Università della Svizzera italiana

Advanced Learning and Research Institute ALaRI

A Guarantee of Service Protocol for Pervasive Distributed Systems

Alberto Ferrante, Roberto Pompei,

Anastasia Stulova, Antonio V. Taddeo

ALaRI, University of Lugano

e-mail: ferrante@alari.ch

Outline

Introduction

The Trusting Protocol

Simulations

Attacks

Conclusions and Future Work

Distributed Pervasive Systems

- Future pervasive systems will adopt innovative architectures;
- they will possibly be distributed:
  - computational nodes organized in networks;
  - nodes may move from one network to another;
  - tasks can be delegated to other nodes.

Delegation Protocol

- Query for availability of nodes;
- evaluate the most appropriate node to execute the task;
- assign the task;
- receive the results.

Problem Statement

- A reliability check of the nodes is required:
  - will the node really complete the jobs assigned to it?
  - will the node do that on time?
  - will the node give back correct results?
- What about the identity of the node?

Related work

- Some works on trust for grid systems:
  - rely on high connectivity and computational resources.
  - e.g., weighted feedback.
- PGP Web of Trust:
  - decentralized trust mechanism for identities.
- Trust for peer to peer networks:
  - e.g., a reputation mechanism for P2P file-sharing;

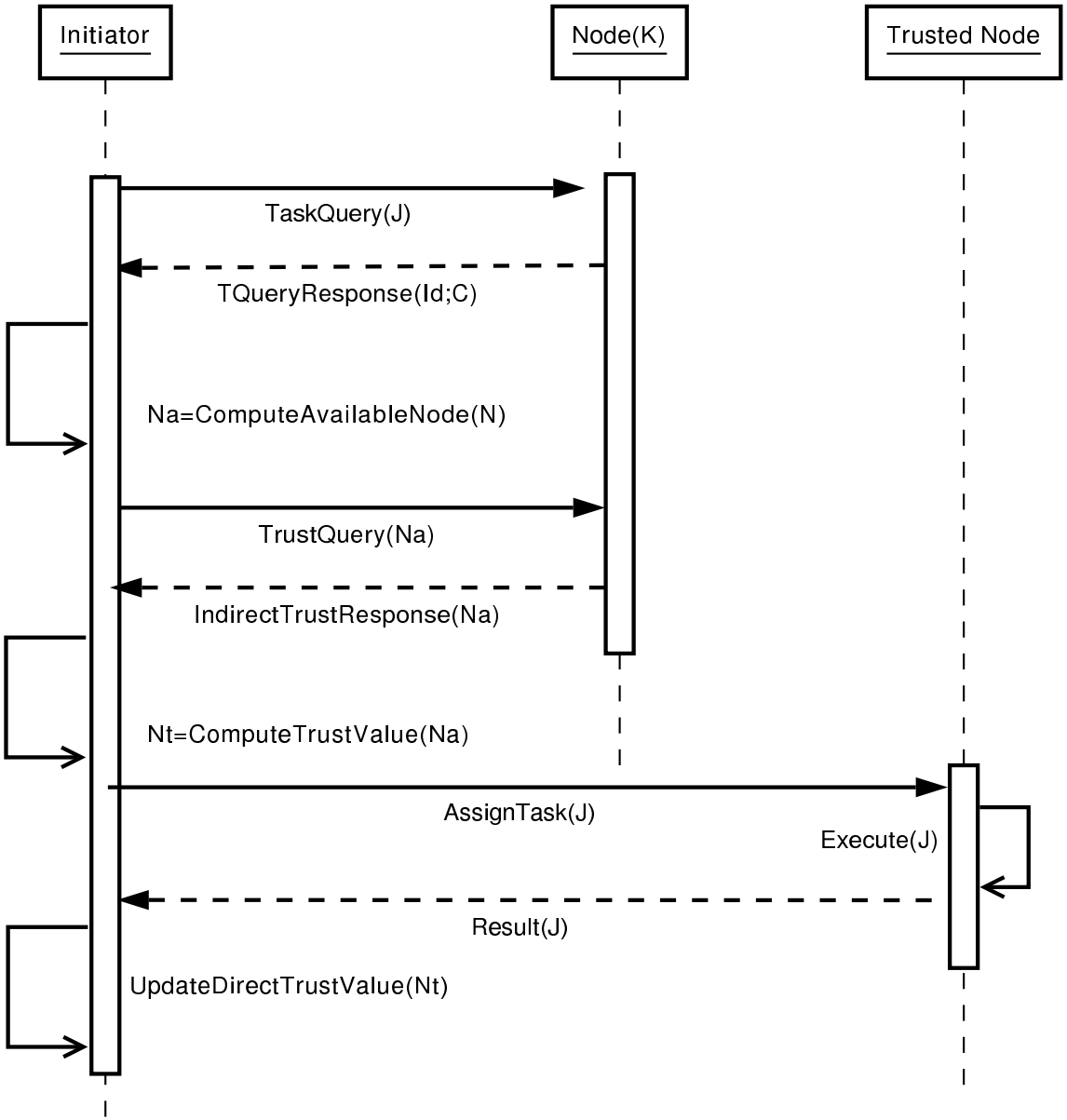
What we miss:

