Reconfiguration of large-scale surveillance systems

(reconfiguration in Metis)

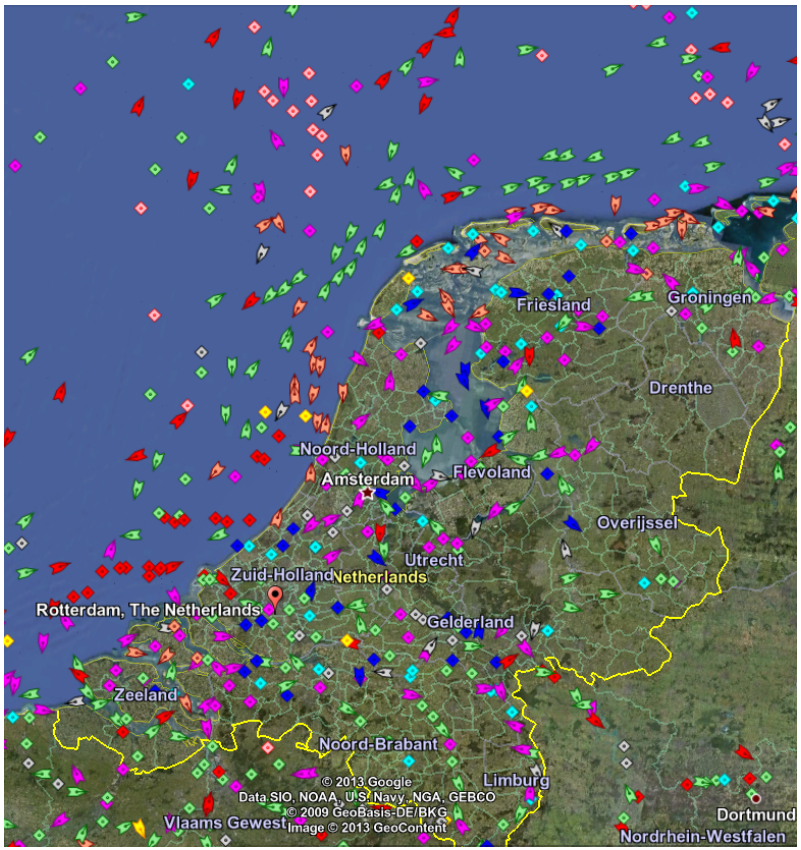
Peter Novák (with Cees Witteveen)

Algorithmics, EEMCS, Delft University of Technology

Motivation: Metis project

Metis

Continuous monitoring of a maritime coastal zone, detection of anomalies and malicious activities of vessels.

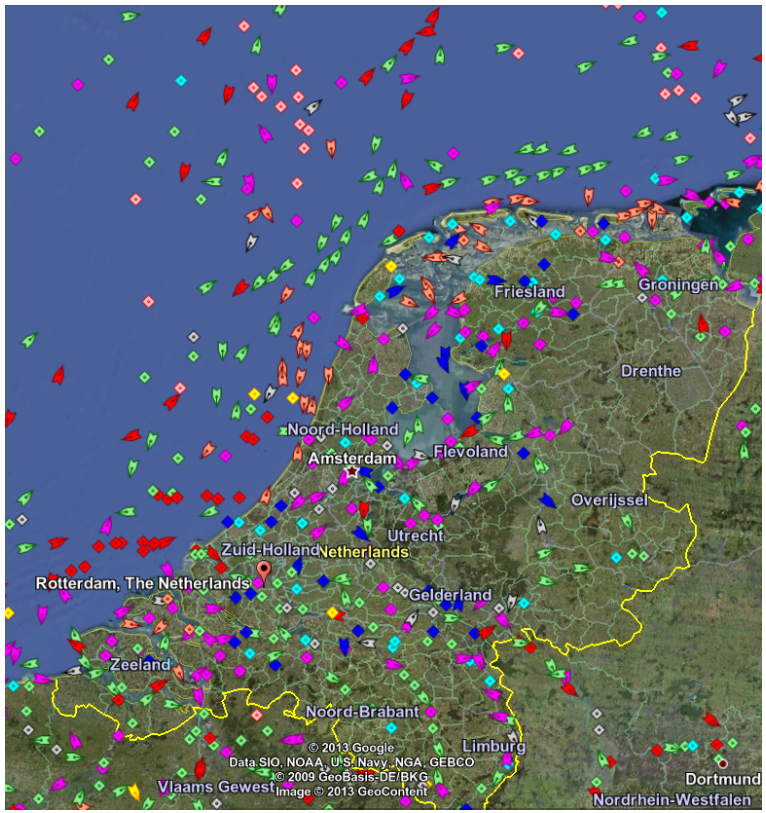


Motivation: Metis project

Metis

Continuous monitoring of a maritime coastal zone, detection of anomalies and malicious activities of vessels.

- thousands of vessels
- dozens of info-sources per ship



Problem

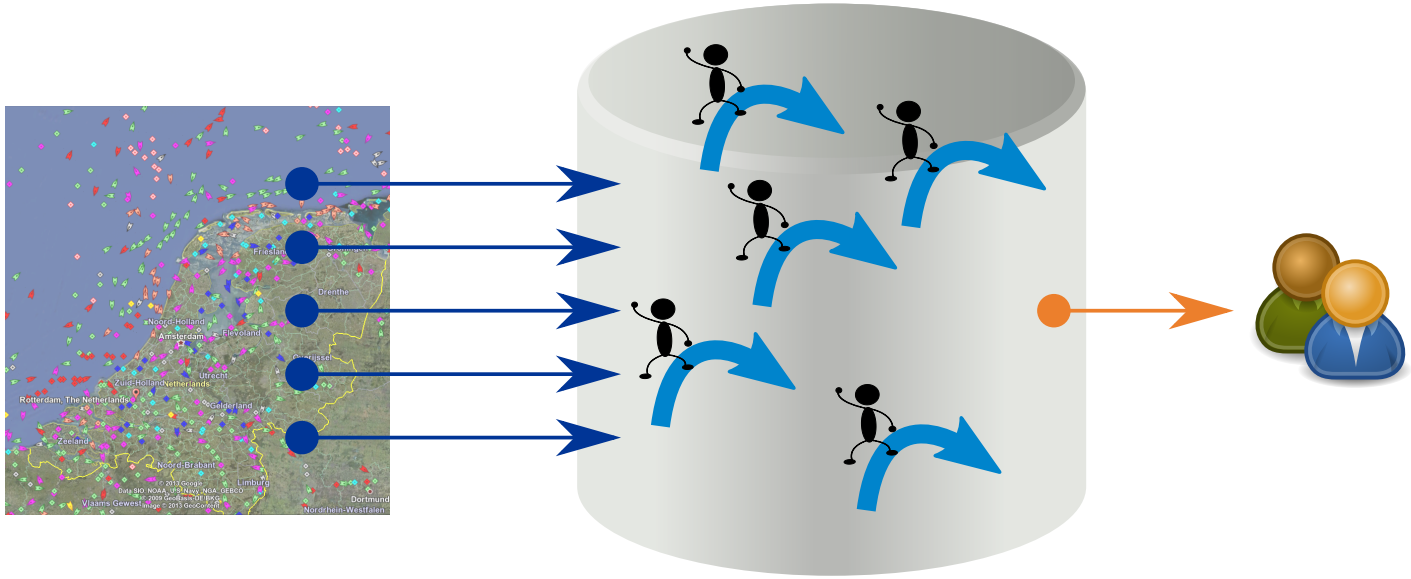
Scalability of the system!

Solution idea

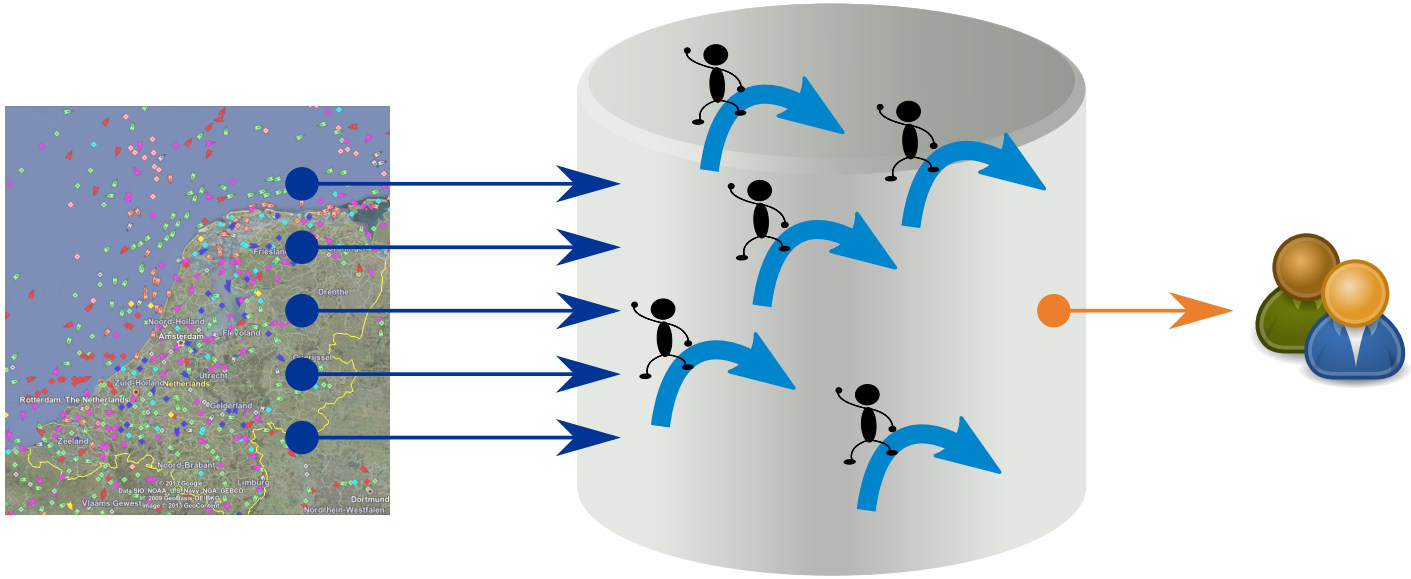
Run-time reconfiguration between vessel run-levels.

