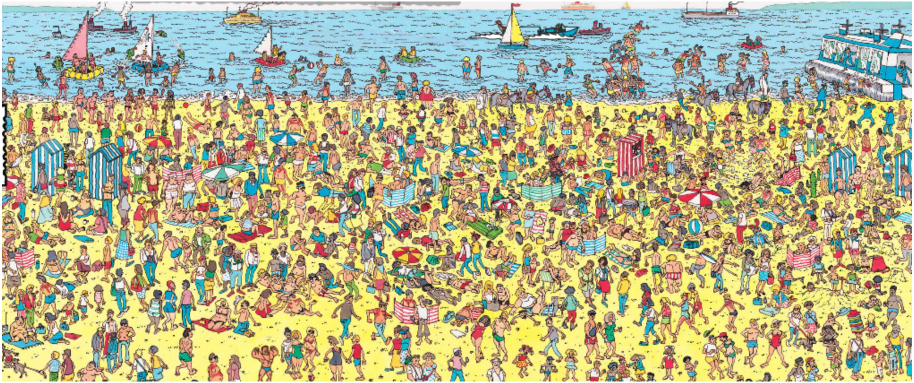
A Topological Categorization of Agents for the Definition of Attack States in Multi-Agent Systems

Katia Santacà[1], Matteo Cristani[1], **Marco Rocchetto**[2], Luca Viganò[3]
[1] Università di Verona, Italy
[2] University of Luxembourg, Luxembourg
[3] King's College London, UK

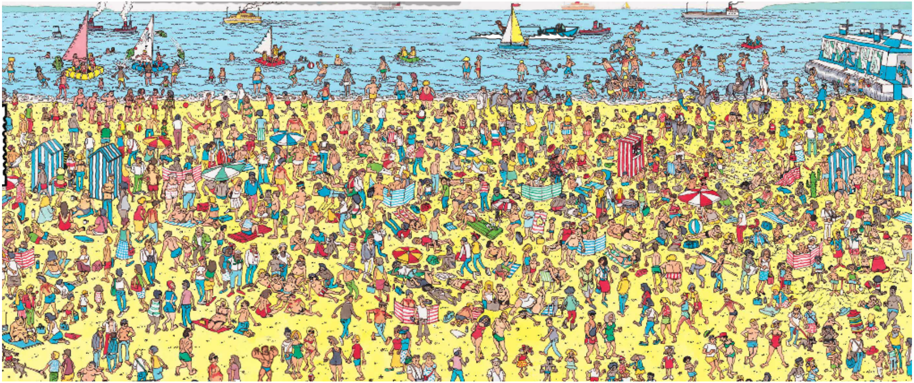
EUMAS, 16/12/2016

Context and Motivation

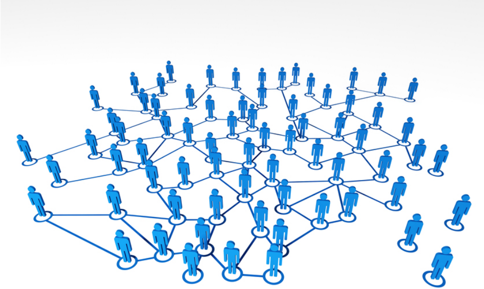


- Where is Wally?
- Who is Wally?

Context and Motivation

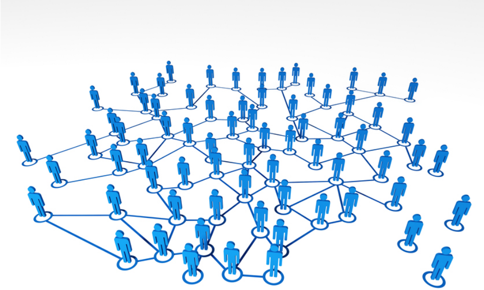


Context and Motivation



- Where is the malicious agent?
- What is a malicious agent?

Context and Motivation



- Where is the malicious agent?
- What is a malicious agent?

Research questions

- How can we define an agent in a MAS?
- How many different type of agents can we define in a MAS?

Background: Multiple-channel logic (MCL)

MCL is a labeled, modal logic framework

- Propositional calculus to express what agents share (the logical representation of an assertion)

$$\varphi := A \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi$$

- B (*belief*), to assert that an agent **believes** that a proposition is true,
- $T_\Box$ and $T_\Diamond$ If a proposition is *asserted* by an agent respectively in every **channel** or at least one channel.

$$\mu := \mathrm{B}[\lambda : \varphi] \mid \mathrm{T}_\Box[\lambda : \varphi] \mid \mathrm{T}_\Diamond[\lambda : \varphi] \mid \sim\mu$$

