Social Computational Trust Model (SCTM): A Framework to Facilitate the Selection of Partners

Ameneh Deljoo
Systems and Networking Lab
University of Amsterdam
a.deljoo@uva.nl
Motivation

- Network of organizations evolve over time and become more complex,
- Find a “right” partner is a challenging task

We need to:
- Define a more **sophisticated** and **computationally executable** method to select the “right” partner for **sharing data** and **intelligence**.
Contributions

- **The Social Computational Trust Model (SCTM)** represents social trust and its components, which are important for evaluating the partners.

- **Risk assessment** through the SCTM model. The SCTM facilitates risk-based partner selection to select the "right" partner to collaborate in joint tasks.
Trust and its Antecedents

- “x” expects “y” to do task (τ) and “y” will not exploit vulnerabilities of “x” when “y” faced with the opportunity to do so. Therefore, “y”:
  - Has the **potential ability** to perform a given task (competence),
  - **Adheres** to a set of **rules** agreed upon and acts accordingly to **fulfill the commitments** (integrity), and
  - **Acts** and does **good** even if unexpected contingencies arise (benevolence).

Adopted from Mayer et al. (1995) “An Integrative Model of Organizational Trust”
Social Computational Trust Model (SCTM)

- Identify two distinctive trustworthiness factors (Benevolence and Competence)
- Evaluate Trust in a dynamic way
- Gather the direct and indirect evidence on a trustee
- Update Trust value

1 Integrity has been considered as a part of Benevolence function.
### Notation

<table>
<thead>
<tr>
<th>Description</th>
<th>Representation</th>
<th>Value Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>$x,y$</td>
<td></td>
</tr>
<tr>
<td>Society of Agents (trustor, trustee)</td>
<td>$x, y \in A$</td>
<td></td>
</tr>
<tr>
<td>Knowledge based of trustor $x$</td>
<td>$Kb_{x}$</td>
<td></td>
</tr>
<tr>
<td>Set of Situations</td>
<td>$S = {s_1, s_2, \ldots s_n}$</td>
<td></td>
</tr>
<tr>
<td>Tasks</td>
<td>$\tau$</td>
<td></td>
</tr>
<tr>
<td>Sub-tasks</td>
<td>$\tau_{s_1}, \ldots \tau_{s_n}$</td>
<td></td>
</tr>
<tr>
<td>Context</td>
<td>$D = {d_1, d_2, \ldots d_8}$</td>
<td>$1, 0.5, 0$</td>
</tr>
<tr>
<td>$d_8$ All the direct evidence on $y$ in the situation $s_i$</td>
<td>$Ed(x, y, s_i; Kb_{x})$</td>
<td></td>
</tr>
<tr>
<td>All the available evidence on $y$ from $y$’s neighbors in the situation $s_i$</td>
<td>$Ec(nbr_{y}, y, s_i)$</td>
<td></td>
</tr>
<tr>
<td>Trustee’s trustworthiness toward trustor $x$ in the situation $s_i$</td>
<td>$TW(x, y; s_i)$</td>
<td>$[0,1]$</td>
</tr>
<tr>
<td>Trust $x$ on $y$ in the situation $s_i$</td>
<td>$Tr(x, y; s_i)$</td>
<td>$[0,1]$</td>
</tr>
</tbody>
</table>

1Dimensions are: $d_1 =$ trustor, $d_2 =$ trustee , $d_3 =$ time, $d_4 =$ location, $d_5 =$ task, $d_6 =$ complexity, $d_7 =$ deadline, $d_8 =$ Outcome
In order to define the situations that lead to an agreement between a trustor and a trustee:

- $d_1 = \text{trustor}$,
- $d_2 = \text{trustee}$,
- $d_3 = \text{time}$,
- $d_4 = \text{location}$,
- $d_5 = \text{task}$,
- $d_6 = \text{complexity}$,
- $d_7 = \text{deadline}$,
- $d_8 = \text{Outcome}$