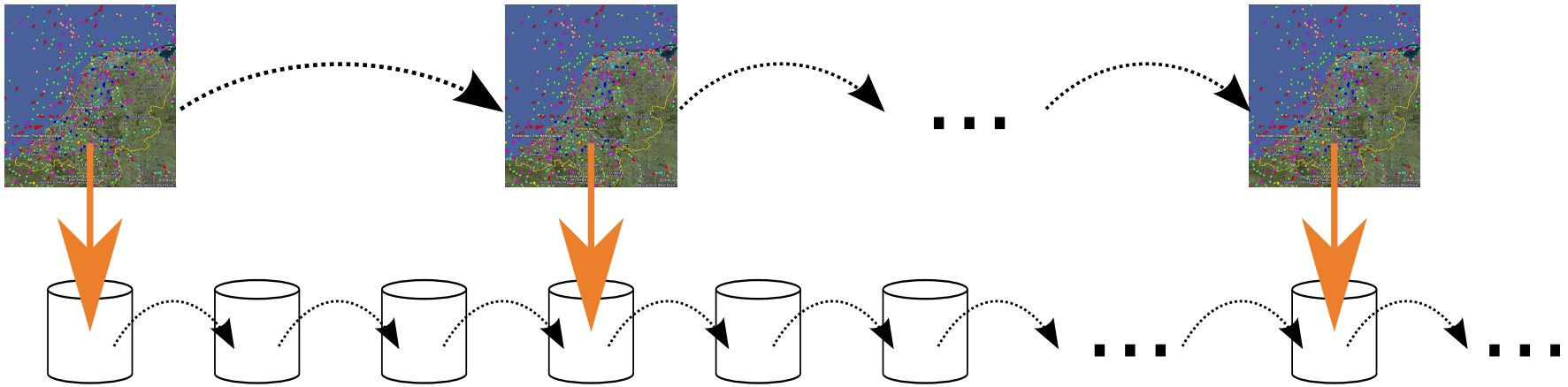
Talk outline

Info-aggregation system: scheme



Info-aggregation system: scheme





Info-aggregation system: definition

information-aggregation system $\mathcal{S} = (\mathcal{A}, \mathcal{D}, cost)$

database D: a set of variable valuations $\{x \mapsto \{\top, \bot, \varnothing\}\}$

agents $\mathcal{A}$: database updating function objects $A : D \mapsto D'$

$cost : \mathcal{A} \to \mathbb{R}^+$: cost of executing an agent

configuration C of $\mathcal{S}$

$C \subseteq \mathcal{A}$ a set of agents of $\mathcal{S}$

Notation

in_A, out_A input/output variables of an agent A

$D|x$, $D|in_A$ valuation of a variable/set of variables in D

Database evolution

update of a database D by a configuration C

$D' = C(D)$ iff D' *is a result of computation of some agent from* C

- for each variable x:
  $D|x \neq D'|x$ implies $D'|x = A(D|in_A)|x$ for some agent $A \in C$

Database evolution

update of a database D by a configuration C

$D' = C(D)$ iff D' *is a result of computation of some agent from* C

- ⇝ for each variable x:
  $D|x \neq D'|x$ implies $D'|x = A(D|in_A)|x$ for some agent $A \in C$

database evolution and stabilisation

evolution $\lambda = D_0, \ldots, D_k, \ldots$: for all i, $D_{i+1} = C(D_i)$

normal configuration $C \subseteq \mathcal{A}$: all C-evolutions of $\mathcal{S}$ from some D_0 on, eventually reach *the same* fixpoint

- ⇝ $C^*(D_0) = D^* = C(D^*)$
- ⇝ computations of all agents are reflected in D^*:
  $A(D^*|in_A) \subseteq D^*$ and $A(D^*|out_A) \subseteq D^*$

Environment

environment

$\mathcal{E}$ a database schema

evolution a sequence of $\mathcal{E}$ snapshots $\lambda_{\mathcal{E}} = E_0, E_1, \ldots, E_k, \ldots$

Environment

environment

$\mathcal{E}$ a database schema

evolution a sequence of $\mathcal{E}$ snapshots $\lambda_{\mathcal{E}} = E_0, E_1, \ldots, E_k, \ldots$

system embedded in an environment

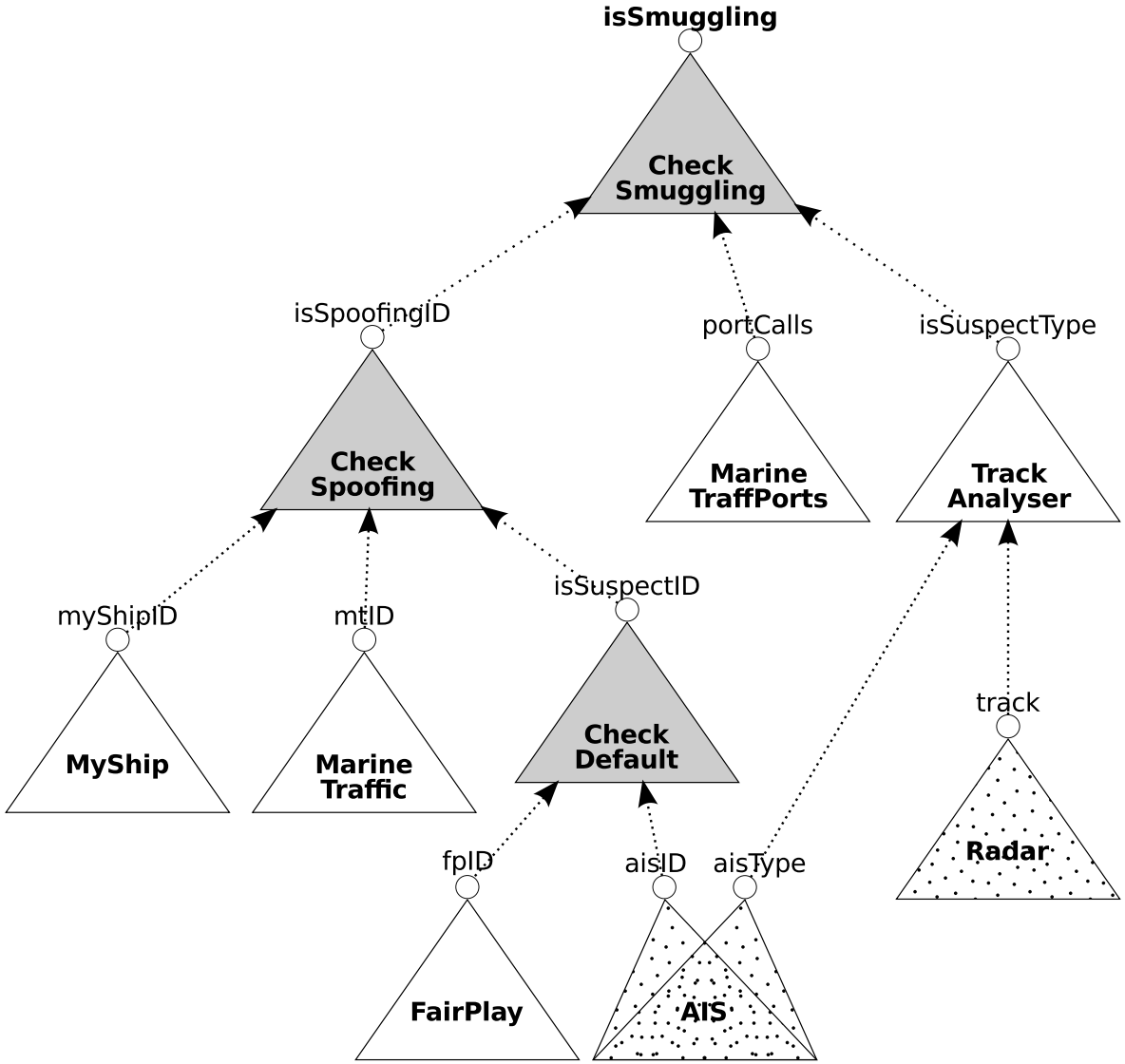
information-source agents: no input variables/output variables are shared with the environment

$\rightsquigarrow$ $in_A = \emptyset$ implies $out_A \subseteq \mathcal{D}^{\mathcal{E}}_{in} = \mathcal{E} \cap \mathcal{D}$

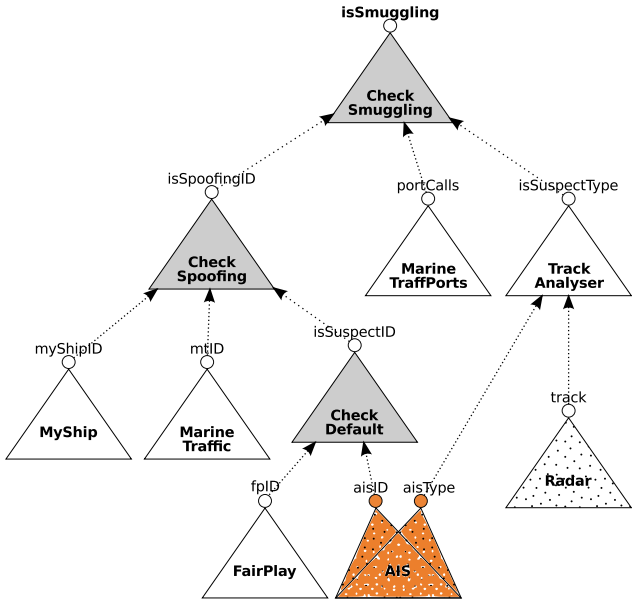
information-aggregating agents: $in_A \neq \emptyset$ and $out_A \neq \emptyset$

embedding of $\mathcal{S}$ in E: computations of information-source agents reflect the state of the environment

Metis info-aggregation system



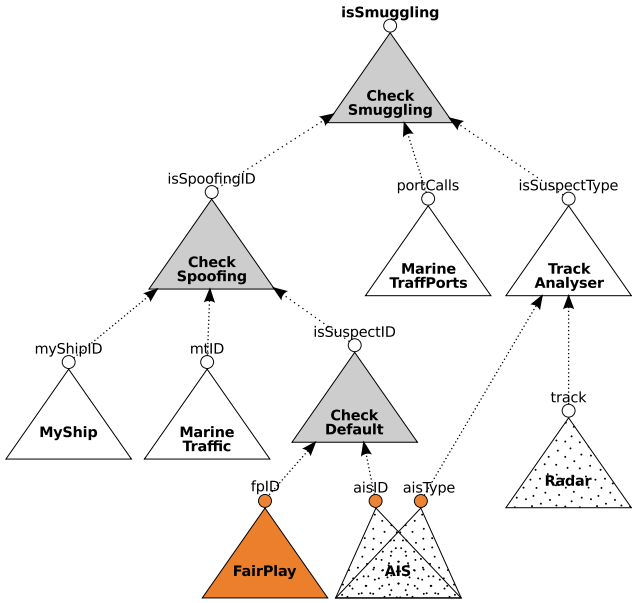
Metis info-aggregation system



D_0

$\mathbf{D_0}, \mathbf{E_0}$ (stable)	$\mathbf{D_1}$	$\mathbf{D_2}$ (stable)	$\mathbf{D_3}, \mathbf{E_1}$	$\mathbf{D_4}$ (stable)	$\mathbf{D_5}, \mathbf{E_2}$	$\mathbf{D_6}$ (stable)
$\text{aisID}^{\mathcal{E}}$	aisID	aisID	$\text{aisID}^{\mathcal{E}}$	aisID		
$\text{aisType}^{\mathcal{E}}$	aisType	aisType	$\text{aisType}^{\mathcal{E}}$	aisType	$\text{aisType}^{\mathcal{E}}$	aisType
	fpID	fpID	fpID	fpID	fpID	fpID
		isSuspectID	isSuspectID	isSuspectID	isSuspectID	
			$\text{track}^{\mathcal{E}}$	track	$\text{track}^{\mathcal{E}}$	track
				isSuspectType	isSuspectType	isSuspectType

