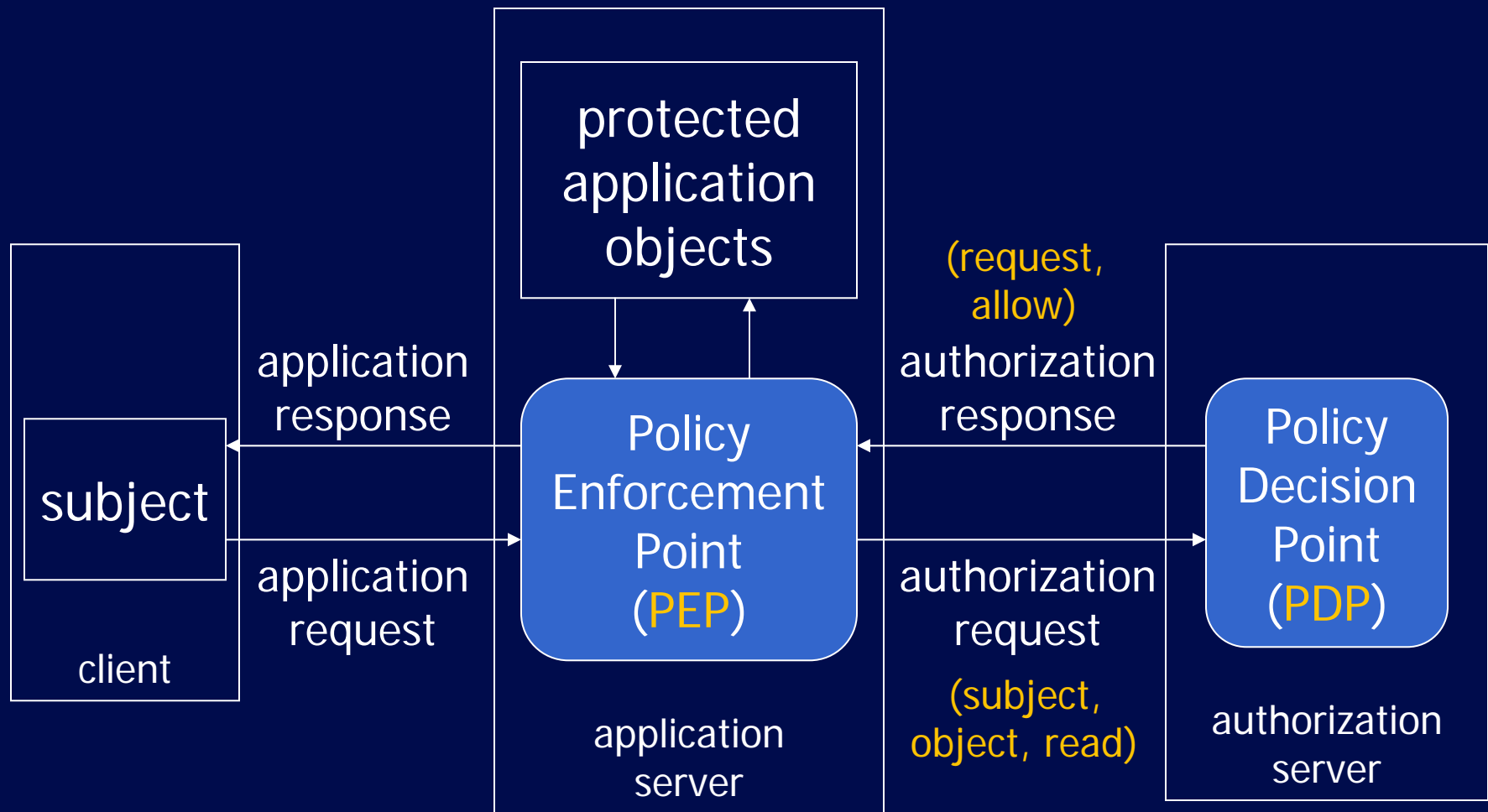# Cooperative Secondary Authorization Recycling