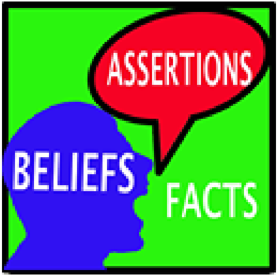
Example

- $\varphi =$Valencia is in Spain
- $\mathrm{B}[\text{Wally} : \varphi]$, Wally believes that Valencia is in Spain
- $\mathrm{T}_\Diamond[\text{Wally} : \varphi]$, Wally says on Facebook that Valencia is in Spain
- $\mathrm{T}_\Box[\text{Wally} : \varphi]$, Wally says on Facebook, Twitter, . . . that Valencia is in Spain

Reasoning on agents

The three main elements to reason on agents in MCL are:

- *Announcements* $\mathbb{A}_\lambda = \{\varphi.\mathrm{T}_\diamond[\lambda : \varphi]\}$ one or more channels.
- *Beliefs* $\mathbb{B}_\lambda = \{\varphi.\mathrm{B}[\lambda : \varphi]\}$ is the set of the formulae believed to be true by an agent
- *Facts* $\mathbb{F}$ is the set of *axiomatic* formulae.



Categorization of Agents ($\mathbb{A}_\lambda$,$\mathbb{B}_\lambda$,$\mathbb{F}$ Permutations)

$(\mathbb{A}_\lambda, \mathbb{B}_\lambda)$

- The relation between Beliefs and announcements of an agent λ.
- *Collaboration* as a *quantity* of data announced.

E.g. if an agent asserts everything he Believes, he is collaborative

$(\mathbb{B}_\lambda, \mathbb{F})$

- The relation between Beliefs of an agent λ and true facts.
- *Competence* of λ as the *quality* of data an agent produces.

E.g. if everything an agent Believes is also true, he is competent

$(\mathbb{A}_\lambda, \mathbb{F})$

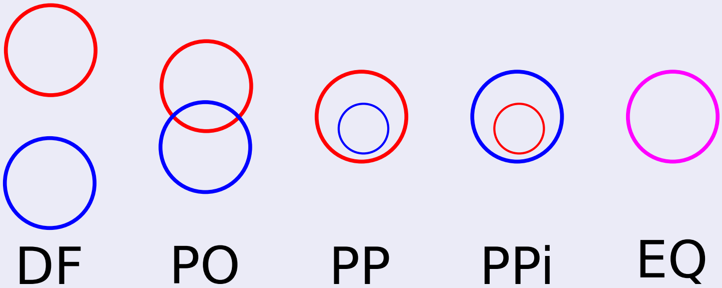
- The relation between announcements of the agent λ and true facts.
- Defines the level of *Honesty* of λ.

E.g. If everything an agent shares on a channel is true, then he is honest.

RCC and Definition of agent

- How many different relations can we define over the three pair of sets?
- If we consider each set as a spacial region we can use RCC-5 (Region Connection Calculus)
- RCC is an axiomatization of certain spacial concept and relation in first order logic

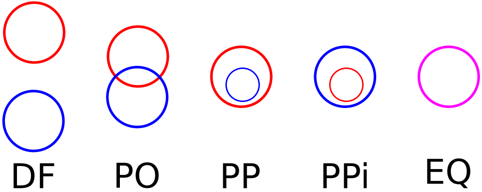
RCC-5 relations between spatial regions X, Y and Z (P = Part of)



RCC and Definition of agent

Agent tagging

$(\mathbb{A}_\lambda, \mathbb{B}_\lambda)$	$(\mathbb{B}_\lambda, \mathbb{F})$	$(\mathbb{A}_\lambda, \mathbb{F})$
$DR(\mathbb{A}_\lambda, \mathbb{B}_\lambda)$Braggart	$DR(\mathbb{B}_\lambda, \mathbb{F})$ Ignorant	$DR(\mathbb{A}_\lambda, \mathbb{F})$ False
$PO(\mathbb{A}_\lambda, \mathbb{B}_\lambda)$ Saboteur	$PO(\mathbb{B}_\lambda, \mathbb{F})$ Incompetent	$PO(\mathbb{A}_\lambda, \mathbb{F})$ Incorrect
$PP(\mathbb{A}_\lambda, \mathbb{B}_\lambda)$ Sincere	$PP(\mathbb{B}_\lambda, \mathbb{F})$ Competent	$PP(\mathbb{A}_\lambda, \mathbb{F})$ Honest
$PPi(\mathbb{A}_\lambda, \mathbb{B}_\lambda)$ Collaborative	$PPi(\mathbb{B}_\lambda, \mathbb{F})$ Omniscient	$PPi(\mathbb{A}_\lambda, \mathbb{F})$ Oracle
$EQ(\mathbb{A}_\lambda, \mathbb{B}_\lambda)$ Fair	$EQ(\mathbb{B}_\lambda, \mathbb{F})$ Wise	$EQ(\mathbb{A}_\lambda, \mathbb{F})$ Right



RCC and Definition of agent

RCC-5 relations between spatial regions X, Y and Z (P = Part of)

