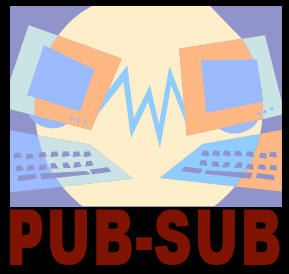

THE UNIVERSITY OF BRITISH COLUMBIA




# Authorization Using the Publish-Subscribe Model

**Qiang Wei, Matei Ripeanu, Konstantin Beznosov**

Laboratory for Education and Research in Secure Systems Engineering

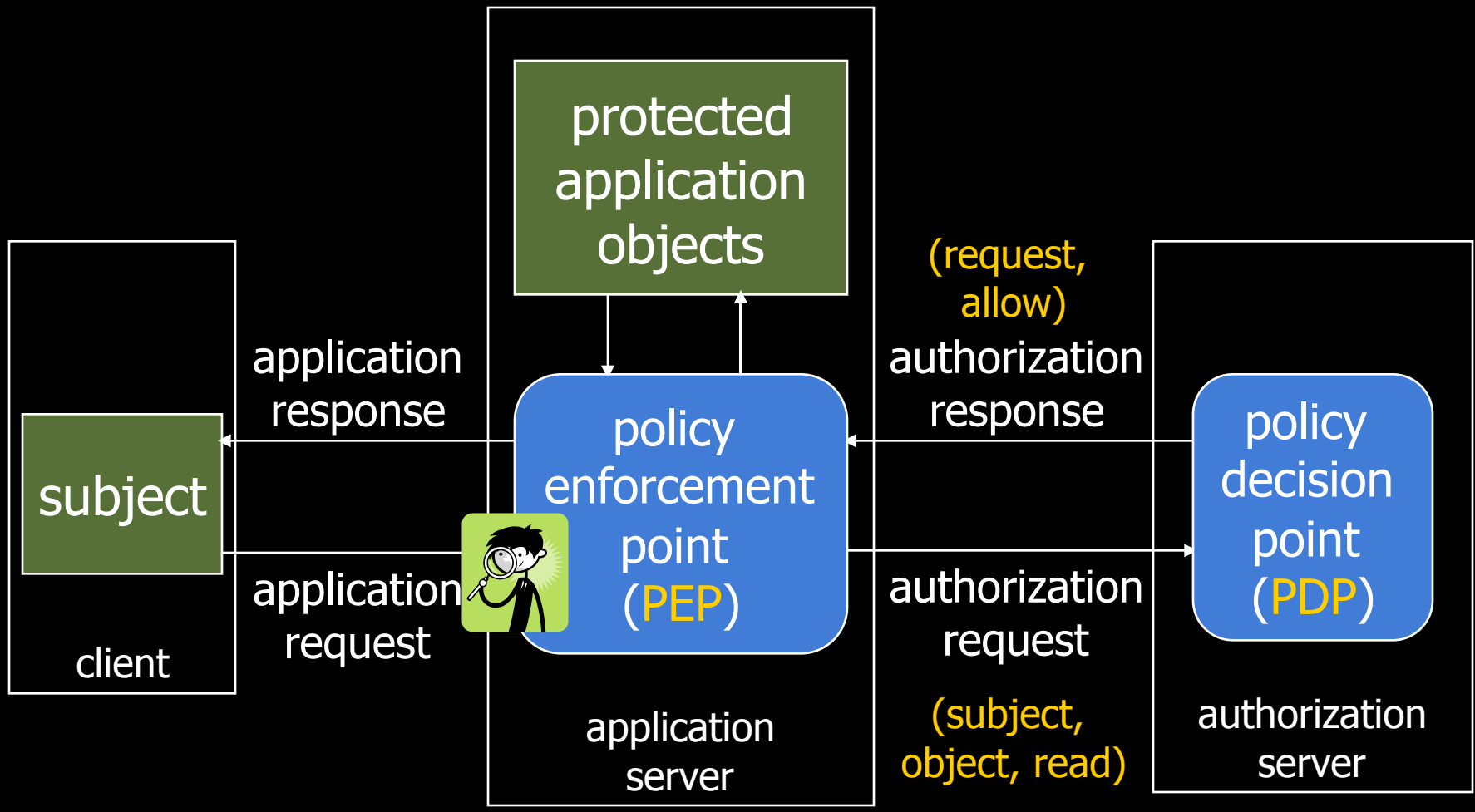
lersse.ece.ubc.ca

Department of Electrical and Computer Engineering

# outline

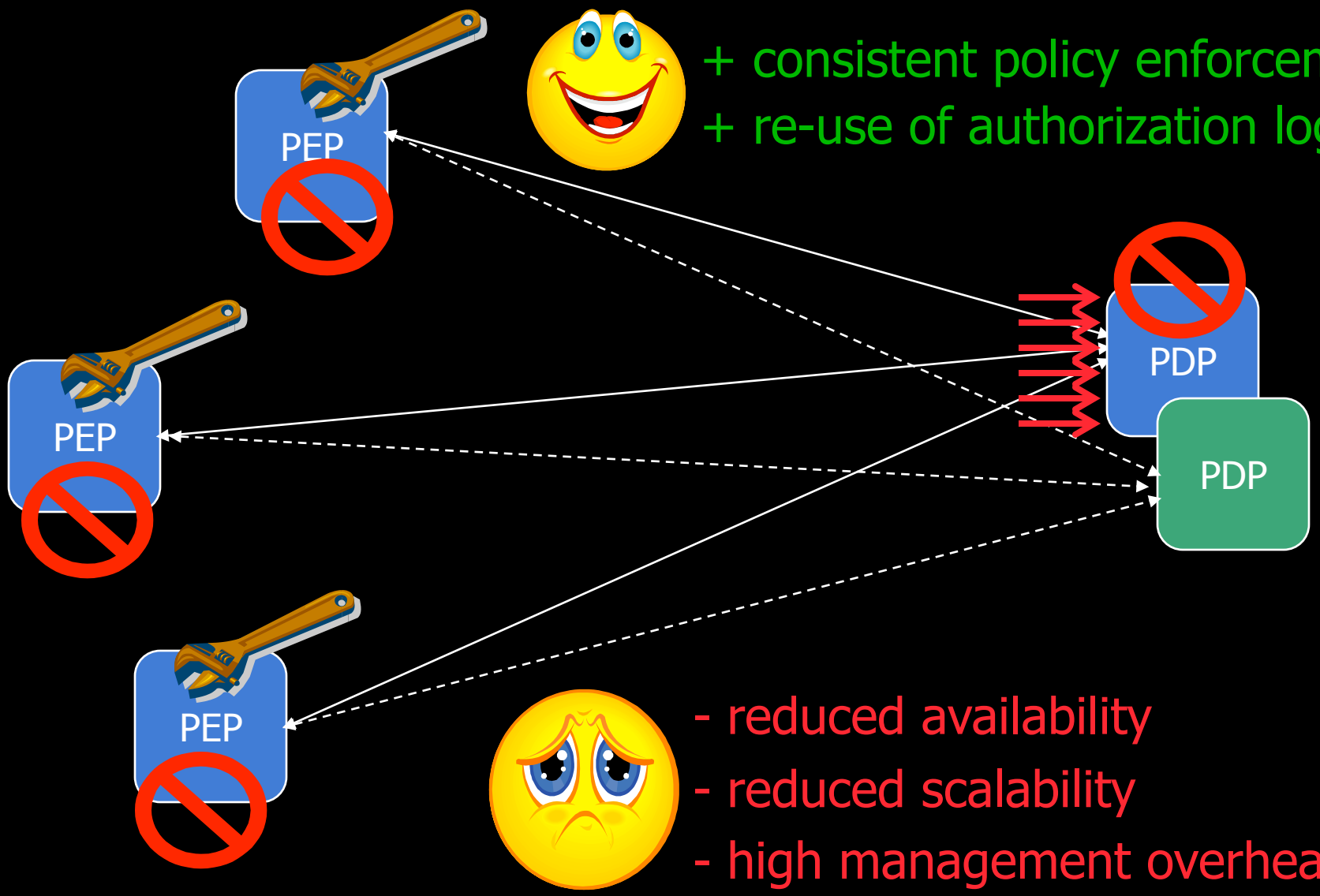
- the overview
- system design
- evaluation
- summary & future work

