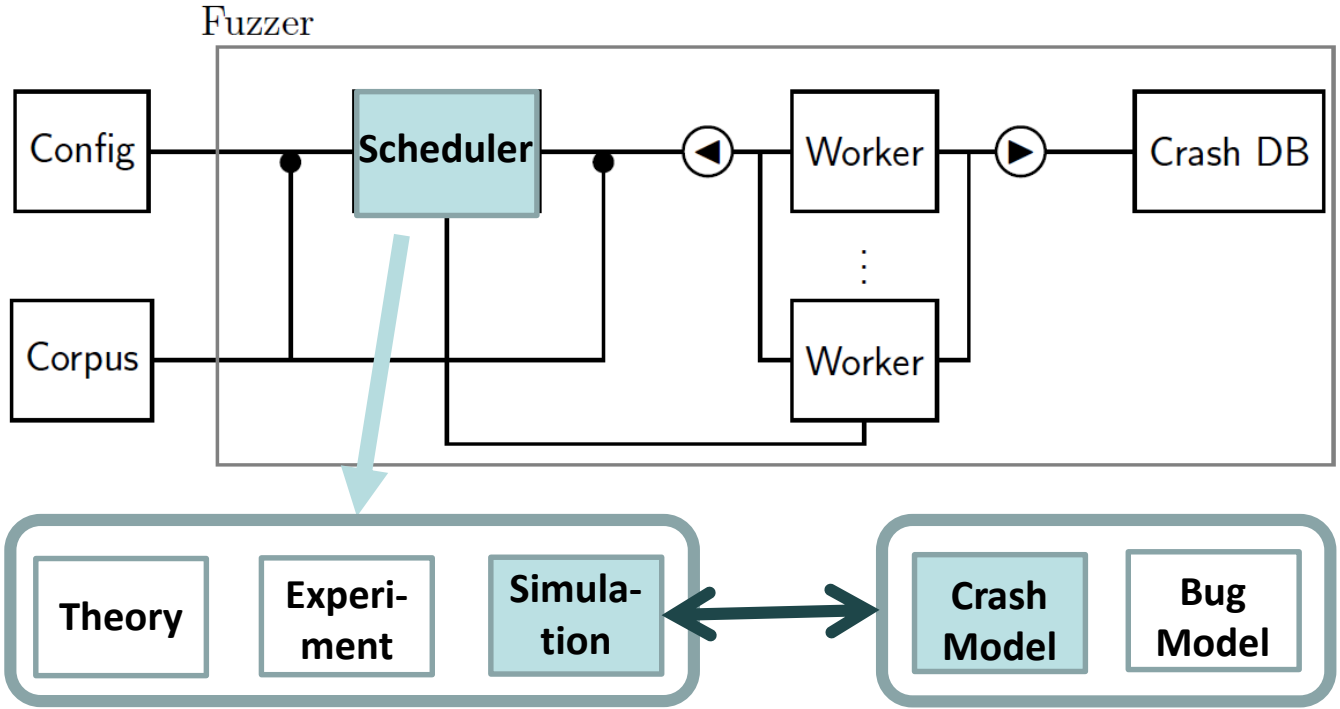
Fuzzing Tests



Fuzzing Tests



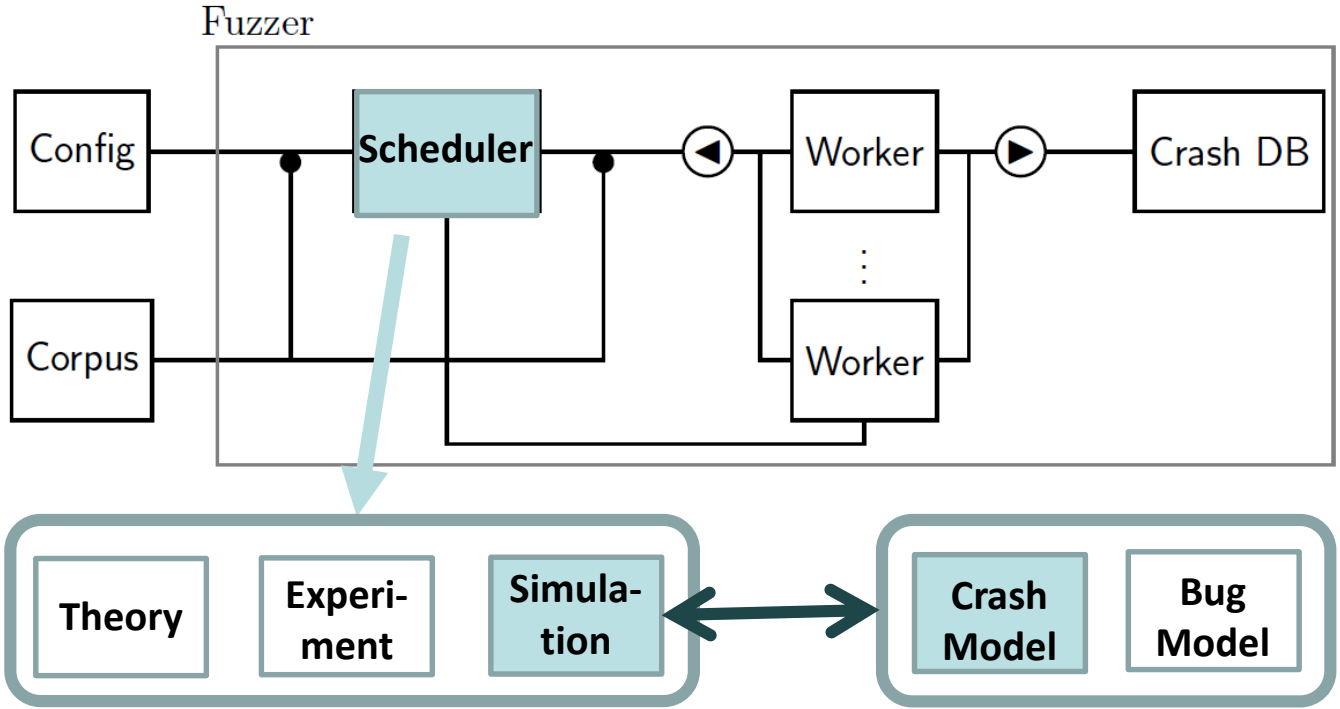
Fuzzing Tests



Follow the Leader

One Target

Fuzzing Tests

