Model-Based Load Testing for Performance and Security

Cornel Barna Mark Shtern Michael Smit Marin Litoiu

Computer Science and Engineering
York University

April 17, 2012

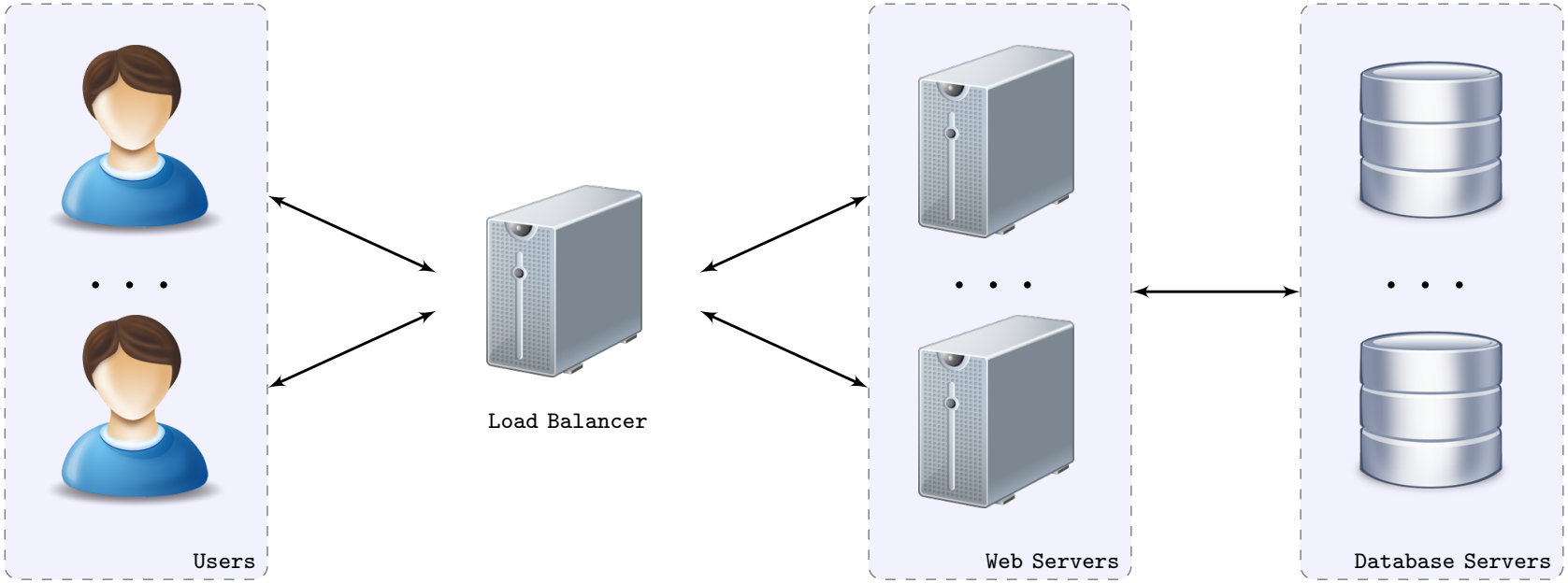
Performance Testing
- The Performance Stress Space
- The Framework
- Results
- Search Complexity

DoS Attack Mitigation
- DoS Attacks
- Adaptive DoS Mitigation
- Experiments
- Results

Performance Testing
- The Performance Stress Space
- The Framework
- Results
- Search Complexity

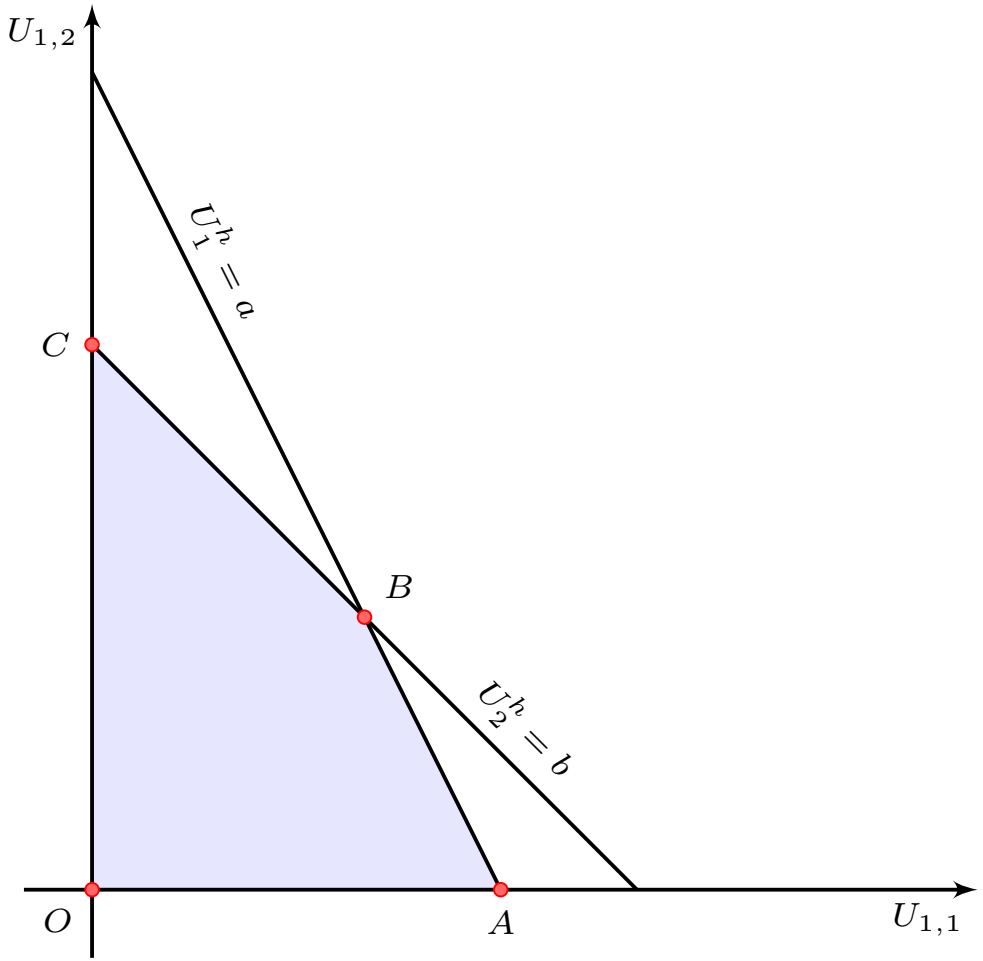
DoS Attack Mitigation
- DoS Attacks
- Adaptive DoS Mitigation
- Experiments
- Results

Introduction



The Performance Stress Space

Consider a system with two *hardware* resources, two *software* resources and two *classes of service*.