# authorization (access control) architecture

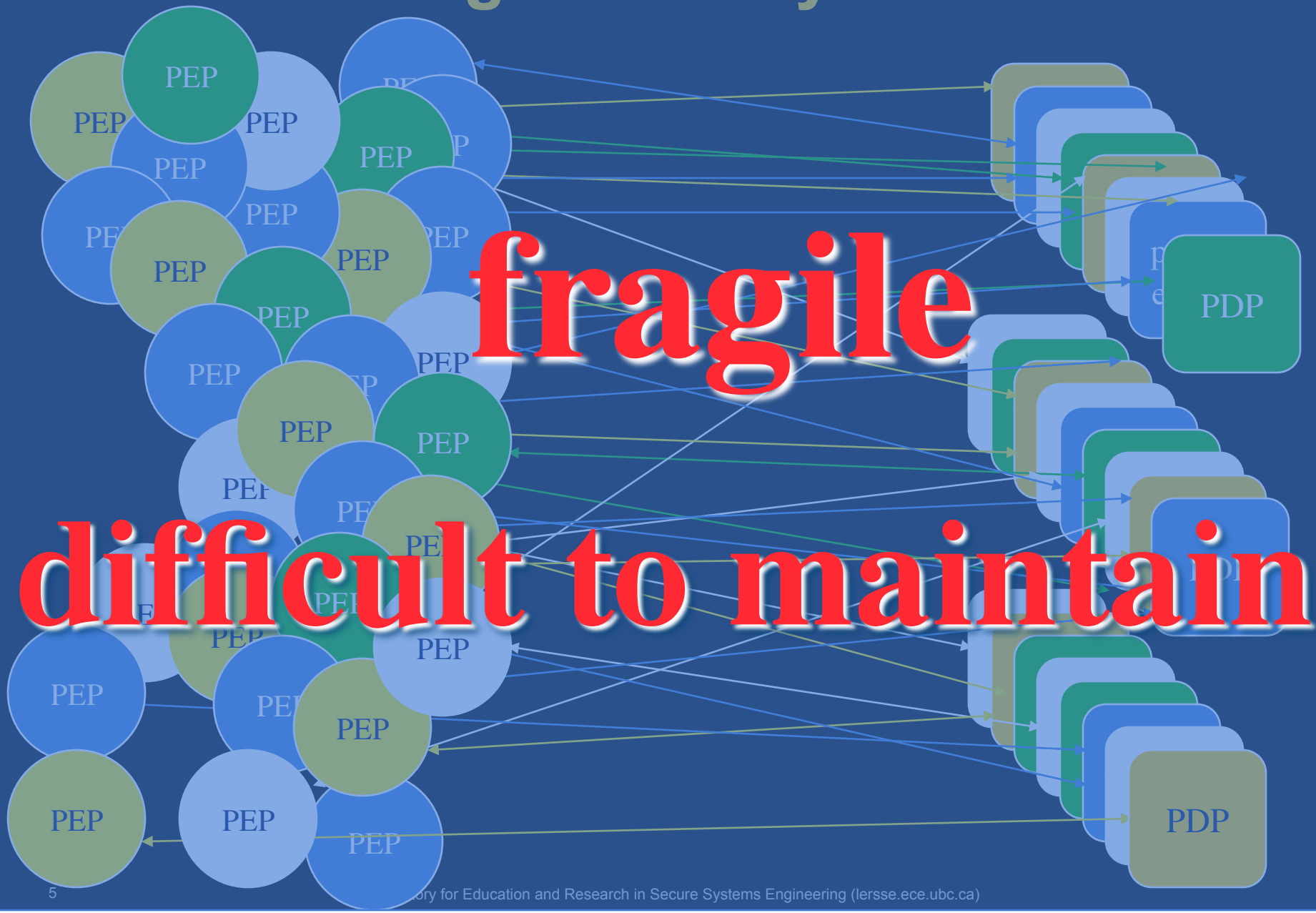



this architecture is based on the point-to-point model,
used by IBM Access Manager, Entrust GetAccess, CA SiteMinder, etc.

