

Foundations of Adaptive Networked Societies of Tiny Artefacts

## PerAda Workshop

# FRONTS: Foundations of Adaptive Networked Societies of Tiny Artefacts

Ioannis Chatzigiannakis

Research Academic Computer Technology  
Institute (RACTI, Greece)

June 2009

## The Partners

- 1 Research Academic Computer Technology Institute (RACTI, Greece)
- 2 Technische Universität Braunschweig (TUBS, Germany)
- 3 Universität Paderborn (UPB, Germany)
- 4 University of Athens (UOA, Greece)
- 5 Ben-Gurion University of the Negev (BGU, Israel)
- 6 Università di Roma “La Sapienza” (UDRLS, Italy)
- 7 Università degli Studi di Salerno (UNISA, Italy)
- 8 Wrocław University of Technology (WROC, Poland)
- 9 Universitat Politècnica de Catalunya (UPC, Spain)
- 10 University of Geneva (UNIGE, Switzerland)
- 11 University of Lübeck (UZL, Germany)

## Project Main Concept

- Our life is now full of small devices that communicate with each other when they are close.
- Actually such devices form networks that can potentially support myriads of new and exciting applications.
- **Technology would like such systems to be dependable and adaptive:**
  - to the user needs
  - sudden changes of the environment
  - specific applications characteristics
- FRONTS focuses on the algorithmic foundations of such adaptive networks.

## Modelling Adaptive Nets of Tiny Artefacts

The aim of this project is to establish the foundations of adaptive networked societies of small or tiny heterogeneous artefacts.

### Main Questions

- **How to program them?**  
Must capture scalability, self-\*, (and emerging behaviour), ad hoc, adaptiveness, local, restrictions on devices, simplicity
- **How to model local interactions?**  
Must capture dynamic situations, movement, faults & collisions
- **What to Optimize?**  
Energy, Communication, Time to compute globally, robustness, . . .

## Population Protocols (1)

- A **formal model for programming such networks** and for anticipating their behaviour.
- The model nicely **captures notions of fairness and scalability**.
- Considers systems that consist of huge numbers of very small resource limited artefacts.
- Artefacts are **anonymous** (indistinguishable).
- **Distributed inputs and outputs**.
  - The input to a protocol is distributed across the initial state of the entire population.
  - The output is distributed to all agents.

## Population Protocols (2)

- **Convergence rather than termination**
  - Protocols generally cannot detect when they have finished
  - instead, the artefacts' outputs are required to converge after some finite time to a common, correct value.
- Each artifact has limited, **constant size memory**
  - $\mathcal{O}(1)$  bits
  - independent of the size of the network
- Artifacts do not have control over their own motion
- Artifacts interact in pairs
  - via a local low-power wireless communication mechanism
  - when they are sufficiently close to each other
  - have little control over which other artefact they interact with.

## Population Protocols (3)

### Example

To know if in a flock of birds, if one is infected (high temperature).

- We attach one temperature sensor (artefact) to each bird.
- Each artefact has 2 states:
  - 1 Temperature is low (0)
  - 2 Temperature is high (1)
- When an initiating artefact at state 1 interacts with a responding artefact at state 0, it changes the responders state to 1 –  $(1, 0) \rightarrow (1, 1)$
- When an initiating artefact at state 0 interacts with a responding artefact at state 1, the initiators state changes to 1 –  $(0, 1) \rightarrow (1, 1)$
- All other interactions do not affect the states of the artefacts

## Population Protocols (4)

- This is a simple one-way epidemic protocol.
- If interactions between artefacts are random then protocol stabilizes after  $\Theta(n \log n)$  steps
  - i.e., number of interactions for epidemic to spread to all population
- Many open problems:
  - 1 How schedule of interaction affects performance ?
  - 2 What if protocol (rules of interaction) change ?  
(e.g., to adapt to certain events)
  - 3 What if some artefacts have unlimited storage ?
  - 4 Can we build a generic protocol verifier ?  
(i.e., given any protocol, examine if it eventual stabilizes ?)

## Need for Adaptation

The architecture of the network infrastructure of such systems is composed of two almost orthogonal dimensions:

- 1 The functionalities that are responsible for the **internal continual self-organization of the network**.
- 2 The components that **adapt to environmental changes** in a dynamic way.

## Internal continual adaptation (1)

How to organize (self) the net in order to adapt (internal preparation of the net) ?

### Main Questions

- What are the main parts of our “**System**” for which the internal organization is crucial?
- How to **self-stabilize**? (execute forever)
- What are the **basic functionalities** needed to be able to adapt the **internal communication** and to **re-organize**? How to make them efficient?

## Internal continual adaptation (2)

- We identified the **critical functionalities that such networks should always maintain, in order to be ready to adapt** to external challenges.
- Properties such as Connectivity, Security, Self-Organisation, Role Assignment are among this list.
- This “eternal preparation” for adaptation is crucial
- Eternal preparation: the work that the adaptive network performs in order to be ready to adapt (in timely manner) when an external cause is detected.
- Our methods **focus on reducing the overhead caused** by this “alert” network state.