Qiang Wei, Matei Ripeanu, Konstantin Beznosov

Laboratory for Education and Research in Secure Systems Engineering
(lersse.ece.ubc.ca)
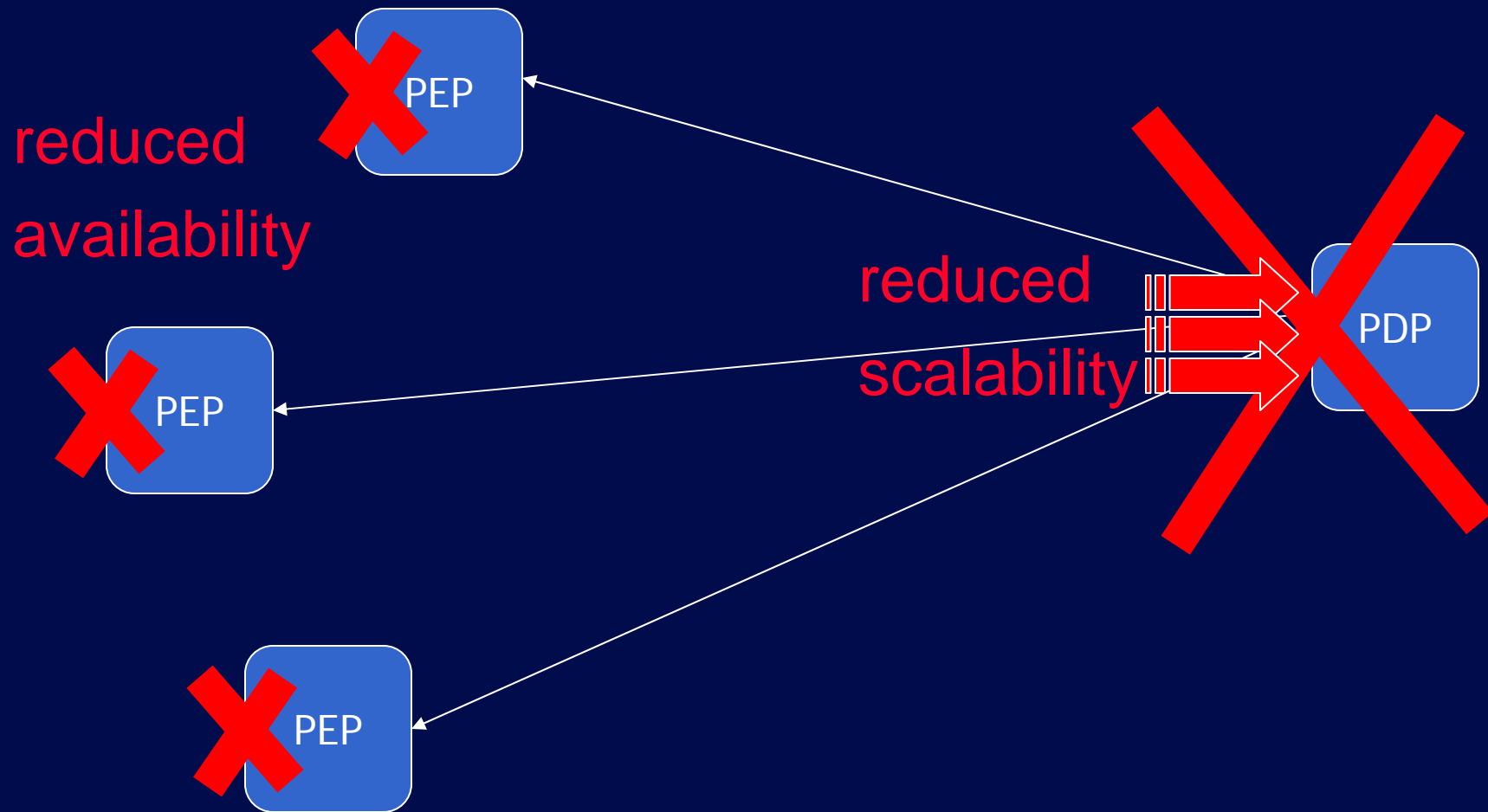
University of British Columbia
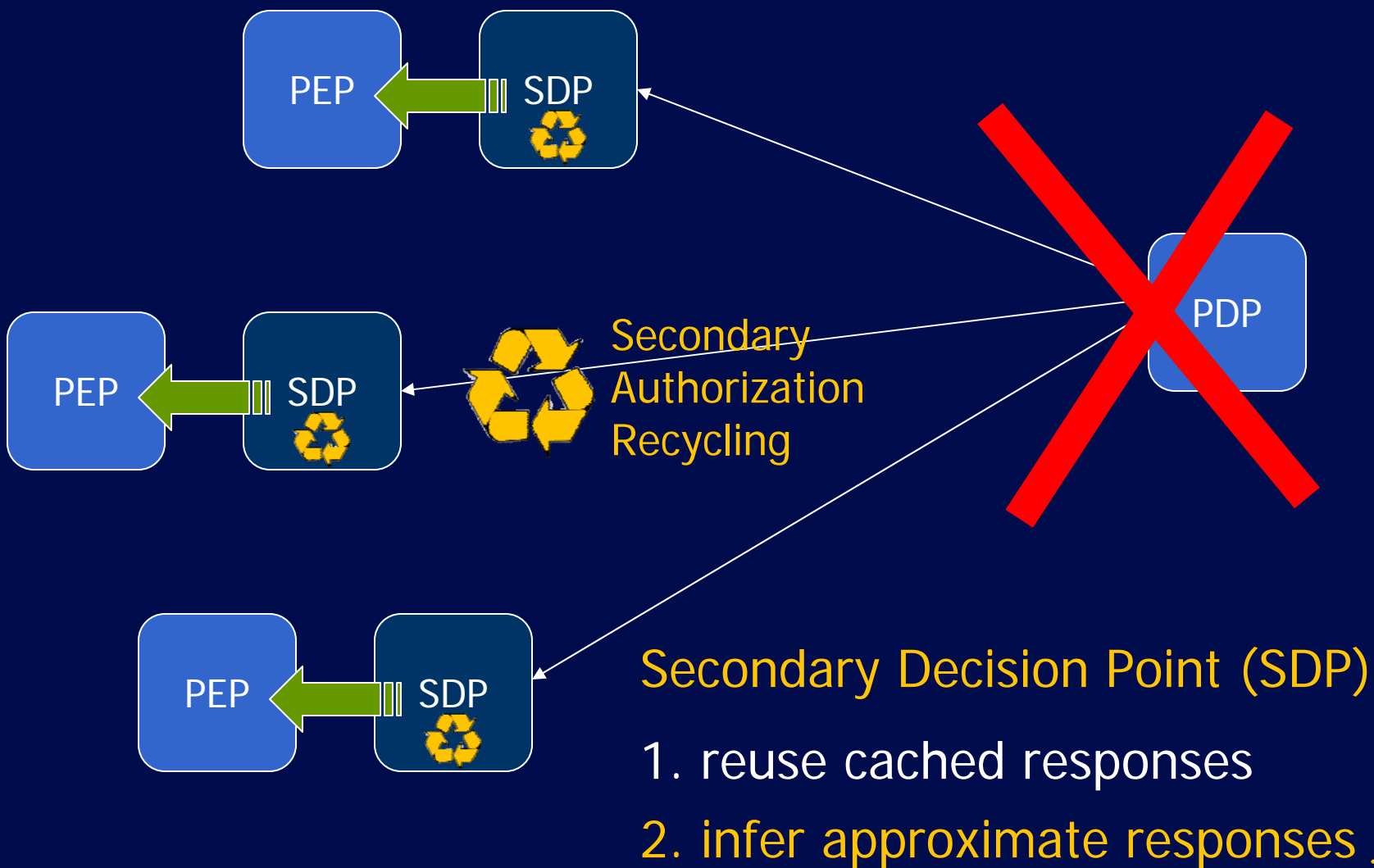
Typical Authorization Architecture

protected application objects

subject

client

application response

application request

Policy Enforcement Point (PEP)

application server

(request, allow)

authorization response

authorization request

(subject, object, read)

Policy Decision Point (PDP)

authorization server

Also known as request-response paradigm
e.g. IBM Access Manager, EJB, XACML

Motivation Problems

reduced availability

reduced scalability

PEP

PEP

PEP

PDP

Laboratory for Education and Research in Secure Systems Engineering   (lersse.ece.ubc.ca)

Secondary and Approximate Authorization Model (SAAM)

PEP ← SDP ♻

PEP ← SDP ♻

♻ Secondary Authorization Recycling

PEP ← SDP ♻

PDP

Secondary Decision Point (SDP)
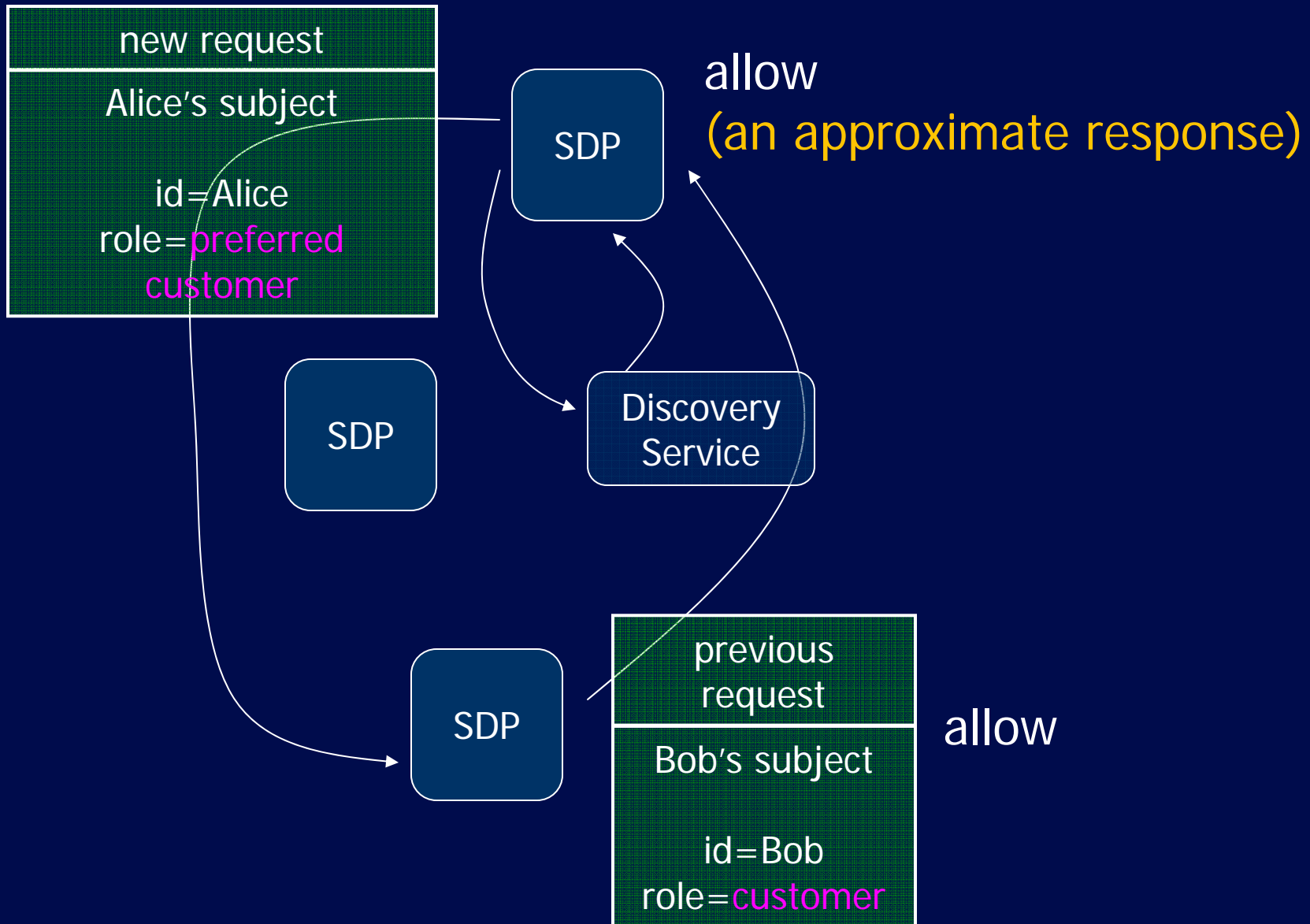
1. reuse cached responses

