Robust Trust Management for Cloud Service Provisioning

Jie Zhang

School of Computer Science and Engineering
Nanyang Technological University, Singapore
Agenda

• Why Trust
• Definitions and Characteristics of Trust
• Example Models of Trust and Reputation
• Many Challenges
• Coping with Unfair Ratings
• Remaining Issues
Why Trust?

• Common Characteristics of Online Systems/Networks
  – Open, distributed, dynamic, non-transparent
  – Composed of individual users, enterprises or other things
  – Varying capability, self-interested and deceptive
Why Trust?

Traditional (Hard) Security vs. Trust as (Soft) Security

- Authentication or access control
- Protect resources from malicious users

- Protect from those who offer resources and services
- Model the capability, reliability and honesty
Why Trust?

- Cloud service providers provide cloud services/resources to consumers
- Service level agreement (SLA)
  - Vague clauses, unclear technical specifications, not consistent, not matching
Definitions of Trust

- In literature, trust has been described as attitudes, beliefs, probabilities, expectations, and honesty

  – “Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of his capacity of ever to be able to monitor it) and in a context in which it affects [our] own action”

  – “Trust itself consists of beliefs. Trust is a mental attitude of an agent x towards another agent y about the behavior/action relevant for the result (goal)”
Characteristics of Trust

• Subjective
Characteristics of Trust

• Transitive

Thanks to Bob's advice, Alice trusts Eric to be a good mechanic.

Bob has proven to Alice that he is knowledgeable in matters relating to car maintenance.

Eric has proven to Bob that he is a good mechanic.
Characteristics of Trust

• Transitive

\[
\text{Alice's trust in David} = \text{Alice's trust in Bob} \times \text{Bob's trust in Clark} \times \text{Clark's trust in David}
\]

\[
= 0.8 \times 0.8 \times 0.6
\]

\[
= 0.384
\]
Characteristics of Trust

• Dynamic and Uncertain
  – Based on prior knowledge and experience
  – Increase or decrease over time

• Context Dependent and Multi-faceted
  – While you may trust a mechanic (in the context of fixing your car), you would not trust him to perform heart surgery on you (in the context of a medical problem)
Trust Modeling

• Direct Trust
  – Based on personal experience

• Reputation
  – General public’s opinion about a person’s or thing’s character or standing

“I trust you because of your good reputation.”
“I trust you despite your bad reputation.”
Models of Trust

• Models of Dynamic Trust and Uncertainty

<table>
<thead>
<tr>
<th>$T_i(j)^t$</th>
<th>Cooperation by $j$</th>
<th>Defection by $j$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$&gt; 0$</td>
<td>$T_i(j)^t + \alpha(1 - T_i(j)^t)$</td>
<td>$(T_i(j)^t + \beta)/(1 - \min{</td>
</tr>
<tr>
<td>$&lt; 0$</td>
<td>$(T_i(j)^t + \alpha)/(1 - \min{</td>
<td>T_i(j)^t</td>
</tr>
<tr>
<td>$= 0$</td>
<td>$\alpha$</td>
<td>$\beta$</td>
</tr>
</tbody>
</table>

$-1 \leq \omega_i \leq 1$

$-1 \leq \Omega_i \leq 1$

Dempster-Shafer Theory

Chernoff Bound theorem

$$N_{\min} = -\frac{1}{2e^2} \ln \frac{1 - \gamma}{2}$$


Models of Trust

• Chains of Trust

Models of Trust

• A Multi-Faceted Trust Model for VANET

Models of Reputation

• Beta Reputation System

\[ \varphi(p \mid r_T^X, s_T^X) = \frac{\Gamma(r_T^X + s_T^X + 2)}{\Gamma(r_T^X + 1) \Gamma(s_T^X + 1)} p^{r_T^X} (1 - p)^{s_T^X} \]

\[ \mathbb{E}(\varphi(p \mid r_T^X, s_T^X)) = \frac{r_T^X + 1}{r_T^X + s_T^X + 2} \]

\[
\begin{align*}
  b &= \frac{r}{r+s+2} \\
  d &= \frac{s}{r+s+2} \\
  u &= \frac{2}{r+s+2}
\end{align*}
\]

where \( u \neq 0 \)

Models of Reputation

- Bayesian Network Model

Challenges of Trust and Reputation Modeling

- Re-entry/Change of identity
- Value imbalance
- No incentive to provide ratings
- Hard to elicit negative feedback
- Reputation lag
- Discrimination
- ...
- Unfair ratings (spam review, 50 cents, water army...)
Dealing with Unfair Ratings: Filtering

- Iterated Filtering
  - Filter out ratings that are not in the majority
  - Overall reputation score is inside the lower and upper boundaries of fair ratings
  - Effective when majority ratings are fair

