Trust-based Task Assignment in Military Tactical Networks

1MoonJeong Chang, 2Jin-Hee Cho, Ing-Ray Chen, Kevin S. Chan, Ananthram Swami

1Virginia Tech, Department of Computer Science, U.S.A.
2Army Research Laboratory, Computational and Information Sciences Directorate, U.S.A.
Outline

• Background
• Motivation
• Goal & Contributions
• Related Work
• System Model
• Proposed Task Assignment Protocol
• Numerical Results & Analysis
• Conclusions & Future Work
What is Trust?

• Degree of a subjective belief about the behaviors of a particular entity
• Willingness to take a risk

What is Trust Management? (Blaze06)

• A separate component of security services in networks

Measure of Trust

• Measure of potential risks
• Context-dependency
• Subjectivity
• Cognitive learning process
• System reliability
Motivation

Example Scenarios: rescuing personnel, constructing military facilities, conducting surveillance or monitoring, destroying certain targets, or managing disasters

Task Assignment

• An efficient and effective task assignment in tactical military networks is key to successful mission completion
• The best match between entities and tasks can maximize mission completion ratio

Use of Trust

• Trust-based soft security approaches can increase mission completion ratio in the presence of untrustworthy entities where traditional security services may not be practical
Goal

- Develop a trust-based task assignment protocol that maximizes mission completion ratio while meeting an acceptable risk level using composite trust metric

\[
\text{maximize } P_m^{\text{completion}}(t), \\
given \sum_{j \in M} r_{m,j}(t) \leq P_m^{\text{risk}}
\]

Contributions

- Proposed a task assignment protocol based on the tradeoff analysis between trust and risk
- Reflected the context-dependent characteristic of trust
- Employed a composite trust metric
- Assigned multiple tasks to an entity and multiple entities to one task
Related Work

- Distributed computing systems (Jiang09)
- Wireless sensor networks (Johnson10)
- Multi-hop wireless networks (Jin12)
- Autonomous underwater vehicle networks (Kulkarni10)
- Mobile ad hoc networks (Cho11)

Limitations

- Mostly one node is assigned to one task;
- Analysis between trust and risk is not employed in task assignment;
- Required trust level of each task is not considered;
- Missions are not specifically modeled in terms of their characteristics
System Model:
Network Model

- Heterogeneous networks with multi-hop communications (sensors, mobile entities)
- Hierarchical structure: commander - task leaders - members
- Dynamic multiple tasks where a task arrives and ends at different times
- Heterogeneity of entities with various speed, detection error, group join/leave, and trust behaviors

Description of Node Type

- **NT₄**: Manned vehicles equipped with devices
- **NT₃**: Humans carrying devices
- **NT₂**: Unmanned vehicles or robots carrying devices
- **NT₁**: Sensors
## System Model: Trust Properties

<table>
<thead>
<tr>
<th>Trust property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Social Trust</strong></td>
<td><strong>Social Connectedness</strong></td>
</tr>
<tr>
<td></td>
<td>Number of social connections in social circle</td>
</tr>
<tr>
<td><strong>Reciprocity</strong></td>
<td>Degree of mutual giving and receiving</td>
</tr>
<tr>
<td><strong>QoS Trust</strong></td>
<td><strong>Competence</strong></td>
</tr>
<tr>
<td></td>
<td>An entity’s capability to serve the received request</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>Honesty of an entity in attack behaviors</td>
</tr>
</tbody>
</table>
Unique Task Properties

- Minimum required node type
- Minimum trust threshold for each trust property

Common Task Properties

- **Importance** ($I_m$): How much impact is expected upon mission completion after the given task failure
- **Urgency** ($U_m$): How urgently the given task should be completed
- **Difficulty** ($D_m$): How much workload is required to execute the given task

(1-5 levels from low to high)
System Model: Trust Metric

\[ T_{i,j}^X(t) = \alpha T_{i,j}^{D-X}(t) + (1 - \alpha) T_{i,j}^{ID-X}(t), \quad 0 < \alpha < 1 \]

**Direct Trust** (\(T_{i,j}^{D-X}\))

\[ T_{i,j}^{D-X}(t) = \begin{cases} T_{i,j}^{D-X}(t), & \text{if } \text{HD}(i,j) = 1 \\ \gamma T_{i,j}^X(t - \Delta t), & \text{otherwise} \end{cases} \]

**Indirect Trust** (\(T_{i,j}^{ID-X}\))

\[ T_{i,j}^{ID-X}(t) = \begin{cases} \sum_{k \in R_{i}^{trw}} T_{k,i}^X(t) T_{k,j}(t) / |R_{i}^{trw}|, & \text{if } |R_{i}^{trw}| > 0 \\ \gamma T_{i,j}^X(t - \Delta t), & \text{otherwise} \end{cases} \]

\(R_{i}^{trw}\): set of 1-hop neighbors of node i providing trustworthy recommendations
**Task Assignment (1/2)**

\[ s_{i,m} = v_m - p_{i,m} \text{ where } v_m = \frac{D T_m}{D T_{\text{max}}} \quad \& \quad p_{i,m} = \frac{W_m}{w_i} \]

- **Compute tasks' scores**
- **Select a task with \( \text{MAX} \, s_{i,m} \)**
- **Winner determination based on trust-based risk analysis**

For \( r_{m,j}^X(t) \):

\[ r_{m,j}^X(t) = e^{-\rho_1 \frac{T_{i(m),j}^X(t)}{T_m} \frac{U_m}{U_{\text{max}}} \frac{D_m}{D_{\text{max}}}} = \frac{\sum_{X \in T} r_{m,j}^X(t)}{|T|} \quad \sum_{j \in M} r_{m,j}(t) \leq p_m^{\text{risk}} \]
Dynamic Task Reassignment

- When a task leader could not recruit a sufficient number of members or finds a current member cannot continue task execution:
  1) Check if current members can execute the task with extended deadline of the task when the deadline is extensible;
  2) Look for qualified members from available members pool;
  3) Terminate the contract if either 1 or 2 does not work
  4) Label the task as incomplete (task failure)
• Node Type 4 with four trust properties

**Trust bias**: Time-averaged difference between measured trust and objective trust

\[ B_{i,j} = \frac{\int_0^{MT} B_{i,j}(t) \, dt}{MT}, \text{ where } B_{i,j}(t) = \left| T_{i,j}(t) - OT_j(t) \right| / OT_j(t) \]

• Trust bias < 2% with trust decay factor \( \gamma = 0.95 \), direct trust weight \( \alpha = 0.2 \)
Numerical Results & Analysis: Trust Bias vs. Mission Completion

- 20 tasks & 100 nodes, 24 hours mission time
- Trust-based TA outperforms non-trust based TA
- Trust bias adversely affects mission completion ratio where inaccurate trust evaluation can mislead decision making
Numerical Results & Analysis:
Optimal Acceptable Risk Level

- There exists an optimal acceptable risk level that maximizes mission completion ratio.
- Composition of tasks with different importance levels may change an optimal acceptable risk level.
Conclusions

• Trust bias adversely affects mission completion ratio
• The proposed trust-based task assignment outperformed non-trust based counterpart
• There exists an optimal acceptable risk level that maximizes mission completion ratio

Future work

• Examine task assignment scenarios for coalition networks
• Investigate multiple objective optimization techniques for coalition networks
Any Questions?

Contact us at:
Virginia Tech
MoonJeong Chang, Ph.D.
mjjang@vt.edu

Army Research Laboratory
Jin-Hee Cho, Ph.D.
jinhee.cho@us.army.mil