Three different outcome of tasks

- $F_d (\text{Fullfil duty})$
- $F_{dd} (\text{Fullfil duty with delay})$
- $V (\text{Violate})$

$$\text{val} (d_8) = \begin{cases} 1, & \text{if } d_8 = F_d \\ 0.5, & \text{if } d_8 = F_{dd} \\ 0, & \text{if } d_8 = V \end{cases}$$
Calculate the Outcome

- $d_8$: Outcome
- Three different outcome of tasks
  - $Fd$: (Fullfil duty)
  - $Fdd$: (Fullfil duty with delay)
  - $V$: (Violate)

$$\text{val}(d_8) = \begin{cases} 
1, & \text{if } d_8 = Fd \\
0.5, & \text{if } d_8 = Fdd \\
0, & \text{if } d_8 = V 
\end{cases}$$
A trustor looks at its Kb to collect the evidence on a trustee based on past interactions.

\[ \text{val}_d(\cdot) \rightarrow [0,1] \]

\[ Ed(x, y, s_i; kb_x) = \{ d_8(x, y, s_i) \in kb_x \} \]

\[ \text{val}_d(Ed(x, y, s_i; kb_x)) = \frac{1}{N_x} \sum_{d_8(x,y,s_i) \in Ed(x,y,s_i; kb_x)} \text{val}(d_8(x, y, s_i)) \]

\[ \text{val}(d_8) = \begin{cases} 1, & \text{if } d_8 = Fd \\ 0.5, & \text{if } d_8 = Fdd \\ 0, & \text{if } d_8 = V \end{cases} \]

\( N_x = \text{number of entries in the Kb's} \)
Evidence Gathering: Indirect evidence

A trustor asks a trustee’s direct neighbors to send him their evidence on a given trustee.

\[ val_c(\cdot) \rightarrow [0,1] \]

\[ Ec(nbr_y, y, s_i) = \{ Ed(u, y, s_i, kb_u) | u \in nbr_y \} \]

\[ val_c(Ec(x, y, s_i)) = \frac{1}{N_{nbr}} \sum_{Ed(u, y, s_i, kb_x) \in Ec(nbr_y, y, s_i)} val_d(Ed(u, y, s_i, kb_u)) \]

\[ N_{nbr} = \text{number of neighbors that contribute to the } val_c \]
**Benevolence Function**

- Based on the **direct** interactions between trustor \( x \) and trustee \( y \) in the situation \( s_i \).

\[
Ben(x, y, s_i) = val_d(Ed(x, y, s_i, kb_x))
\]
Competence Function

- Evaluate based on the all available evidence on Trustee (e.g. y,z)

\[ \text{Com}(nbr_y, y, s_i) = \text{val}_c(Ec(nbr'_y, y, s_i)), nbr'_y = nbr_y \{x\} \]

Estimating Trust\(^1\) based on Competence and Benevolence functions

\[
Tw(x, y, s_i) = \frac{1}{2} (\text{Com}(nbr_y, y, s_i) + \text{Ben}(x, y, s_i))
\]

\[
Tr(x, y, s_i) = Tw(x, y, s_i)
\]

\(^1\) Integrity has been considered as a part of Benevolence function.
Risk Estimation
Risk Estimation

Interaction Risk \( (R_i(x, y, s_i)) \) in the Alliance Consists of:

- Relational Risk \( (R_r(x, y, s_i)) \): The **probability** and **consequence** of **not having** a successful cooperation.
- Performance Risk \( (R_p(x, y, s_i)) \): The **probability** and **consequences** that alliance **objectives** are not **realized** despite **satisfactory cooperation** among the partner.
Propositions

Proposition 1

Benevolent\(^1\) behavior of partners increases trust and reduces former perceived relational risk in the alliance.

\[ R_r(x, y, s_i) \propto (1 - Ben(x, y, s_i)) \]

Proposition 2

The perceived performance risk will be reduced if the competence of the given member is high.

\[ R_p(x, y, s_i) \propto (1 - Com(nbr_y, y, s_i)) \]

\(^1\)Some of the scholars consider faith and good intentions instead of benevolence.
Interaction risk

