TECHNISCHE UNIVERSITÄT DARMSTADT

G-Lab

Studies- and Experimental Facility for the Internet of the Future

Here: An Evaluation of Cooperative Decisions in Peer-to-Peer Systems – Mathematics vs. Testbed Studies

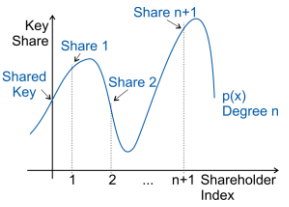
SPONSORED BY THE
Federal Ministry of Education and Research

Outline

- User-based cooperative decisions
- Interaction schemes for a user-based cooperative decision process
- Modeling the interaction of user-based cooperative decisions
- Testbed results

Cooperative Decisions

- Scenario: Peer-to-Peer system to support first responder operations
  - Spontaneously established network, cooperation of many organizations
  - → No central trusted instances, no security policies
- Goal: Counterbalance missing trusted instances
  - Enforce cooperation for security relevant decisions
  - → Distribute required cryptographic operations
    - – E.g. to sign membership certificates or access tokens
- Tool: Threshold Cryptography
  - Based on Shamir's secret sharing
  - One signature key distributed among multiple peers
  - Partial signatures combined by Lagrange interpolation
- But: What about decision policies?

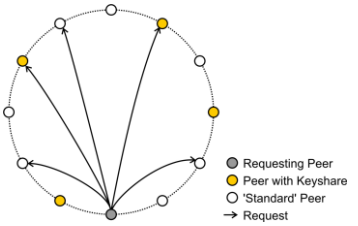


User-based Cooperative Decisions

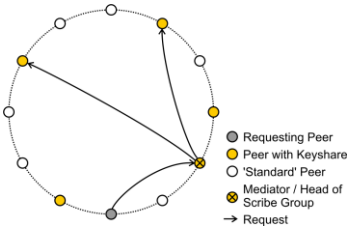
- Challenge: No predefined decision policies
  - Hard to predict all possible security-relevant requests
- Thus: User interaction may be required
  - To decide on non-predefined requests
- But: Number of users involved?
  - 'QoE metric' for cooperative decisions
- Goal: Develop stochastic models
  - Tool set allowing for real-time optimization of number of users involved per decision

Interaction Schemes for User-based Decisions

- Assumption: Structured overlay
  - Implementation in FreePastry
- Non-mediated multicast scheme:
  - Multicast initiated by requesting peer
    → No knowledge on distribution of keyshares
  - Alternative 1: Leafset
    – Limited forwarding in leafset
  - Alternative 2: Random shooting
    – Request sent to arbitrary peer IDs



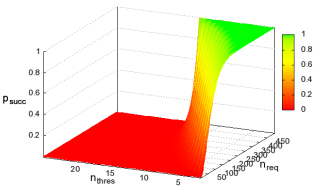
- Mediated multicast scheme:
  - Multicast initiated by mediator
    → Knowledge on distribution of keyshares
  - Alternative 1: Coordinating peer
    – Dedicated peer keeps track on user state
  - Alternative 2: Scribe
    – Authorized peers join multicast group



Modeling User-based Cooperative Decisions

- Non-mediated multicast scheme:
  - $p(n_{rep})$ is hypergeometric random variable

$$p(n_{rep}) = \binom{n_{auth} \cdot p_{rep}}{n_{rep}} \binom{n_{total} - (n_{auth} \cdot p_{rep})}{n_{req} - n_{rep}} \binom{n_{total}}{n_{req}}^{-1}$$

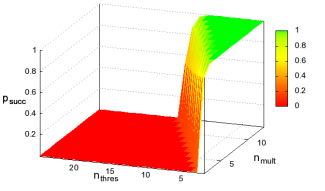


  - Decision process successful if $n_{rep} \geq n_{thres}$

$$p_{succ}(n_{thres}) = \sum_{n_{rep}=n_{thres}}^{n_{req}} \binom{n_{auth} \cdot p_{rep}}{n_{rep}} \binom{n_{total} - (n_{auth} \cdot p_{rep})}{n_{req} - n_{rep}} \binom{n_{total}}{n_{req}}^{-1}$$

- Mediated multicast scheme:
  - $p(n_{rep})$ is binomial random variable

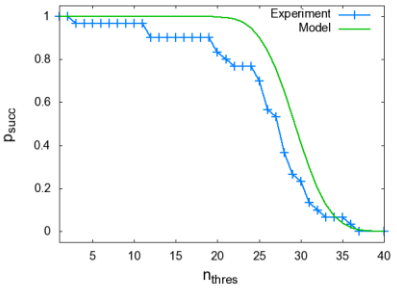
$$p_{succ}(n_{thres}) = \sum_{n_{rep}=n_{thres}}^{n_{req}} \binom{n_{req}}{n_{rep}} p_{rep}^{n_{rep}} (1 - p_{rep})^{n_{req} - n_{rep}}$$



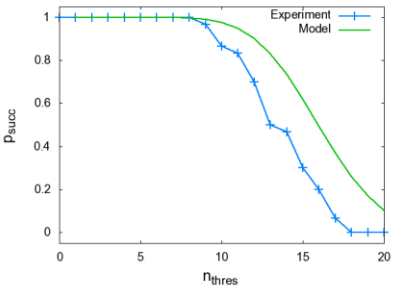
First Testbed Results

- Non-mediated multicast

Alternative 1: Leafset
$n_{total}=400, n_{auth}=100, p_{rep}=0.5, n_{req}=230$
Threshold targeted: 20
→ 57 authorized peers involved,
Overhead: 11.5 (2.85)



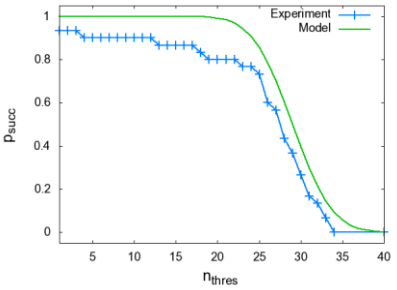
Alternative 2: Random Shooting
$n_{total}=400, n_{auth}=200, p_{rep}=0.5, n_{req}=62$
Threshold targeted: 8
→ 21 authorized peers involved,
Overhead: 7.75 (2.625)



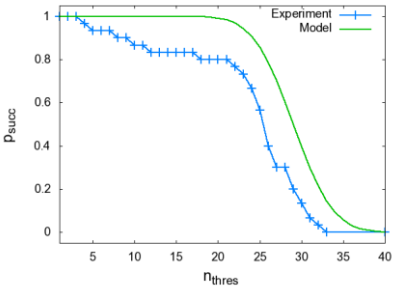
First Testbed Results (cont'd)

- Mediated multicast

Alternative 1: Coordinator
$n_{total}=400, n_{auth}=100, p_{rep}=0.5, n_{req}=57$
Threshold targeted: 20
→ 57 authorized peers involved,
Overhead: 2.85



Alternative 2: Scribe
$n_{total}=400, n_{auth}=57, p_{rep}=0.5, n_{req}=57$
Threshold targeted: 20
→ 57 authorized peers involved
Overhead: 2.85



Thank You for Your Attention!

Department of Electrical Engineering
and Information Technology
Multimedia Communications Lab - KOM

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Dipl.-Inform. André König

Andre.Koenig@KOM.tu-darmstadt.de
Merckstr. 25
64283 Darmstadt
Germany

Phone +49 (0) 6151/166137
Fax +49 (0) 6151/166152
www.kom.tu-darmstadt.de