Multi-objective evolutionary optimization of computation-intensive simulations – The case of security control selection

Bernhard Grill, Andreas Ekelhart, Elmar Kiesling, Christian Stummer and Christine Strauss

SBA Research, Vienna University of Technology, University of Bielefeld, University of Vienna
Austria / Germany

Funded by the Austrian Science Fund under project number P 23122-N23

Outline

- Motivation
- Background – Multi-objective simulation-optimization of security control sets
- Improving performance for multi-objective evolutionary optimization
- Experimental setup, evaluation & preliminary results
- Conclusion

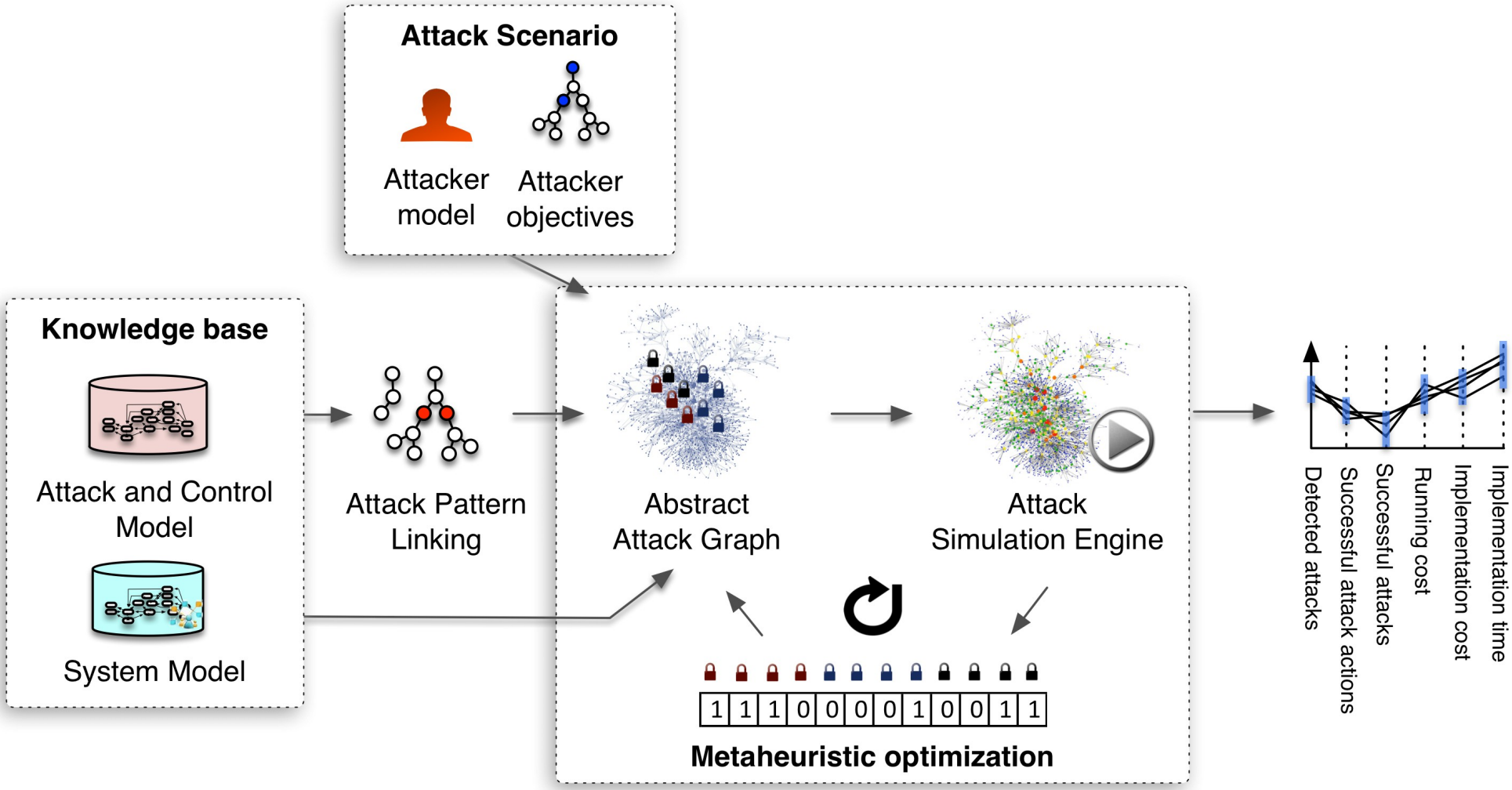
Motivation / Problem

- Multi-objective simulation-based optimization is **challenging**
- Vast **search space**
- Simulation-based evaluation is typically **runtime-intensive**