Hardware Constraints

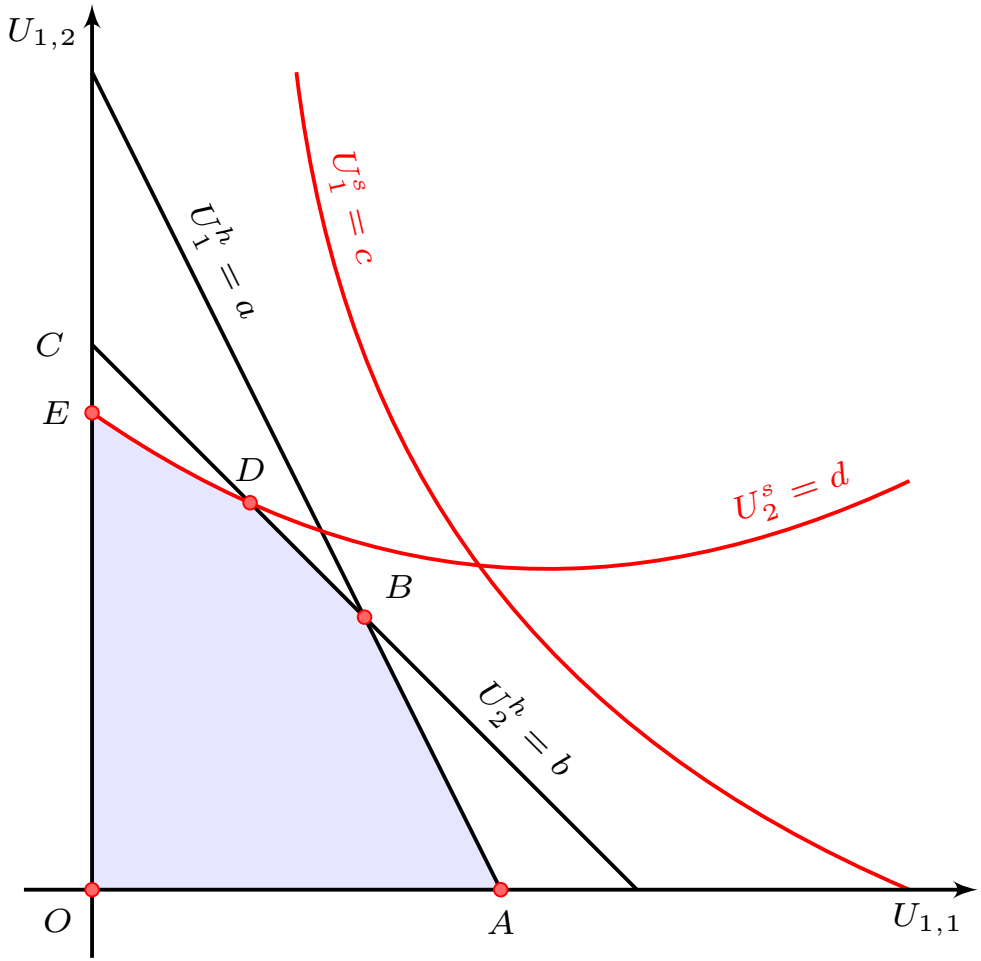
- Linear equations:

$$U_K^h = \sum_{\forall C \in \mathcal{C}} \frac{D_{K,C}}{D_{K_r,C}} \times U_{K_r,C}, \quad \forall K \in \mathcal{K}^h$$

- Feasible space $\longrightarrow$ $OABC$

The Performance Stress Space

Consider a system with two *hardware* resources, two *software* resources and two *classes of service*.



Hardware Constraints

- Linear equations:

$$U_K^h = \sum_{\forall C \in \mathcal{C}} \frac{D_{K,C}}{D_{K_r,C}} \times U_{K_r,C}, \quad \forall K \in \mathcal{K}^h$$

- Feasible space $\longrightarrow$ $OABC$

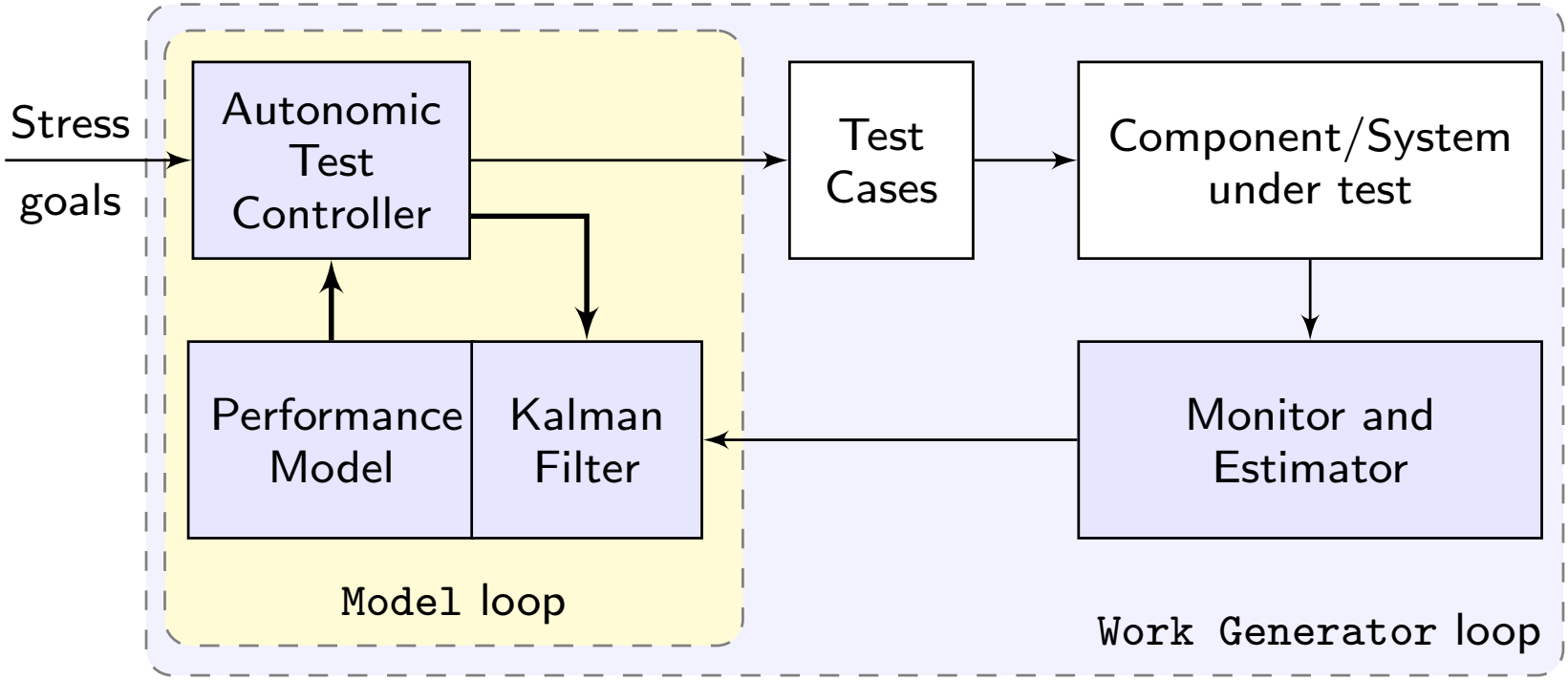
Hardware and Software Constraints

- Non-linear equations:

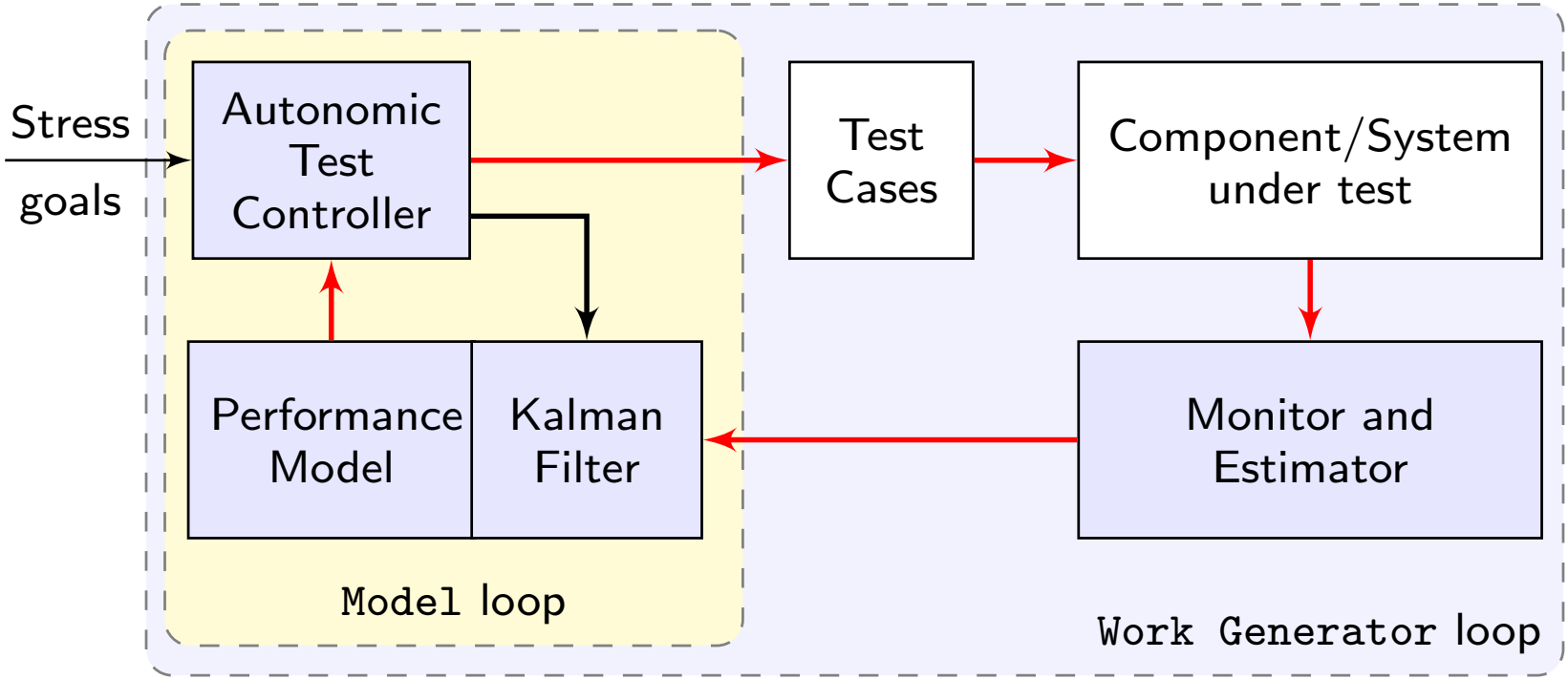
$$U_K^s = \sum_{\forall C \in \mathcal{C}} \frac{R_{K,C}^s}{D_{K_r,C}} \times U_{K_r,C}, \quad \forall K \in \mathcal{K}^s$$

