Cover Sheet of Hongbo's Note

Questions and Research Plan

Hong-Bo Zhang

College of Engineering and Computer Science, Australian National University, Canberra, 2601, Australia
u6170245@anu.edu.au

Course Summer Research Project
Assign No. Report, Question and Plan
Lecturer Steve, Tony & Shane
Date 2016-Dec-2 $\sim$ Dec-5

Abstract: Recently, I read some conference papers and maths books on this topic, and I have some questions. I know this topic is mostly mathematical one, but before fully focusing on the mathematical aspect of this problem, I want to ask some questions on the computer science aspect. I think I will understand the goal of the project and how to simplify the mathematical formulation of this problem, if I know these answers, which serves as the basis of the mathematical problem. After the questions, there will be a temporary research plan.

Contents

1. Questions

What is the Fuzzing Type in Your Simulation? According to the research by Woo, et al. [1], the optimal Multi-Armed Bandit (MAB) algorithm is highly affected by the fuzzing type (fix-run, fix-time, or ... in a fuzzing) and the brief metrics. For example, in the Table 2 in their paper [1], they showed fix-run, weighted random in rate works best among the other alternatives in their experiments. However, in your simulation in slides, it seems weighted random in density (FtL) works best. Therefore, I want to know more information about your simulation, such as fuzzing types, brief metrics you used (other than α/β), and so on. This will be the basis of this mathematical problem, so I think it is very necessary to know.

Statistic Significant I want to know more details of statistic methods you used in your simulation, so that I can understand the statistical significant of the simulation results in your slides. This will become the guideline of our mathematical proof.

Could You Share Your Simulation Code? I would be very grateful if you could share your simulation code (using Monte-Carlo?). From that code, I could understand all the details and I would continue my work basing on your code.

Other Minor Questions (1) In the simulation, you used crash model instead of bug model. But the reference cited above [1] is about bug model. So maybe there is a little difference between your simulation and their works. (2) From the paper [2], the scheduling algorithm (this problem) and the seed selection algorithm (cover set) are strong coupled together. However, this will complicate the problem and we will not consider both of them together at present. (3) There are lots of famous MAB algorithm, such as UCB family, EXP family and so on. Have you tried them?

2. Research Plan

Simulation If you could share your code, I will simulate this problem in more details basing on your code. I will try different fuzzing type, different brief metrics and more MAB algorithms, to see whether "follow the leader" is the most optimal and how it is better than others. I have to get a intuitive picture of the computer science aspect of this problem before deeping into the mathematical one.

Mathematical Aspect I will continue learning some maths. Once I have finished the simulation and got some intuitive picture of the problem, I will focus on Markov decision process.

This is the questions I currently concern about. I will turn to you if I have further questions in the processing of reseaching.

Acknowledgments

References

[1] Woo, M., Cha, S. K., Gottlieb, S., and Brumley, D. Scheduling black-box mutational fuzzing. In proceedings of the 2013 ACM Conference on Computer & Communications Security (2013), p511-522

[2] Rebert, A., Cha, S. K., Avgerinos, T., Foote, J., Warren, D., Grieco, G., Brumley, D., Optimizing Seed Selection for Fuzzing. 23rd USENIX Security Symposium (2014), p861-875