- dynamic update of the trust value of the nodes;
- decentralized system;
- a lightweight protocol.

Protocol Overview (1/2)

- *Reliability*: capability of nodes to respect service agreements;
- reliability is evaluated before assigning tasks to nodes;
- reputation-based protocol.

Protocol Overview (2/2)



Trust Value

Computed:

- By the initiator before assigning the task;
- by using the past experiences with the nodes considered;
- by mixing:
  - personal experience;
  - indirect experience.

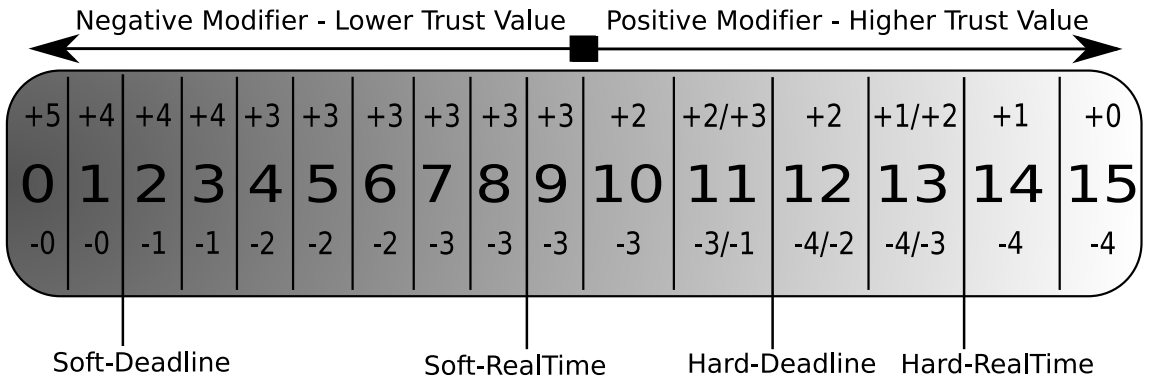
$$T_j^d = w_p \times V_j^d + w_i \times \frac{\sum_i V_j^i}{m} \quad i \neq j; \quad i \neq d$$

Trust Value Update

Personal trust value is updated after each task execution:

- based on the outcome of the execution:

