Scenarios for Trust Management in Swarm Robotics

Daniel Vojnar, Adela Bierska, Barbora Buhnova
15-04-2024 RoSE
Trust in Intelligent Ecosystems

- Sociology definition of trust:
  Subjective probability that another party will perform an action that will not hurt my interest under uncertainty or ignorance.

- Characteristics of trust:
  - Subjective
  - Asymmetric
  - Transitive
Swarm Robotics

- Large amount of simple robots
- Inspired by nature (insect societies)
- Decentralized coordination
Why and How?

- Undetected malicious member of the society can destroy the mission
- To propose usable solutions we need to detect possible threats
Scenarios & Attacks

- we collected possible scenarios of swarm robot missions
- our proposition of attacks taxonomy
Attacks

Information Manipulation or Ignoring
- Personal Information
- External Information
- Passing Information
  - Leak of Information
  - Changing of Shared Information
  - Restrain Access

Manipulation with Communication Channels
- False Performance Promises
  - Permission Regulations
  - Task Allocation

Authority Misusing
- Scenario Attacks
Attacks

Scenario Attacks

Physical Attacks
- Robot Destruction
- Kidnapping/Capture
- Changing or Destruction of the Environment

Attacks to Internal Intelligence

Decision Making Attacks
- Contrarians (Opposing)
- Wishy-washy
- Sect (Wrong Addressing)
- Majority Opinion
Next Steps

- More detail of trust mechanics to prevent attacks
- Applications to modular robotics
- Simulations
- Trust indices mining from data
Thank you for your attention