## The structure of the internal organization “layer”

- **Task 1:** How to re-organize the **Communication Infrastructure**?
- **Task 2:** What are the **roles of artefacts** that can be re-adjusted? What are the methods to do this?
- **Task 3:** What is the approach to re-organize the **security** of the net?

## Continuous Re-organization

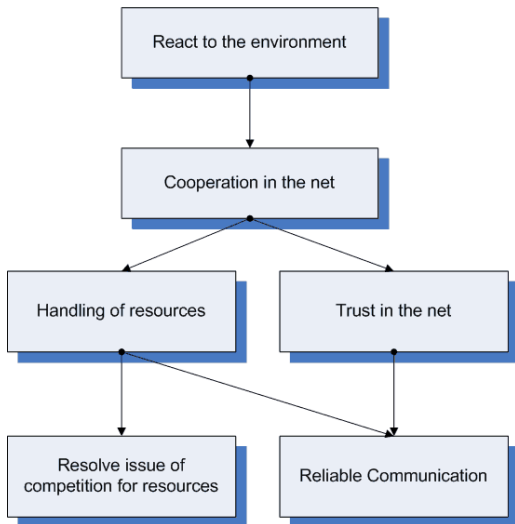
Part of the System	Functionalities needed
Internal Communication	<ul style="list-style-type: none"><li>▷ Reorganize <i>data gathering</i></li><li>▷ Allow for <i>redundancy in connectivity</i></li><li>▷ Maintain <i>hierarchy</i> in the communication graph that can keep a consistent status of the network</li></ul>
Redefine Roles of Artefacts for internal Reorganization	<ul style="list-style-type: none"><li>▷ Local Learning Methods</li><li>▷ Trust enhancement</li><li>▷ “Equilibria” and economic approaches for self-organization</li><li>▷ (Node “colors” are important to indicate and code local constraints)</li></ul>
Security	<ul style="list-style-type: none"><li>▷ Privacy Protection (keys and identities management)</li><li>▷ How to secure the routing?</li></ul>

## Adapting to the Dynamic Environment

### Main Questions

- What is the logical structure of the set of issues identified ?
- What are the crucial external “changes” to which the system should adapt?
- Reaction to a sudden external change may result in chaotic internal competition for resources. How do we handle it?

## The structure of the “react to the external” layer



## Approach to distributed cooperation

Reacts to	Approach
Low energy levels	Hierarchies and clusters Colony algorithms
Defectors (artefacts) exist, due to an external attack	Correlated punishment
External terrain changes	Maintain geometric “formations” of artefacts (similar to robots’ coordination)

## Approach to tracking of resources

Reacts to	Approach
Unknown terrains	Terrain exploration (similar to Robotics)
Target tracking	Use traces (our THTP protocol)
Bypass obstacles	Probabilistic data propagation
Obstacles appear (unknown)	Adaptive routing with backtracking

## Approach to physical changes

Reacts to	Approach
Passive movement of artefacts	Maintain the net via moving (actively) some relay nodes
A request that can be met by some subnetwork while the net changes	Dynamic Facility Location
Dynamic appearance of obstacles	Adaptive routing via “sensing the obstacles” (similar to previous figure)

## Approach to trust

Reacts to	Approach
An attack that may change id's of artefacts	Multi-level dynamic key distribution
Behavior of some artefacts is altered	Emerging Trust via rational selfish choices (a behavior equilibria approach)
System grows too large	Emerging Trust from statistical properties

## Approach to reliable communication

Reacts to	Approach
Random faults - unknown distributions	Learning methods
Adversary captures some nodes	Dynamic altering of communication paths
Nodes sleep / messages not received	Redundancy, probabilistic restarts

## Overall goal for a unifying scientific framework

### The most fundamental question

*Is there a single, unifying, abstract model for such adapting, massive nets of tiny artefacts, that can explain their emergent behavior ?*

- Our overall objective is to create a unifying framework for adaptive networks.
- We apply an iterative research & development process that employs three iterations (one per year).
- The aim of these iterations is to integrate the various elements developed in the project.

## Some unifying actions

- Basic approaches (adaptive)
  - Greedy with backtrack
  - Walks in the network
  - Equilibria building
  - Redundancy structures
- Communication
  - Heavy overlap between techniques for Internal & External adaptation
  - Different objectives
- Security & Trust
  - Heavy overlap between techniques for Internal & External adaptation
  - Overlapping objectives

## Key Knowledge Gap

- How do the capabilities of the artefacts affect system performance ?
  - e.g., if we increase memory in each artefact ?
- How heterogeneity affects system capabilities ?
  - e.g., if we have 2 different types (sexes) ? or 3 ? or 6 ?
- How unprecise measurements of the current system state affect system performance ?
- What cannot be achieved ?
  - Limits of adaptation.

## Future Application Scenarios

### Building Management

- Environment is dynamic
  - Human motion
  - New equipment installed
  - Existing equipment is relocated
  - Equipment is removed
- User needs are dynamic
  - Existing needs change
  - New requests to equipment
  - Users may be misbehaving
- Network needs to adapt to all above changes
  - Speed of network re-organization in dynamical changes of the physical environment.
  - Levels of security, trust and privacy achieved.