Background

- Challenge encountered during a **research project** on **analyzing** and **improving** the **security of complex IT systems**
- We apply multi-objective evolutionary simulation optimization to determine **Pareto-efficient** portfolios of **security controls**
- Evaluating an individual’s (control portfolio) fitness based on numerous simulations' outcome may require **several seconds**

Multi-Objective Simulation-Optimization of Security Control Sets



Aim Of The Work

- We aim to develop general techniques in order to:
  - Reduce **runtime** for an individual’s **fitness evaluation**
  - Reduce **optimization's overall runtime**
  - Reduce the **number** of required **evaluations**

Improving Performance for Multi-objective Evolutionary Optimization 1 / 2

- **Seeding**: Seeding the initial population with good candidate solutions (e.g. by utilizing expert knowledge)
- **Genotype Structure**: Introduce validity constraints on genotypes → may significantly reduce search space
- **Caching**: Using cached results of already evaluated candidates → low impact for large problems

Improving Performance for Multi-objective Evolutionary Optimization 2 / 2

- **Simulation Feedback Loop**: Utilizing feedback from simulation in optimization, e.g. stop simulation if results are far from acceptable [1]
- **Parallel Metaheuristics**: Parallelize evaluation on multiple computation nodes (limited by population size [2])
- **Surrogate Models**: Approximate the evaluation procedure with a surrogate model which is substantially less expensive to evaluate [3, 4]

Status Quo

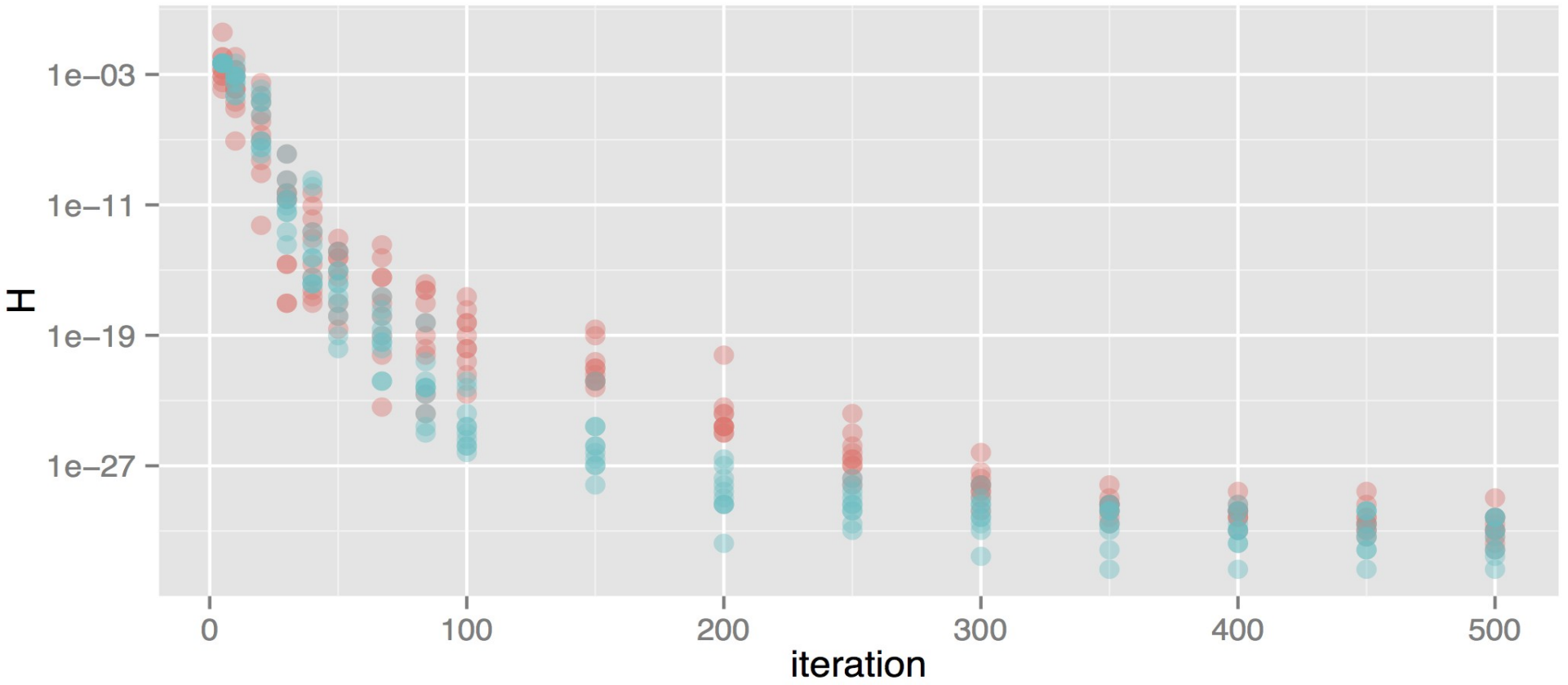
- So far, we have performed experiments with:
  - Improved seeding
  - Exploited genotype structure
  - Applied caching

