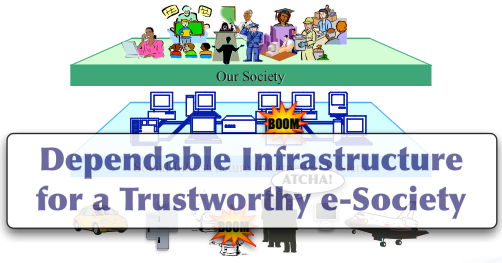
Some Challenges Toward a Dependable Infrastructure for a Trustworthy e-Society

Xavier DÉFAGO
School of Information Science,
Japan Adv. Inst. of Science & Tech. ***(JAIST)***
PRESTO, Japan Science & Tech. Agency ***(JST)***

Motivation



Dependable Infrastructure for a Trustworthy e-Society

Context: e-Society

- **Characteristics**
  - very **heterogeneous**
  - very **large scale**
  - very **dynamic**
- **Requirements**
  - correctness, accountability
  - **availability, reliability, robustness**
  - **adaptability**, evolvability

Goal

Dependable Infrastructure for a Trustworthy e-Society

- **Dependable Infrastructure**
  - Mechanisms, methodologies for dependable infrastructures
- **Trustworthy e-Society**
  - Face **new challenges**

Outline

- **Background**
  - Dependability
  - Agreement
- **Challenges with e-Society**
  - **multi-levels guarantees**
  - **heterogeneity**
  - **scalability**
- **Conclusion**

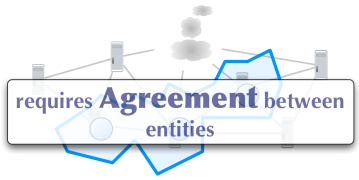
Dependable Systems

- **Dependability**
  - **errors & faults** can occur **anywhere** at **any time**
  - they should have **little or no consequence**
- **Means**
  - **prevention** (specification, verification, testing)
  - **masking** (redundancy, resilience)
  - **recovery** (checkpointing, reparation)

Dependable e-Society

- **e-Society is a System**
- **Correctness**
  - **Behavior** corresponds to **specification**
  - **Specification** corresponds to **expectations**
- **Dependability**
  - **Reliability:** e-Society does not fail.
  - **Availability:** e-Society responds when I needed it.
  - **Accountability:** e-Society can report on actions/decisions.
  - **Privacy:** e-Society protects private sphere.
  - **Fairness:** e-Society maintains fairness / transparency.

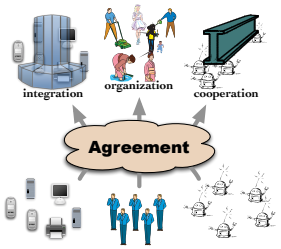
Dependability in Distributed Systems



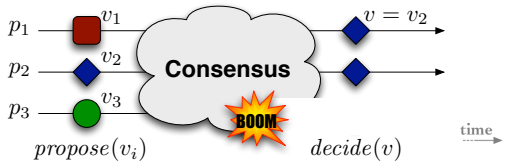
- **Distributed Systems**
  - **Entities/services, communication**
  - **Interactions**

Agreement as Foundation

- **Agreement**
  - **Interact** to reach **common decisions**
  - E.g., elections, ...
  - Also between sub-systems
- **Applications**
  - Consensus,
  - Atomic multicast,
  - Atomic commit,
  - Service replication, ...



Agreement Protocol (e.g., Consensus)

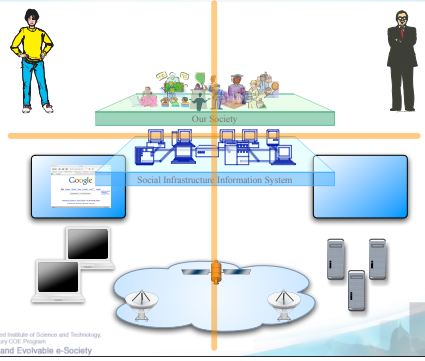


- **Definition**
  - Participants **propose value**
  - Agreement on **decision value**

Challenge 1: multi-perspective guarantees

- **Traditional systems**
  - **computer service: client / server**
  - guarantees for **servers**
  - guarantees for **clients**
- **e-Society infrastructure**
  - system perception **includes** other “clients”
  - **people** also part of the system.
- **Difficulty**
  - Manage **interactions** between **machines** and **people**
  - Provide **guarantees** from **different viewpoints**

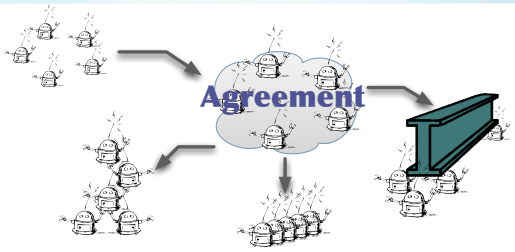
Challenge 1: multi-perspective guarantees



Challenge 2: heterogeneity

- **Active components**
  - computers, servers
  - electronic appliances
  - vehicles, transportation systems
  - robots
  - people
- **Mobility**
  - mobility as **"input"**
  - mobility as **"output"**

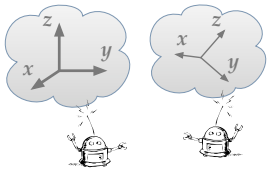
Mobility & Agreement



- **Agreement**
  - Group behaves as **single** entity
  - Many kinds of agreement

Mobility & Agreement

- **Agreement on coordinate system (*"x-y-z"*)**
  - **with GPS**
    - problem is **trivial**
    - ... modulo errors
  - **with landmarks**
    - problem is **easy**
  - **no GPS, no landmarks**
    - problem is **very hard**
    - or even **impossible**



Challenge 3: scalability

- **"Big numbers"**
  - many **participants**
  - high **activity**
  - large amounts of **data** & **computation**
  - large **distances**
- **Effect**
  - complex **interactions**
  - efficiency/performance issues
- **Actions**
  - combination / integration of **techniques**
  - good **abstractions**, scalable **protocols**

Conclusion

- **Trustworthy e-Society**
  - More and more **reliance** on e-Society
  - **Dependability** essential for deserving **trust**
  - **People** are big part of the game
- **Research**
  - Builds upon **state-of-the-art**
  - Many **new challenges**
  - Highly **interdisciplinary**