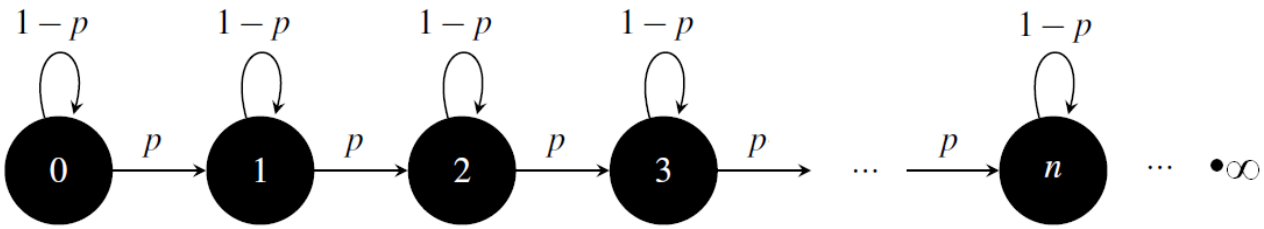


Follow the Leader

- **Is it true**
- **In which cases**
- **Why**

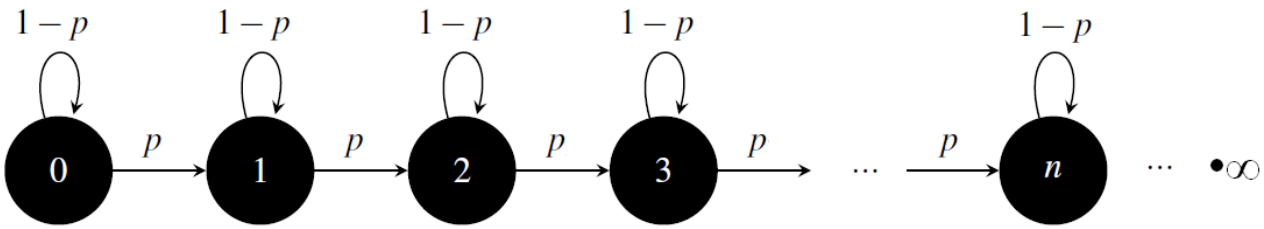
One Target

Crash Models



Bernoulli Model

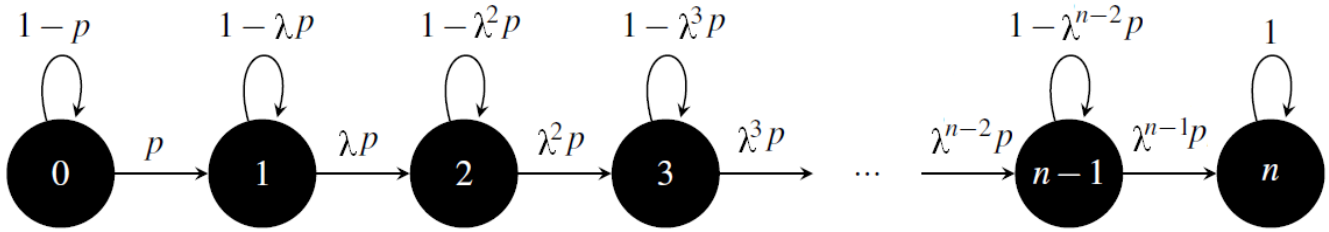
Crash Models



Bernoulli Model

- Infinite is impossible
- Probability to find a new unique crash should decrease.
- Follow the leader is optimal