2. infer approximate responses

Cooperative Secondary Authorization Recycling
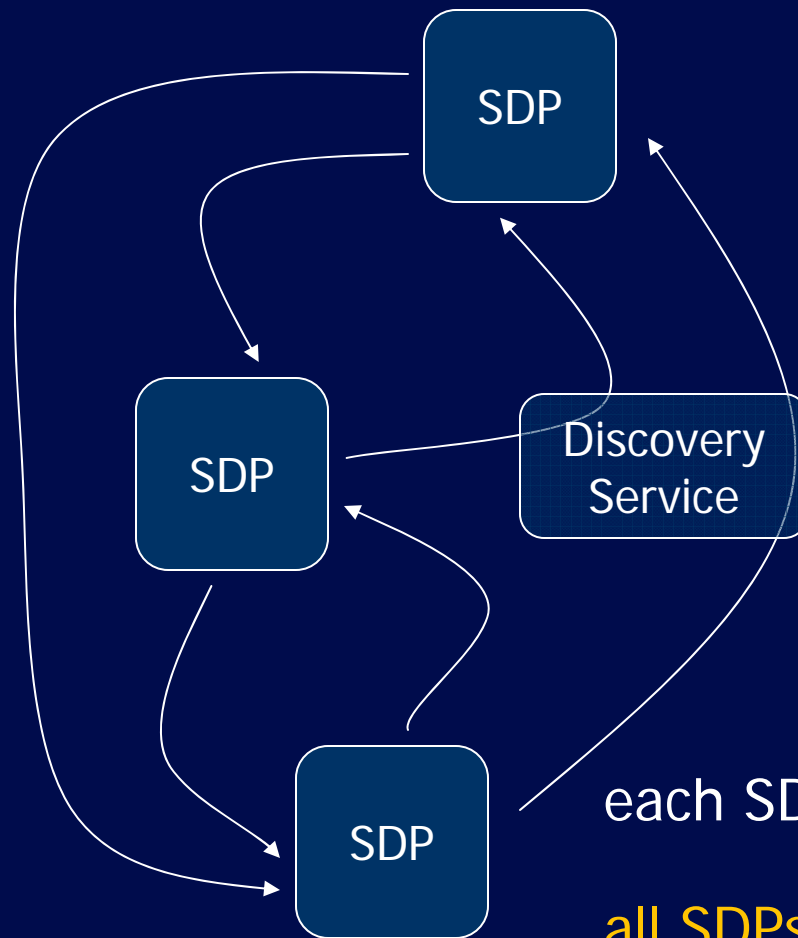
each SDP serves only its own PEP!

all SDPs cooperate to serve all PEPs

A Simplified Example

new request

Alice's subject

id=Alice
role=preferred customer

SDP

allow
(an approximate response)

SDP

Discovery Service
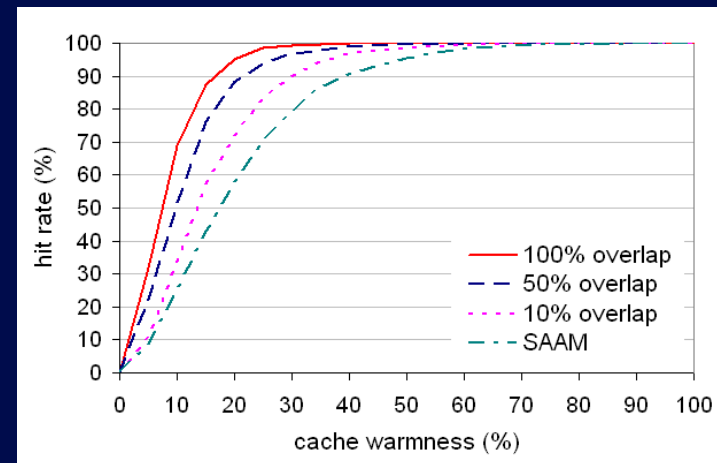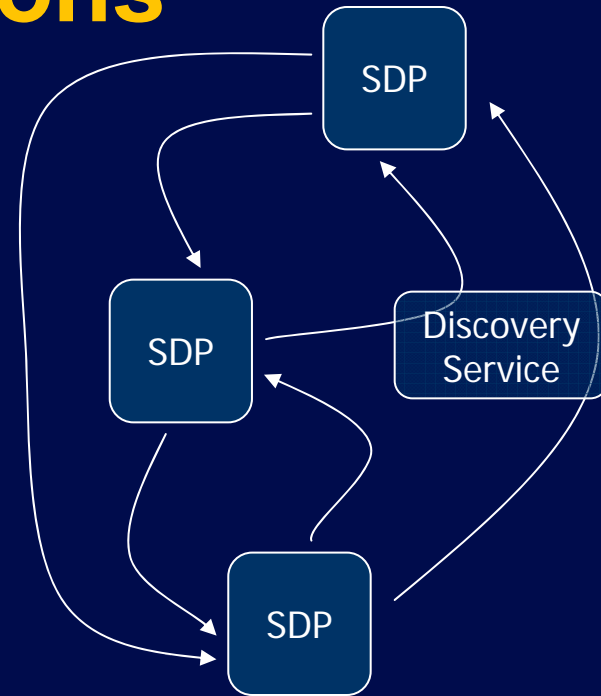
SDP