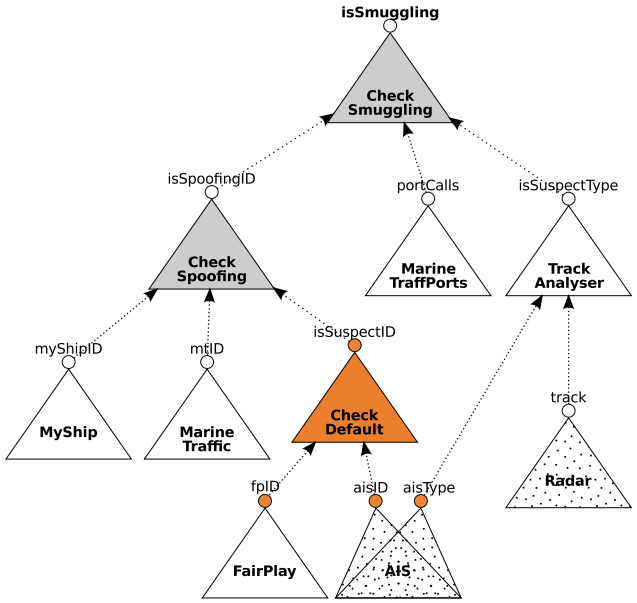
Metis info-aggregation system



D_1

$\mathbf{D_0}, \mathbf{E_0}$ (stable)	$\mathbf{D_1}$	$\mathbf{D_2}$ (stable)	$\mathbf{D_3}, \mathbf{E_1}$	$\mathbf{D_4}$ (stable)	$\mathbf{D_5}, \mathbf{E_2}$	$\mathbf{D_6}$ (stable)
$\text{aisID}^{\mathcal{E}}$	aisID	aisID	$\text{aisID}^{\mathcal{E}}$	aisID		
$\text{aisType}^{\mathcal{E}}$	aisType	aisType	$\text{aisType}^{\mathcal{E}}$	aisType	$\text{aisType}^{\mathcal{E}}$	aisType
	fpID	fpID	fpID	fpID	fpID	fpID
		isSuspectID	isSuspectID	isSuspectID	isSuspectID	
			$\text{track}^{\mathcal{E}}$	track	$\text{track}^{\mathcal{E}}$	track
				isSuspectType	isSuspectType	isSuspectType

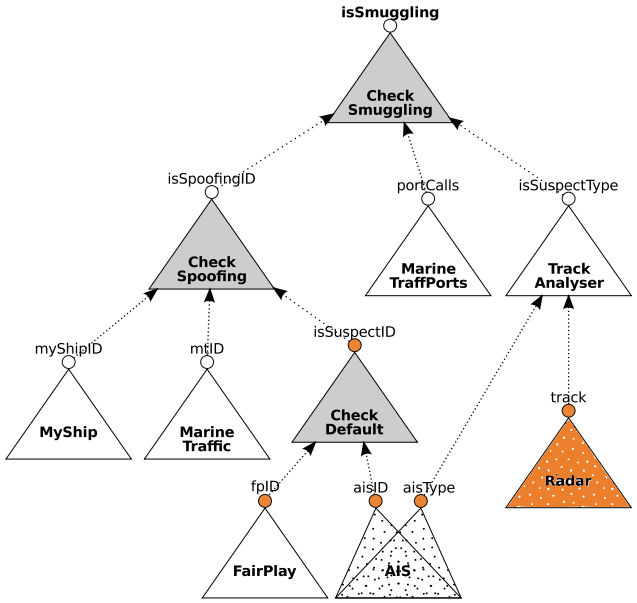
Metis info-aggregation system



D_2

$\mathbf{D_0}, \mathbf{E_0}$ (stable)	$\mathbf{D_1}$	$\mathbf{D_2}$ (stable)	$\mathbf{D_3}, \mathbf{E_1}$	$\mathbf{D_4}$ (stable)	$\mathbf{D_5}, \mathbf{E_2}$	$\mathbf{D_6}$ (stable)
aisID$^{\mathcal{E}}$	aisID	aisID	aisID$^{\mathcal{E}}$	aisID		
aisType$^{\mathcal{E}}$	aisType	aisType	aisType$^{\mathcal{E}}$	aisType	aisType$^{\mathcal{E}}$	aisType
	fpID	fpID	fpID	fpID	fpID	fpID
		isSuspectID	isSuspectID	isSuspectID	isSuspectID	
			track$^{\mathcal{E}}$	track	track$^{\mathcal{E}}$	track
				isSuspectType	isSuspectType	isSuspectType

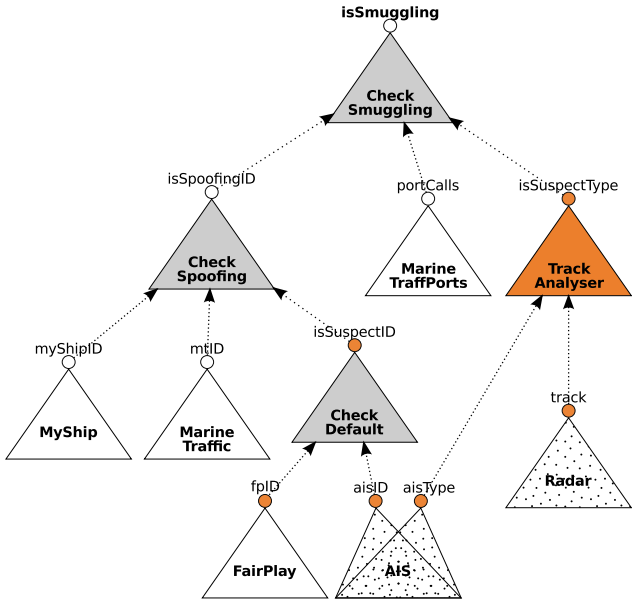
Metis info-aggregation system



D_3

$\mathbf{D_0}, \mathbf{E_0}$ (stable)	$\mathbf{D_1}$	$\mathbf{D_2}$ (stable)	$\mathbf{D_3}, \mathbf{E_1}$	$\mathbf{D_4}$ (stable)	$\mathbf{D_5}, \mathbf{E_2}$	$\mathbf{D_6}$ (stable)
aisID$^{\mathcal{E}}$	aisID	aisID	aisID$^{\mathcal{E}}$	aisID		
aisType$^{\mathcal{E}}$	aisType	aisType	aisType$^{\mathcal{E}}$	aisType	aisType$^{\mathcal{E}}$	aisType
	fpID	fpID	fpID	fpID	fpID	fpID
		isSuspectID	isSuspectID	isSuspectID	isSuspectID	
			track$^{\mathcal{E}}$	track	track$^{\mathcal{E}}$	track
				isSuspectType	isSuspectType	isSuspectType

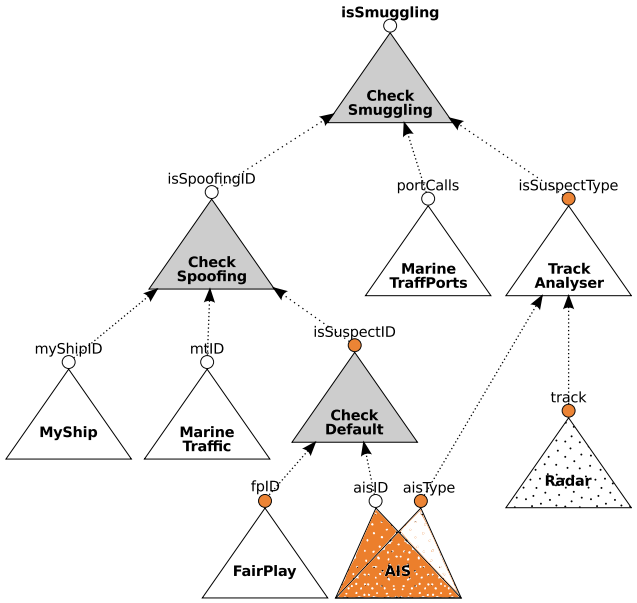
Metis info-aggregation system



D_4

$\mathbf{D_0}, \mathbf{E_0}$ (stable)	$\mathbf{D_1}$	$\mathbf{D_2}$ (stable)	$\mathbf{D_3}, \mathbf{E_1}$	$\mathbf{D_4}$ (stable)	$\mathbf{D_5}, \mathbf{E_2}$	$\mathbf{D_6}$ (stable)
aisID$^{\mathcal{E}}$	aisID	aisID	aisID$^{\mathcal{E}}$	aisID		
aisType$^{\mathcal{E}}$	aisType	aisType	aisType$^{\mathcal{E}}$	aisType	aisType$^{\mathcal{E}}$	aisType
	fpID	fpID	fpID	fpID	fpID	fpID
		isSuspectID	isSuspectID	isSuspectID	isSuspectID	
			track$^{\mathcal{E}}$	track	track$^{\mathcal{E}}$	track
				isSuspectType	isSuspectType	isSuspectType