Name	Notation	Definition
Equal to	$EQ(X, Y)$	$P(X, Y) \wedge P(Y, X)$
DiscRete from	$DR(X, Y)$	$\neg O(X, Y)$
Partial-Overlap	$PO(X, Y)$	$O(X, Y) \wedge \neg P(X, Y) \wedge \neg P(Y, X)$
Proper-part-of	$PP(X, Y)$	$P(X, Y) \wedge \neg P(Y, X)$
Proper-part-of-inverse	$PPi(X, Y)$	$P(Y, X) \wedge \neg P(X, Y)$

Type of agent: defined by a tuple

$$Agent = \langle RCC5_1(\mathbb{A}_\lambda, \mathbb{B}_\lambda), RCC5_2(\mathbb{B}_\lambda, \mathbb{F}), RCC5_3(\mathbb{F}, \mathbb{A}_\lambda)\rangle$$

where $RCC5_1$, $RCC5_2$ and $RCC5_3$ are relations in RCC-5.

$$E.g., \; Agent_1 = \langle EQ(\mathbb{A}_\lambda, \mathbb{B}_\lambda), EQ(\mathbb{B}_\lambda, \mathbb{F}), EQ(\mathbb{F}, \mathbb{A}_\lambda)\rangle$$

How many agents?

Research questions

- ✓ How can we define an agent in a MAS?
- How many different type of agents can we define in a MAS?

- Hence, applying RCC over $\mathbb{A}_\lambda, \mathbb{B}_\lambda, \mathbb{F}$, we obtain a definite number of different types of agents.
- Some combinations of $RCC5_1$, $RCC5_2$ and $RCC5_3$ are topologically incorrect (e.g., $\mathbb{A}_\lambda = \mathbb{B}_\lambda$, $\mathbb{A}_\lambda = \mathbb{F}$, $\mathbb{B}_\lambda \neq \mathbb{F}$)

	Theoretical	**Correct**
RCC-3	$3^3 = 27$	15
RCC-5	$5^3 = 125$	54
RCC-8	$8^3 = 512$	193

Figure: Number of agents with respect to different RCC

We identify a theoretical limit to the maximum number of different types of agents in a MAS (defined using MCL)

How many agents?

Research questions

✓ How can we define an agent in a MAS?

✓ How many different type of agents can we define in a MAS?

- Hence, applying RCC over $\mathbb{A}_\lambda, \mathbb{B}_\lambda, \mathbb{F}$, we obtain a definite number of different types of agents.
- Some combinations of $RCC5_1$, $RCC5_2$ and $RCC5_3$ are topologically incorrect (e.g., $\mathbb{A}_\lambda = \mathbb{B}_\lambda$, $\mathbb{A}_\lambda = \mathbb{F}$, $\mathbb{B}_\lambda \neq \mathbb{F}$)

	Theoretical	**Correct**
RCC-3	$3^3 = 27$	15
RCC-5	$5^3 = 125$	54
RCC-8	$8^3 = 512$	193

Figure: Number of agents with respect to different RCC

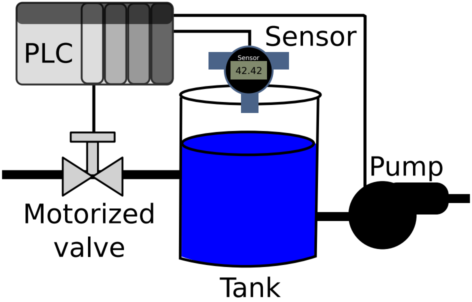
We identify a theoretical limit to the maximum number of different types of agents in a MAS (defined using MCL)

Case studies?

Marvin Minsky - MIT Media Lab 30th anniversary

CPS

- Systems that consist of networked embedded systems, which are used to sense, actuate, and control physical processes
- Examples: industrial water treatment facilities, electrical power plants, public transportation infrastructure, or even smart cars.



Case study

I apply our topological categorization to define attack states for a MAS that describes a general CPS. I can summarize our mapping as follows:

- $\mathbb{A}_\lambda$ defines the values communicated by the agent λ.
- $\mathbb{B}_\lambda$ defines the computational results of the agent λ.
- $\mathbb{F}$ defines the environmental values, i.e., the real values of the system.

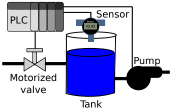


Figure: Representation of the test case

Table: Example of attack states for the water level sensor

State of the sensor	$(\mathbb{A}, \mathbb{B})$	$(\mathbb{B}, \mathbb{F})$	**honesty** $(\mathbb{A}, \mathbb{F})$
optimal	EQ	EQ	EQ
sensor compromised	EQ	DR	**DR**
communication compromised	DR	EQ	**DR**
fully compromised	DR	DR	**DR**

One of the most difficult task is to define all the different attack state of a System.

Summary

Categorization of Agents in MCL

1. We defined a topological categorization of agents in MAS, obtaining 50 new rules in the MCL framework.
2. We identified a theoretical limit to the maximum number of different types of agents in a MAS (defined using MCL).
3. A case study on the security of CPS and, more generally, MAS.

Thank you.
Any questions?