- Feasible space $\longrightarrow$ $OABDE$

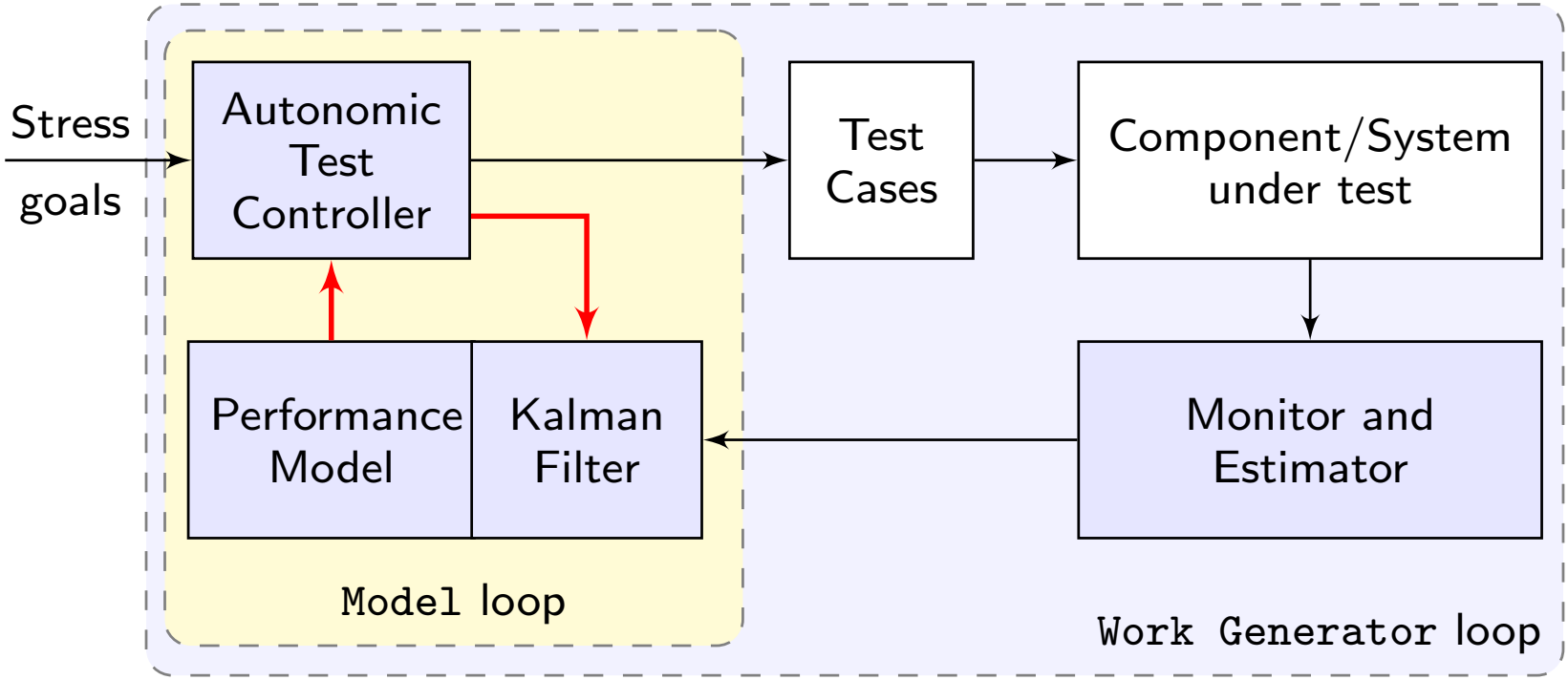
The Framework



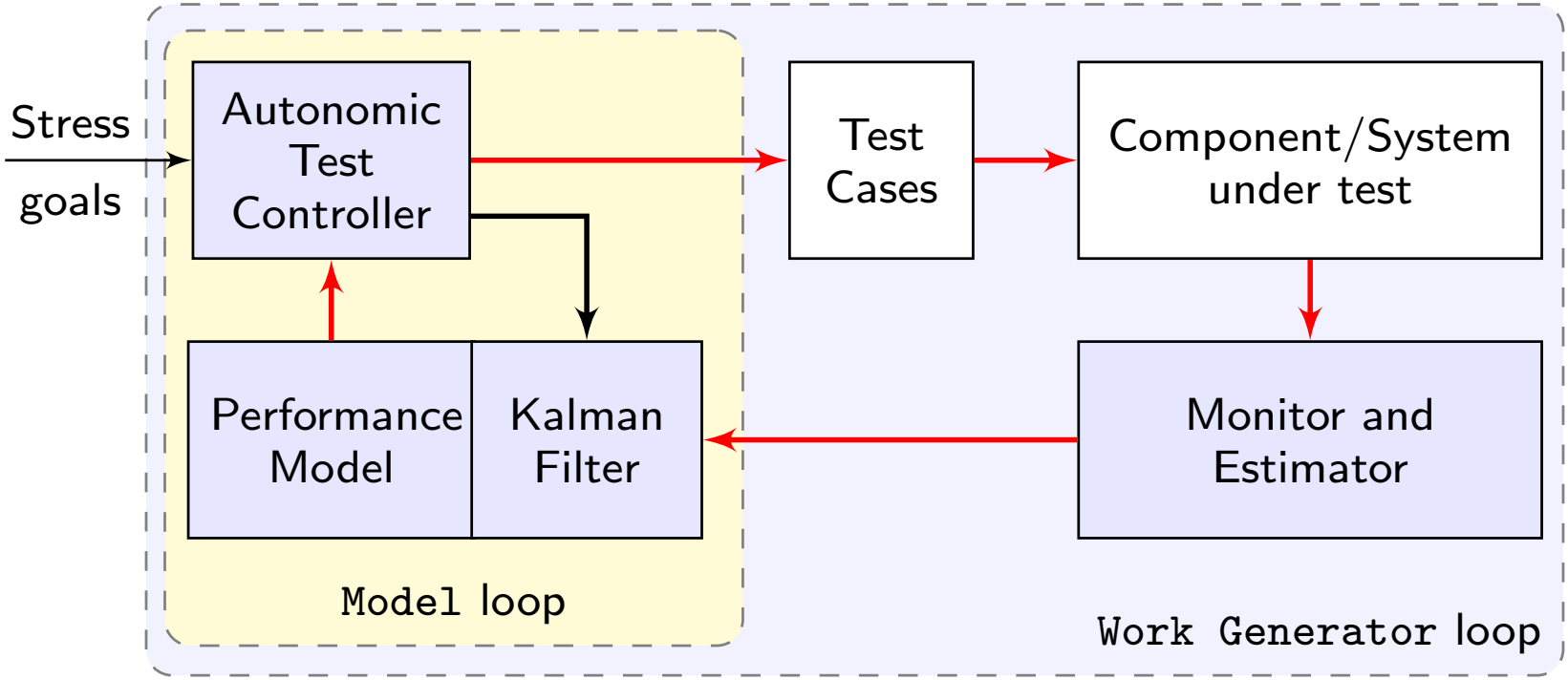
The Framework



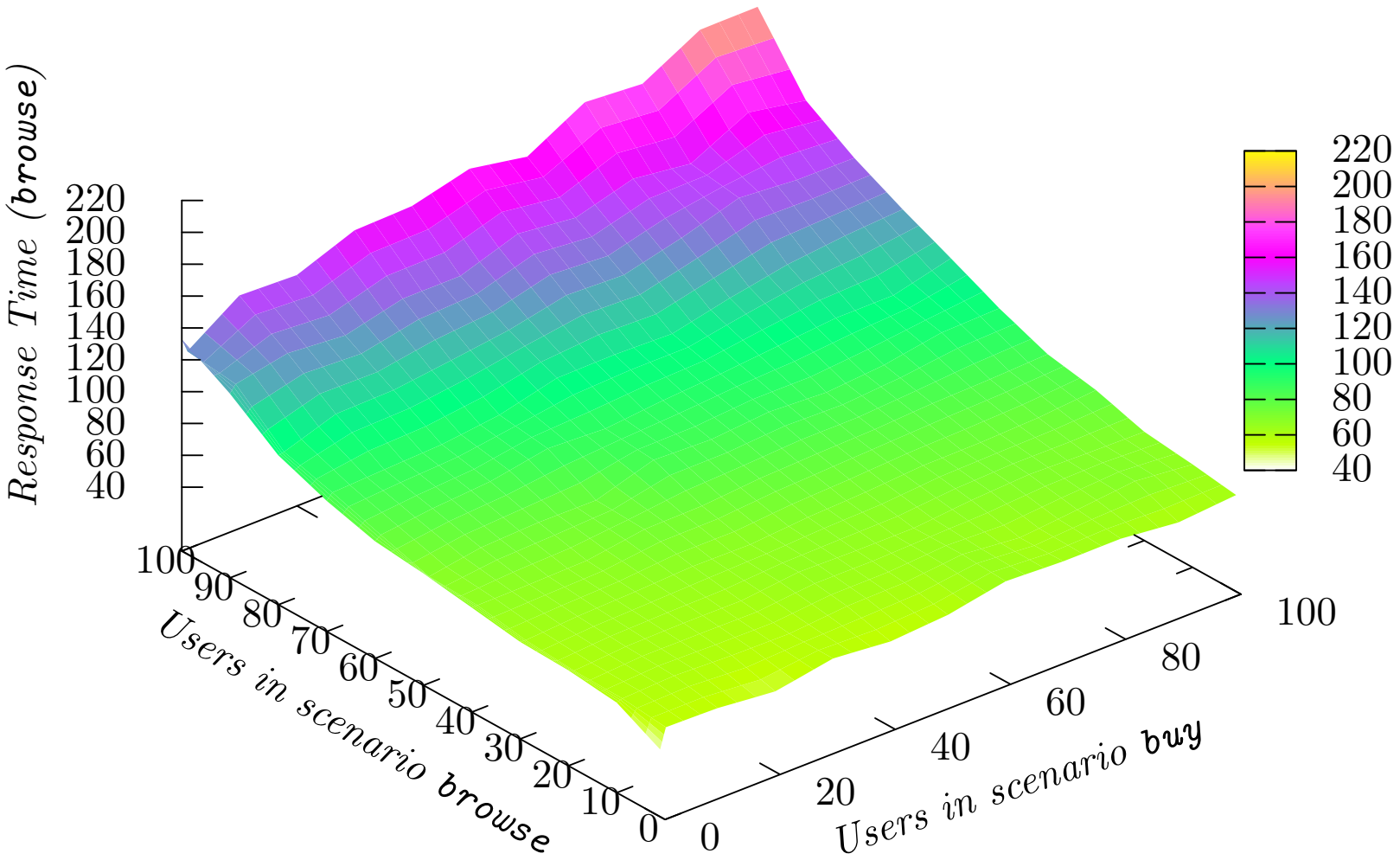
The Framework



