Dynamic Trust in Mixed Service-oriented Systems
- Models, Algorithms, and Applications -

PhD Defense, June 18th 2010, Vienna, Austria

Florian Skopik
Advisors: Prof. Schahram Dustdar, Prof. Frank Leymann

Distributed Systems Group
Vienna University of Technology, Austria
skopik@infosys.tuwien.ac.at
Environment and Motivation

- **Open and dynamic** Web-based environment
  - Humans and resources (e.g., Web services)
  - **Joining/leaving** the environment **dynamically**
  - Humans perform **activities** and **tasks**
- **Massive collaboration** in SOA/Web 2.0
  - Large sets of **humans** and **resources**
  - Dynamic **compositions**
  - Distributed communication and coordination
- **Keep track of the dynamics** to control
  - Future interactions
  - Resource selection
  - Compositions of actors
  - Disclosure of information
Motivating Scenario: The Expert Web

- How do actor discovery and selection mechanisms work?
- What is the technical grounding for the proposed Mixed System?
- How can actors be flexibly involved in a service-oriented manner?
- How do interactions and behavior influence future collaboration?

Structure of Presentation
Challenges in Collaborative SOA

- **Loose coupling**
  - flexible collaborations
  - environment model

- **Discovery**
  - dynamic properties
  - metrics
  - context
  - network structure

- **Dynamic binding**
  - selection
  - Automatic inference of personal trust
  - Bootstrapping trust
  - definition meaning applications
Contributions

- Collaborative mixed service-oriented systems
  - Interaction models
  - Delegation patterns
- Social trust and reputation models
  - Definitions and metrics
  - Inference approach
  - Temporal Evaluation
- Trust mining and prediction
  - Bootstrapping
  - Interest and expertise mining
  - Trust and reputation mining on the Web
- Trust-based service-centric applications
  - Expert discovery and ranking in virtual communities
  - Trusted information sharing/disclosure
  - Trust-based interest group formation

Definition of Dynamic Trust

- Trust reflects an **expectation**
  - one actor has about another’s future behavior
  - based on **previous interactions**
  - to **perform particular activities** dependably, securely, and reliably.


Flexible Collaborations

- **Traditional** project management (PM)
  - **Predefined** processes and *work breakdown structures*
  - Most important steps (tasks) are planned
  - Temporal order and dependencies

- Underneath the PM layer: **ad-hoc** activities
  - Structures to describe loosely coupled collaborations
  - Not modeled in advance
  - Emerging when performing tasks
  - User-defined

- **Typical Example:** Expert Web
  - Collaboration partners are discovered based on availability
  - Temporal constraints are dynamically set based on urgency
  - Required resources are flexibly selected based on RFS
Mixed Systems Approach

- **Fundamental concepts**
  - Mix of human- and software services collaboration
  - Humans provide services using SOA concepts

- **Expert Web Scenario**
  - Humans provide support in a service-oriented manner
  - Expert actors ‘implemented’ in software
    - knowledge bases
    - expert systems
    - oracles with reasoning capabilities
  - One harmonized environment to enable interactions between humans and software components (SOA)

Human-Provided Services (HPS)

- User contributions modeled as services
  - Users define their own services
  - Reflect willingness to contribute
- Technical realization
  - Service description with WSDL (capabilities)
  - Communication via SOAP messages
- Example: Document Review Service
  - Input: document, deadline, constraints
  - Output: review comments

Collaboration Network Concepts

Collaboration Metrics: reliability, responsiveness, success rate, collected experience, joint activities,…

\[ \text{Personal TRUST Inference} \]

(see later)

The Cycle of Trust

Analyzing Interactions
Establishing Trust Network

Trust-aware collaboration planning

Monitoring Collaboration

Executing Activities/Tasks

Structure of Presentation

- Loose coupling
- Discovery
- Dynamic binding

Flexible collaborations

Dynamic properties

Selection

Bootstrapping trust

Automatic inference of personal trust

Environment model

Metrics

Monitoring

Network structure

Definition meaning applications

12 of 31
Trust Inference Overview

<soap:Envelope xmlns:soap="...
  <soap:Header>
    <vietypes:timestamp value="2010-06-18T10:59:00"/>
    <vietypes:delegation hops="3" deadline="..."/>
    <vietypes:activity url="http://.../Activity#42"/>
    <wsa:MessageID>uuid:722B1240-...<wsa:MessageID>
    <wsa:ReplyTo>http://.../Actor#Florian<wsa:ReplyTo>
    <wsa:From>http://.../Actor#Florian<wsa:From>
    <wsa:To>http://.../Actor#Daniel<wsa:To>
    <wsa:Action>http://.../Type/RFS<wsa:Action>
  </soap:Header>
  <soap:Body>
    <hps:RFS>
      <rfs:requ>Can you review my slides?</rfs:requ>
      <rfs:generalterms>review, ...
      <rfs:keywords>computer science, ...
      <rfs:resource url="http://.../phd-defense.ppt"/>
    </hps:RFS>
  </soap:Body>
</soap:Envelope>

Trust Inference (2)

Calculate Metrics

- Measure collaboration attitude
  - Define metrics that describe trustworthy behavior
  - Calculate metrics upon captured interactions