previous request

Bob's subject

id=Bob
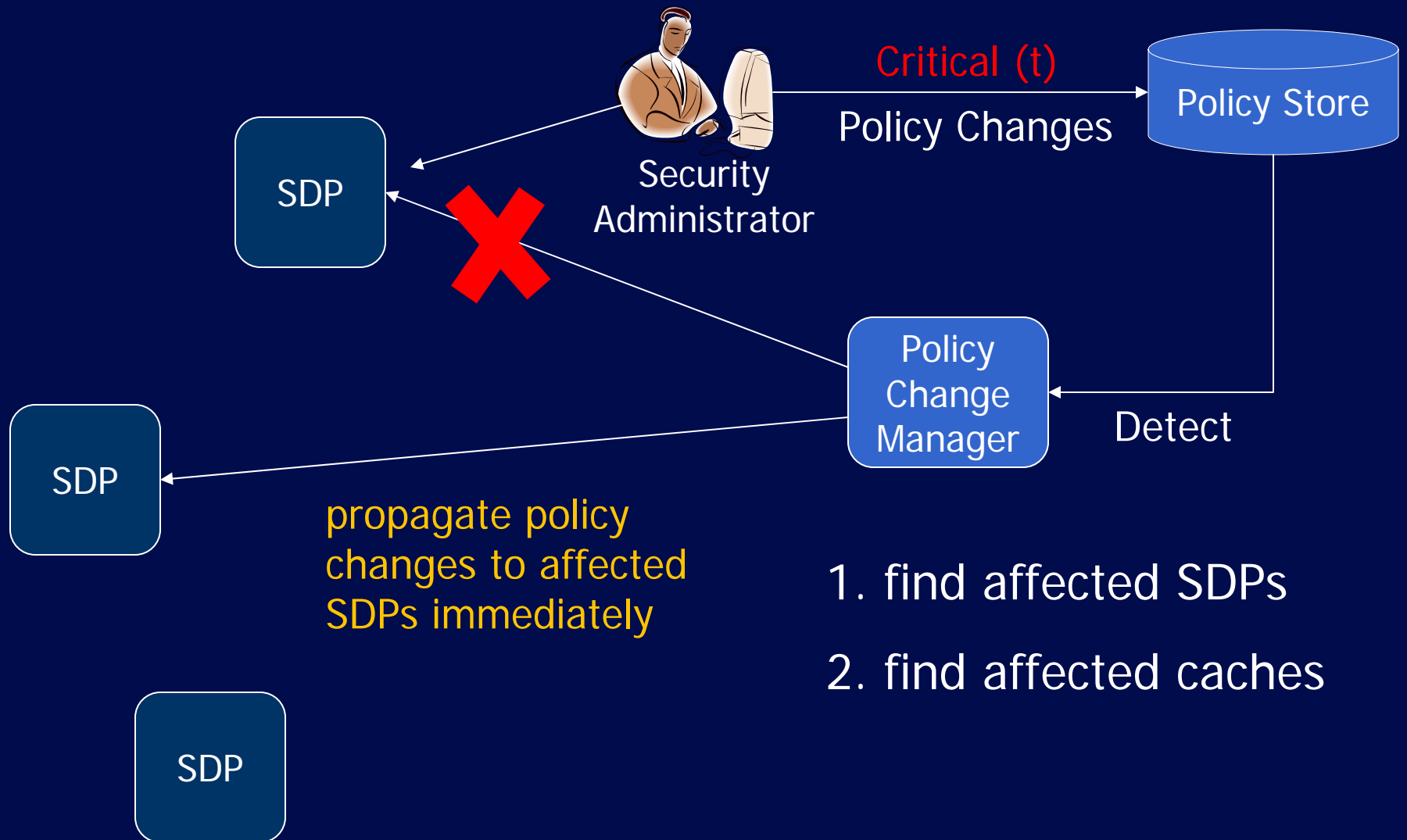role=customer

allow

Contributions

- Proposed
  - the concept of cooperative secondary authorization recycling
  - system architecture & detailed design
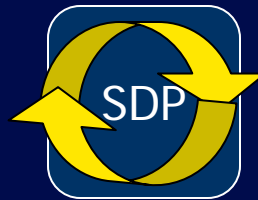- Evaluated
  - availability
  - performance

Key Design Features

Laboratory for Education and Research in Secure Systems Engineering   (lersse.ece.ubc.ca)

Consistency: Support Critical Policy Changes

Critical (t)

Policy Changes

Policy Store

Security
Administrator

SDP

Policy
Change
Manager

Detect

SDP

propagate policy
changes to affected
SDPs immediately

1. find affected SDPs

2. find affected caches

SDP

Consistency: Support Time-sensitive Policy Changes

SDP

Time-sensitive
Policy Changes

Policy Store

Security
Administrator

SDP

A TTL approach:
delete expired
responses periodically

Policy
Change
Manager

Detect

SDP

Support Untrusted Remote SDPs

PEP — Trusts → SDP — Trusts → PDP   Trusted by all SDPs

Does NOT Trust ✖

Malicious SDP

Verify responses made by remote SDPs

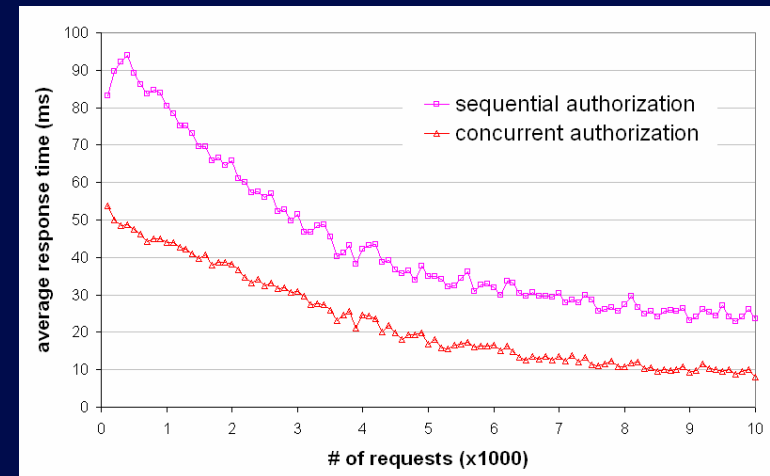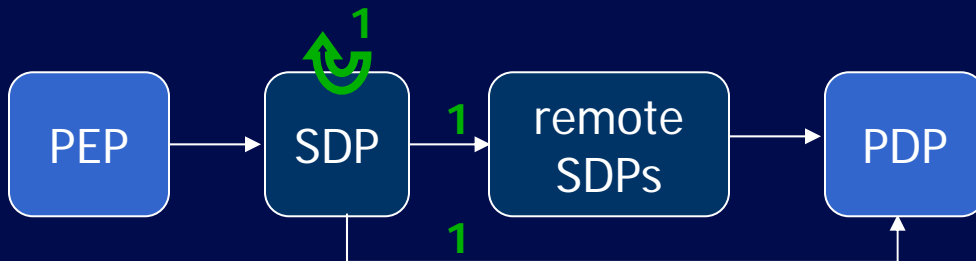1. verify the authenticity and integrity