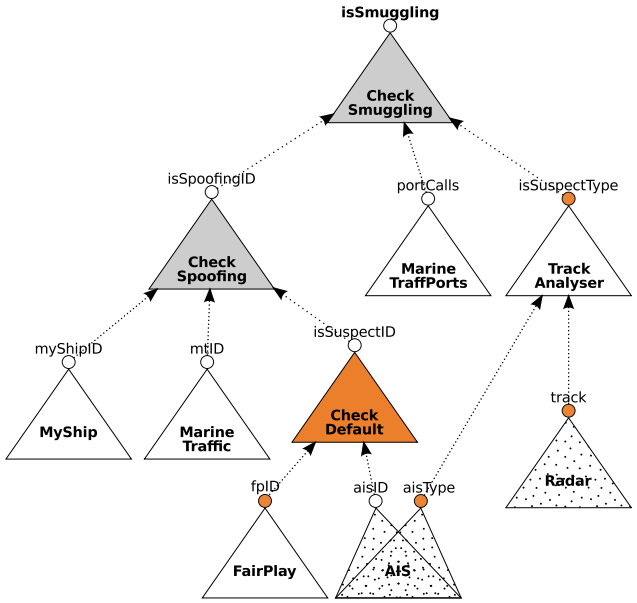
Metis info-aggregation system



D_5

$\mathbf{D_0}, \mathbf{E_0}$ (stable)	$\mathbf{D_1}$	$\mathbf{D_2}$ (stable)	$\mathbf{D_3}, \mathbf{E_1}$	$\mathbf{D_4}$ (stable)	$\mathbf{D_5}, \mathbf{E_2}$	$\mathbf{D_6}$ (stable)
aisID$^{\mathcal{E}}$	aisID	aisID	aisID$^{\mathcal{E}}$	aisID		
aisType$^{\mathcal{E}}$	aisType	aisType	aisType$^{\mathcal{E}}$	aisType	aisType$^{\mathcal{E}}$	aisType
	fpID	fpID	fpID	fpID	fpID	fpID
		isSuspectID	isSuspectID	isSuspectID	isSuspectID	
			track$^{\mathcal{E}}$	track	track$^{\mathcal{E}}$	track
				isSuspectType	isSuspectType	isSuspectType

Metis info-aggregation system



D_6

$\mathbf{D_0}, \mathbf{E_0}$ (stable)	$\mathbf{D_1}$	$\mathbf{D_2}$ (stable)	$\mathbf{D_3}, \mathbf{E_1}$	$\mathbf{D_4}$ (stable)	$\mathbf{D_5}, \mathbf{E_2}$	$\mathbf{D_6}$ (stable)
$\text{aisID}^{\mathcal{E}}$	aisID	aisID	$\text{aisID}^{\mathcal{E}}$	aisID		
$\text{aisType}^{\mathcal{E}}$	aisType	aisType	$\text{aisType}^{\mathcal{E}}$	aisType	$\text{aisType}^{\mathcal{E}}$	aisType
	fpID	fpID	fpID	fpID	fpID	fpID
		isSuspectID	isSuspectID	isSuspectID	isSuspectID	
			$\text{track}^{\mathcal{E}}$	track	$\text{track}^{\mathcal{E}}$	track
				isSuspectType	isSuspectType	isSuspectType

Research question

Which information sources?

Which aggregators?

Detect malicious intents early and cost-efficiently!

Research question

Which information sources?

Which aggregators?

Detect malicious intents early and cost-efficiently!

Security-related systems:

- answer distinguished queries (*isSmuggling?*)
- presumption of innocence: conclusions must be justified

Configuration problem

configuration problem $\mathfrak{C} = (\mathcal{S}, \phi, D)$

$\mathcal{S} = (\mathcal{A}, \mathcal{D})$ information-aggregation system

$\phi \in \mathcal{D}$ query variable

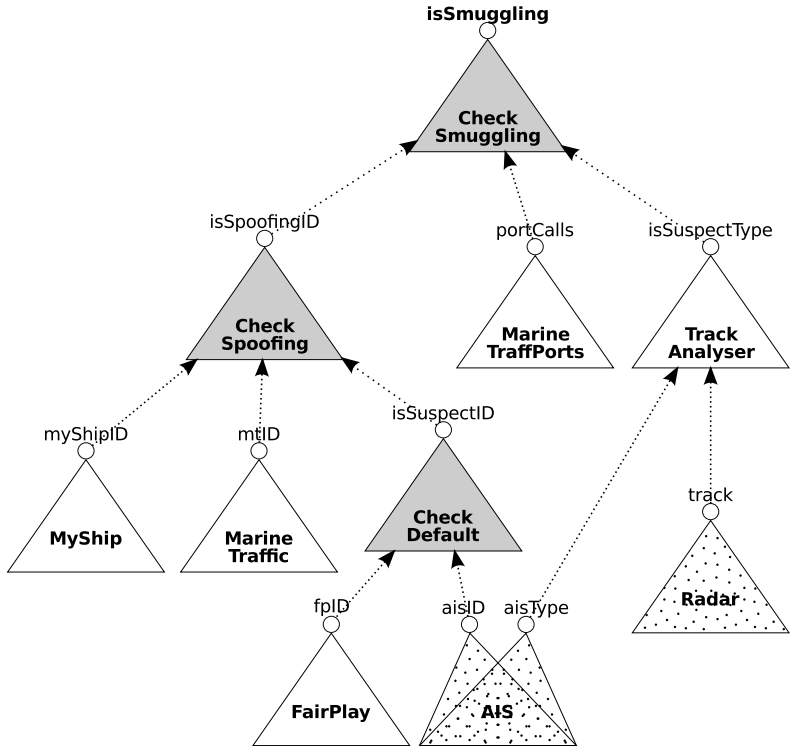
D initial snapshot of $\mathcal{D}$.

solution configuration $C \subseteq \mathcal{A}$

- normal: all C-evolutions eventually stabilise in $C^*(D)$
- computes a query solution: $\phi \in out_C$
- no doubt about query solution: C is maximal, i.e., there is no C' with $C \subset C'$ satisfying the above concluding different $D|\phi$
- conclusions are justified: all input variables of C are also computed by C and crisply valued

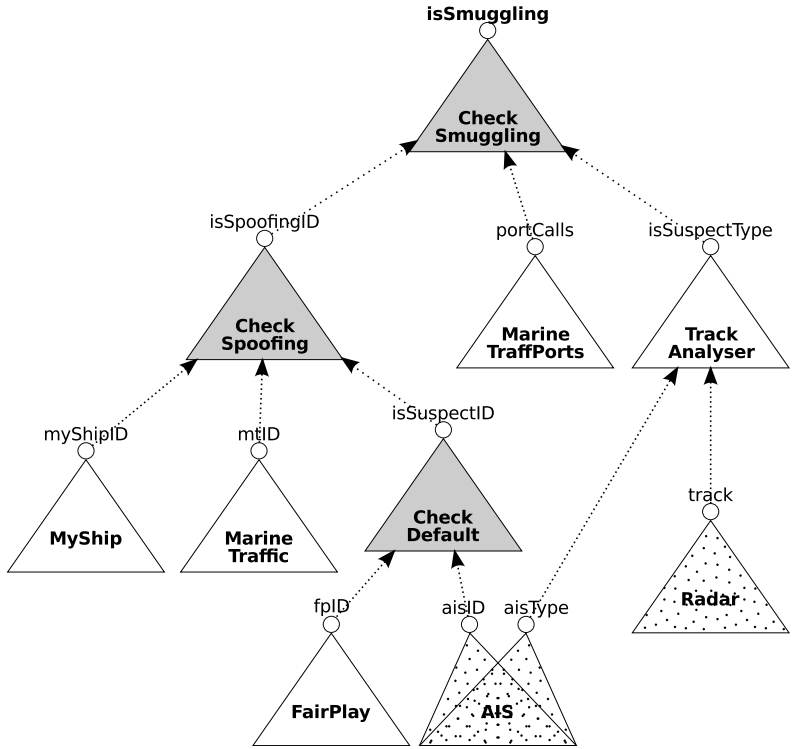
$\rightsquigarrow$ *optimal* solution is the cheapest one!

Metis example



- query: *isSmuggling?*

Metis example



- query: *isSmuggling?*
- solution: all info-sources + all info-aggregators

Reconfiguration problem

reconfiguration problem $\mathfrak{R} = (\lambda_{\mathcal{E}}, \mathcal{S}, \phi)$

$\lambda_{\mathcal{E}} = E_0, \ldots, E_k, \ldots$ evolution of an environment $\mathcal{E}$

$\mathcal{S} = (\mathcal{A}, \mathcal{D})$ information-aggregation system embedded in $\mathcal{E}$

$\phi \in \mathcal{D}$ query variable

solution configuration sequence $C_0, \ldots, C_l, \ldots$

each C_i is a solution to $\mathfrak{C}_i = (\mathcal{S}, \phi, D_i)$ and $\mathcal{S}$ reflects $\mathcal{E}$

- $D_0 = D_\varnothing \oplus E_0|\mathcal{D}^{\mathcal{E}}_{in}$
- $D_i = C^*_{i-1}(D_{i-1}) \ \oplus \ E_i|\mathcal{D}^{\mathcal{E}}_{in}$

weak solution

C_i is a solution to $\mathfrak{C}_i = (\mathcal{S}, \phi, D_i)$ only if it exists

Abstract argumentation

defeasible logical inference in terms of interdependencies of arguments, rather than their internal structure

argument: an abstract entity determined solely by its relations to other arguments (*blackbox*)

semantics: a set of coherent arguments, an extension

argumentation framework $AF = (\mathcal{A}, attack)$

$\mathcal{A}$ a set of arguments

$attack$ an attack relation $\mathcal{A} \times \mathcal{A}$

Info-aggregation as argumentation $(\mathcal{S}, D)$

configuration argumentation framework $CAF = \langle \mathcal{A}, attack \rangle$

