Securing Dynamic Robotic Coordination in Unpredictable Environments: Enhancing Trust through Adaptive Learning and Cyber Defense

Giselle Roman | Dr. Yugyung Lee | 07/07/2025

Problem Statement Overview

In post-disaster zones, robots need to work together reliably even when facing cyber attacks like GPS spoofing or sensor tampering. This research aims to build a system that can detect these anomalies in real time, adjust trust in each robot, and reassign tasks as needed to keep the assignments on track.

Hypothesis

1. Using trust-based anomaly detection with adaptive task assignment will lead to higher task success rates and make the system more resilient to attacks

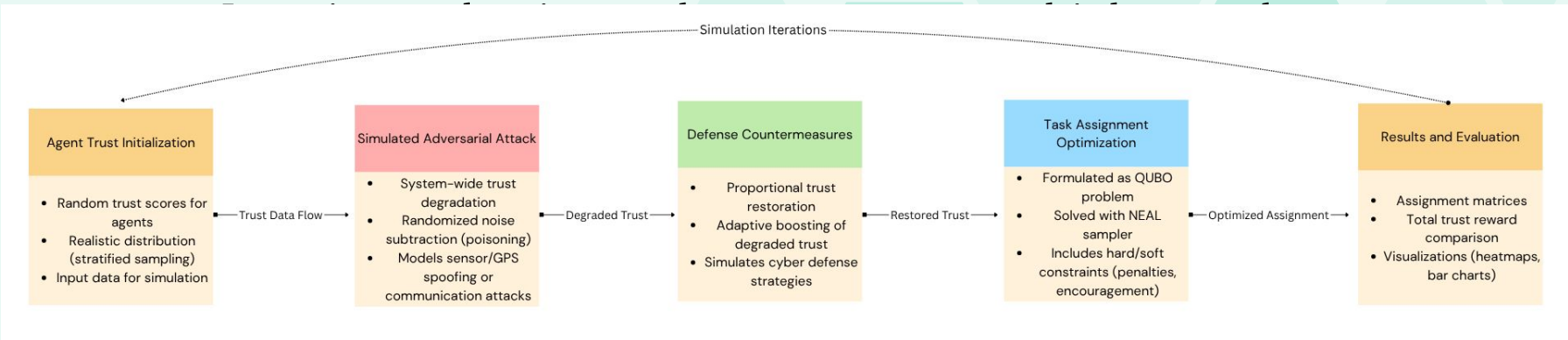
Research Questions

1. How can trust-related anomalies be detected in real time to prevent coordination failures during cyber-attacks?

2. How can adaptive task assignment based on updated trust improve mission success?

Conceptual Diagram

- Trust-aware coordination simulation
  - Agents initialized with trust scores reflecting reliability
  - Adversarial attacks degrade trust system-wide
  - Defense countermeasures restore trust proportionally
  - QUBO optimization assigns tasks under trust constraints



Method Overview

Simulation Framework

- Agents initialized with randomized trust scores
- Simulated attacks degrade trust
- Defense countermeasures restore trust

Optimization Algorithm

- Task assignment as QUBO
- Hard/soft constraints, penalties and encouragement
- Solved with D-Wave's NEAL sampler

Workflow

- Multiple rounds update trust scores
- Trust matrices extracted, rescaled, and normalized
- Assignment matrices decoded from QUBO solutions
- Total trust rewards evaluated for baseline, poisoned, and defended scenarios

Preliminary Results: Trust Matrices (Inputs)

- Trust scores between agents and tasks
- Three scenarios
  - Baseline (best-case)
    - Normal trust scores
  - Poisoned (attack impact)
    - Simulates cyber attack effects
    - Trust degraded
  - Defended (defense effectiveness)
    - Simulates applying a cyber defense countermeasure
    - lower than baseline, but better than poisoned

```
Baseline Trust Matrix
[[0.97209373 0.94761353 0.88724676 0.99233005 0.84928413]
 [0.97209373 0.94761353 0.88724676 0.99233005 0.84928413]
 [0.97209373 0.94761353 0.88724676 0.99233005 0.84928413]
 [0.97209373 0.94761353 0.88724676 0.99233005 0.84928413]
 [0.97209373 0.94761353 0.88724676 0.99233005 0.84928413]]
```

```
Poisoned Trust Matrix
[[0.5688474  0.48941461 0.4463877  0.68005262 0.48861762]
 [0.66956451 0.63120195 0.51011491 0.65209987 0.37243654]
 [0.55143457 0.61169281 0.56447331 0.63183647 0.42028942]
 [0.58336412 0.55730781 0.53527882 0.61910026 0.47538505]
 [0.57668675 0.4520083  0.45445525 0.50615094 0.47589406]]
```

```
Defended Trust Matrix
[[0.7688474  0.68941461 0.6463877  0.68005262 0.68861762]
 [0.66956451 0.63120195 0.71011491 0.65209987 0.57243654]
 [0.75143457 0.61169281 0.76447331 0.63183647 0.62028942]
 [0.78336412 0.75730781 0.73527882 0.61910026 0.67538505]
 [0.77668675 0.6520083  0.65445525 0.70615094 0.67589406]]
```