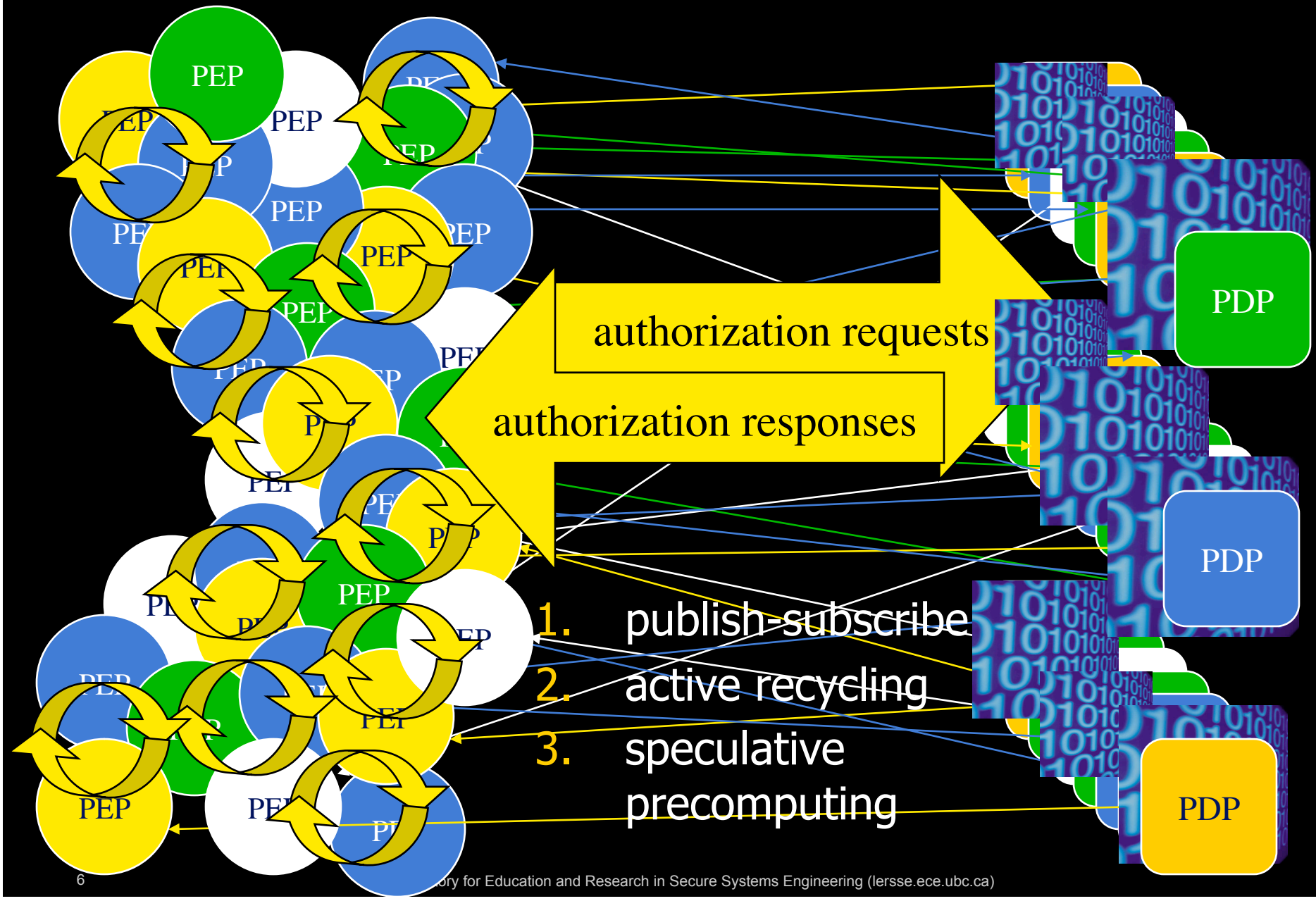
# problem motivation



# in large-scale systems



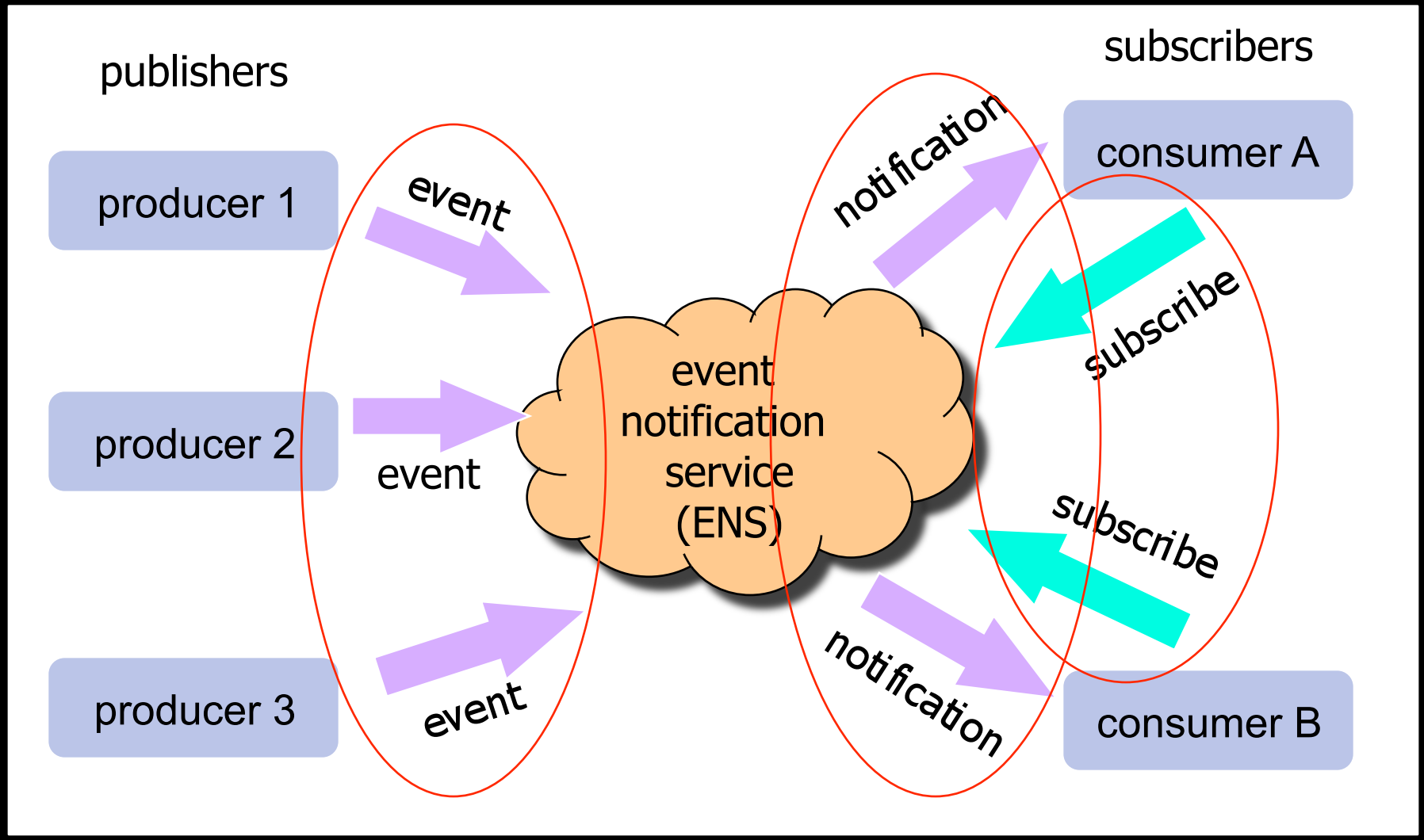
# addressing the problem: big picture



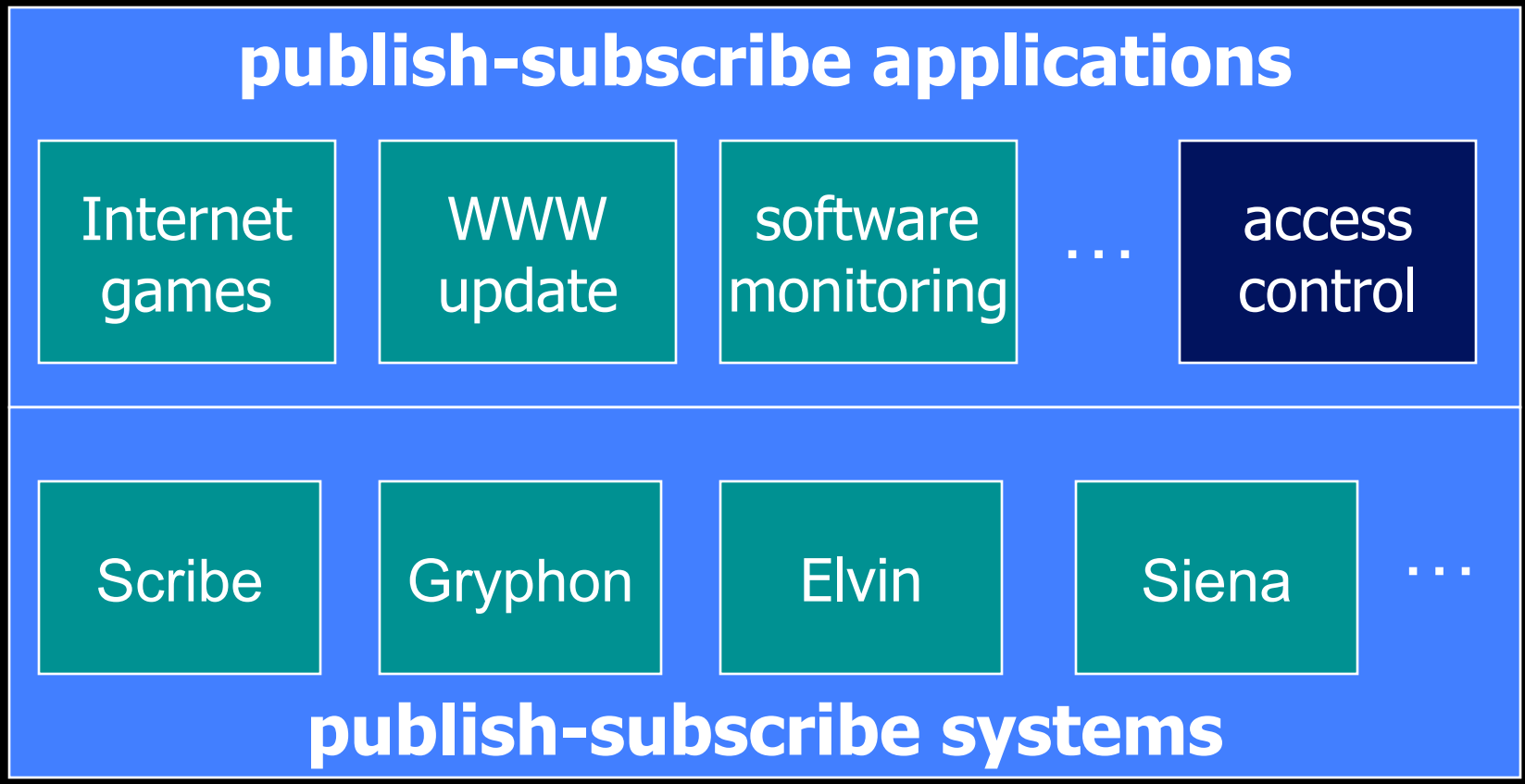
# the contribution of this paper

- study the use of a publish/subscribe (pub-sub) channel between PEPs and PDPs
  - design system architecture and data flow
  - analyze the expected benefits
  - propose the pub-sub requirements and the methods to meet these requirements
- evaluate system availability improvement and performance