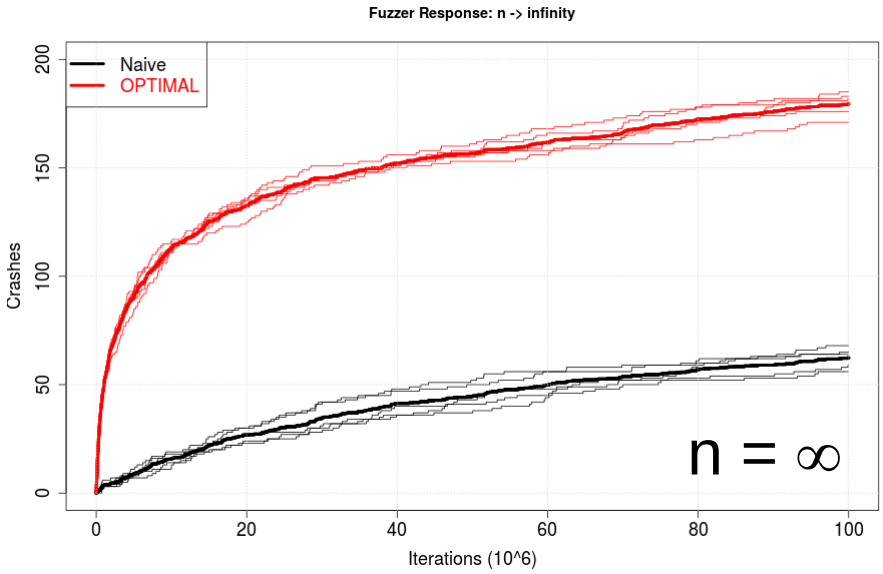
Crash Models

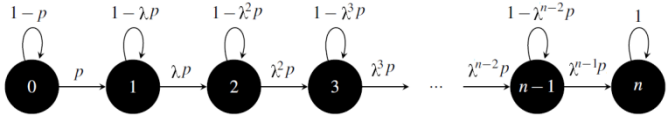


Limited Crashes Model

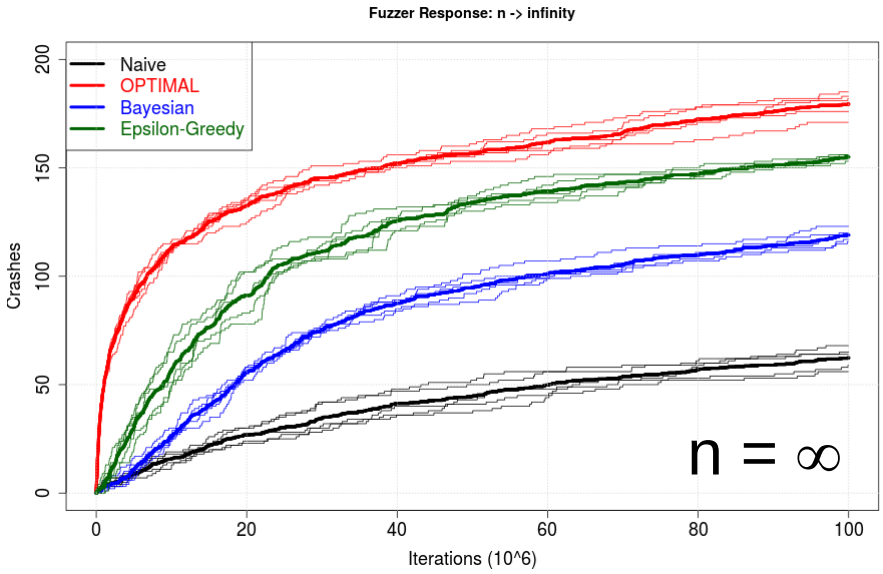
- λ is decay parameter
- n is unique crashes triggered by a seed potentially
- p is much smaller than 1.
- All of them are unknown as a priori.