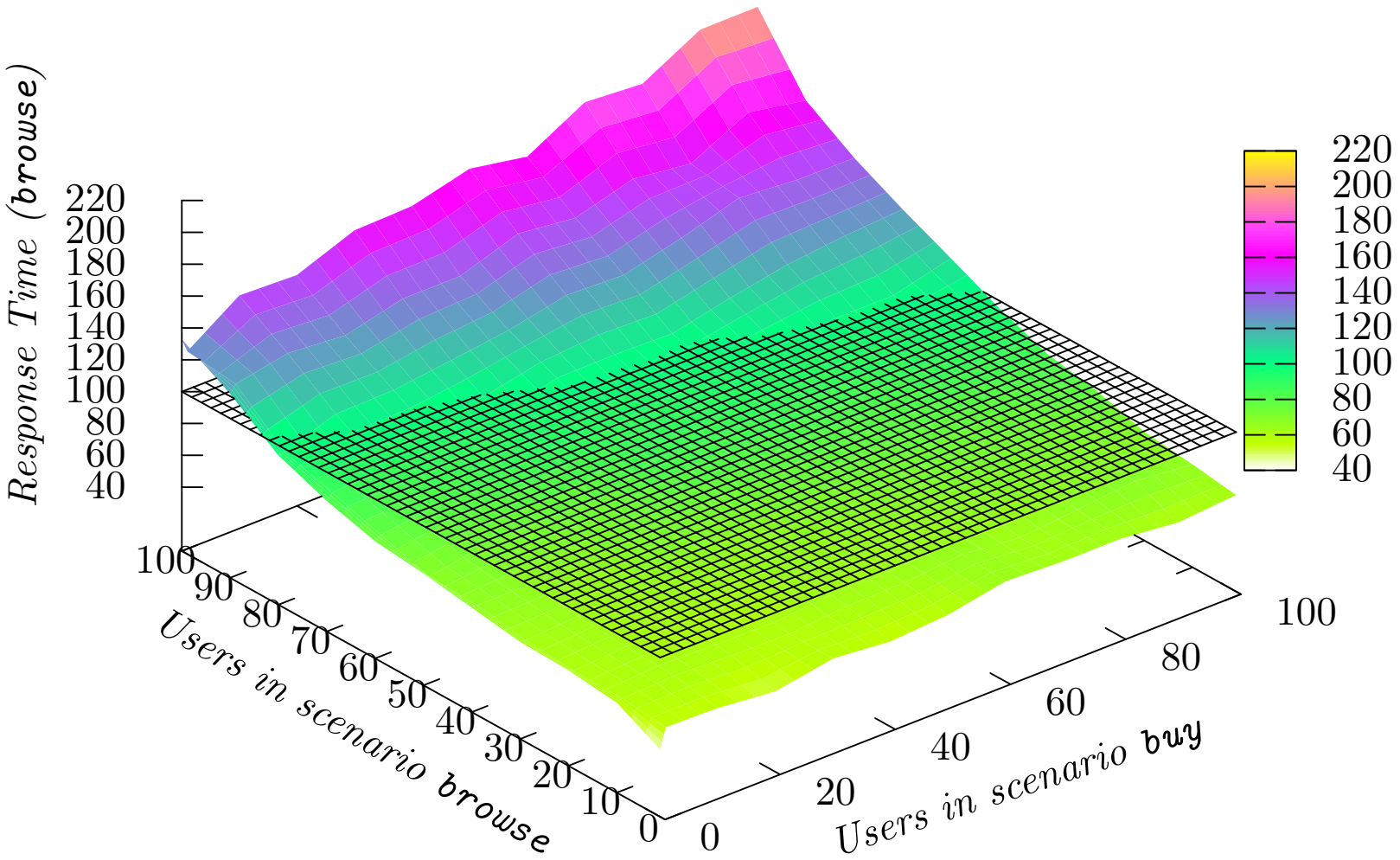
The Framework



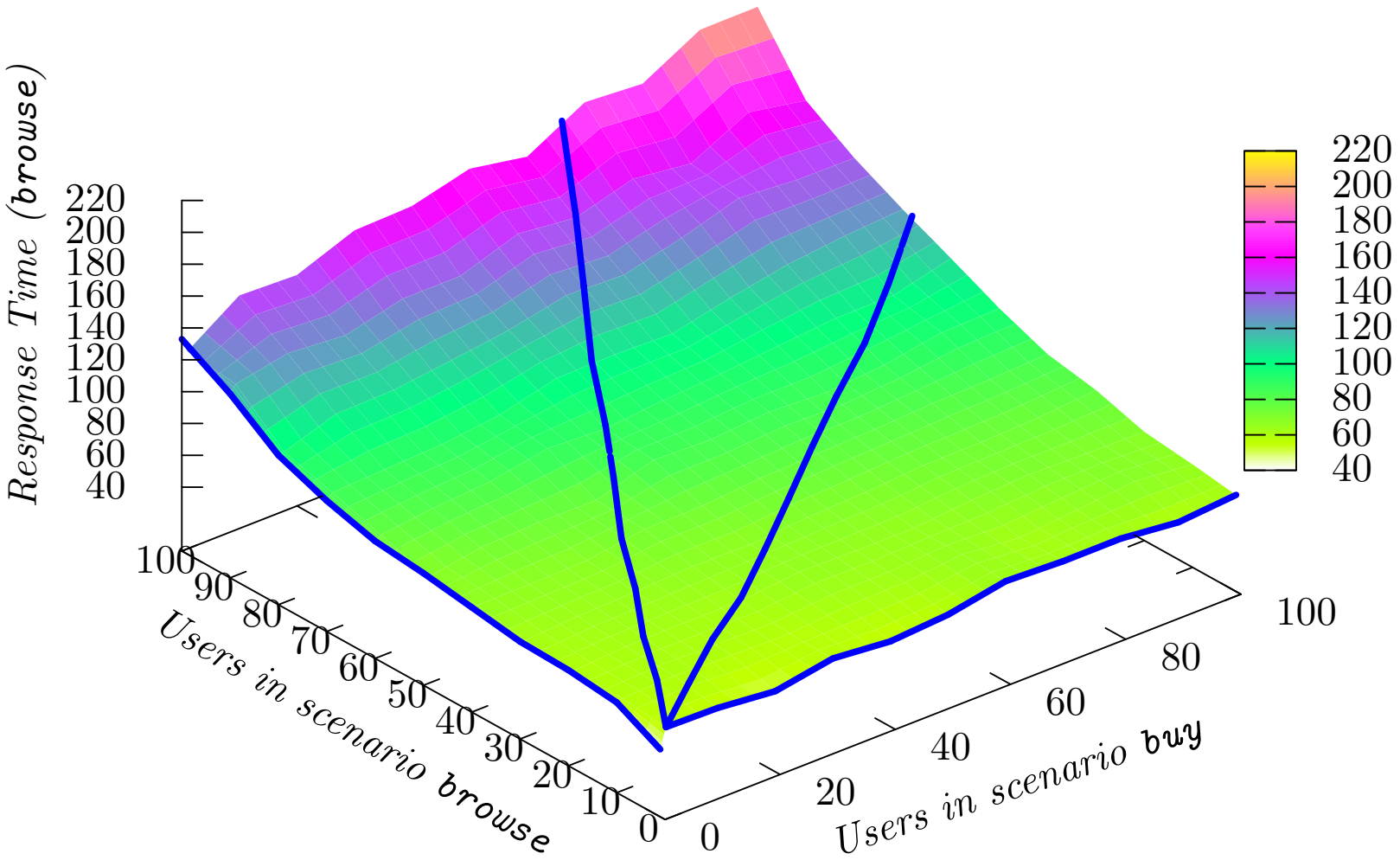
Results (response time goal)



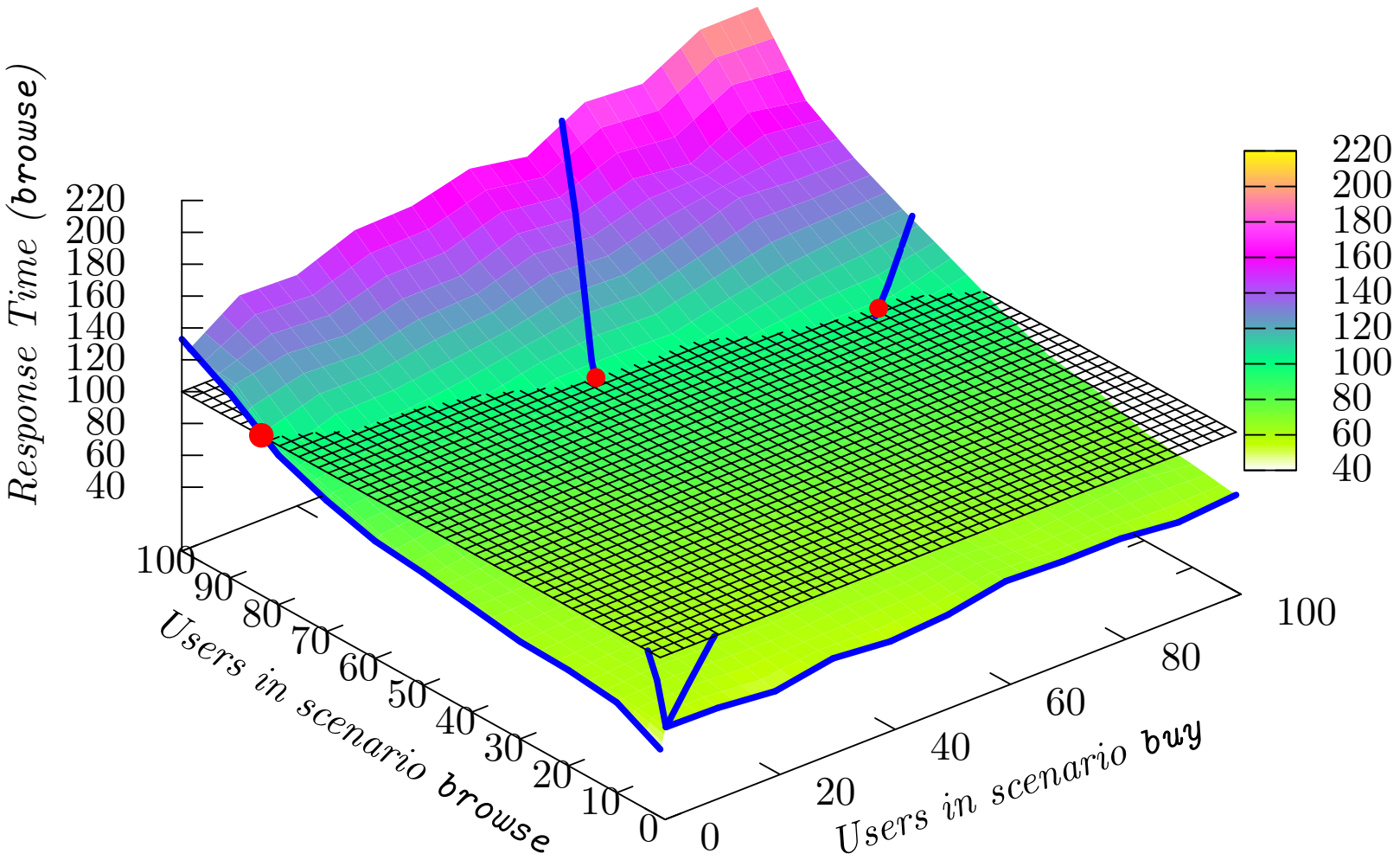
Results (response time goal)



Results (response time goal)



Results (response time goal)



Complexity

Exhaustive search:

$$\left.\begin{array}{r}\text{6 classes of service}\\ \text{at most 200 users}\end{array}\right\} \Rightarrow 98\,619\,368\,490 \text{ workload mixes}$$