Interaction Risk is given by:

\[ R_i(x, y, s_i) = R_r(x, y, s_i) + R_p(x, y, s_i) \]

\[ R_i(x, y, s_i) = w_1(1 - Com(x, y; s_i)) + w_2(1 - Ben(x, y; s_i)) \]

\[ R_i(x, y, s_i) = \alpha \left(1 - \text{Com}(nbr_y, y, s_i)\right) + (1 - \alpha)\left(1 - \text{Ben}(x, y, s_i)\right), \quad 0 \leq \alpha \leq 1 \]

\[ w_1 = \alpha, \quad w_2 = 1 - \alpha \]

Case Study

A Collaborative Network
## Simulation settings and their illustrations

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
<th>Illustrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A$</td>
<td>Fixed</td>
<td>Number of nodes in the network</td>
</tr>
<tr>
<td>$\tau$</td>
<td>Fixed</td>
<td>Type of task (defend and mitigate the attack)</td>
</tr>
<tr>
<td>$N_x$</td>
<td>6</td>
<td>Number of entries in the Kbs</td>
</tr>
<tr>
<td>$t_{request}$</td>
<td>Initiate the simulation</td>
<td>Request time</td>
</tr>
<tr>
<td>$t_{report}$</td>
<td>Receive the feedback on the request</td>
<td>Report time</td>
</tr>
<tr>
<td>$\Delta t_w$</td>
<td>10 s</td>
<td>Time window</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>0.3</td>
<td>Weight factor</td>
</tr>
<tr>
<td>$S$</td>
<td>4</td>
<td>number of situations</td>
</tr>
<tr>
<td>$\tau_s$</td>
<td>4</td>
<td>number of sub-tasks</td>
</tr>
</tbody>
</table>
Scenario

Domain “N” wants to choose ideal domains for collaboration in order to mitigate and defend against a certain attack.

Task ($\tau$): Mitigate and defend against a certain attack.

Sub-tasks:
- $\tau_{s1}$: provide resources within a certain time window,
- $\tau_{s2}$: monitor a certain traffic,
- $\tau_{s3}$: block a certain link,
- $\tau_{s4}$: implement a certain counter measurement.
Selecting a “right” partner algorithm

Algorithm 2 Selecting a “right” partner (trustee) to collaborate on performing a task. Input: benevolence, competence and $Ri(x, y, s_i)$

1: Employ the benevolence (see Section 3.3) and the competence (see Section 3.4) functions to calculate the competence and benevolence for all the members.
2: Identify the first trust discriminator for each task to assign the weight to each factor.
3: Use the value of the benevolence and competence to evaluate the interaction risk for each member (see Section 5).
4: Recommend a domain for each task such that its estimated interaction risk $Ri(x, y, s_i)$ is minimal.
5: if two members have the same $Ri(x, y, s_i)$ then
6: Select a member with the maximum benevolence value.
7: end if
8: return Selected member(s)
Evaluation

- Epinion\(^1\) dataset a popular product review site.
  - Each user gives a trust value (−1 to 1) on other users.
  - And gives feedback ratings (1 to 5) on entities/items.

- \(V = 1, \ Fdd = 2\) and \(Fd = 3; 4; 5\).

- Select five items from the dataset and evaluate benevolence and competence of each item.

- SELCSP Algorithm and SOLUM Algorithm.

\(^1\)http://www.trustlet.org/epinions.html
Evaluation Result

The value of benevolence for three different algorithms

The value of competence for three different algorithms
Conclusion

- To evaluate the trustworthiness of a trustee the direct and indirect evidence on the given trustee were taken into account.
- The trust value is computed by two trust factors, namely competence and benevolence.
- Benevolence is computed from direct evidence between a trustee and a trustor.
- Competence is assessed on the base of the received feedback from the other alliance members (a trustee's direct neighbors).
- We are able to collect a variety of evidence on a trustee by introducing eight dimensions for each context.
Conclusion

- The interaction risk estimated through the SCTM by combining benevolence and competence.
- The weighting factors used to determine different weights to define the main trust factors in different trusting scenarios.
- We have shown that the stability of the alliance is dependent on the value of benevolence that led to a lower interaction risk.
- We demonstrated that the SCTM is able to obtain comparable results to the other trust models that we evaluated.
Thank you.

Ameneh Deljoo
a.deljoo@uva.nl