Dealing with Unfair Ratings: Discounting

• Credibility-Based Trust

\[ T_r(s) = \sum_{l=1}^{\left| \mathcal{V}(s) \right|} \frac{\mathcal{F}_c(l, s)}{\left| \mathcal{V}(s) \right|} \]

\[ \mathcal{F}_c(l, s) = \mathcal{F}(l, s) \cdot \mathcal{C}_r(l, s) \]

• Credibility Model
  – Majority consensus: expert cloud consumers
  – Feedback density: prefers a large number of feedback providers

Noor, T. H. and Sheng, Q. Z. 2011a. Credibility-Based Trust Management for Services in Cloud Environments. 9th Int. Conf. on Service Oriented Computing (ICSOC'11).
Dealing with Unfair Ratings: Discounting

• A Personalized Approach
  – Private knowledge about advisors
    • Buyer and advisor’s ratings for commonly rated sellers
    • Rating pair \((r_{b,s}, r_{a,s})\) is positive, if \(r_{b,s} = r_{a,s}\), otherwise, negative
      \[
      \alpha = N_p + 1, \quad \beta = N_{all} - N_p + 1; \quad R_{pri}(a) = \frac{\alpha}{\alpha + \beta}
      \]
  – Public knowledge about advisors
    • All ratings for sellers ever rated by advisor
    • Comparing advisor’s rating with others’
    • Consistent rating (e.g. close to average of others’ ratings)
Dealing with Unfair Ratings: Discounting

• A Personalized Approach
  – Public knowledge about advisors
    • $N_{\text{all'}}$: total # of ratings; $N_{c}$: total # of consistent ratings
    
    $\alpha' = N_{c} + 1$,  $\beta' = N_{\text{all'}} - N_{c} + 1$,  $R_{\text{pub}}(a) = \frac{\alpha'}{\alpha' + \beta'}$
  
  – Overall trustworthiness
    • Combine private and public knowledge
    • Reliability of private reputation (weight w)
      
    $T_{\text{r}}(a) = w R_{\text{pri}}(a) + (1 - w) R_{\text{pub}}(a)$

Dealing with Unfair Ratings: Alignment

• Alignment Approach

Dealing with Unfair Ratings: Alignment
Dealing with Unfair Ratings: Alignment

• Cluster Analysis
  – First layer: Cluster users into different groups and outliers
    • input: advisors + parameters for DENCLU
      output: subjectivity groups + outliers
    • input: outliers + parameters for DENCLU
      output: two types of dishonest types (direct, indirect) + outliers (misguidance)
  – Second layer: **Fuzzy smoothing process** to adjust clustering results
    • Each subjective user belongs to two nearest subjectivity groups
    • Each dishonest user (w/o misguidance ones) belongs to two dishonesty types
Dealing with Unfair Ratings: Alignment

• Group Alignment
  – Adopt ratings provided by advisors, and discard ratings from misguidance ones
  – A rating provided by advisor is aligned to a rating of the user:

\[ r_u = r + \text{mean}(r_{cu_1}) * m_{u_1} + \text{mean}(r_{cu_2}) * m_{u_2} \]

\[ - \text{mean}(r_{cu_1}) * m_{c_1} + \text{mean}(r_{cu_2}) * m_{c_2} \]
Robustness Evaluation

- Simulated Environment
- Real Data + Simulated Attacks
- Mean Absolute Error (MAE)

<table>
<thead>
<tr>
<th></th>
<th>Constant</th>
<th>Camouflage</th>
<th>Whitewashing</th>
<th>Sybil</th>
<th>Sybil + Cam</th>
<th>Sybil + Ww</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iterated Filtering</td>
<td>0.19 +/- 0.06</td>
<td>0.11 +/- 0.04</td>
<td>0.58 +/- 0.02</td>
<td>0.99 +/- 0.00</td>
<td>0.73 +/- 0.01</td>
<td>0.64 +/- 0.01</td>
</tr>
<tr>
<td>Referral Chain</td>
<td>0.06 +/- 0.02</td>
<td>0.16 +/- 0.01</td>
<td>0.97 +/- 0.03</td>
<td>0.10 +/- 0.02</td>
<td>0.19 +/- 0.02</td>
<td>0.99 +/- 0.01</td>
</tr>
<tr>
<td>Personalized</td>
<td>0.02 +/- 0.01</td>
<td>0.01 +/- 0.00</td>
<td>0.06 +/- 0.01</td>
<td>0.20 +/- 0.21</td>
<td>0.05 +/- 0.00</td>
<td>0.96 +/- 0.02</td>
</tr>
</tbody>
</table>

S. Jiang, J. Zhang and Y. Ong, An Evolutionary Model for Constructing Robust Trust Networks, 12th AAMAS, 2013
Remaining Issues

• Collusive Attacks

• Discrimination + Unfair Ratings

• Infinite Number of Possible Unfair Rating Attacks

• How to Quantify Robustness

• …
Thank You.