With our framework:

$$\left.\begin{array}{r}\text{6 classes of service}\\ \text{no limit for users}\end{array}\right\} \Rightarrow 119 \text{ workload mixes}$$

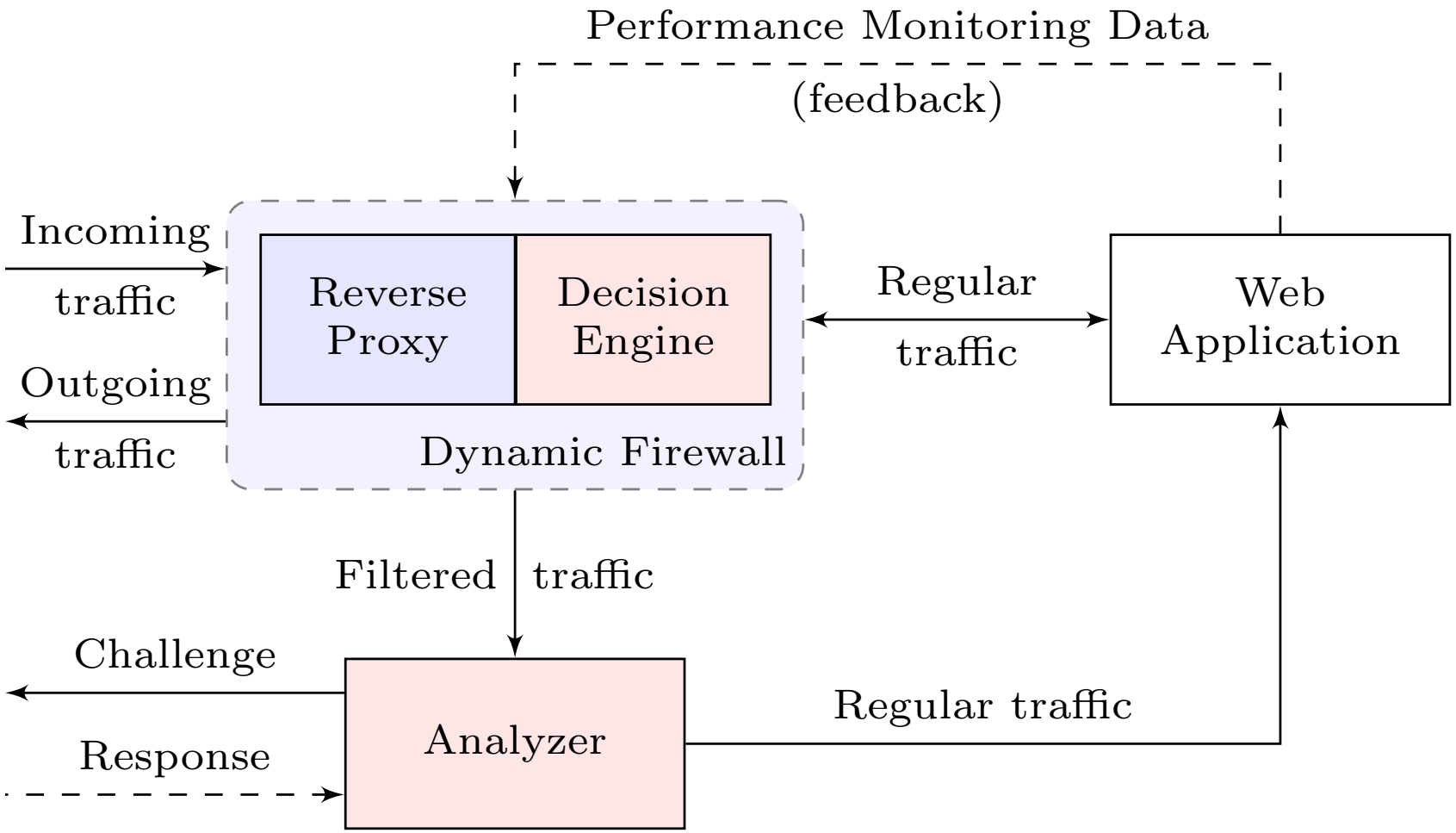
Performance Testing
The Performance Stress Space
The Framework
Results
Search Complexity

DoS Attack Mitigation
DoS Attacks
Adaptive DoS Mitigation
Experiments
Results

DoS Attacks

- Flood the target server with requests in an attemt to saturate the bottlenecks;
- DDoS attacks: the requests can come from multiple machines;
- Challenging to defend against them;
- Methods of mitigation: firewalls and intrusion detection systems.

