Formalising the Comhordú Protocol

Colm Bhandal  bhandalc@tcd.ie  Dr. Arthur Hughes  Arthur.Hughes@cs.tcd.ie

Motivation
Comhordú is a coordination model & protocol developed by Mélanie Bouroche from the distributed systems group.

- Alternative to the standard consensus approach.
- Key is to ensure safety e.g. vehicles in the system must not collide.
- Applies to multiagent systems MAS e.g. systems of automated traffic control in cities.
- Example: An early warning feedback system for ambulances in a city.
- Protocol is currently formalised or verified- that is the goal of this work.

Overall System Structure

Structural Operational Semantics of TCCS
These are the extended SOS of TCCS over regular CCS, the base language which is to be extended to formally model the Comhordú system.

The syntax of the language TCCS is that of CCS extended by the following structure:

\[ \epsilon \] \( \langle d \rangle \).P

Active Component Algebraic description

\[ \Sigma = \{ \text{read, toServer, switch} \} \]

\[ \text{Active}(i) = \text{read}(\langle i \rangle).\text{toServer}(A, i, s) + (\text{read}(\langle i \rangle).\text{Active}(i)) + A' + A' \]

\[ A' = \text{switch}(j).\text{Active}(j) \]

Dormant & Waiting Components, Algebraic description

\[ \Sigma = \{ \text{read, toServer, switch, start, trans, abort} \} \]

\[ \text{Dormant}(i) = \Sigma_{j \neq i}.\text{start}(j).\text{Waiting}(i, j, w(i, j)) + D(i) \]

\[ D'(i) = \text{trans}.\text{Waiting}(i, 0, w(i, 0)) + \text{abort}.\text{Dormant}(i) \]

\[ \text{Waiting}(i, j, t) = \Sigma_{j \neq i}.(\text{toServer}(W, j, s).W'(i, j, t) + D'(i)) + D'(i) \]

\[ W'(i, j, t) = \sigma(p(j)).\text{Waiting}(i, j, t - p(j)) + \epsilon(t).\text{abort}(i).\text{Dormant}(j) + D'(i) \]

Future Development Plan

- Extend the language of TCCS to include broadcast actions, value passing, and process parameterisation.
- Use the UPPAAL tool or a similar model checking tool to approximate the model.
- Verify the model i.e. machine check it for safety.