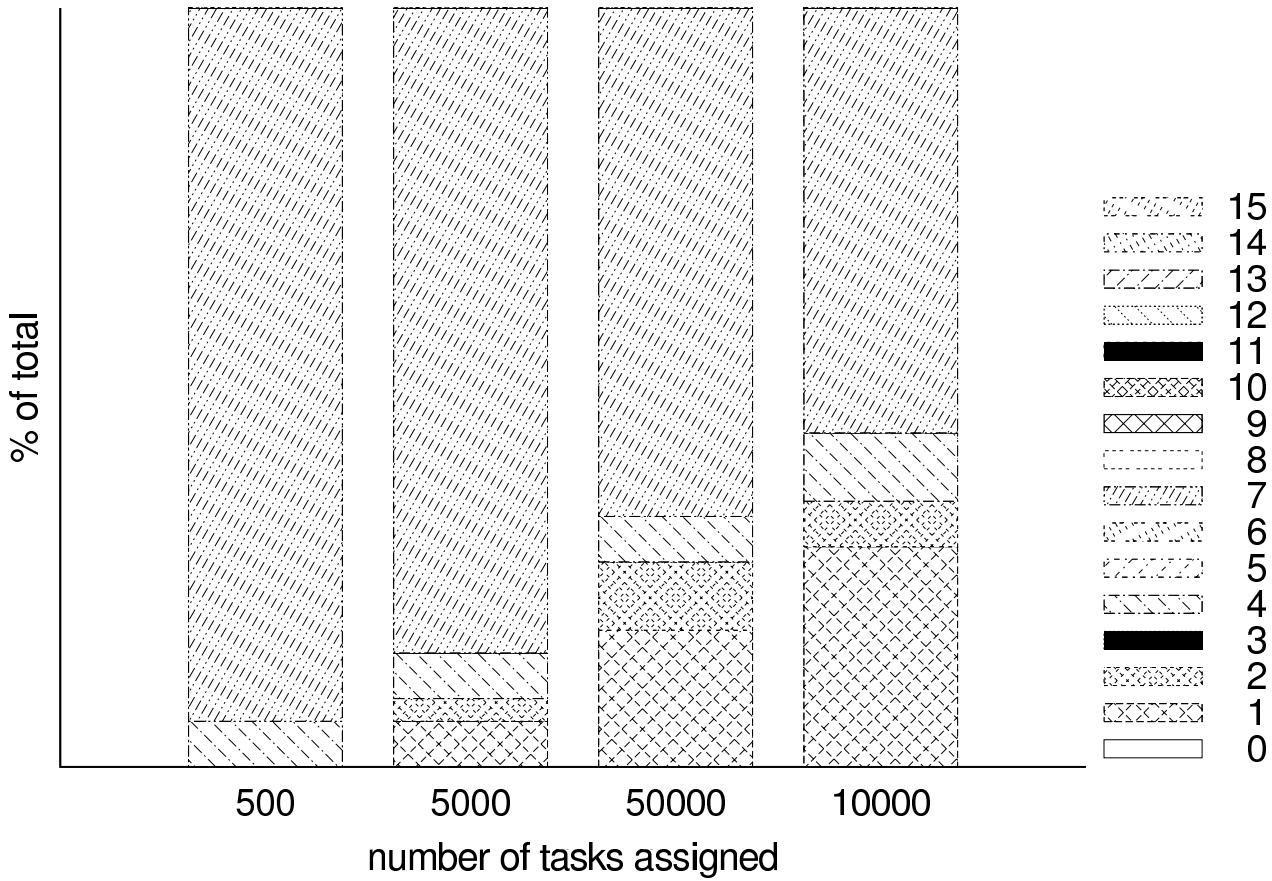
$$V_j^d(t') = V_j^d(t) + M$$



Simulation Model

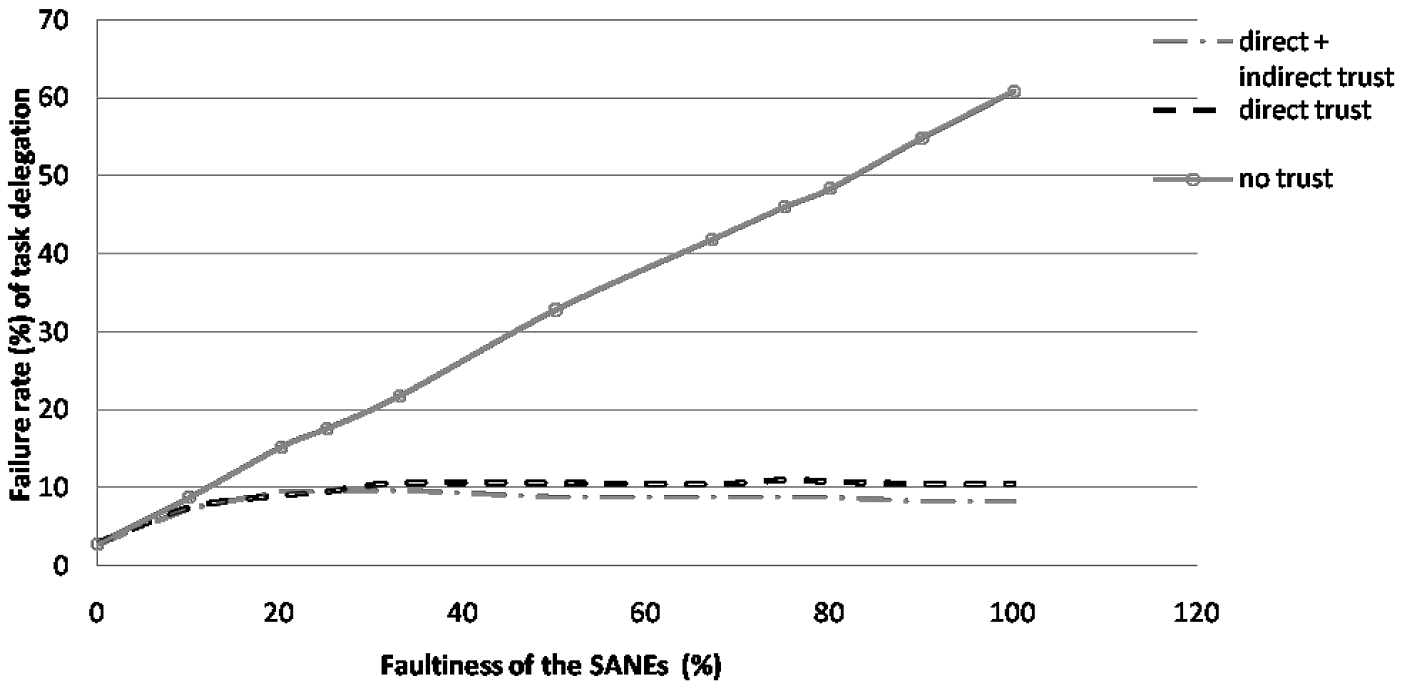
- A SystemC model:
  - it models the delegation process;
  - it models the evolution of trust.

Simulation Results (1/2)



Faulty node

Simulation Results (2/2)



50% of nodes are 10% faulty; the others have different levels of faultiness

Attack Description

- *Bad Mouthing*

  nodes provide wrong recommendations.
- *Sybil*

  nodes fake their identity.
- *On-off*

  alternate behavior of a node.
- *Conflicting behavior*

  node behaves in different ways depending on the peer.

Results (1/2)

- Our protocol provides protection against:
  - Bad mouthing attack:
    - many malicious nodes (30% in simulations) are required to degrade performance of the system.
  - On-off attack:
    - a node behaving well in 50% of the cases quickly reaches a trust value of 7.

Results (2/2)

- The Conflicting-behavior attack
  only influences systems in which we also rate the reliability of nodes in providing recommendations.
- Sybil attack
  can be prevented by using an identity check mechanism.

Conclusions

We have proposed a protocol that:

- provides the ability to evaluate trust of the nodes;
- provides protection against some well known attacks.

Future Work

- Study the network overload due to the protocol;
- better study of the coefficient of the trust formula;
- study different forms of the trust formula;
- better study the modifier values;
- include identity checking and evaluate its overload.