2. verify the correctness of inference

Configurability

- **Three decision points**
  - local SDP & remote SDPs & the PDP
- **To reduce network traffic & PDP's load**
  - **sequential** authorization
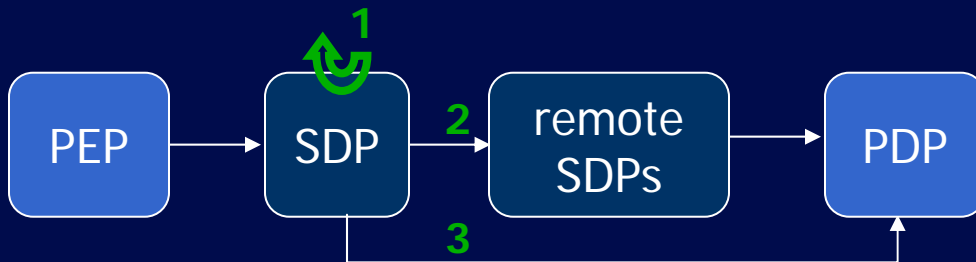
- **To reduce the response time**
  - **concurrent** authorization

Evaluation Results

via simulation & prototype implementation

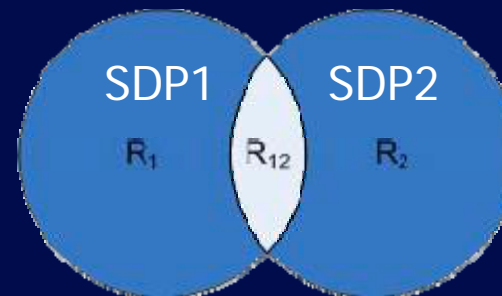# Simulation-based Evaluation

- **Metrics**
  - cache hit rate

training set

simulation engine

testing set

- **Methodology**
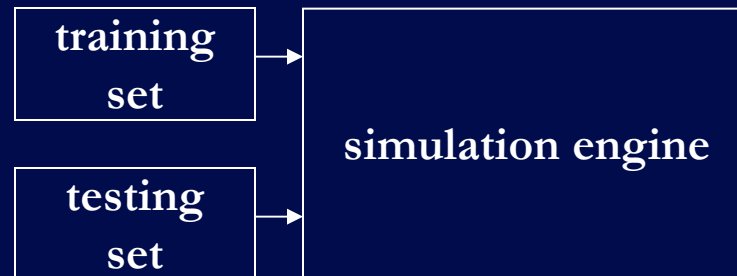
- **Affecting factors**
  - cache warmness $= \dfrac{|\text{cached requests without replacement}|}{|\text{total possible requests}|}$
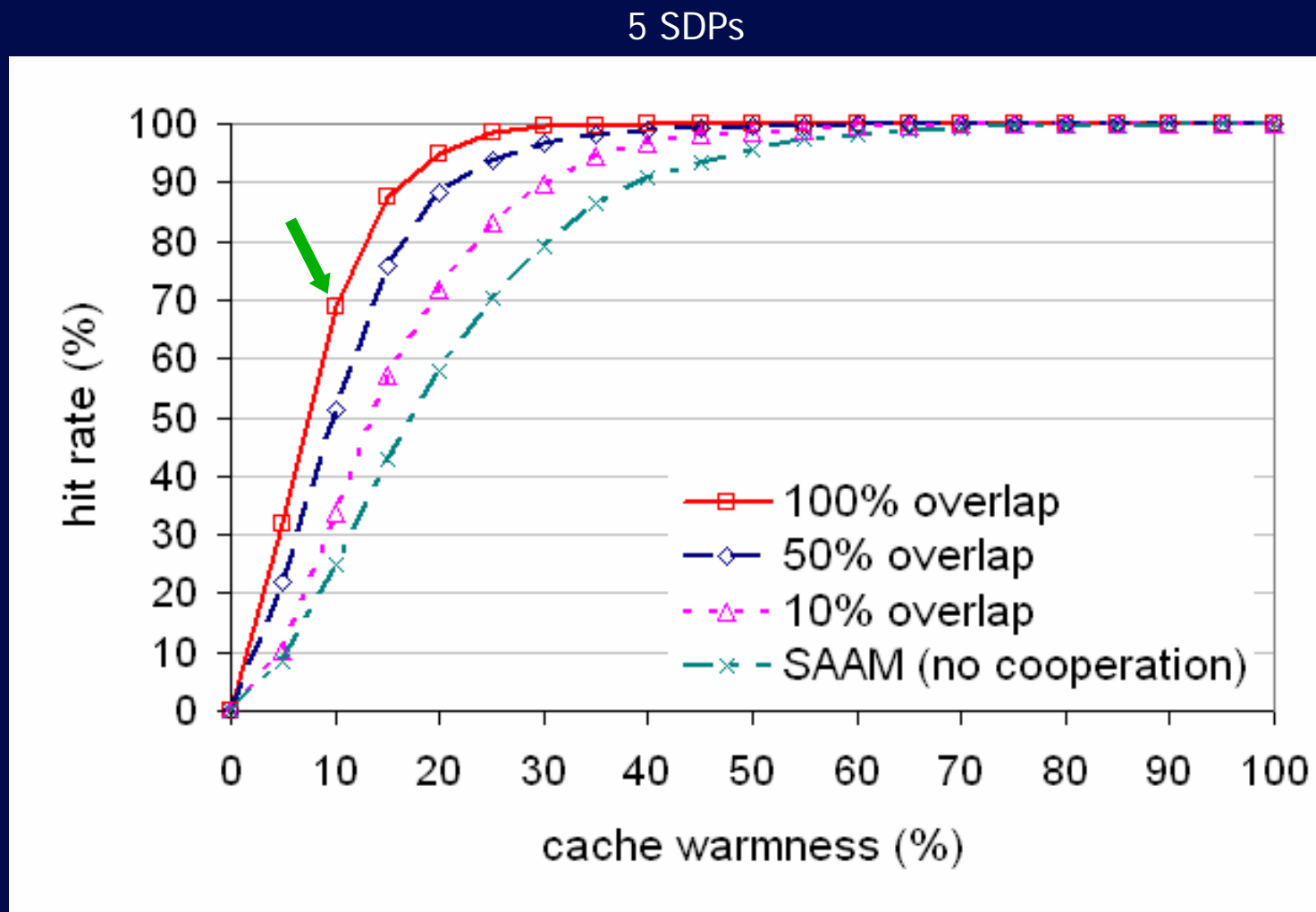
  - number of cooperating SDPs

  - overlap rate $O_{12} = \dfrac{|R_{12}|}{|R_1|}$

  SDP1   SDP2

  R_1 R_{12} R_2

  R – resource space

Hit Rate Dependence on Cache Warmness

5 SDPs

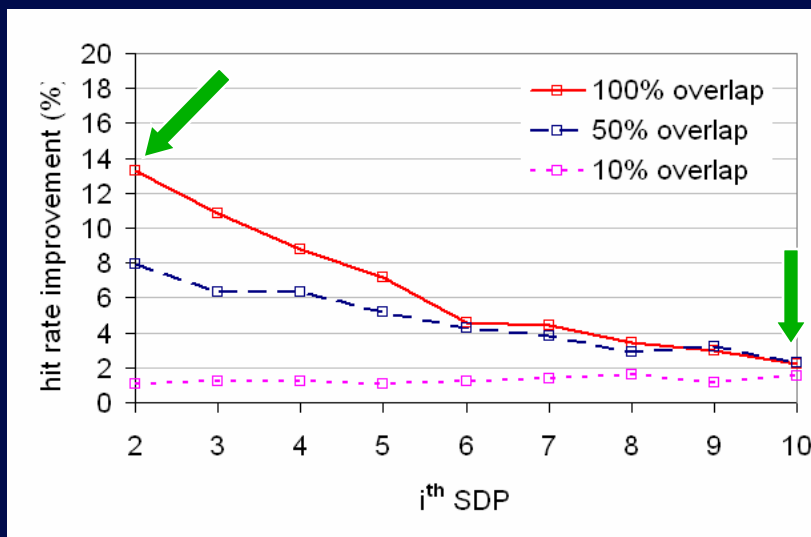High hit rate is achieved even when cache warmness is low