arguments agents of a system $\mathcal{S} = (\mathcal{A}, \mathcal{D})$

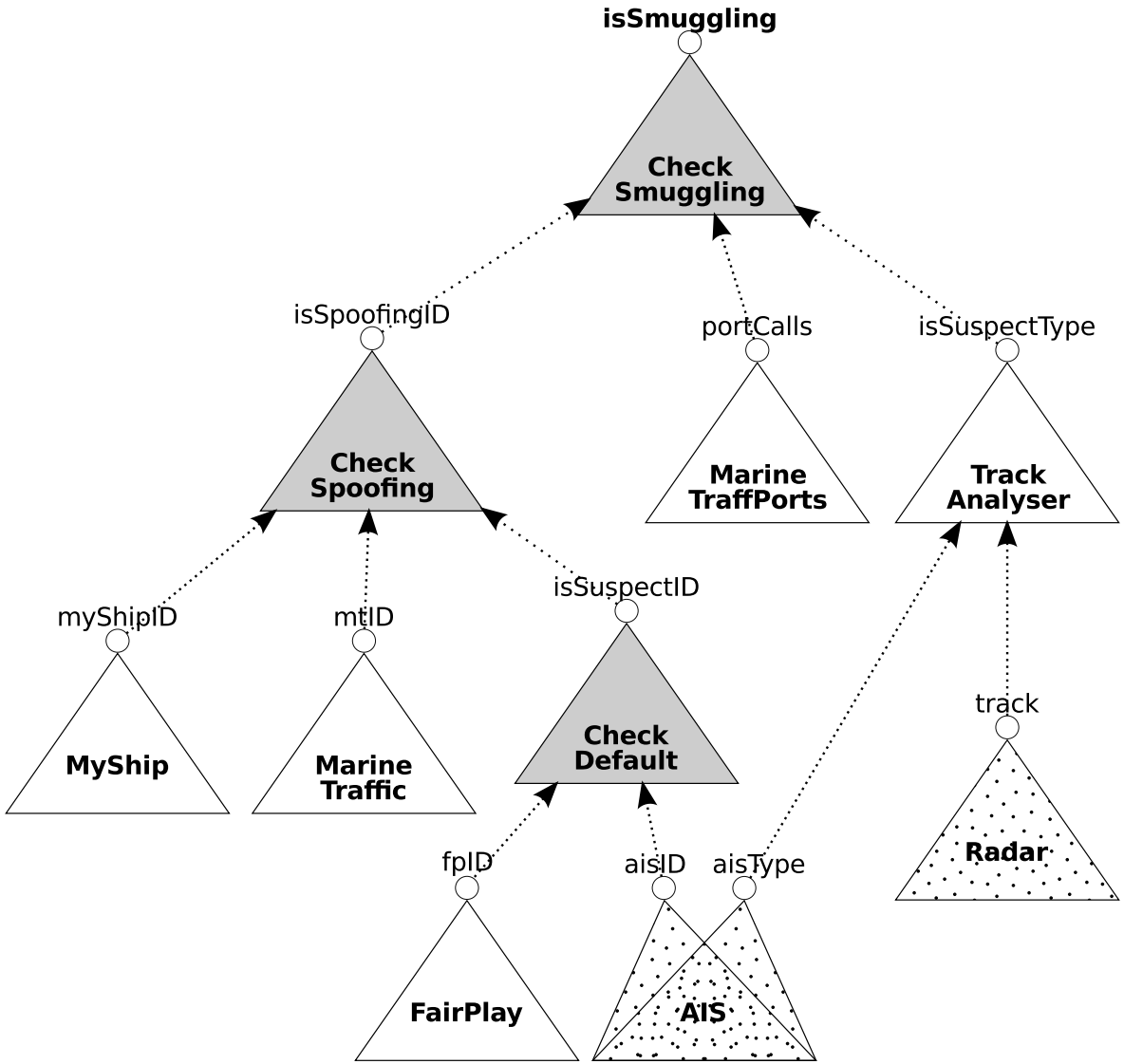
attack A *attacks* A' when it disagrees with an output of A' in D

- $\rightsquigarrow$ there exists $x \in out_A \cap out_{A'}$, s.t., $A(D|in_A)|x \neq \varnothing$ and $A(D|in_A)|x \neq A'(D|in_{A'})|x$

valid arguments input is crisply valued and supported by $\mathcal{D}$

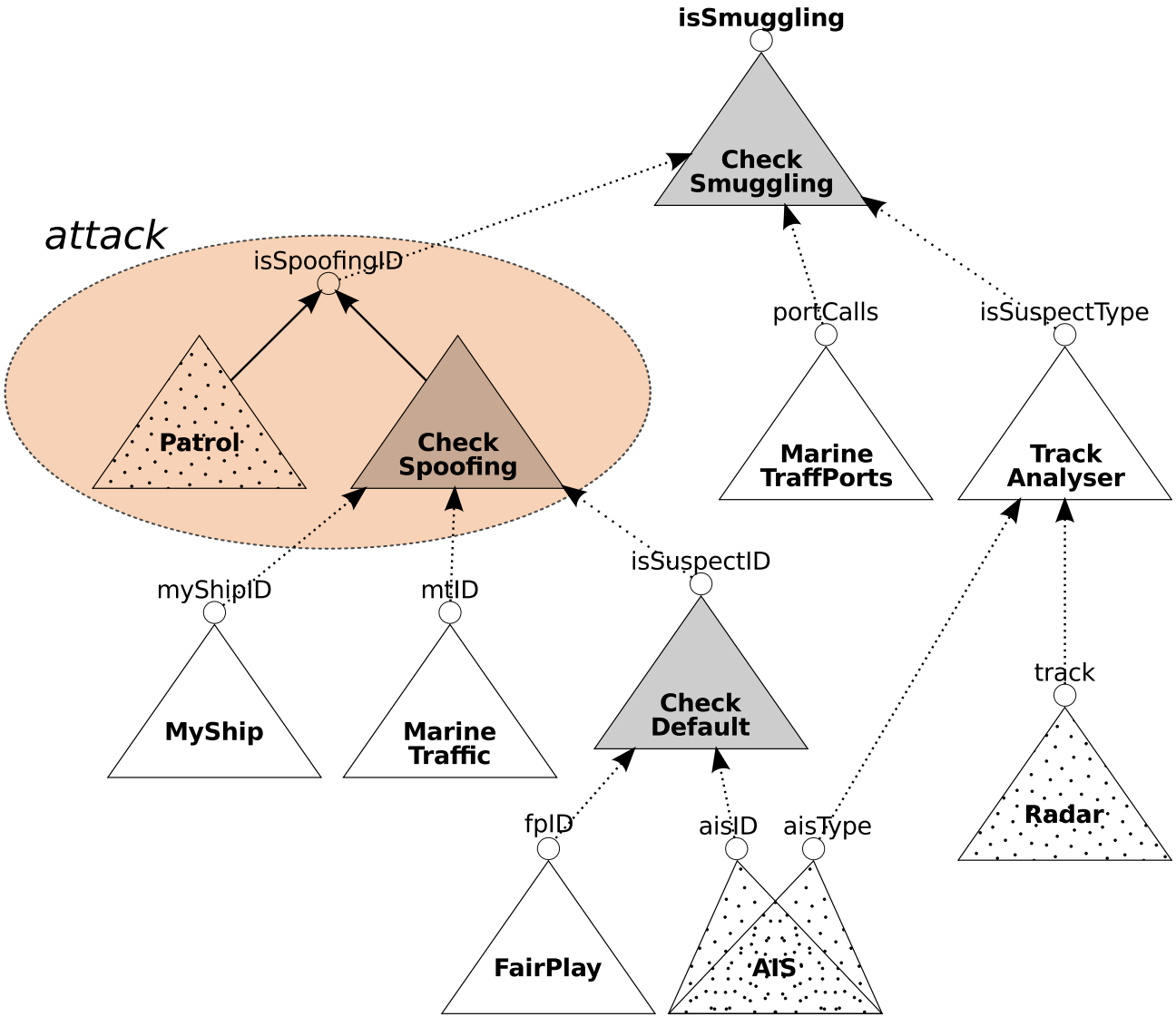
Metis argumentation

A natural fit!



Metis argumentation

A natural fit!



Sceptical argumentation

cautiously infer only justified & non-controversial conclusions!

incremental extension construction

A valid argument A is acceptable to a conflict-free C iff

- A does not attack any other argument, or
- if A attacks A', then C already attacks A' and thus supports A

valid argument input is crisply valued and supported by $\mathcal{D}$

Sceptical argumentation

cautiously infer only justified & non-controversial conclusions!

incremental extension construction

A valid argument A is acceptable to a conflict-free C iff

- A does not attack any other argument, or
- if A attacks A', then C already attacks A' and thus supports A

valid argument input is crisply valued and supported by $\mathcal{D}$

grounded extension of CAF over $\mathcal{S}$ and D

$GE_{CAF} = F^*_{CAF}(\emptyset)$ the least fix-point of

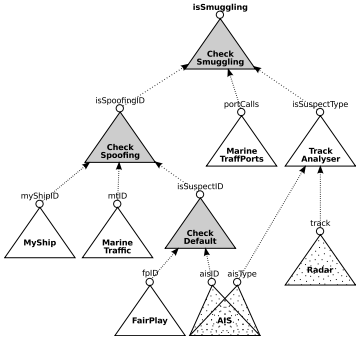
$$F_{CAF}(C) = \{A \mid A \in \mathcal{A} \text{ is acceptable to } C\}$$

$\rightsquigarrow$ preserves presumption of innocence!

Configuration as sceptical argumentation

issue: grounded extension always exists, *but sometimes multiple*

solution: acyclic/stratified systems
$\rightsquigarrow$ hierarchical (lattice) structure!



Theorem (config. problem $\mathfrak{C} = (\mathcal{S}, \phi, D)$, with stratified $\mathcal{S}$)

Let C be the grounded extension of $CAF_{\mathfrak{C}}$ over $C^*(D)$.

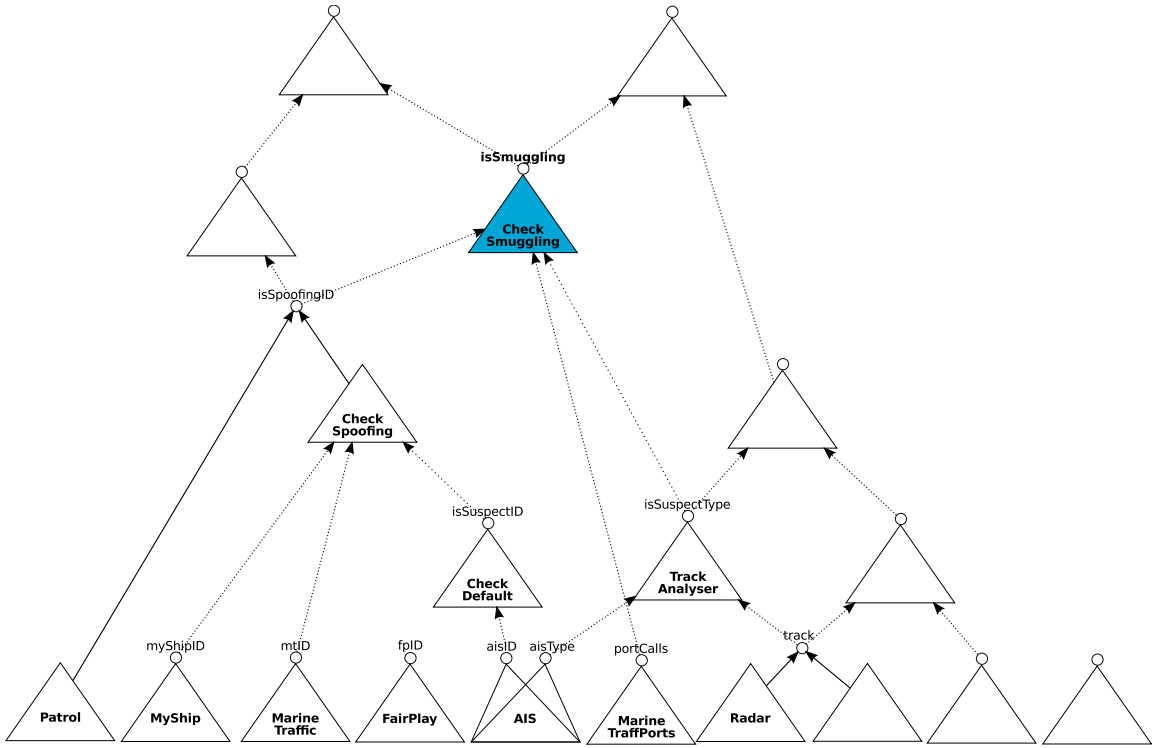
if $\phi \in out_C$, then C is a solution to $\mathfrak{C}$.