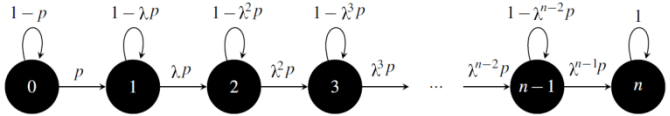
Result: Limited Crashes Model



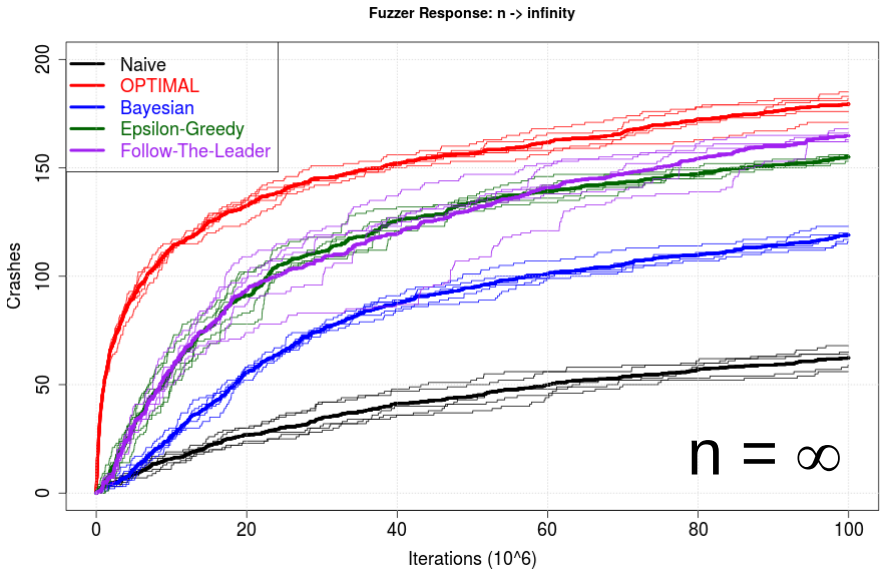


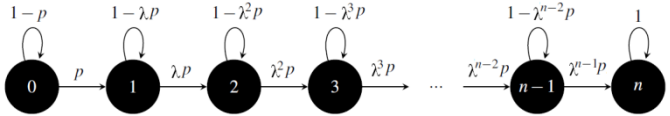
Result: Limited Crashes Model



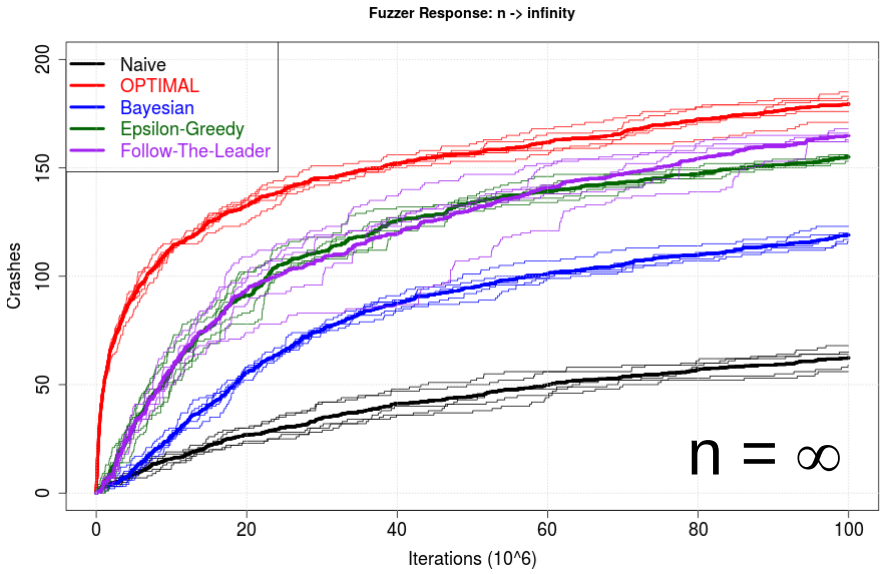


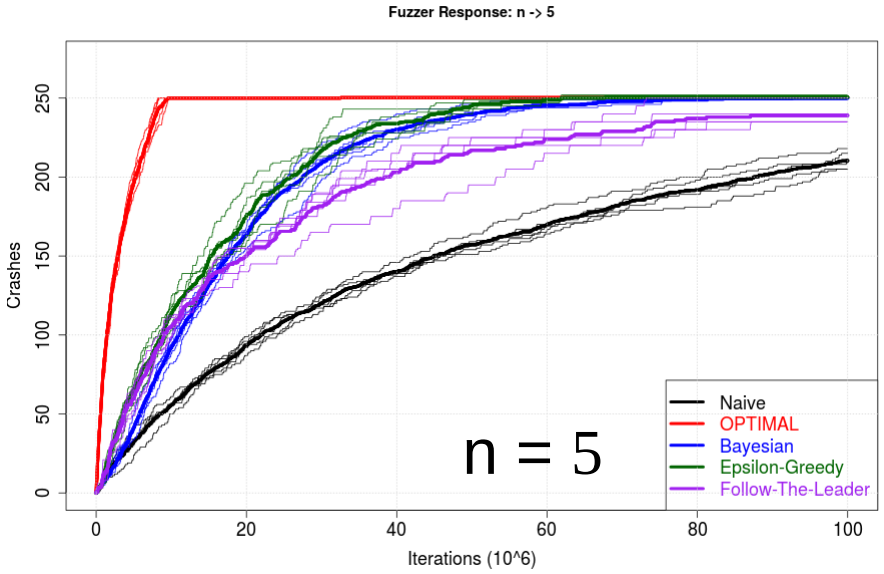
Result: Limited Crashes Model

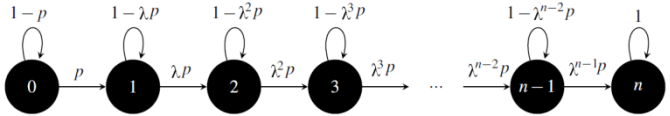




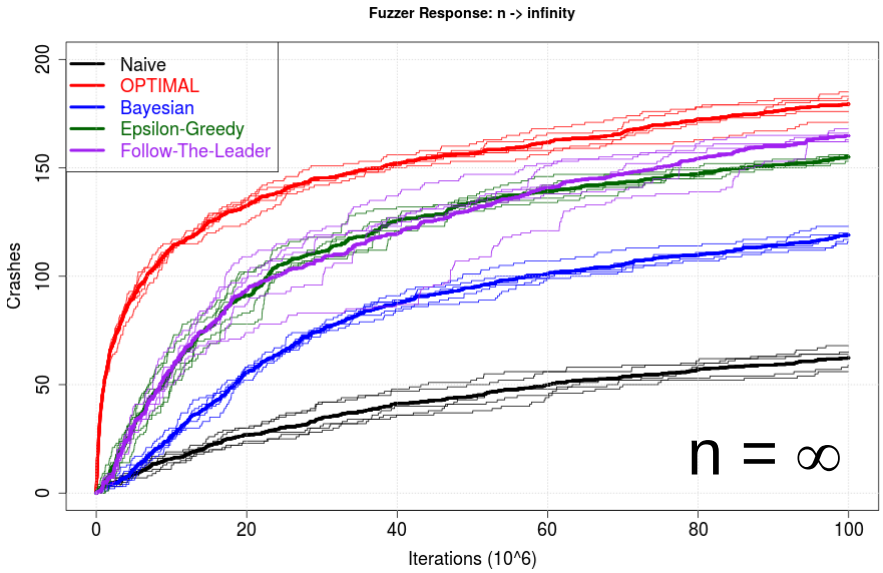