Hit Rate Dependence on Number of SDPs

10% cache warmness at each SDP
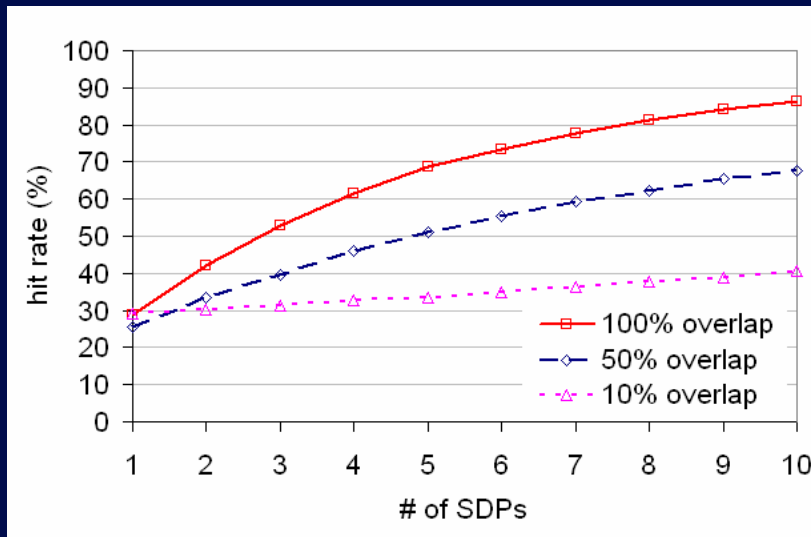
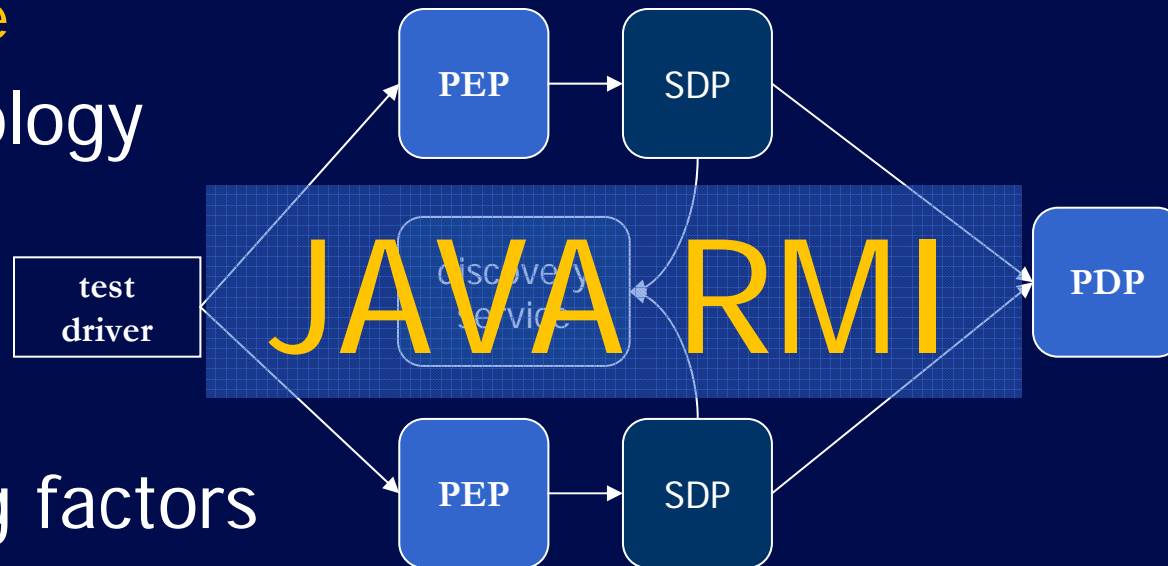Increasing the number of cooperating SDPs leads to higher hit rates

Additional SDPs provide diminishing returns

Prototype-based Evaluation

- **Metrics**
  - average client-perceived response time
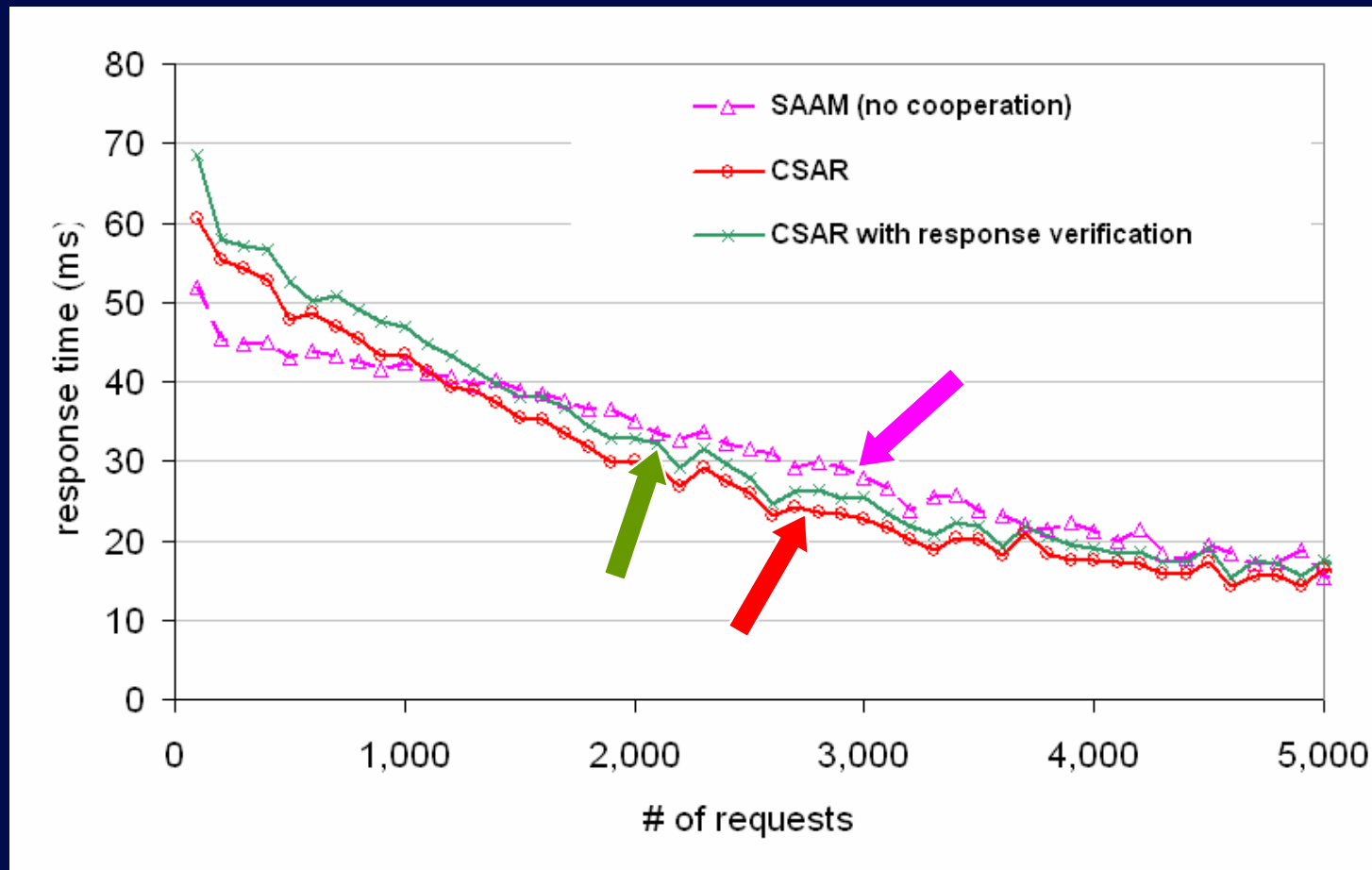 - hit rate
- **Methodology**