# basic components in a publish/subscribe system



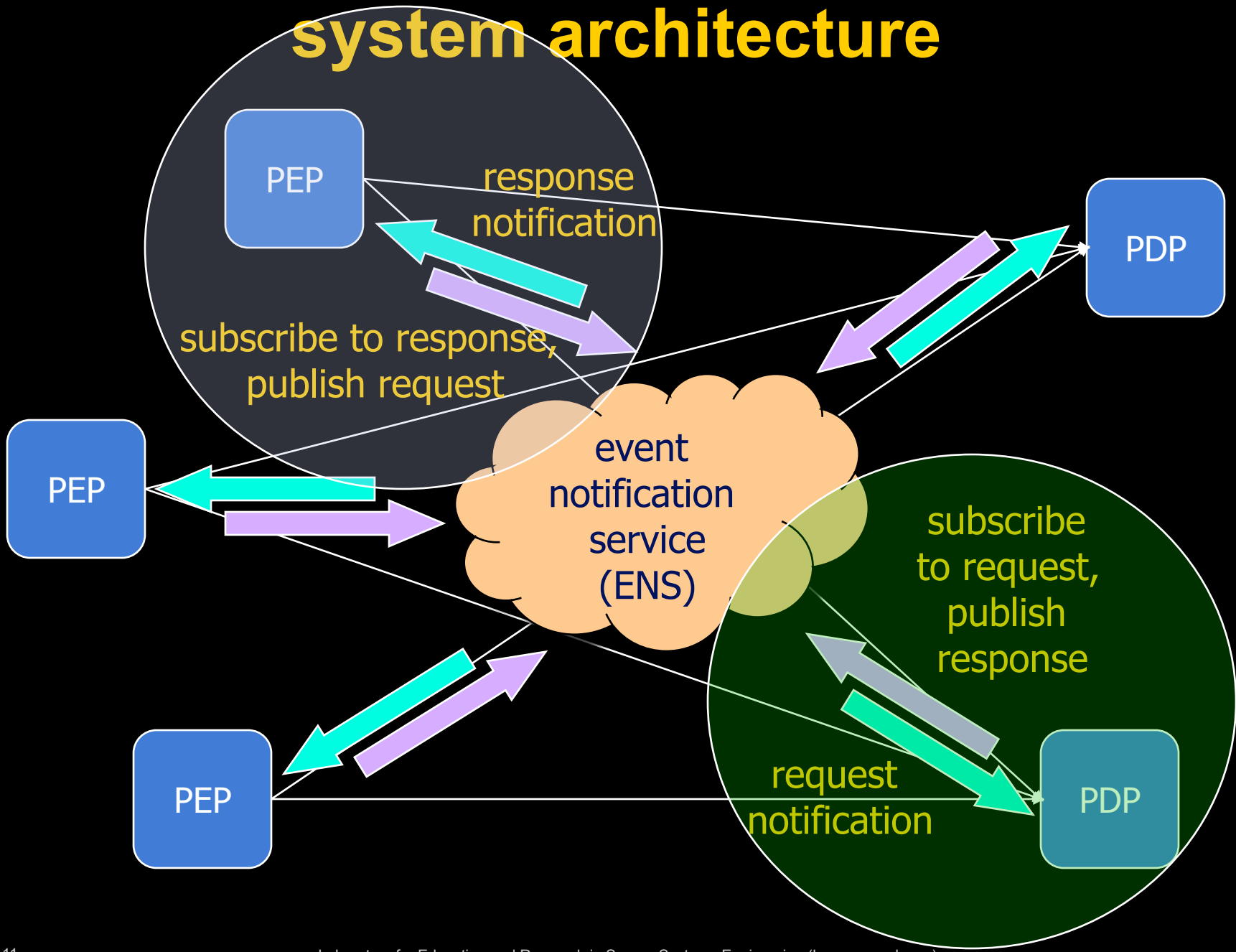
# related work



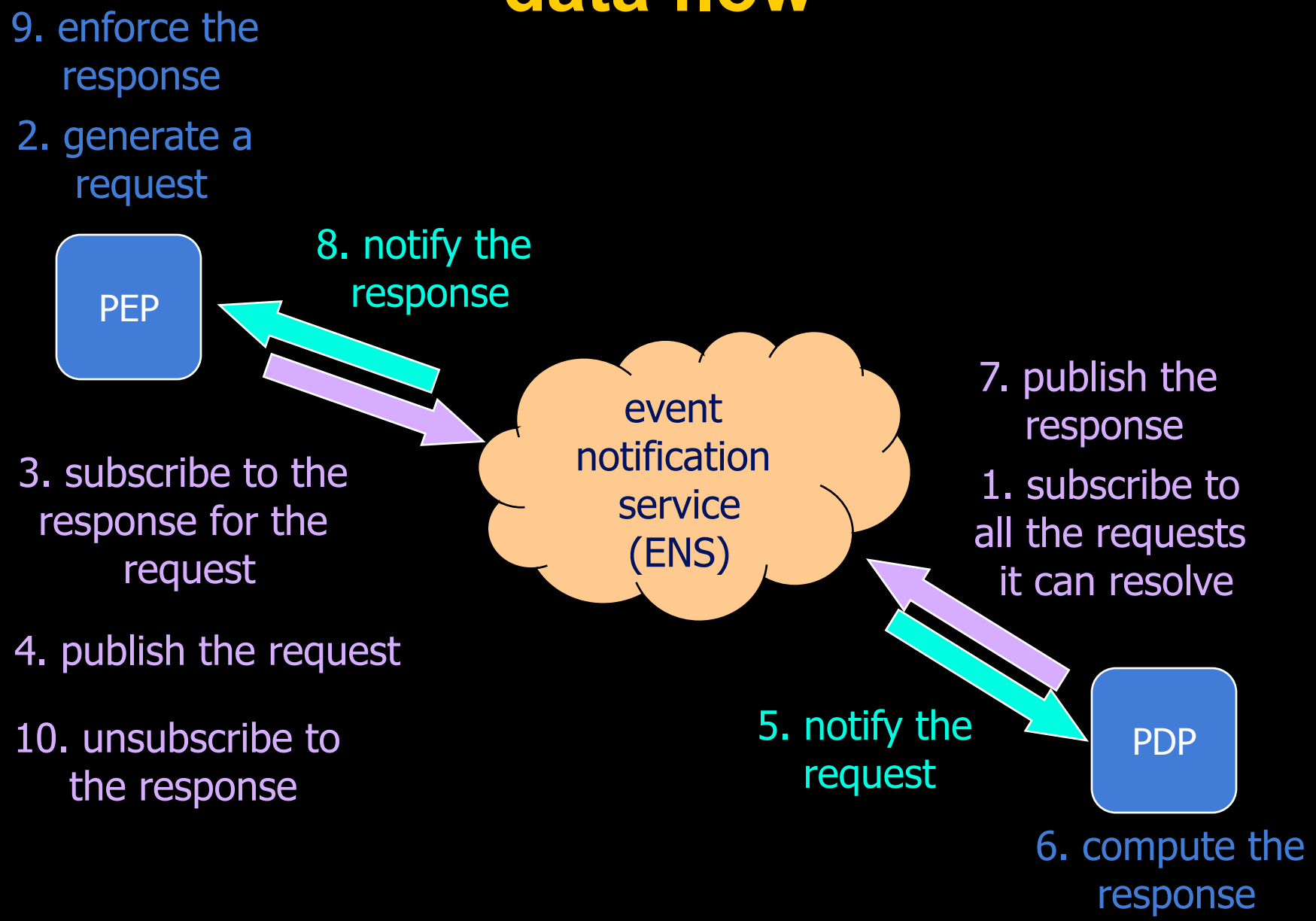
# outline

- the overview
- system design
- evaluation
- summary & future work

# system architecture

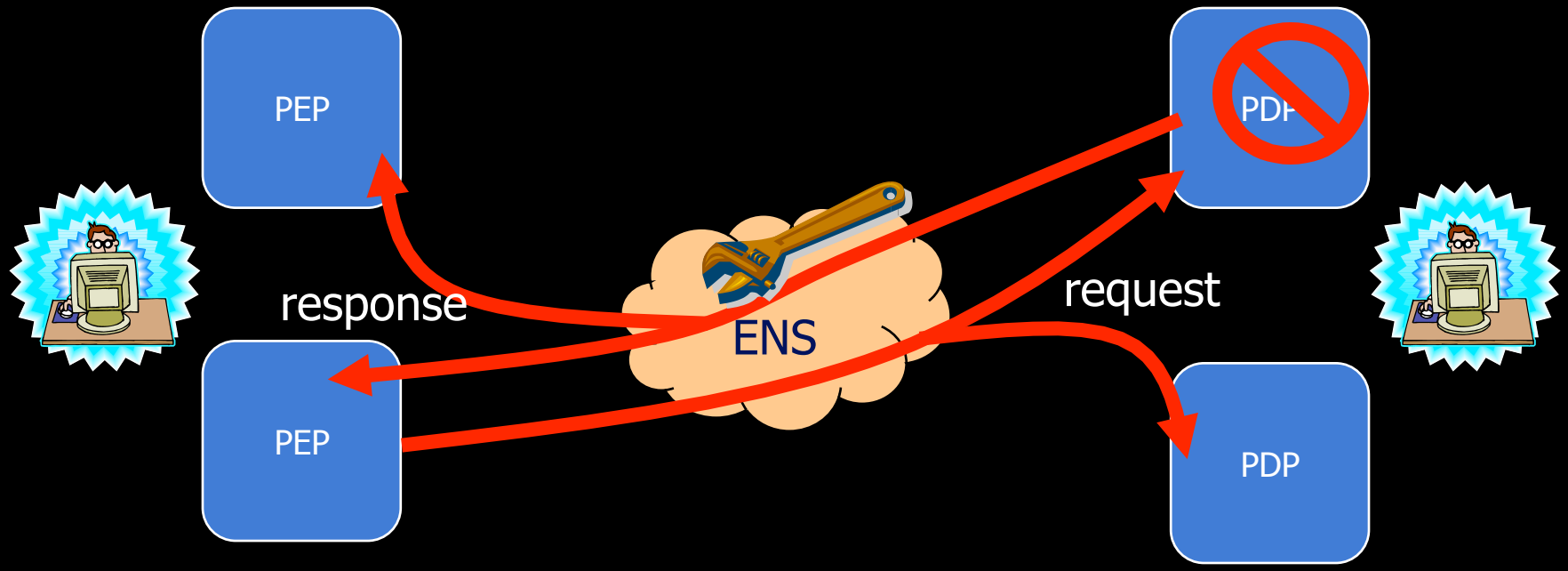


# data flow


9. enforce the response
2. generate a request
PEP
8. notify the response
event notification service (ENS)
7. publish the response
1. subscribe to all the requests it can resolve