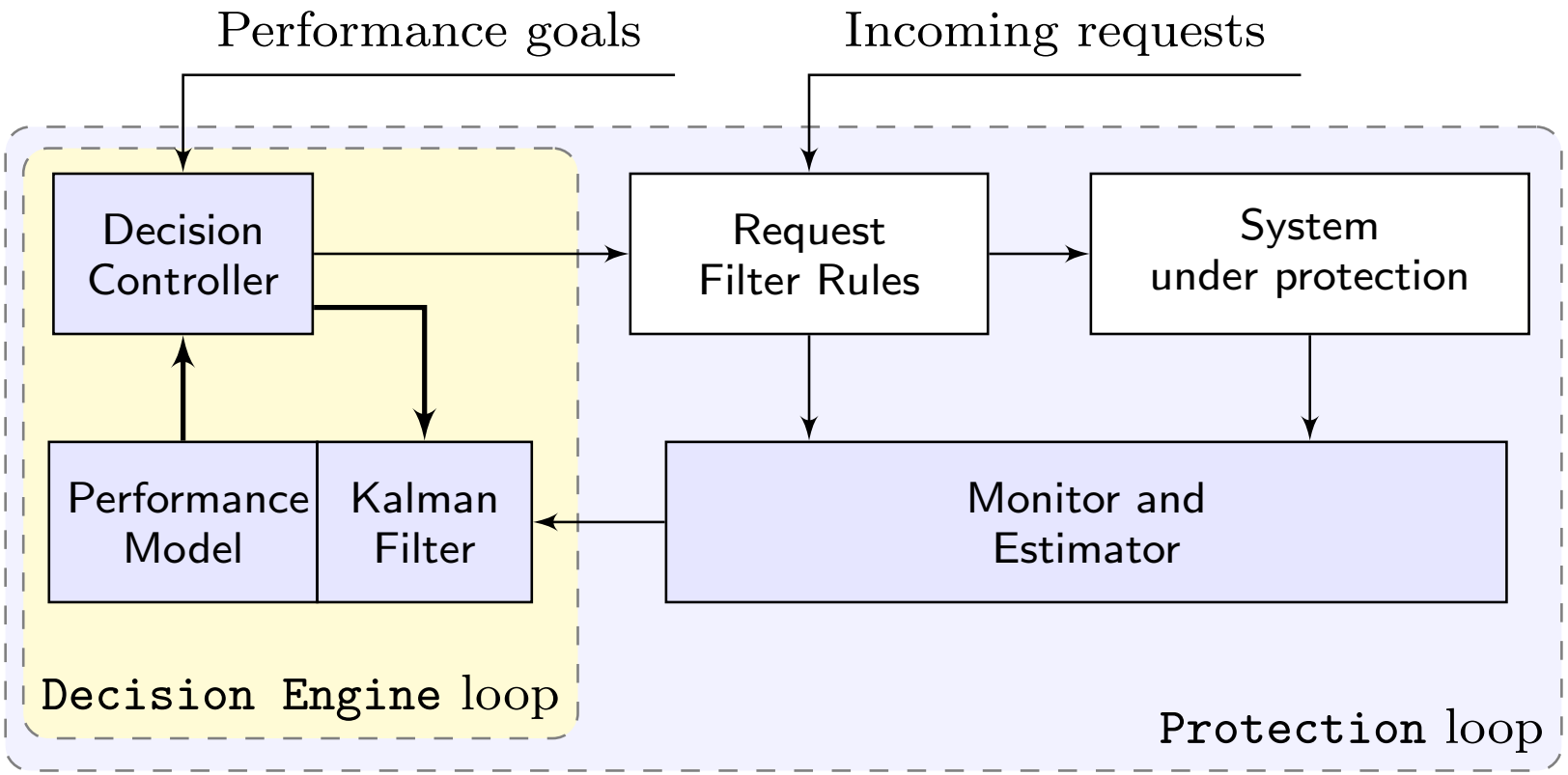
Adaptive DoS Mitigation



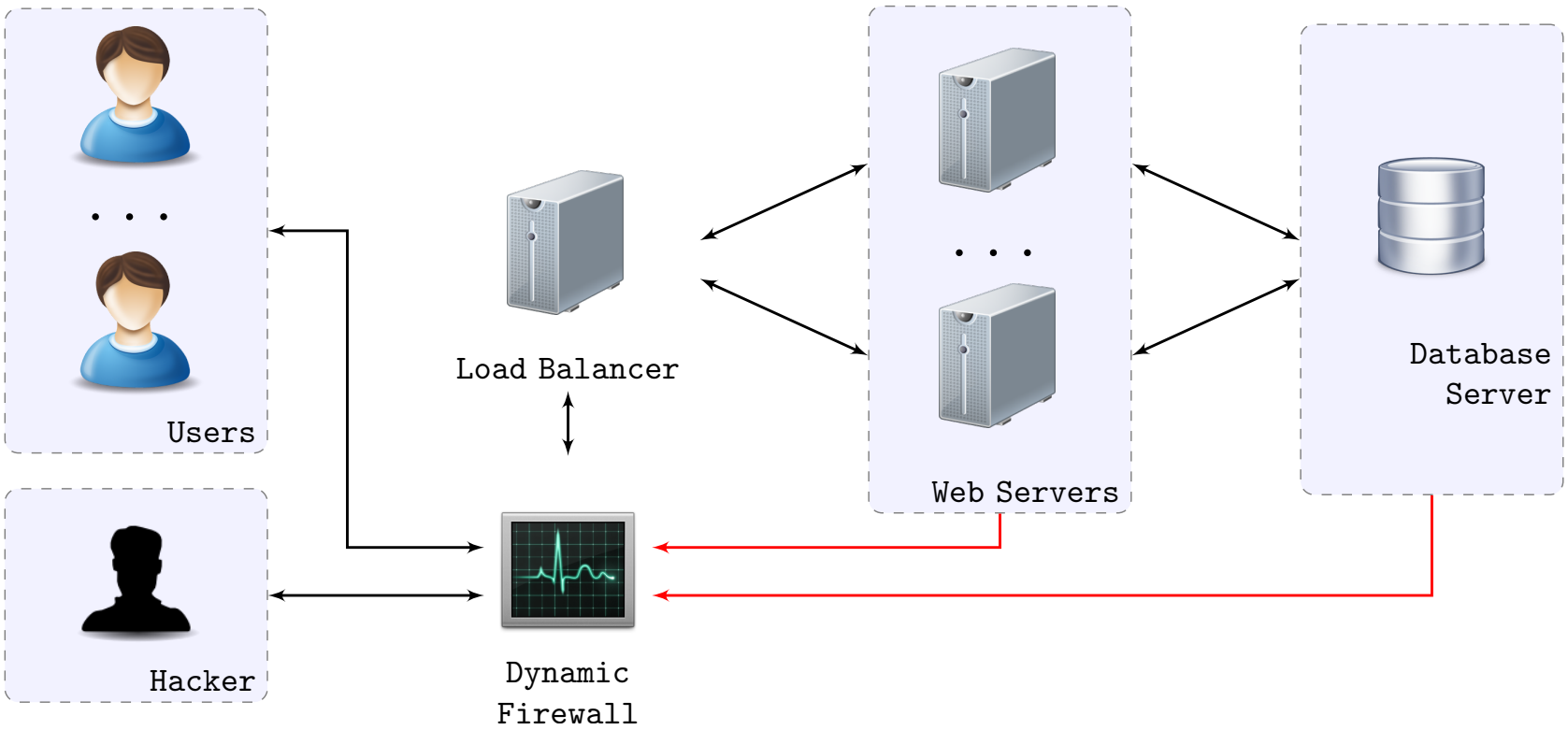
Decision Engine

- Use OPERA model to analyze the performance metrics;
- Constantly synchronize the model with the real system;
- When system is *overloaded*:
  - Identify the scenario(s) that should be filtered;
  - Create filtering rules;
- When system is functioning *normally*:
  - Identify the scenario(s) that should be unfiltered (if any);
  - Remove filtering rules;