Baseline Setup for Experiments

- Attack simulation based optimization framework
- NSGA2
- Generations: 500
- Population size: 100
- 2 point crossover
- 25 simulation replications per phenotype (fitness evaluation)
- 10 optimization runs (10 different optimization seeds)
- Search space: $2^{58} = 2.9 \times 10^{17}$
- Each evaluation (simulation) may take up to several seconds
- Each optimization run took about 12h

Seeding Experiment

- Utilized domain expert knowledge in order to create the initial population



Red = baseline, blue = utilizing improvement seeding, x-axis = generations, y-axis = 1 – amount of dominated space (the lower, the better)

Caching Experiment

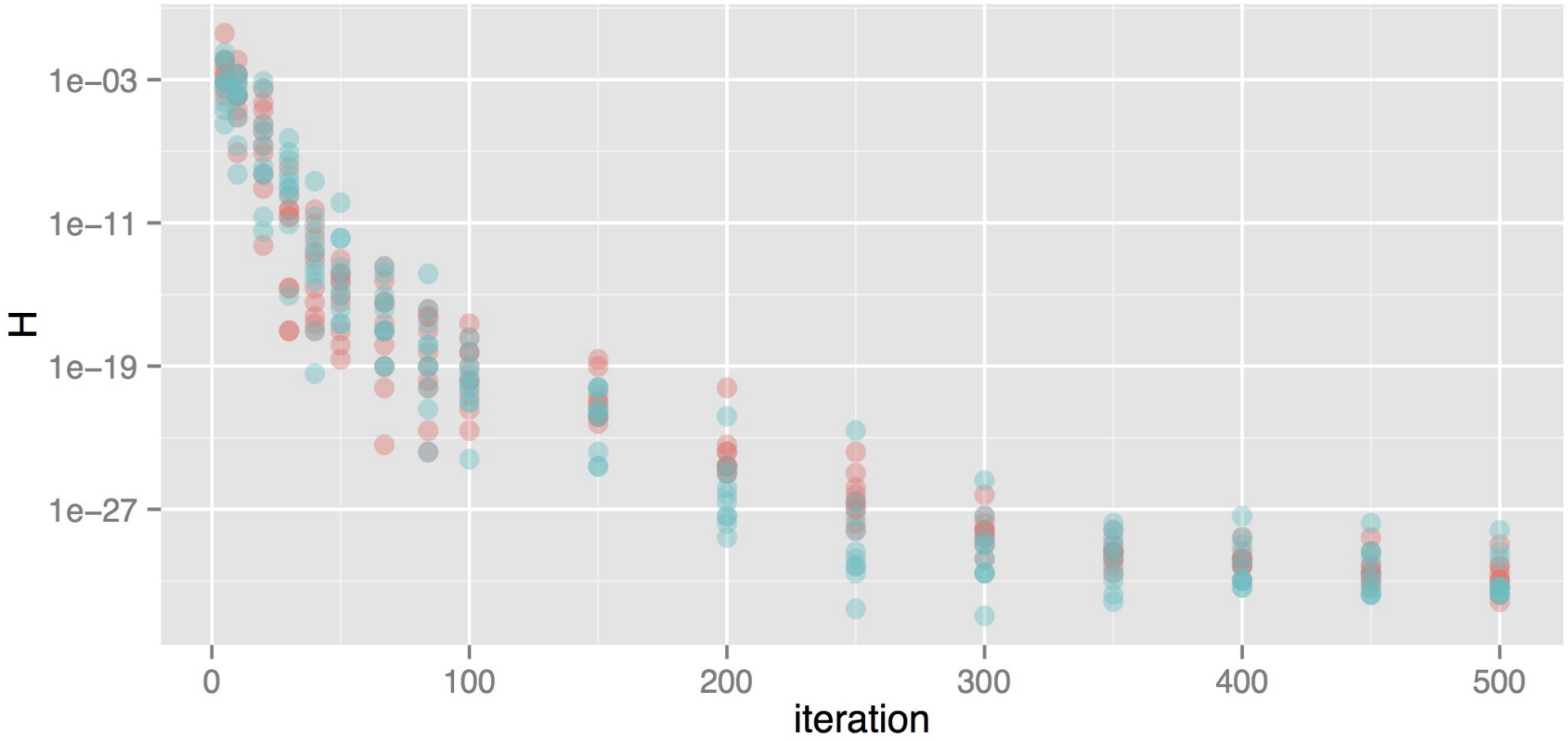
- Measured **how many genotypes** were **reevaluated during runtime** (12.500 genotypes x 10 optimization runs)
- No cache hit during the experiment → due to massive search space
- Utilize similarity measuring to improve caching performance