- **Affecting factors**
  - number of requests
  - presence of response verification
  - frequency of policy change

Response Time Dependence on Number of Requests

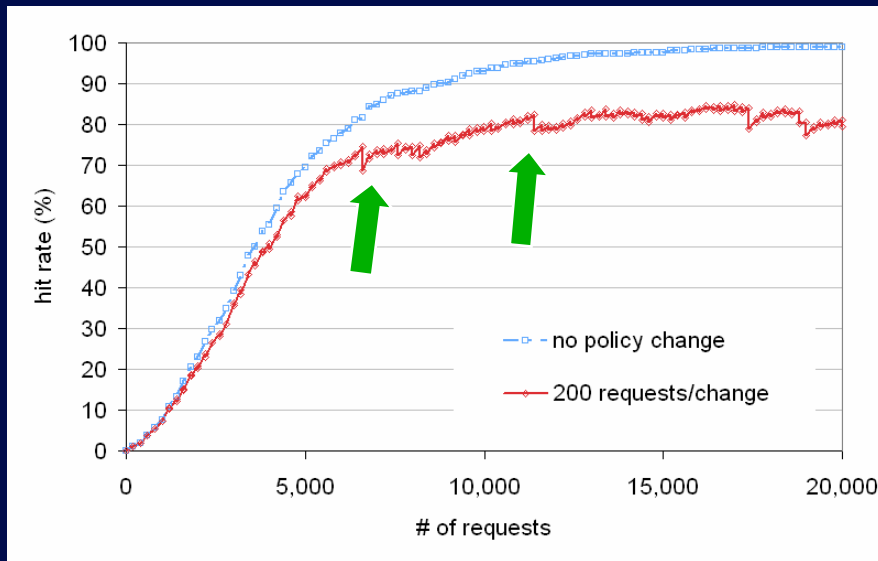4 SDPs (CSAR), 100% overlap, 40ms RTT between PDP and each SDP

1. Cooperation can contribute to reduced response time
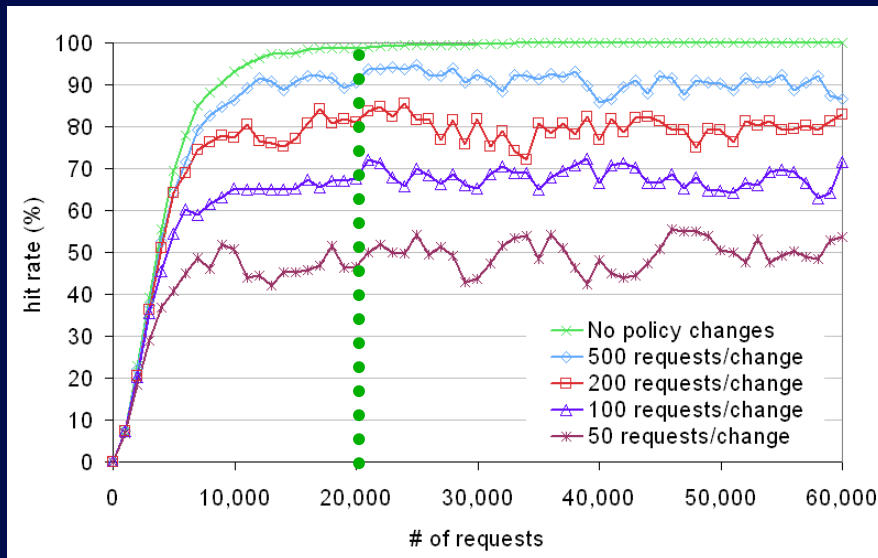2. The impact of response verification is small

How will regular policy changes affect hit rate?

1 SDP

2. Cumulative effect of policy changes is significant
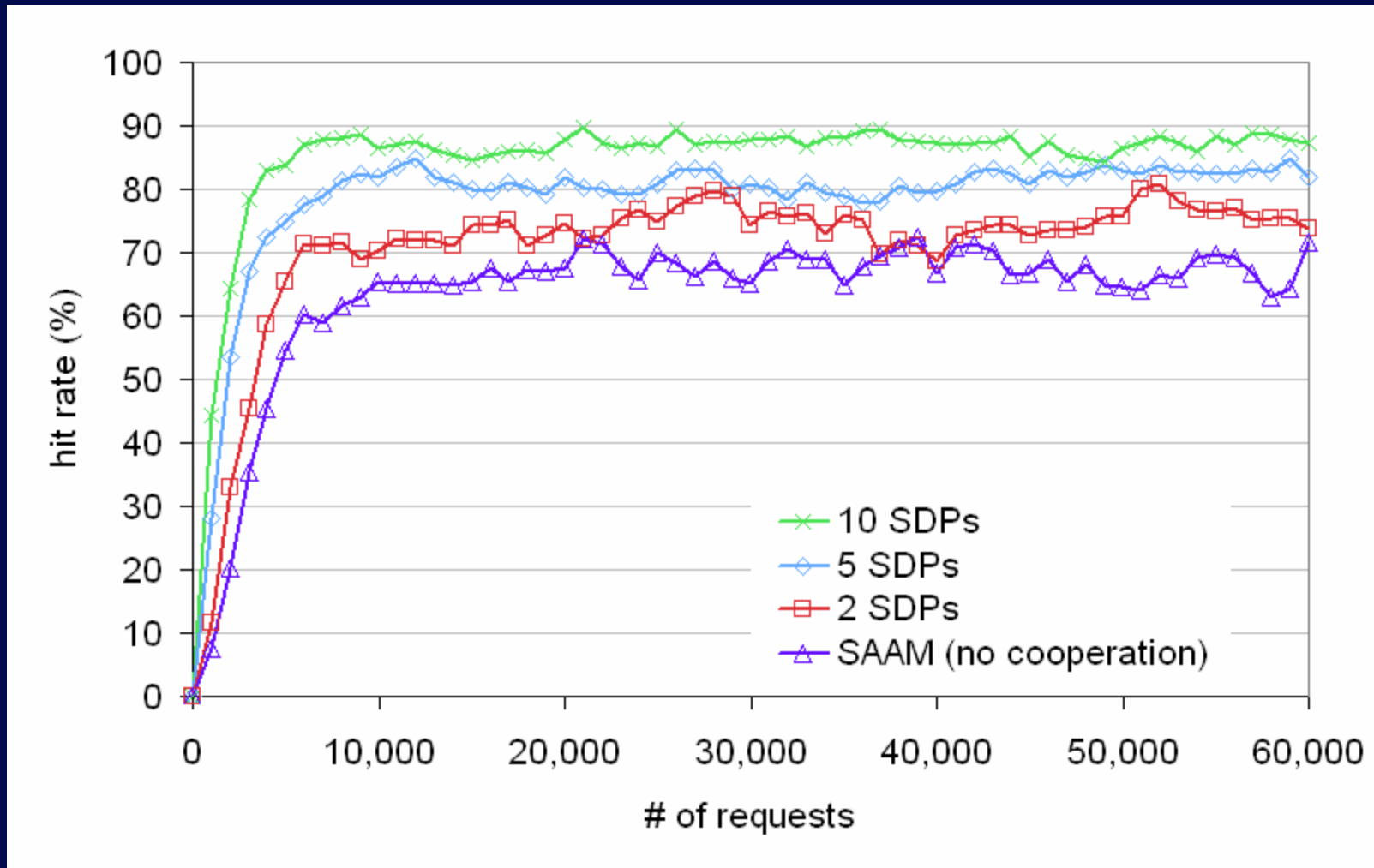
1. Hit-rate drop caused by each policy change is small