Naïve reconfig algorithm

1: compute the most compact stratification $\mathcal{A}_0, \ldots, \mathcal{A}_m$ of $\mathcal{S}$
2: **loop** (start with $i = 0$)
3: update D according to the environment in E_i
4: **loop** (start with $j = 0$) ▷ iteratively compute $F^*_{CAF}(\emptyset)$
5: execute all $A \in \mathcal{A}_j$ and update D accordingly
6: select the valid $A \in \mathcal{A}_j$
7: extend C with the selected agents
8: **end loop** (increment j)
9: **if** $\phi \in out_C$ **then** inform operator about the query solution
10: **end loop** (increment i)

- $F_{CAF}(\emptyset) \subseteq \mathcal{A}_0$, $F_{CAF}(\mathcal{A}_i) \subseteq \mathcal{A}_{i+1}$
- invariant: $D|out_C \subseteq C^*(D_0) \rightsquigarrow$ theorem exploitation

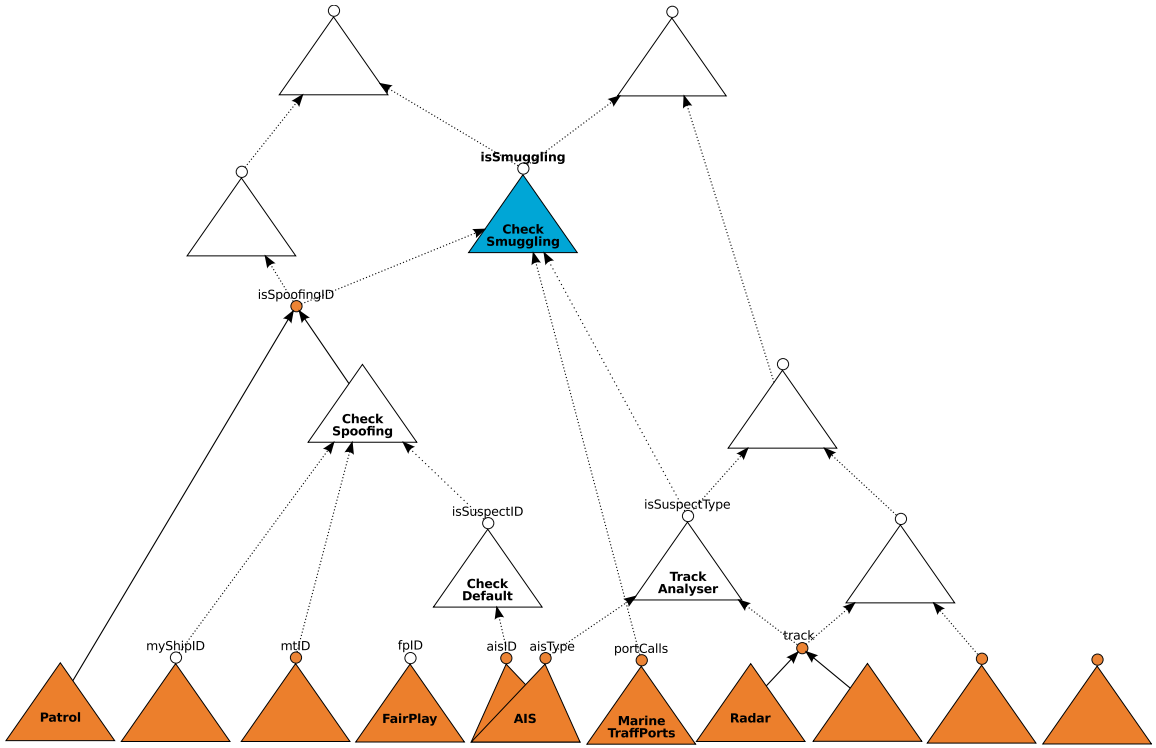
Naïve algorithm example



Naïve algorithm example

information sources

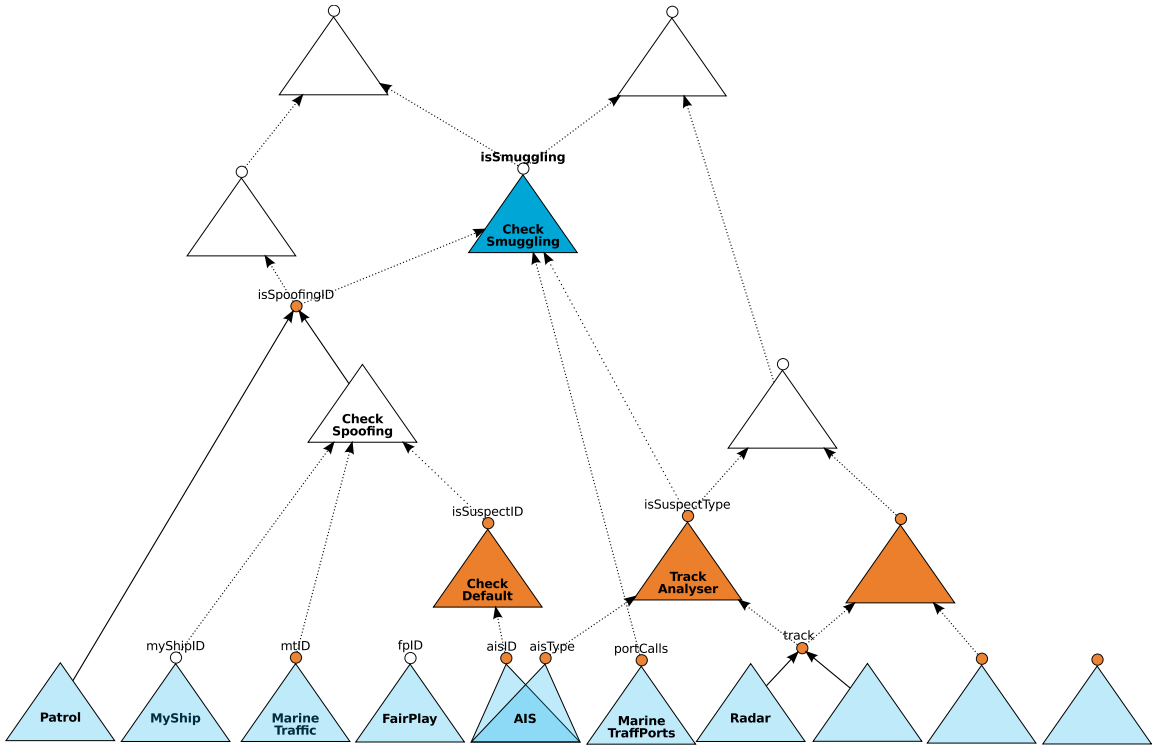
$\mathcal{A}_0$



Naïve algorithm example

inference propagation

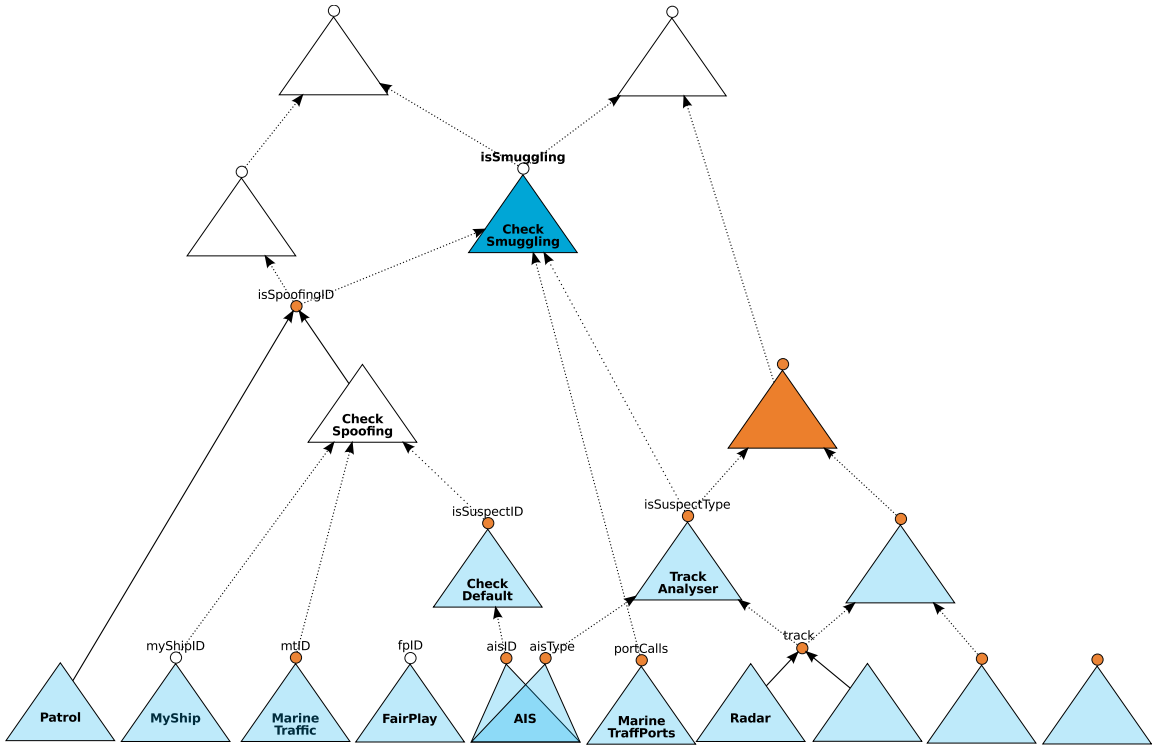
$\mathcal{A}_1$



Naïve algorithm example

$(x \mapsto \varnothing) \in D|in_{CheckSpoofing}$

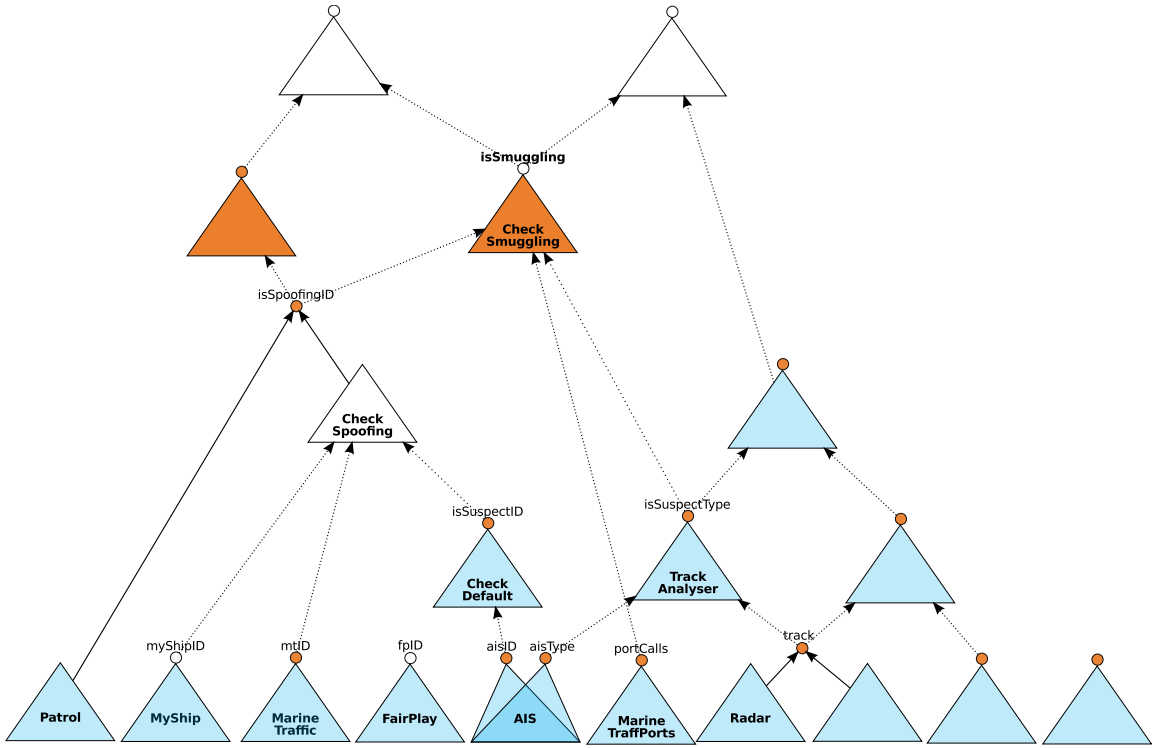
$\mathcal{A}_2$