3. subscribe to the response for the request
4. publish the request
10. unsubscribe to the response
5. notify the request
PDP
6. compute the response

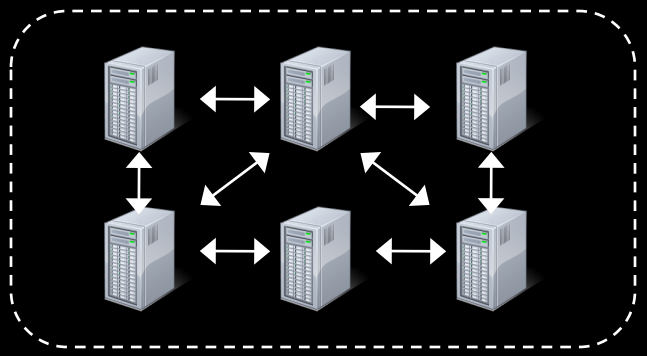
# expected benefits

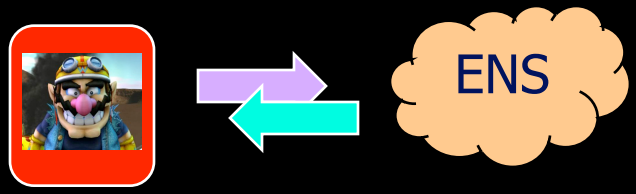
- increased availability
- reduced administration overhead
- reduced integration costs



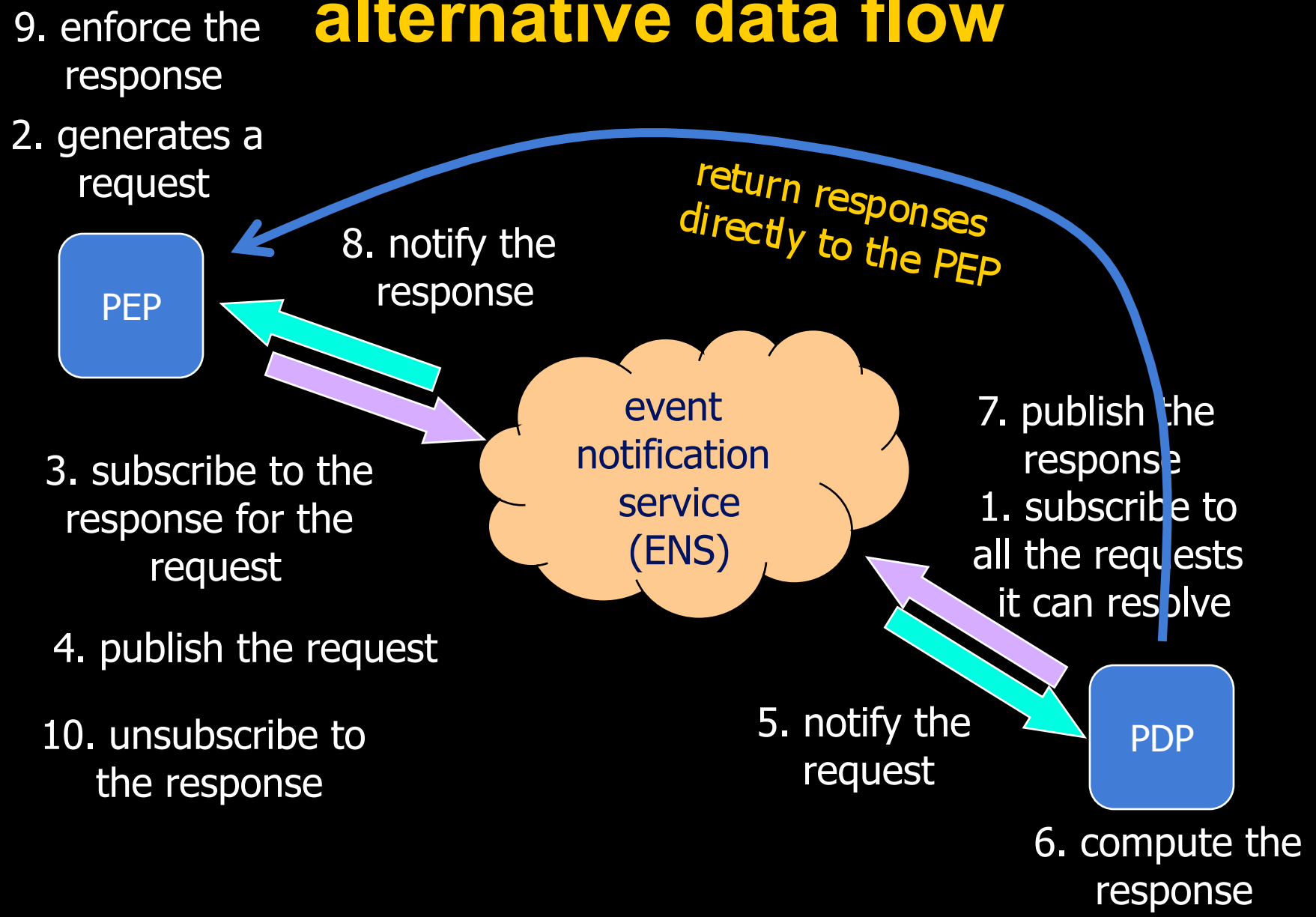
# ENS requirements

- robustness
  - distributed ENS
- security
  - integrity
- performance
  - optimization techniques



