Kihong Heo

Rm 312-2, Bldg 302
Programming Research Laboratory
ROSAEC (Research on Software Analysis for Error-free computing) Center
Department of Computer Science & Engineering
Seoul National University
1 Gwanak-ro Gwanak-gu, Seoul 151-742, Republic of Korea

☎ : +82.2.880.1865 ✉ : khheo@ropas.snu.ac.kr
: +82.10.3568.5501 : http://ropas.snu.ac.kr/~khheo

Research Interests

I am interested in semantic-based static analysis for safe and reliable softwares. In particular,

- **Sound, Scalable & Precise Static Analysis**
  I have been developing techniques to achieve sound, scalable, yet precise static analysis in a single analyzer. The challenge has been handled by making the analysis compute only right part at right moment (sparse analysis) and apply expensive sensitivities only when they benefit (selective X-sensitivity). The key part of these approaches is to estimate the sparsity and the impact of the sensitivities. To this end, I have been working on statistical approaches (e.g., machine learning) as well as logical techniques (e.g., pre-analysis).
- **Data-driven Adaptive Program Analysis guided by Machine Learning**
  Thanks to the abundance of program code and analysis result, now it is possible to exploit machine learning techniques for improving the performance of program analyses. In particular, I am working on inferring effective abstractions using machine learning. For example, I try to infer an effective variable clustering strategy for selectively relational analysis and harmless unsoundness for selectively unsound analysis.

Education

Computer Science and Engineering, Seoul National University Mar 2009 – Present
Ph.D candidate
Advisor: Prof. Kwangkeun Yi

Computer Science and Engineering, Seoul National University Mar 2005 – Feb 2009
Bachelor of Science in Computer Science

Experience

The Hong Kong University of Science & Technology Sep 2011 – Feb 2012
Visiting Student
Advisor: Prof. Sunghun Kim

Research Project

- **Inferbo: Infer-based buffer overrun analyzer** 2016 – present
  I have been a core developer of Inferbo that is a buffer overrun detector for C-like languages. Inferbo, which is based on Facebook Infer's modular analysis framework, scales to large and quickly changing codebases. I designed and implemented a modular interval analysis for the buffer detection. Inferbo is now merged in Facebook Infer and available via the Infer github. (`https://github.com/facebook/infer`)

- **Sparrow: a static analyzer for C program** 2011 – present
  I have been a core developer of Sparrow and mainly involved in its relational analysis engine. Sparrow is a state-of-the-art static analyzer that aims to verify the absence of fatal bugs in C source. In particular, I have been developing techniques for cost-effective relational analysis, context-sensitive analysis, unsound analysis enabled by semantic-based pre-analysis and machine learning. (`http://ropas.snu.ac.kr/sparrow`)

- **Selective X-sensitive Analysis** 2013 – present
  I have been working on the selective X-sensitive analysis framework and mainly developing selectively relational analysis. Selective X-sensitive analysis applies certain sensitivity X (e.g. context, flow, or relational analysis) only when and where doing so is likely to improve the precision of the main analysis. The challenge is to estimates the impact of X on the main analysis's precision. To this end, we have developed 1) impact pre-analyses that are based on the abstract interpretation framework, and 2) machine learning techniques that learn the behaviors of the impact pre-analyses. In the project, I mainly designed an impact pre-analysis and machine learning techniques for the octagon relational analysis.

- **Global Sparse Analysis Framework** 2011 – 2012
  I joined the sparse analysis project and designed the sparse interval analysis engine part. Our sparse analysis framework provides a general method for achieving global static analyzers that are precise, sound, yet also scalable. Based on the framework, we have derived a sparse version of Sparrow which is 175x more scalable than the baseline in terms of lines of code and scales to a million lines of C programs. In the project, I participated in designing a pre-analysis for the interval analysis and implementing the sparse interval analysis. (`http://ropas.snu.ac.kr/sparseanalysis`)

- **SNEC: Semantic-based Non-Essential Change Detection** 2011 – 2012
  I have developed SNEC, a semantic-based non-essential change detector. Non-essential change is a code change that does not alter the semantics such as refactoring. Abundant non-essential changes in software history have negative impacts on software mining tasks. SNEC identifies non-essential changes by observing semantic equivalence using a semantic-aware static analyzer. I designed and implemented SNEC based on a commercial static analysis engine for JAVA programs. (`http://ropas.snu.ac.kr/snec`)

Publications

1. Machine-Learning-Guided Selectively Unsound Static Analysis
   Kihong Heo, Hakjoo Oh, and Kwangkeun Yi
   ICSE 2017: *The 39th International Conference on Software Engineering*, 2017 (to appear)

2. Learning a Variable-Clustering Strategy for Octagon from Labeled Data Generated by a Static Analysis
   Kihong Heo, Hakjoo Oh, and Hongseok Yang
   SAS 2016: *The 23rd International Static Analysis Symposium*, 2016

3. Selective X-Sensitive Analysis Guided by Impact Pre-Analysis
   Hakjoo Oh, Wonchan Lee, **Kihong Heo**, Hongseok Yang, and Kwangkeun Yi
   TOPLAS: *ACM Transactions on Programming Languages and Systems*, Vol. 38, Issue 2, Jan. 2016

4. Widening with Thresholds via Binary Search
   Sol Kim, **Kihong Heo**, Hakjoo Oh, Kwangkeun Yi
   SP&E: *Software-Practice and Experience*, 2016 (to appear)

5. Selective Context-Sensitivity Guided by Impact Pre-Analysis
   Hakjoo Oh, Wonchan Lee, **Kihong Heo**, Hongseok Yang, and Kwangkeun Yi
   PLDI 2014: *The 35th ACM SIGPLAN Conference of Programming Language Design and Implementation*, 2014

6. Design and Implementation of Sparse Global Analyses for C-like Languages
   Hakjoo Oh, **Kihong Heo**, Wonchan Lee, Woosuk Lee, and Kwangkeun Yi
   PLDI 2012: *The 33rd ACM SIGPLAN Conference of Programming Language Design and Implementation*, 2012

7. General Sparse Analysis Framework
   Hakjoo Oh, **Kihong Heo**, Wonchan Lee, Woosuk Lee, Daejun Park, Jeehoon Kang, and Kwangkeun Yi
   TOPLAS: *ACM Transactions on Programming Languages and Systems*, Vol. 36, Issue 3, Sept. 2014

8. A Sparse Evaluation Technique for Detailed Semantic Analyses
   Yoonseok Ko, **Kihong Heo**, and Hakjoo Oh
   Computer Languages, Systems, & Structures, Vol. 40, Issues 3–4, October–December 2014

Teaching Experience

- **Teaching Assistant** : SNU 4541.664 Program Analysis (grad) Spring 2010
- **Teaching Assistant** : SNU 4190.210 Programming Languages Spring 2009

References

Kwangkeun Yi
Professor
Dept. of Computer Science and Engineering
Seoul National University
Email: kwang@ropas.snu.ac.kr

Hongseok Yang
Professor
Dept. of Computer Science
University of Oxford
Email: hongseok.yang@cs.ox.ac.uk

Hakjoo Oh
Assistant Professor
Dept. of Computer Science and Engineering
Korea University
Email: hakjoo_oh@korea.ac.uk

Sunghun Kim
Associate Professor
Dept. of Computer Science and Engineering
The Hong Kong University of Science and Technology
Email: hunkim@cse.ust.hk

Last updated: January 23, 2017
http://ropas.snu.ac.kr/~khheo