Model-based Protection

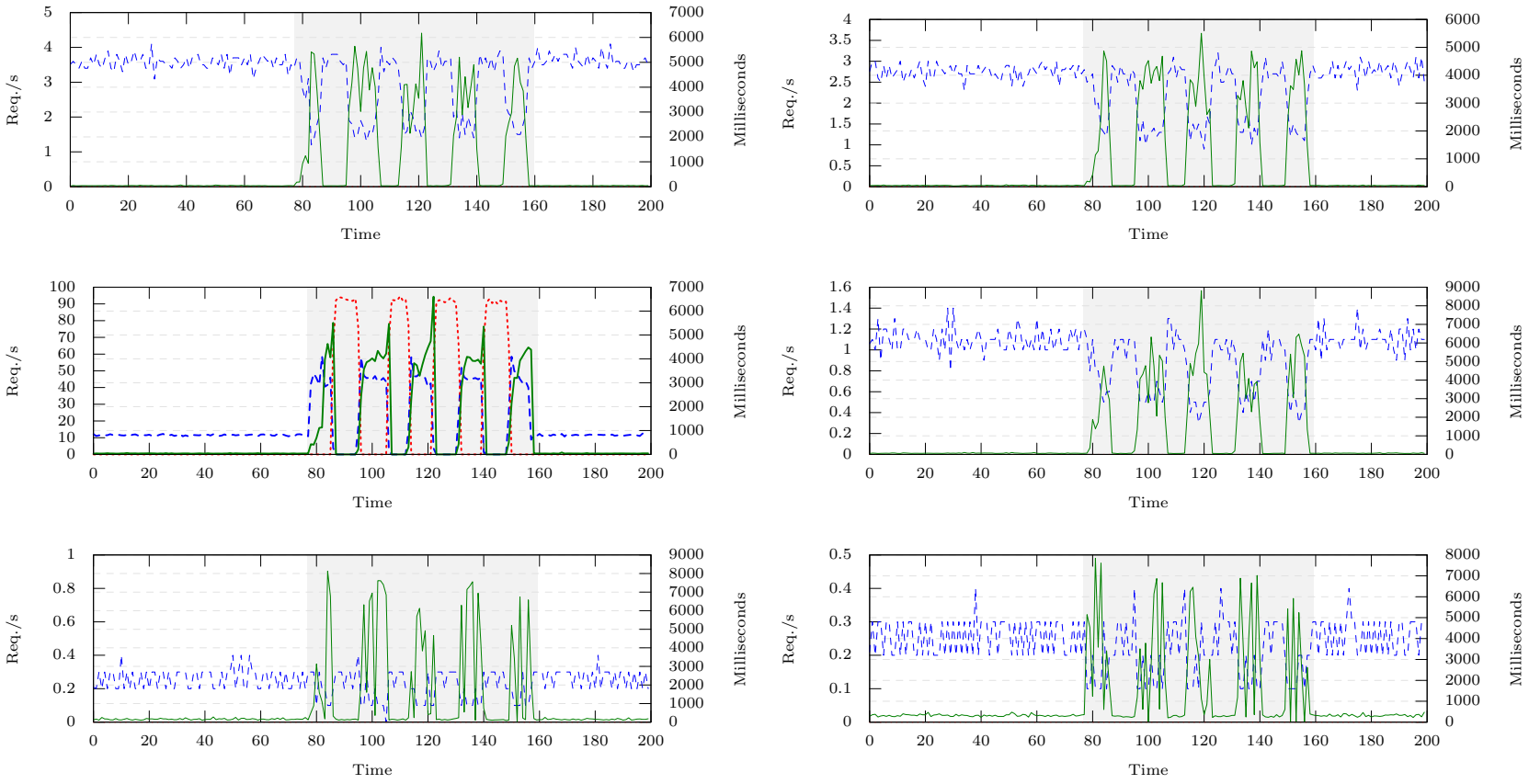


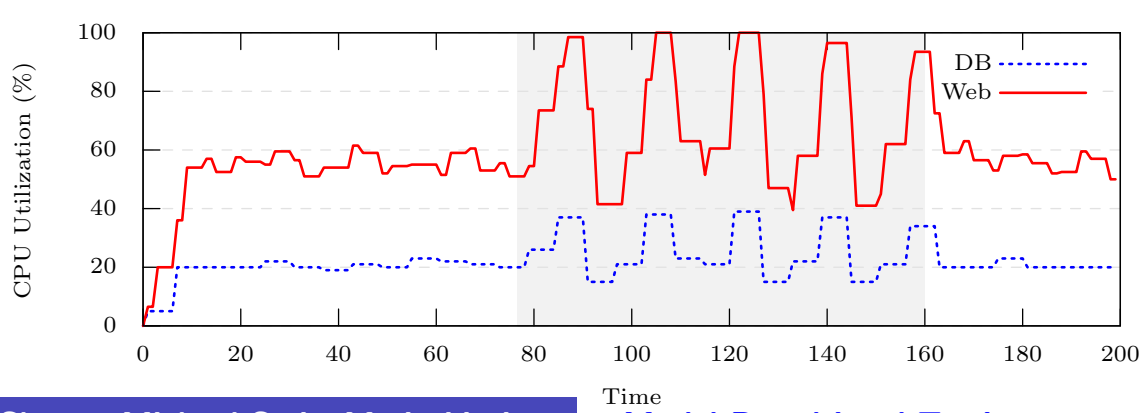
Deployment Topology



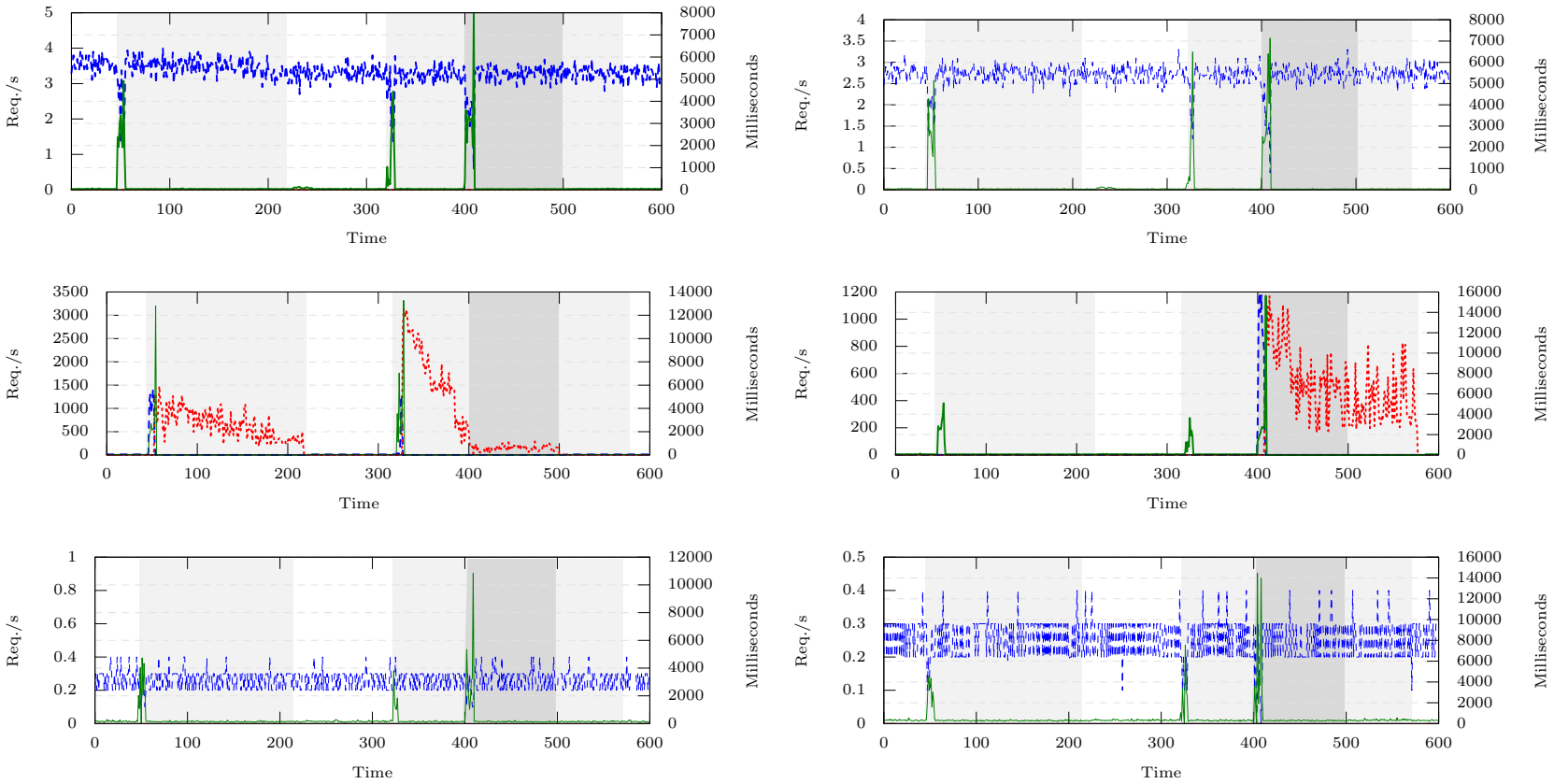
- Web Application with 6 scenarios: `marketing`, `product selection`, `buy`, `pay`, `inventory`, `auto bundles`.

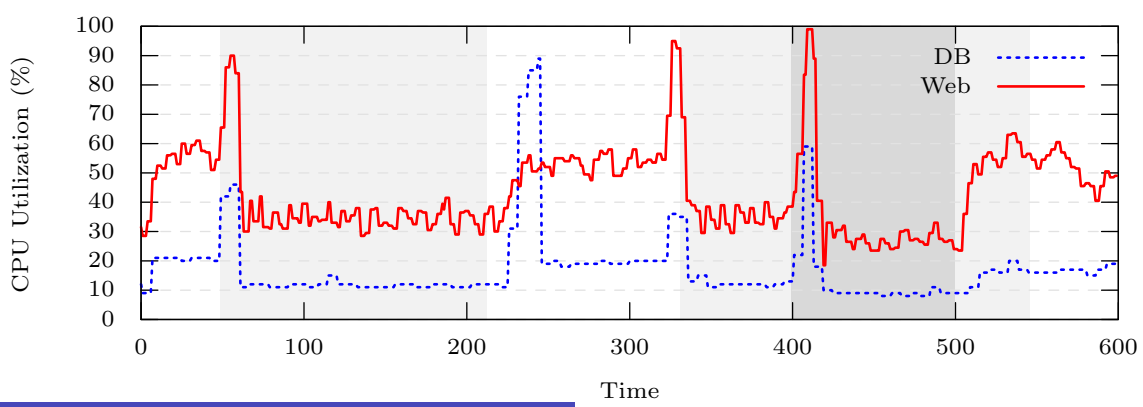
Results without a model





Results with OPERA





References

- OPERA (**O**ptimization, **P**erformance **E**valuation and **R**esource **A**llocator), https://muscat06.cs.uwaterloo.ca/saas/, February, 2012.
- C. Barna, M. Litoiu, and H. Ghanbari, Model-Based Performance Testing, NIER Track of ICSE 2011, May 2011.
- C. Barna, M. Litoiu, and H. Ghanbari, Autonomic Load Testing Framework, in *Proceedings of the* 8th *ACM International Conference on Autonomic Computing*. ACM, 2011, pp. 91–100.
- C. Barna, M. Shtern, M. Smit, V. Tzerpos, and M. Litoiu, Model-Based Adaptive DoS Attack Mitigation, in *Proceedings of the* 7th *International Symposium on Software Engineering for Adaptive and Self-Managing Systems*, ser. SEAMS 2012. ACM, 2012.