ADVANCED OPERATING SYSTEMS

PGS: INFORMATION AND COMMUNICATION TECHNOLOGIES - M131

Serpanos Dimitrios - ic1200018

Paper for review:

Snowcat: Efficient Kernel Concurrency Testing using a Learned Coverage Predictor

Sishuai Gong, Dinglan Peng, Deniz Altınbüken, Pedro Fonseca, Petros Maniatis

ΕΙΣΑΓΩΓΗ

- Τυχαίοι αλγόριθμοι για την επιλογή σεναρίων δοκιμής του κώδικα του πυρήνα
  - Εκτέλεση περιττών ή αχρείαστων test που προκαλούν φόρτο
  - Αδυναμία επαρκή εντοπισμού σφαλμάτων
- Ανάγκη για την επιβολή προτεραιότητας στα σενάρια που πρέπει να τρέξουν
  - Tests που καλύπτουν και ελέγχουν κομμάτια κώδικα που δεν έχουν προηγουμένως ελεγχθεί
- Δυναμική ταξινόμηση των σεναρίων που πρέπει να τρέξουν
  - Συμβολή της Μηχανικής Μάθησης
    - Προβλήματα και περιορισμοί
    - Αναπαράσταση των δεδομένων σε bytes
    - Περιορισμένα δεδομένα εισόδου και εξόδου από το δίκτυο ΜΜ
- Εύρεση όσο το δυνατόν περισσότερων σφαλμάτων στον κώδικα μέσα από τα σενάρια
- Πρόβλεψη σημείων του κώδικα που δε καλύπτονται

SNOWCAT • ΣΤΟΧΟΙ

- Δημιουργία ενός predictor μέσα από τα σενάρια που θα τρέξουν
  - Τροφοδότηση και εκπαίδευση του συστήματος
- Αποδοτική χρήση και εκτέλεση των σεναρίων
  - Πρόβλεψη μη καλυμμένων blocks του κώδικα
- Αξιολόγηση του συστήματος
  - Linux 5.12, 5.13 και 6.1

SNOWCAT • ΑΡΧΙΚΗ ΥΛΟΠΟΙΗΣΗ

- Αναγνώριση δεδομένων εισόδου των σεναρίων
- Ομαδοποίηση των σεναρίων
- Εκτέλεση των σεναρίων
- Συνθήκη τερματισμού
  - Μπορεί να προκληθούν πολλές περιττές επαναλήψεις μέχρι να βρεθεί η συνθήκη – Μειωμένη απόδοση

SNOWCAT • ΛΥΣΗ

- Το Snowcat πρόκειται να λύσει το προηγούμενο πρόβλημα βάζοντας στη ροή εργασιών ένα ενδιάμεσο τμήμα ελέγχου
  - Ένα σενάριο θα τρέξει μόνο αν έχει κάτι να προσφέρει

- Μερικές παραδοχές για την απόδοση του συστήματος
  - Το σύστημα θα πρέπει να είναι γρήγορο
  - Τα σενάρια δε θα πρέπει να έχουν λάθη
  - Δε θα πρέπει να γίνονται λανθασμένες εκτιμήσεις για την επιλογή των σεναρίων
  - Η εκπαίδευση του συστήματος θα πρέπει να γίνεται γρήγορα
  - Το σύστημα θα πρέπει να προσαρμόζεται αποδοτικά στις καινούριες εκδόσεις του λειτουργικού

SNOWCAT • ΣΧΕΔΙΑΣΜΟΣ

- Εκπαίδευση συστήματος σε πολυμορφικά δεδομένα
  - Συντακτικά, σημασιολογικά, μονονηματικές διεργασίες
- Πρόβλεψη της κάλυψης των block και επιλογή των σεναρίων
  - Εκτέλεση των χρήσιμων σεναρίων
- Εκτίμηση των μπλοκ που καλύπτονται και αυτών που δεν καλύπτονται
  - Χρήση γράφων που αποτυπώνουν όλο τον κώδικα του πυρήνα