- Example Scenarios
  - Expert Web: *fast and reliable responses*
    - Average response time
    - (Activity support) success rate
  - Information disclosure in science collaboration: *matching interests and beneficial behavior*
    - Interest/expertise profile similarity
    - Reciprocity: mutual ‘give and take’

\[
t_r^a = \frac{\sum_{rfs \in RFS} (t_{receive}(rfs) - t_{send}(rfs))}{|RFS|}
\]

\[
sr^a = \frac{num(sRFS)}{num(sRFS) + num(fRFS)}
\]

Trust Inference (3)

Fuzzy Interpretation

- Interpretation using fuzzy set theory
  - define membership functions (SLA, best practice)
    - define rule base
      - if \( t_r \) is low and \( sr \) is low then trust is low
      - if \( t_r \) is medium and \( sr \) is high then trust is high
    - mapping of values, inference and defuzzification

What is the meaning of trust in the given scenario?

- **absolute trust limits** (e.g., pre-defined constraints for collaboration)
- **relative ranking** (e.g., who is the most trusted expert from one’s personal perspective?)
Problem: Usually, always the most trusted expert is selected
  - Successful interactions lead to more trust: “The rich get richer”
  - Multiple selections lead to temporary overload

Solution: Balancing through delegations (triadic interaction pattern)
Evaluation: Interaction Balancing (1/3)

- Group formation through invitations
  - All members are connected to initiator 0
  - All members send requests to the initiator
  - Initiator delegates requests using the *Triad pattern*
  - Delegation receiver responds to the initial requester
  - On Success, members get introduced to each others

- Simulation of different actor behavior
  - Fair players (green)
  - Erratic actors (yellow)
  - Malicious attackers (red)
Evaluation: Interaction Balancing (2/3)

- Round-based simulation (r=250)
  - One request per round per actor sent and served or delegated.
  - Untrustworthy actors are punished and excluded from the community after \( r=100 \).

Detailed simulation setup and experiment results in:
Evaluation: Interaction Balancing (3/3)

- **Global success rate**: amount of finished tasks.
- Varying number of requesters in the network

- **RFS**: sending, delegating, and processing takes exactly one round.
- **RFSs** (and delegations) are considered failed if not replied after 15 rounds.
Structure of Presentation

- Loose coupling
- Discovery
- Dynamic binding

- Flexible collaborations
  - Environment model
  - Metrics
  - Monitoring
  - Network structure

- Dynamic properties
  - Selection

- Automatic inference of personal trust

- Bootstrapping trust

22 of 31
Bootstrapping of Trust

- **Problem:** What if no interactions with a potential collaboration partner have been captured?

- **Trust Mirroring**
  - people tend to trust ‘similar minded’ persons
  - calculation of interest similarities

- **Trust Teleportation**
  - people benefit from trust relations in actors from the same group (i.e., advanced trust due to similar profiles as existing trustees)

Bootstrapping Trust Overview (through similarity of tagging behavior)

- Observe collaboration tagging actions
- Actor tagging profiles
- Global interest tree (taxonomy)
- Hierarchical similarity measurement
- Trust mirroring and teleportation

Bootstrapping Approach (1)

Observe Collaborative Taggings

Dynamic tagging profiles characterize actors.

**Problem:** Compare tagging behavior (usage of tags)!
Bootstrapping Approach (2)

Global Interest Tree (Taxonomy) Creation

- Use tagging actions (actor—tag—resource)
  - degree of tags’ co-occurrence determines closeness
  - clustering: compare tag frequency vectors (tf*idf)
  - different similarity thresholds → hierarchy

- Global interest tree
  - express global areas of interests and relations
Actor tagging profiles (ATPs)
- describe mainly used tags of an actor
- tag usage vector

A) General ATPs
- use tagging actions (actor—tag—resource)
- independent from resources

B) Tailored ATPs
- use tagging actions (actor—tag—resource)
- used tags on a specified subset of resources
- “What is someone’s understanding of a given resource set?”
Hierarchical similarity measurement
- weighting of ATP vectors wrt. the global interest tree
- cosine-similarity of profile vectors
- on different levels of the global tree

Result: two outputs
- similarity in [0,1]
- reliability of similarity (dep. on level of comp.)

Apply profile similarities
- trust mirroring
- trust teleportation

Evaluation: Bootstrapping

- Compare ATPs of citeulike users
  - 45 comparisons (all with each other)
  - General ATP similarity (left fig.)
  - Tailored ATP similarity (right fig.)
    (tags used on SNA papers only)
Conclusion

- **Delegation** patterns lead to an emergence of trust
  - No traditional point-to-point relations only (see balancing)

- **Behavior models** and patterns influence trust
  - Social metrics: interest similarity, reciprocity, …
  - Temporal properties: actor uniformity, reliability, …
  - Context awareness of metrics and relations

- **Discovery and selection** of trustworthy partners
  - Bootstrapping mechanisms
  - Network structures: recommendation, reputation
  - Personal experience: trust

- Various applications of dynamic **system adaptations**
  - Information disclosure
  - Resource allocation
  - Actor compositions
Thank you.

skopik@infosys.tuwien.ac.at