Result: Limited Crashes Model

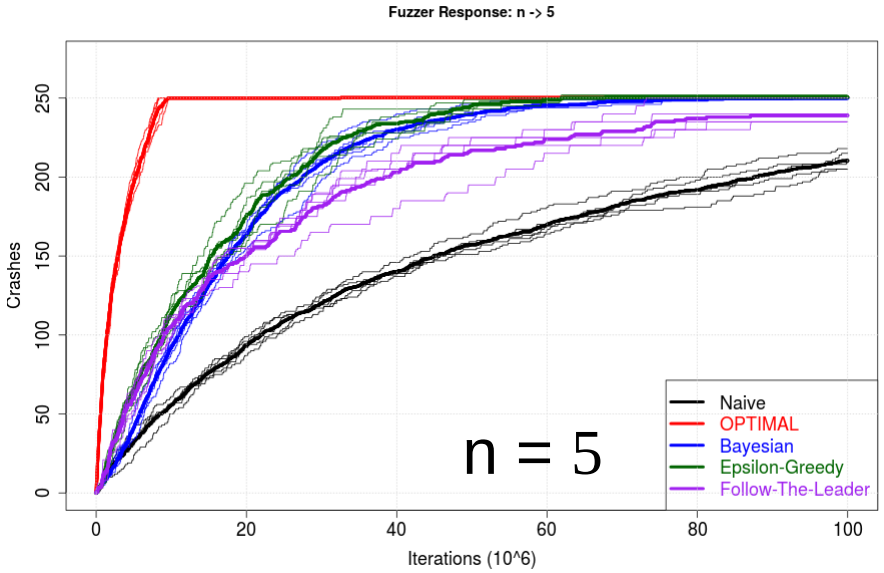




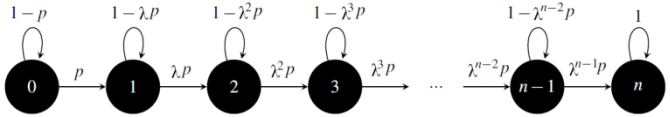


Result: Limited Crashes Model

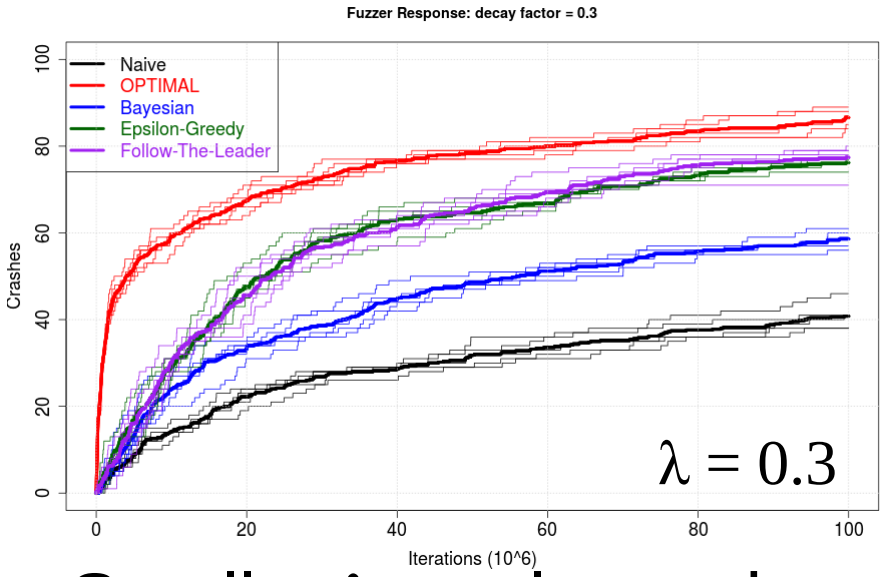


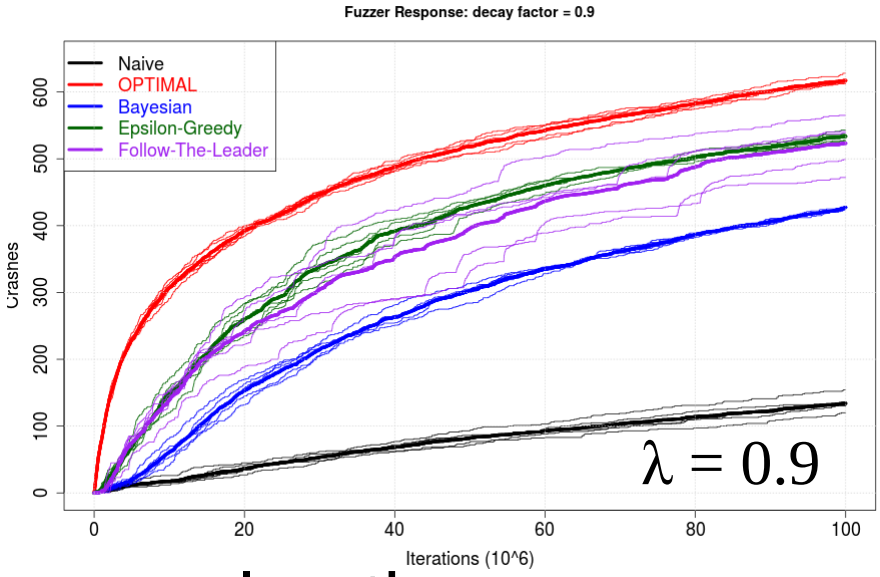


- Exploration vs. Exploitation
- A critical number n*

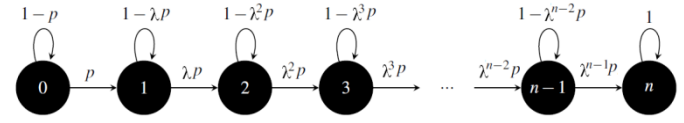


Result: Decay factor





- Smaller λ, early crash, more exploration