Preliminary Results: Assignment Matrices (Outputs)

- QUBO optimizer
  - Reads those trust scores (input)
- Assign agents to tasks
  - Maximize total trust
- Baseline
  - Optimal assignments in good conditions
- Poisoned
  - Forced to work with worse trust
- Defended
  - Should be better than poisoned

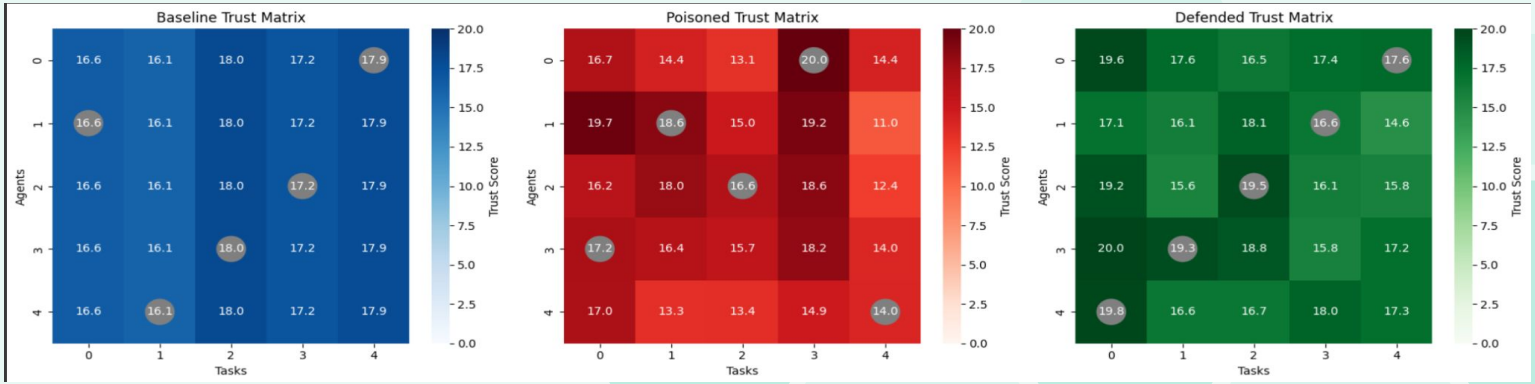
```
Baseline QUBO Assignment Matrix
[[0 0 0 0 1]
 [1 0 0 0 0]
 [0 0 0 1 0]
 [0 0 1 0 0]
 [0 1 0 0 0]]
```

```
Poisoned QUBO Assignment Matrix
[[0 0 0 1 0]
 [0 1 0 0 0]
 [0 0 1 0 0]
 [1 0 0 0 0]
 [0 0 0 0 1]]
```

```
Defended QUBO Assignment Matrix
[[0 0 0 0 1]
 [0 0 0 1 0]
 [0 0 1 0 0]
 [0 1 0 0 0]
 [1 0 0 0 0]]
```

Preliminary Results: Heatmaps (Combined)

- Color
  - Show the trust matrix (inputs)
- Circles
  - Overlay the QUBO assignment matrix (outputs)




```
Total Trust Reward (Baseline): 85.68018091663247
Total Trust Reward (Poisoned): 86.31644050831443
Total Trust Reward (Defended): 92.91171910288735
```

Challenges & Limitations

- Some assignments still not perfect after defense
  - Defense doesn't completely fix the trust degradation
- Need to tune attack and defense parameters
  - Find the right balance
- Solving gets slower with more agents and tasks

Next Steps

- Tune penalty and reward scaling in QUBO
- Test new defense strategies
- Explore RL-based trust restoration
- Scale to larger agent/task sets