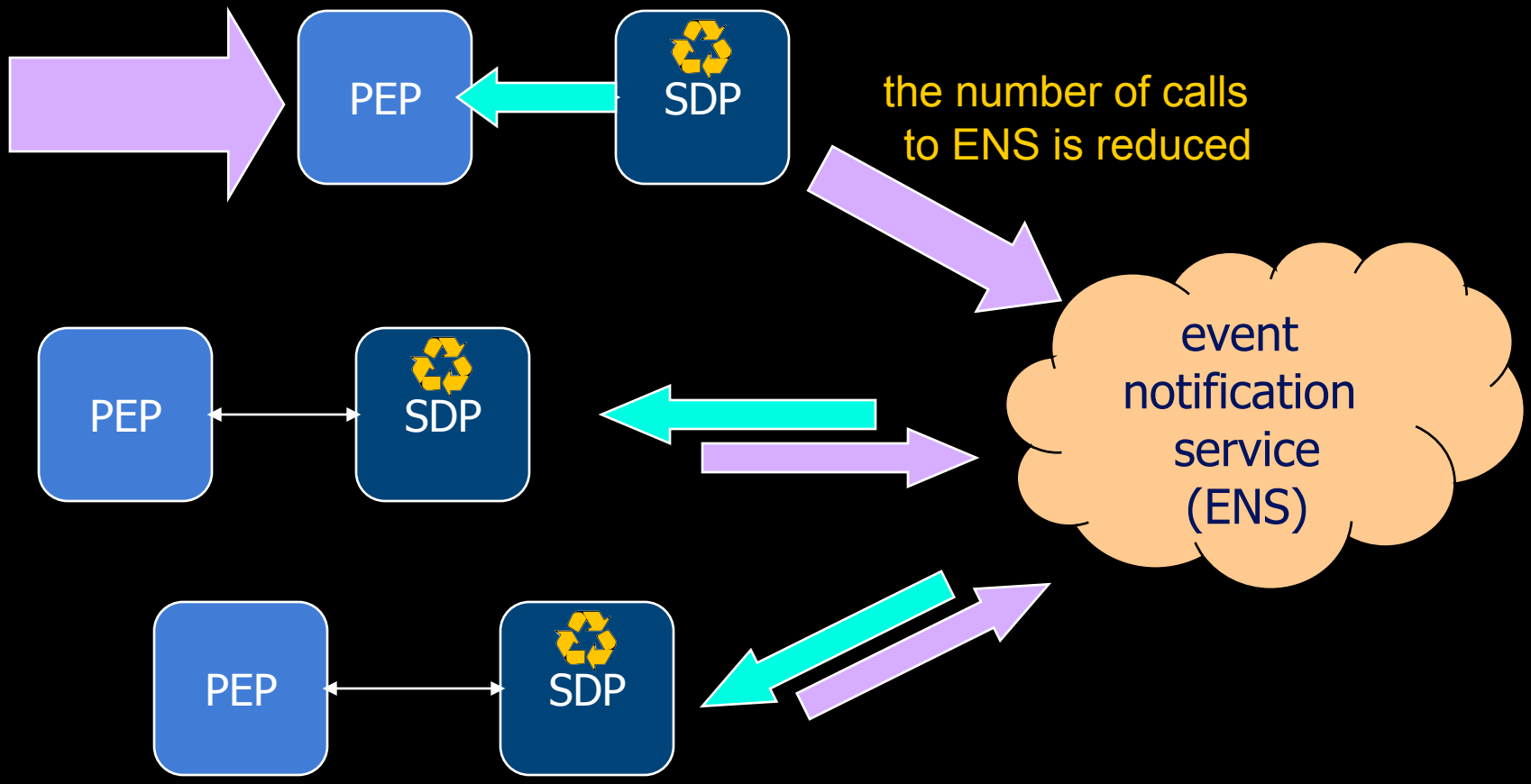


# performance optimization I: alternative data flow



# performance optimization II: using approximate recycling

SDP: secondary decision point

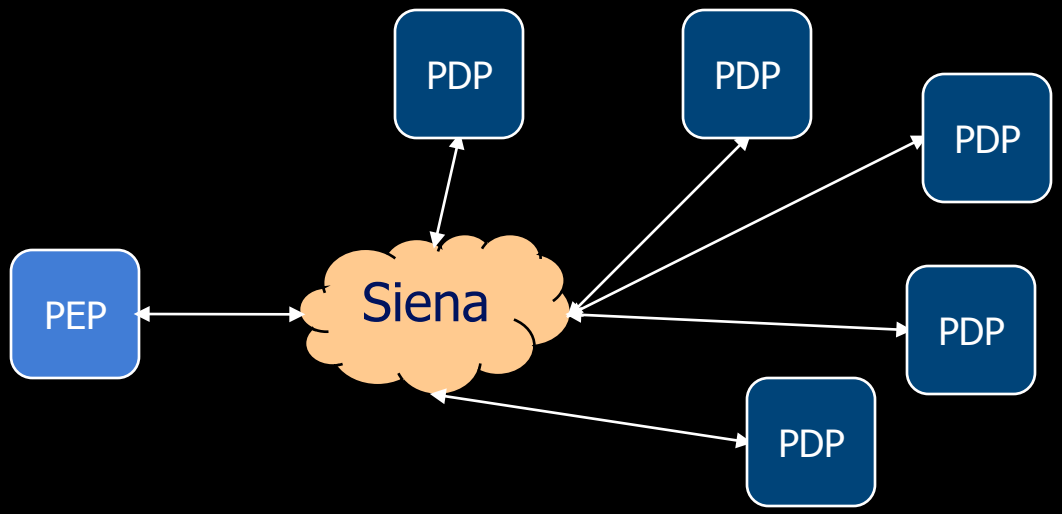


# outline

- the overview
- system design
- evaluation
- summary & future work

# use Siena as the ENS

- popular publish-subscribe system
- designed for wide-area networks
- implemented, available and maintained



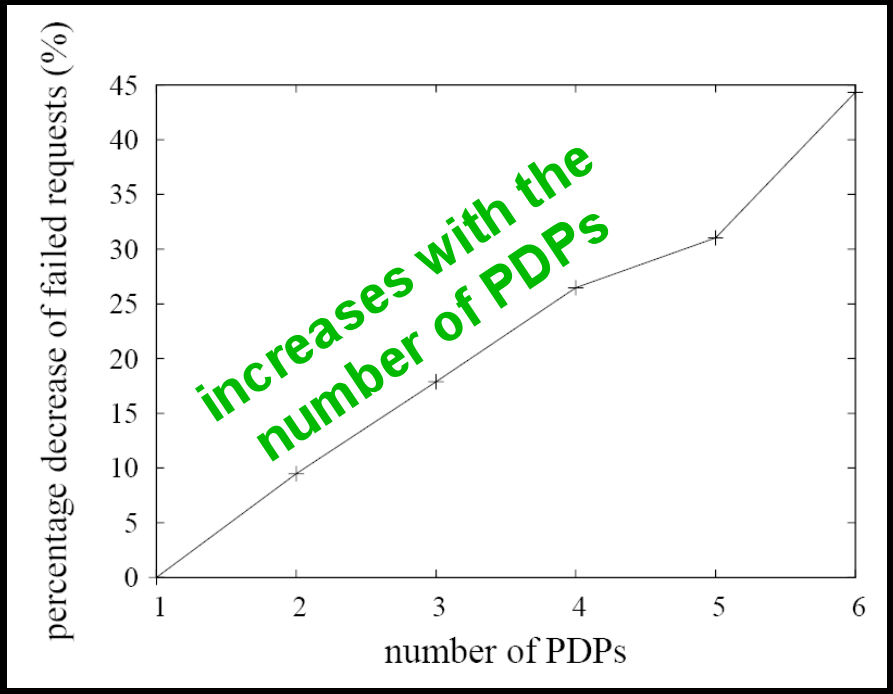
# evaluating availability improvement

- setup
  - multiple PDPs with resource overlap
  - each PDP failed after some time and required some time to repair
  - time-to-failure (TTF) and time-to-repair (TTR) followed an exponential distribution
- metric
  - percentage decrease of failed requests =

$$\frac{|\text{failed\_requets}|_{\text{point-to-point}} - |\text{failed\_requests}|_{\text{pub-sub}}}{|\text{failed\_requests}|_{\text{point-to-point}}}$$

