Cover Sheet of Hongbo's Note

Crash Model 1: Finite Markov Chain

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. Understand the critical crash number
Lecturer Steve, Tony & Shane
Date 2016-Dec-13 ∼ Dec-?

Abstract: In this note, I will try to understand the effect of crash number in a Markov Chain crash model on MAB algorithm

Contents

1. Critical Crash Number in Crash Model

Given a set of fuzzing parameters, the expected number of crashes triggered by active seed will be given in the following.

In a crash model with infinte nodes in Markov chain, which means a seed could potentially trigger infinite unique crashes The length of fuzzing campaign is c (campaignlength), within each campaign, the number of trial is t (trialblock). So the duration d (duration) in fuzzing simulation will be $d = t \times c$. If the worker in a pull is w, the total number of testing in a fuzzing is $m = d \times w$. In addition, the number of active seeds is a (active). The initial probability of triggering a crash is λ_0 (lambdahigh), and the discount factor is γ (exponentialdecay). The the probability of triggering the (n+1)th unique crash will be

$$\lambda_n = \lambda_0 \times \gamma^n$$

Therefore, the expected number of testing in a fuzzing to trigger the nth unique crash by an active seed is

$$s(n) = \frac{1}{\lambda_0} + \frac{1}{\lambda_1} + \ldots + \frac{1}{\lambda_{n-1}} = \frac{1}{\lambda_0} \times \frac{\gamma^n - 1}{\gamma^n - \gamma^{n-1}}$$

Consequently, the expected number of testing in a fuzzing to trigger the nth unique crash by a active seeds will be $S(n) = a \times s(n)$.

Matching $S(n)$ with d to estimate the value of n in a fuzzing campaign.

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

From above agreba equation, we can solve n.

If $c = 10^3, t = 10^2, w = 10^3, a = 15, \lambda_0 = 10^{-4}, \gamma = 0.6$, n will be $11 \sim 12$.

Consequently, in a fuzzing campaign with above parameters, in average, an active seed will actually trigger $11 \sim 12$ unique crashes.

Acknowledgments

References