- n >> n*

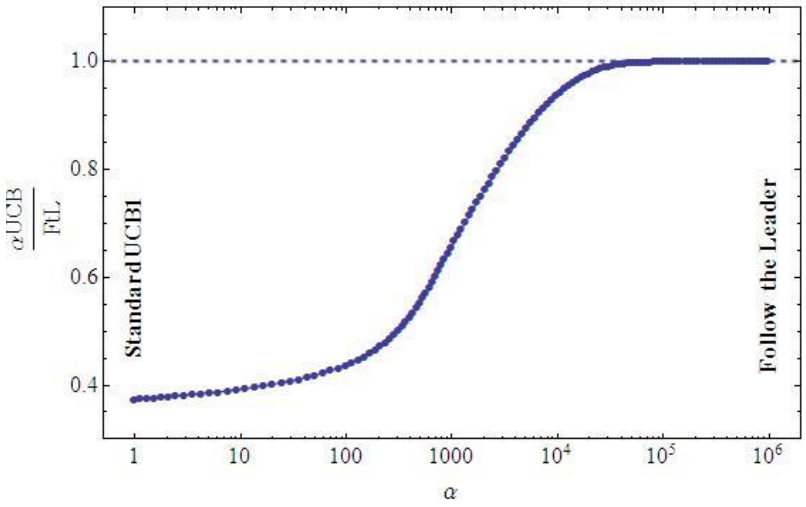


Result: α-UCB1

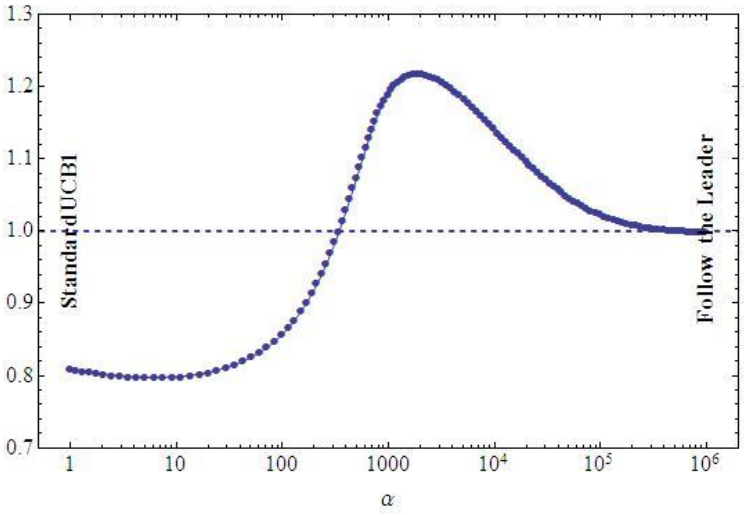
To see “explore vs. exploit” more clearly

UCB1	:	Mean	+	Variance
		↓		↓
		Exploit		Explore
α -UCB1	:	$\alpha \times$Mean	+	Variance

Result: α-UCB1



n -> ∞



n = 5

Conclusion

- Exploration vs. Exploitation
- Accurate crash modeling is essential in designing a scheduling policy.
- Questions
  - Theory: multi-arm bandits with finite lift-time*
  - Bug model

* Chakrabarti D, Kumar R, Filip R, Eli U, Mortal Multi-Armed Bandits, in Advances in Neural Information Processing Systems 21, Curran Associates, Inc., pp. 2730280, 2009

THANKS

Hongbo Zhang
u6170245@anu.edu.au

Appendix

- n*

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