SNOWCAT • ΡΟΗ ΕΡΓΑΣΙΩΝ

- Συλλογή δεδομένων εισόδου (Sequential Test Inputs)
- Εκτέλεση των STIs και συλλογή πληροφοριών
- Εκτίμηση των block μέσα από γράφο (Control Flow Graph)
- Δημιουργία και εκτέλεση των σεναρίων συγχρονισμού (Concurrent Test Inputs)
- Εκπαίδευση του μηχανισμού πρόβλεψης (Per-Interleaving Coverage)
- Αξιοποίηση του PIC για την διαλογή των χρήσιμων σεναρίων
- Επανάληψη της εκπαίδευσης για τις νέες εκδόσεις του λειτουργικού

SNOWCAT • ΓΡΑΦΟΣ

- 2 τύποι κόμβων
  - Κόμβοι που καλύφθηκαν κατά την ακολουθιακή εκτέλεση 2 STIs (SCB)
  - Κόμβοι που είναι προσεγγίσιμοι από τους SCBs αλλά δεν καλύφθηκαν κατά την εκτέλεση (URB)

- 5 τύποι συνδέσμων
  - SCB control flow που δημιουργούνται κατά την εκτέλεση των STIs
  - URB control flow που δείχνουν την ένωση των SCB με τους URB
  - Intrathread data flow που ενώνουν τα blocks εντός του ίδιου thread
  - Δεσμοί που ενώνουν τους κόμβους διαφορετικών thread
  - Δεσμοί που δηλώνουν έναν πιθανό χρονοπρογραμματισμό για το σενάριο που θα τρέξει
    (2 δεσμοί είναι αρκετοί για τον εντοπισμό των πιο χαρακτηριστικών σφαλμάτων)

SNOWCAT • ΕΠΙΛΟΓΗ ΣΕΝΑΡΙΩΝ

- Σενάρια που θα καλύπτουν νέα περιοχή από blocks
  - Μνήμη προηγούμενων blocks
- Σενάριο που θα καλύπτει τουλάχιστον 1 μπλοκ που δεν έχει προηγουμένως καλυφθεί
- Σενάρια με τις λιγότερες δυνατές δοκιμές
  - Δε χρειάζονται πολλές επαναλήψεις για να εντοπίσουν όλα τα λάθη

SNOWCAT • ΥΛΟΠΟΙΗΣΗ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ

- Angr: Εργαλείο που χρησιμοποιείται για την δημιουργία του γράφου του πυρήνα
- Syzkaller: για την δημιουργία και εκτέλεση των STIs
- SKI: για την εκτέλεση των σεναρίων και εκπαίδευση του συστήματος

Η αξιολόγηση απαντά θετικά στα ερωτήματα:

- Μπορεί το σύστημα να προβλέψει τα μπλοκ που δεν έχουν καλυφθεί;
  - Ναι χάρει στον γράφο
- Μπορεί το σύστημα να διαλέξει τα πιο αποδοτικά και χρήσιμα σενάρια;
  - Ναι χάρει στον μηχανισμό πρόβλεψης
- Μπορεί το σύστημα να μην είναι αρκετά κοστοβόρο όσο το ΛΣ αλλάζει εκδόσεις;
  - Ναι διότι δεν αλλάζουν πάρα πολλά πράγματα στο μηχανισμό
- Είναι το σύστημα καλύτερο από προηγούμενες προσεγγίσεις;
  - 100 φορές πιο γρήγορος εντοπισμός των σφαλμάτων
  - 17% περισσότερες εναλλακτικές διαδρομές ελέγχου

SNOWCAT • ΜΕΛΛΟΝΤΙΚΕΣ ΚΑΤΕΥΘΥΝΣΕΙΣ

- Πρόβλεψη των inter-thread ροών δεδομένων και >1 hop κόμβων
- Προσθήκη νέων κόμβων και συνδέσεων στους γράφους
- Πρόβλεψη σε συστήματα με αδύναμα ή περίπλοκα συστήματα μνήμης