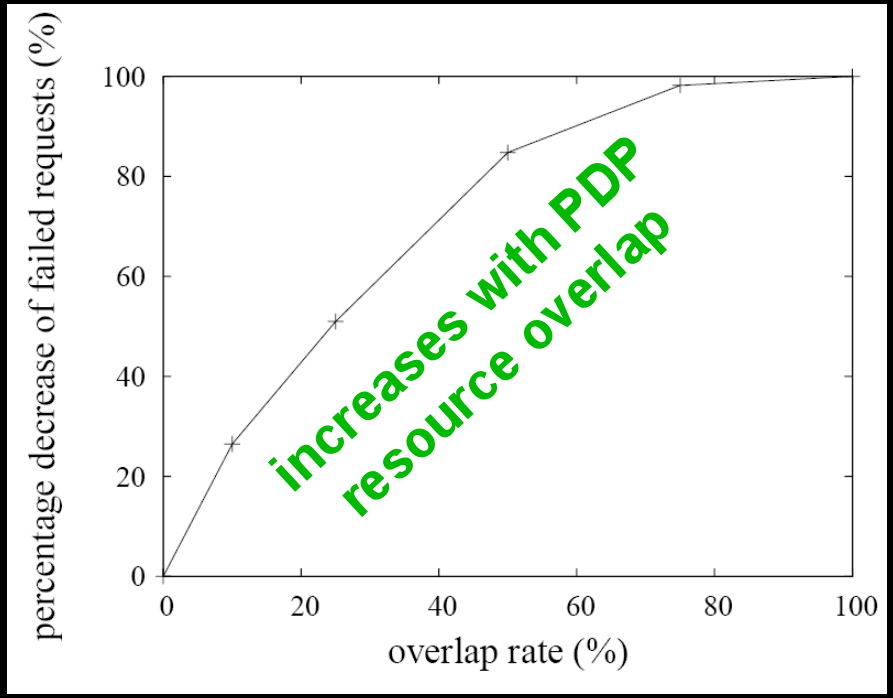
# evaluation results

the impact of the number of PDPs




10% overlap rate between PDP resource

the impact of the overlap rate

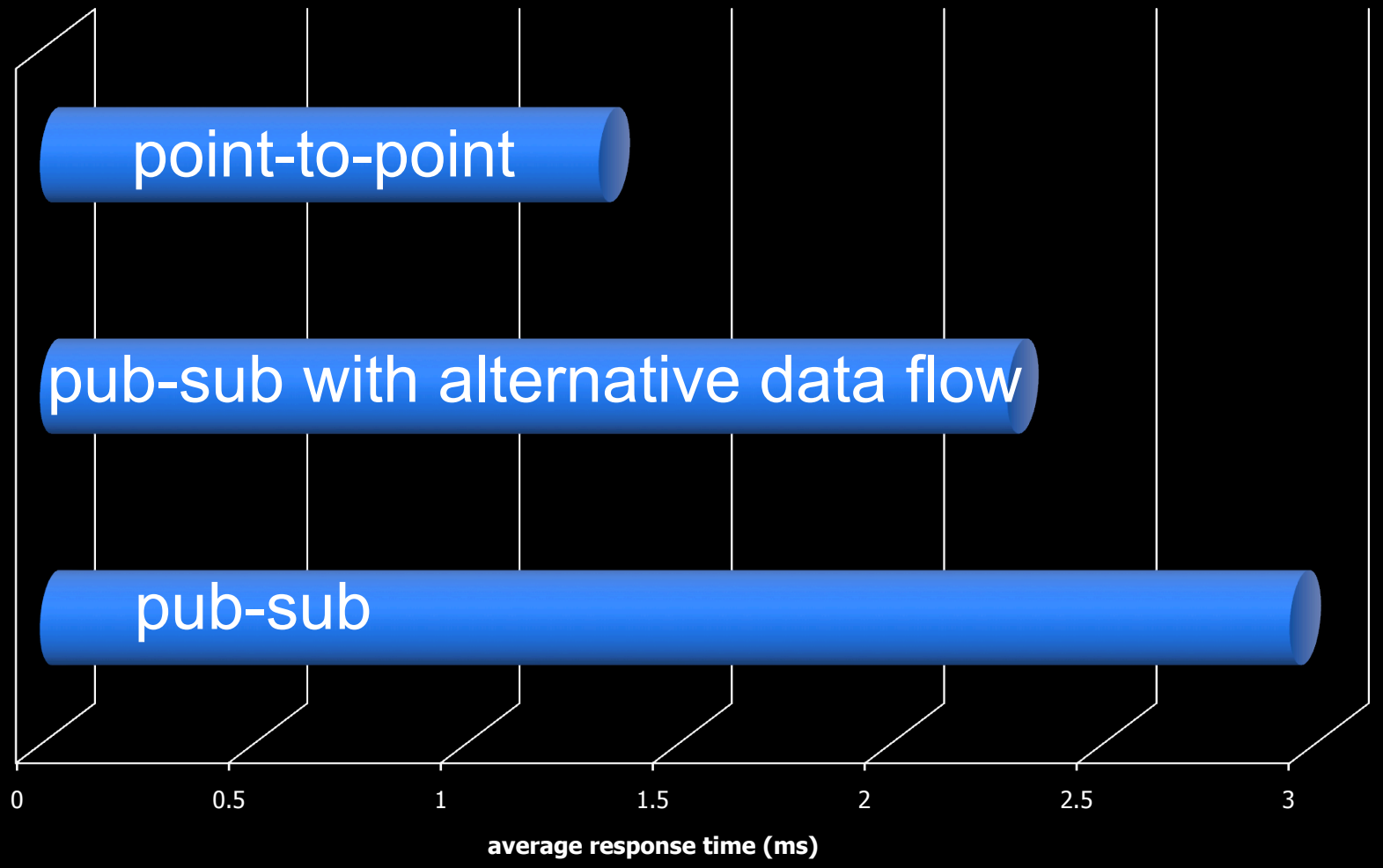



4 PDPs

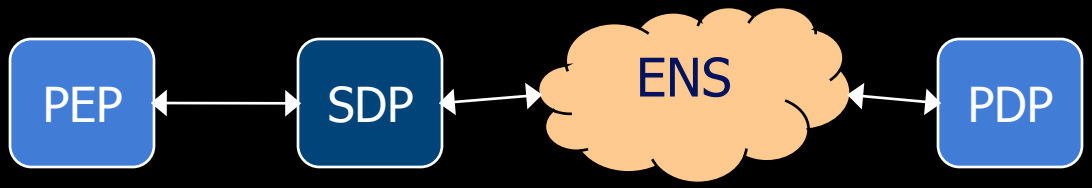
# evaluating performance impact

- metric
  - response time
    - the time between the event that the PEP sends a request and the event that the PEP receives the response
- questions
  - how does our design perform?
  - how do the proposed performance optimization techniques help?