Genotype Structure Experiment

- Applying **constraints during genotype construction**, e.g. max one anti virus system per computer
- Reduced the search space from 2^{58} (2.9×10^{17}) to 2^{36} (6.9×10^{10})

Genotype Structure Experiment

- Adding constraints to genotype construction



Red = baseline, blue = utilizing genotype constraints, x-axis = generations, y-axis = 1 – amount of dominated space (the lower, the better)

Future Work

- Perform more experiments
- Utilize additional measures by Zitzler et. al. [5] (e.g. diversity metrics) in order to evaluate the performance improvements in more detail

Conclusion

- Expensive fitness functions (e.g. simulations) pose a serious challenge in optimization scenarios
- Outlined a number of approaches to tackle this issue
- Evaluated some of those performance improvement techniques using the example of information security control selection

Questions?

References

- [1] Michael C Fu. Optimization for simulation: Theory vs. practice. INFORMS Journal on Computing, 14(3):192–215, 2002.
- [2] El-Ghazali Talbi, Sanaz Mostaghim, Tatsuya Okabe, Hisao Ishibuchi, Günter Rudolph, and Carlos A Coello. Parallel approaches for multiobjective optimization. In Multiobjective Optimization, pages 349–372, Springer, 2008.
- [3] Manuel Laguna and Rafael Mart. Neural network prediction in a system for optimizing simulations. IIE Transactions, 34(3):273–282, 2002.
- [4] Soft Computing Home Page. Fitness approximation in evolutionary computation (bibliography), http://www.soft-computing.de/amec n.html, accessed in March 2015.
- [5] Zitzler, Eckart, et al. "Performance assessment of multiobjective optimizers: an analysis and review." Evolutionary Computation, IEEE Transactions on 7.2 (2003): 117-132.

Moses3 Publications (so far)

- Komplexe Systeme, heterogene Angreifer und vielfältige Abwehrmechanismen: Simulationsbasierte Entscheidungsunterstützung im IT-Sicherheitsmanagement (german language) - Andreas Ekelhart, Bernhard Grill, Elmar Kiesling, Christine Strauss and Christian Stummer
- Evolving Secure Information Systems through Attack Simulation - Elmar Kiesling, Andreas Ekelhart, Bernhard Grill, Christian Stummer and Christine Strauss
- Simulation-based optimization of information security controls: An adversary-centric approach - Elmar Kiesling, Andreas Ekelhart, Bernhard Grill, Christine Strauss and Christian Stummer
- Multi objective decision support for IT security control selection - Elmar Kiesling, Andreas Ekelhart, Bernhard Grill, Christine Strauss and Christian Stummer
- Simulation based optimization of IT security controls: Initial experiences with metaheuristic solution procedures - Elmar Kiesling, Andreas Ekelhart, Bernhard Grill, Christine Strauss and Christian Stummer