2. More frequent policy changes lead to lower hit rates

1. The hit rates stabilize after the knee

How does cooperation help?

100% overlap, policy changes at 100 requests/change

Cooperation improves hit rates when policy changes

Related Work

Collaborative security
(Locasto et al. 2006, Costa et al. 2005)

CSAR

Secondary and Approximate Authorization Model (SAAM)
(Crampton et al. 2006, Beznosov 2005)

Collaborative web caching
(Lyer et al. 2002, Wolman et al. 1999, Chankhunthod et al. 1996)

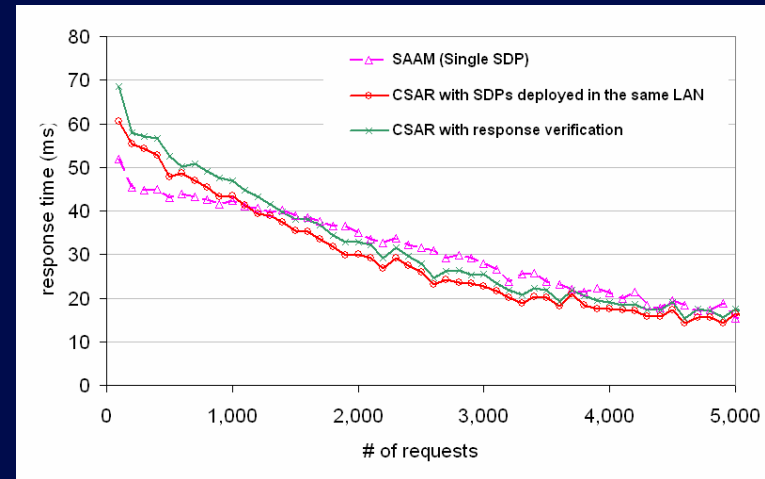**Authorization recycling**
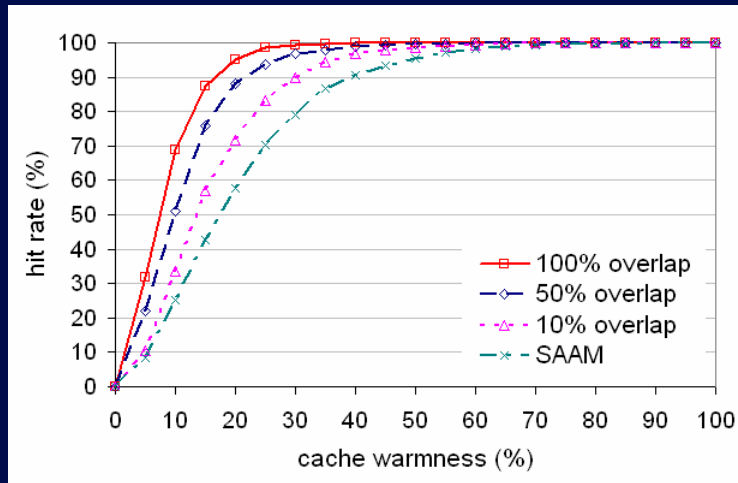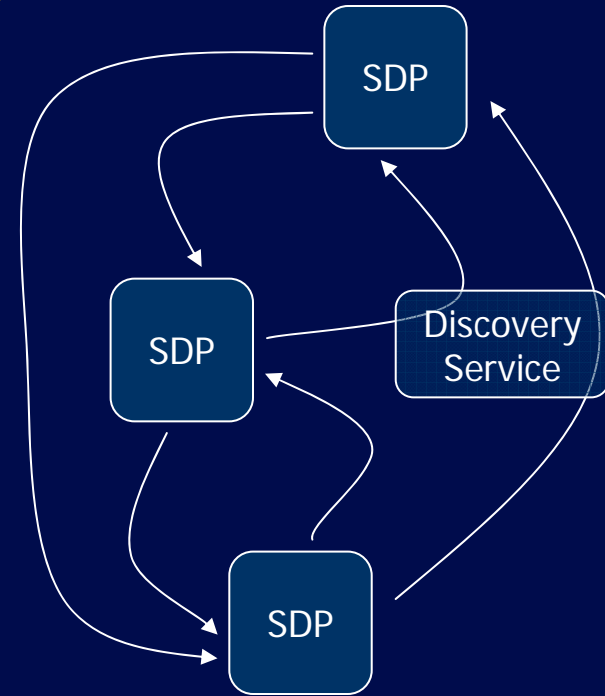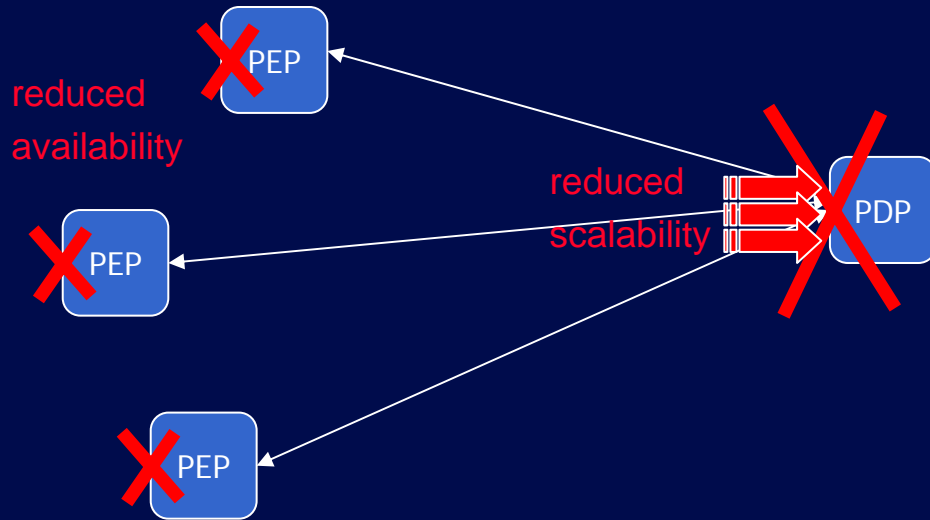*(Bauer et al. 2005, Borders et al. 2005)*

Future Work

- More active cooperation
- Integrate the prototype with real applications
- Speculative authorization
- Publish-subscribe model

Summary

lersse.ece.ubc.ca