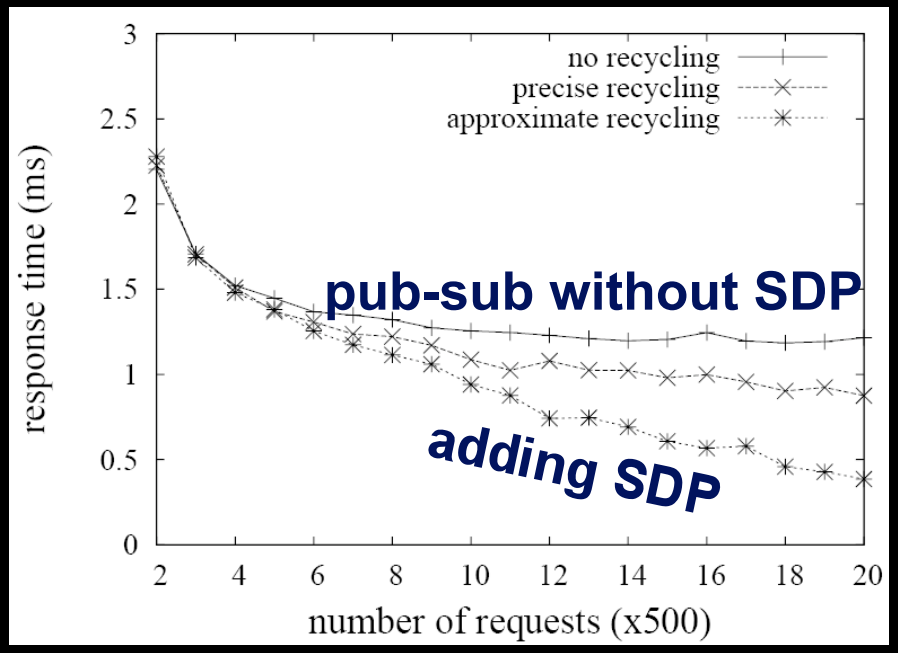
# response time comparison



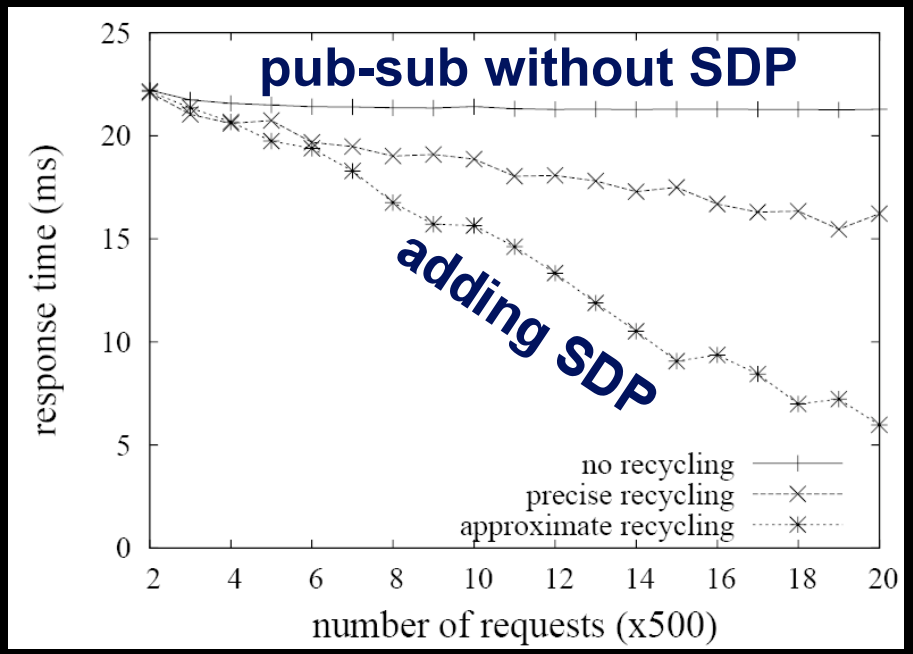
# reduced response time by adding SDPs




PDP is local and fast



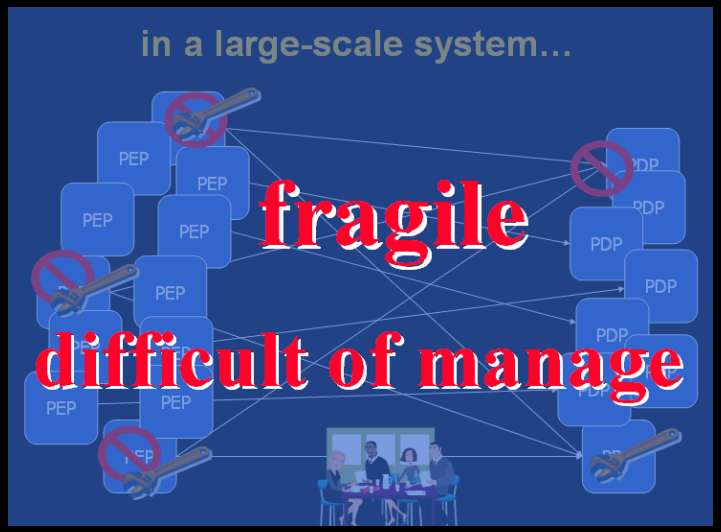

PDP is remote or slow

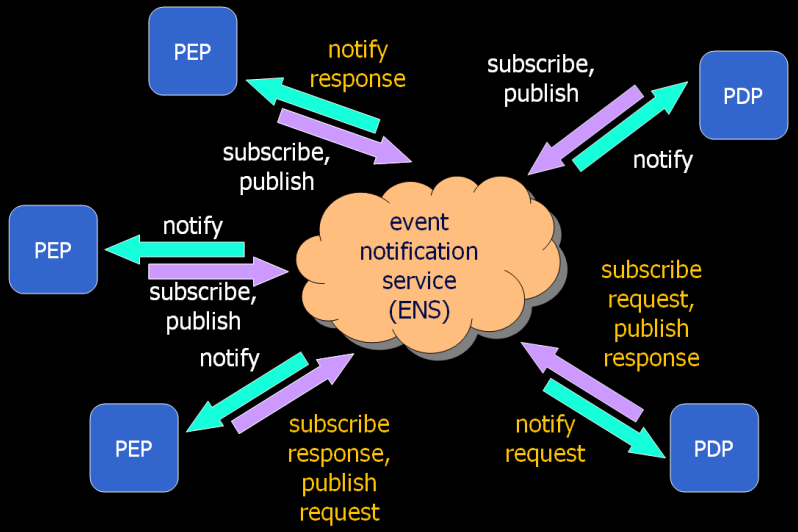


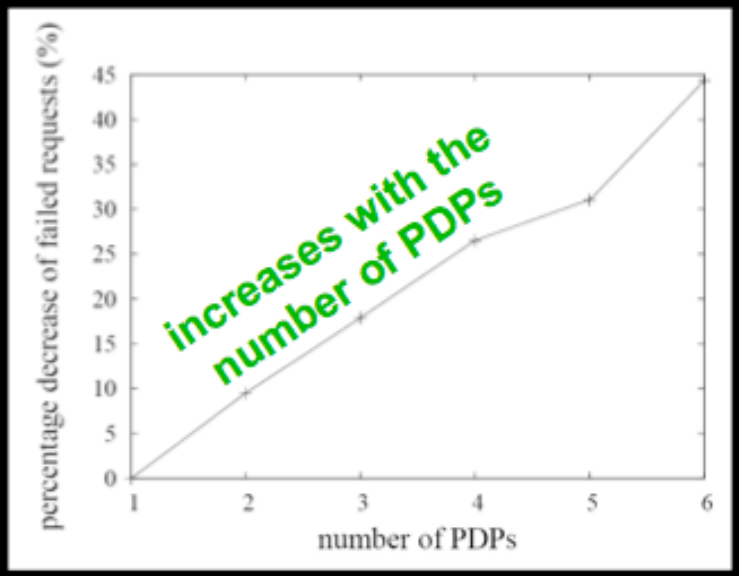
# outline

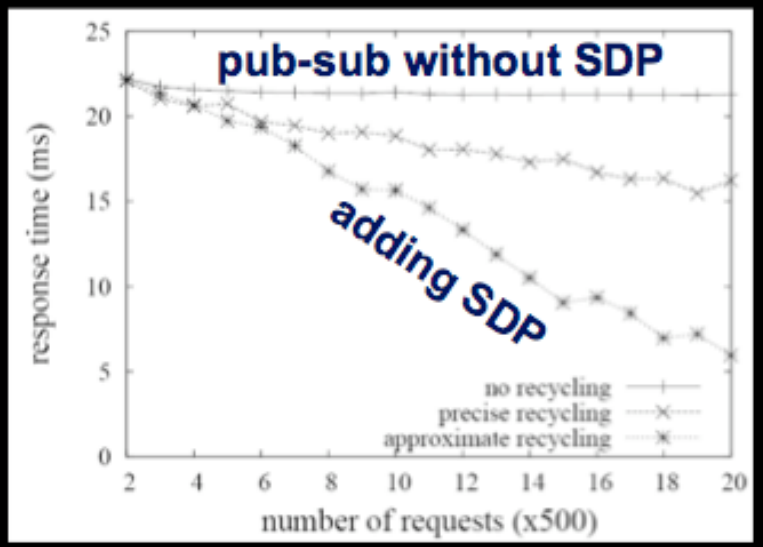
- the overview
- system design
- evaluation
- summary & future work

# summary


in a large-scale system…
fragile
difficult of manage
PEP
PDP

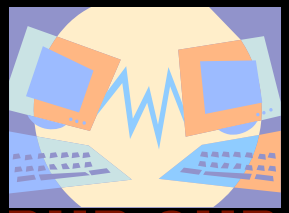

PEP
PDP
notify
response
subscribe,
publish
subscribe,
publish
notify
PEP
notify
subscribe,
publish
event
notification
service
(ENS)
subscribe
request,
publish
response
notify
PEP
subscribe
response,
publish
request
notify
request
PDP


percentage decrease of failed requests (%)
number of PDPs
increases with the
number of PDPs
0
5
10
15
20
25
30
35
40
45
1
2
3
4
5
6


pub-sub without SDP
adding SDP
response time (ms)
number of requests (x500)
no recycling
precise recycling
approximate recycling
0
5
10
15
20
25
2
4
6
8
10
12
14
16
18
20

# future work

- large scale experiments
  - a distributed ENS
  - multiple PEPs and PDPs
- comprehensive security mechanisms
  - threat model
  - defense techniques


PUB-SUB


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