Naïve algorithm example

deferred exec of *isSpoofingID*
query solution inferred, but ∅

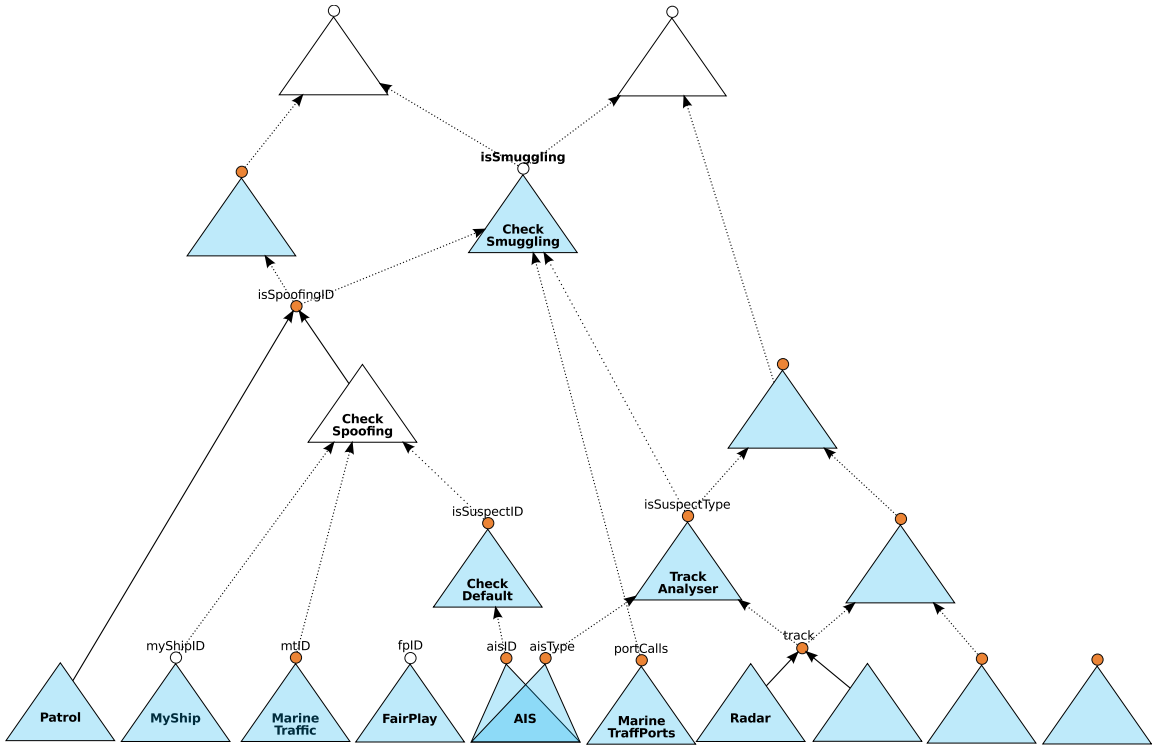
$\mathcal{A}_3$



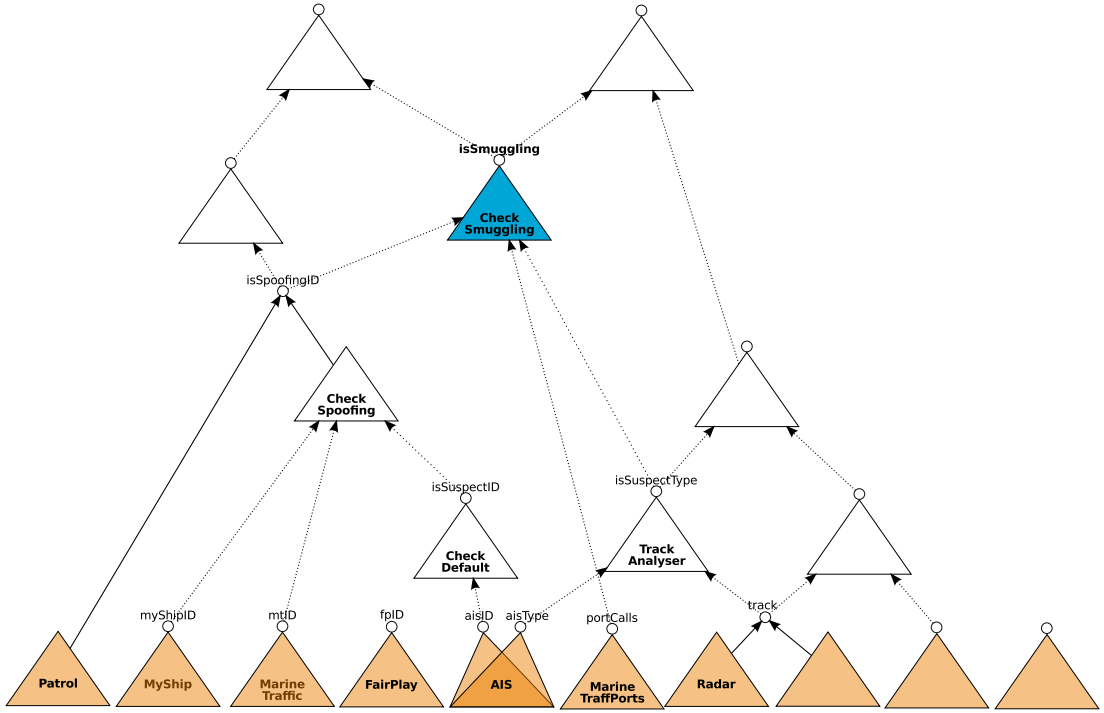
Naïve algorithm example

no more acceptable agents

$\mathcal{A}_4$

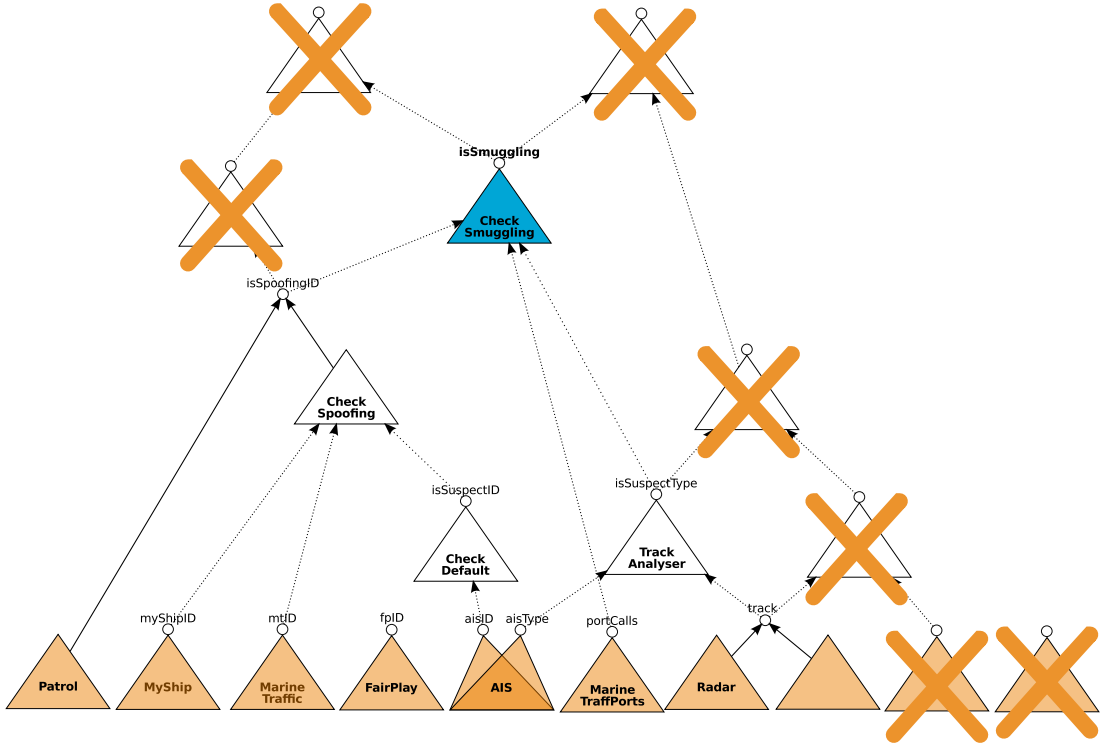


Naïve algorithm: issues



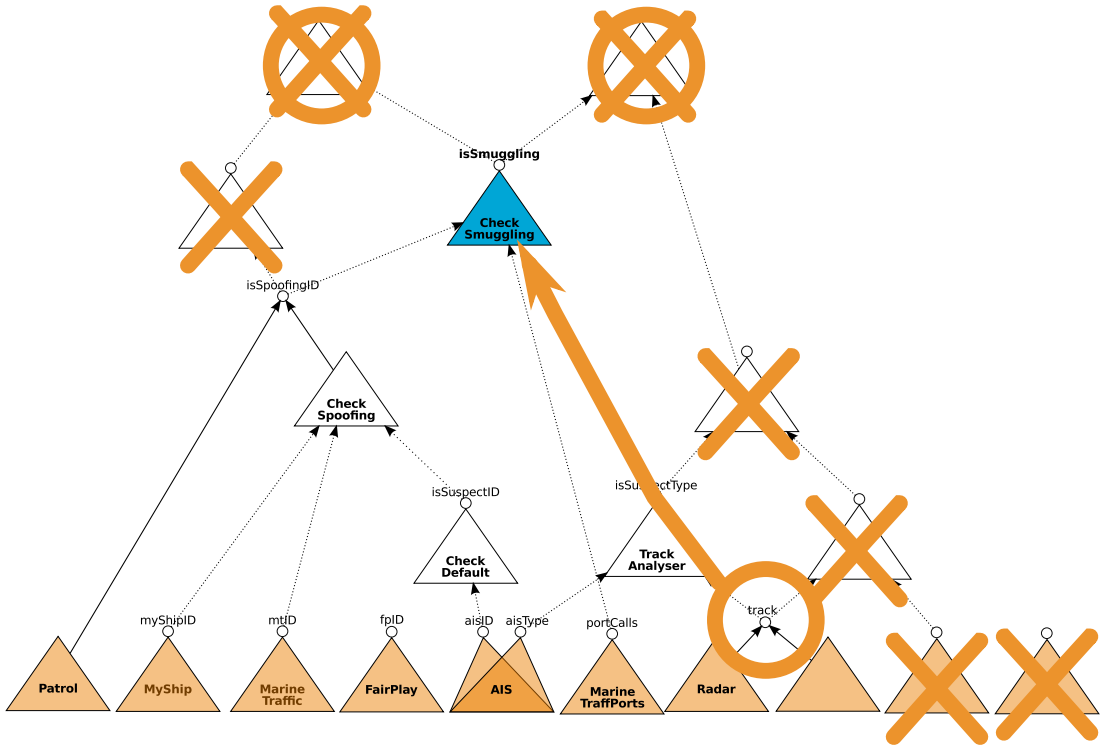
1 considers **all information sources**

Naïve algorithm: issues



1. considers **all information sources**
2. executes also **irrelevant agents**

Naïve algorithm: issues



1. considers **all information sources**
2. executes also **irrelevant agents**
3. **does not stop early enough:**
   1. when ϕ is safely derived
   2. when ϕ is not derivable any more

Cheaper/greedy algorithm

#1: consider only agents relevant to ϕ

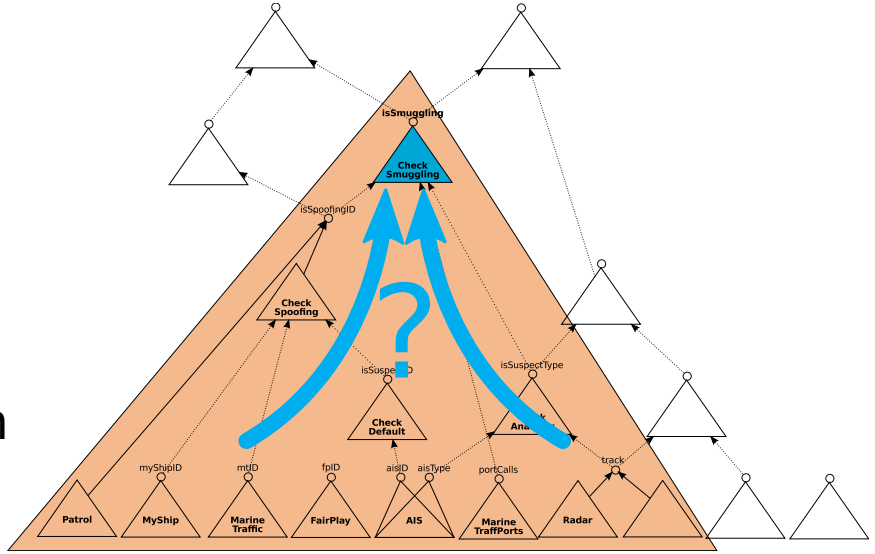
- cheap to collect - no exec cost

#2: always accept a single cheapest agent

- jumps across "layers"
- hence, careful clean-up/backtrack

#3: detect "hopeless" computations

- if hopeless, terminate configuration
- cheap to check - no exec cost

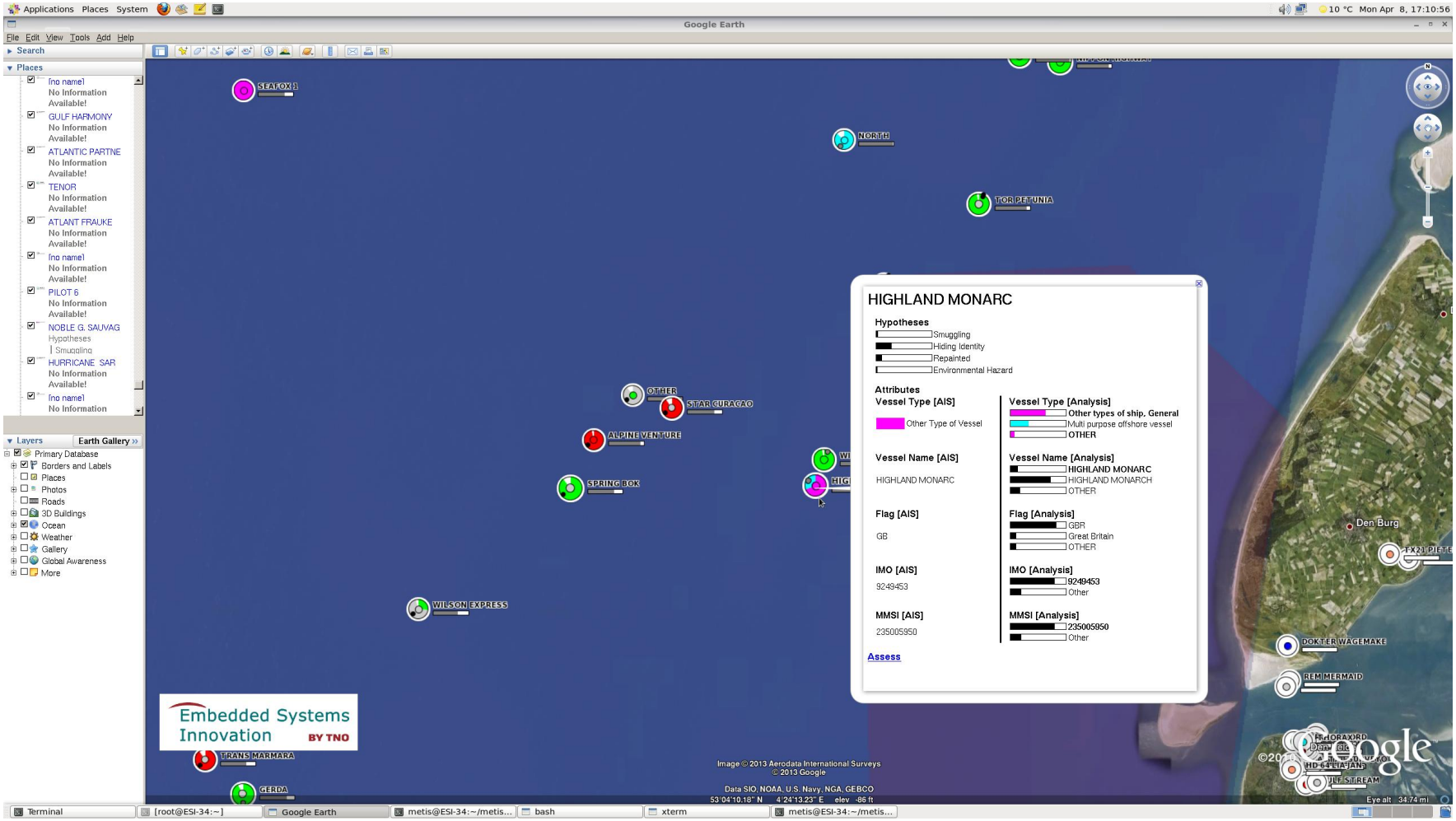


Theorem (config. problem $\mathfrak{C} = (\mathcal{S}, \phi, D)$, with stratified $\mathcal{S}$)

Let C be the grounded extension of $CAF_{\mathfrak{C}}$ over $C^*(D)$.

If $\phi \in out_C$, then $C \cap \mathcal{A}^*_\phi$ is the minimal and optimal solution to $\mathfrak{C}$.

Metis reconfiguration prototype



Summary & outlook

1. modelling framework for info-aggregation systems
2. configuration & reconfiguration problems
3. ideas from abstract argumentation for system reconfiguration
4. Metis prototype description

Summary & outlook

1. modelling framework for info-aggregation systems
2. configuration & reconfiguration problems
3. ideas from abstract argumentation for system reconfiguration
4. Metis prototype description

Future research:

- reconfiguration with a limited budget & aging information
- explore relationships to dynamic logic programming, evolving databases, belief revision, etc.
- reconfiguration of probabilistic info-aggregation systems

Thank you for your attention.

Questions?

▷ The presented research was supported by the Dutch national program COMMIT and carried out as a part of the Metis project under the responsibility of the *TNO-Embedded Systems Innovation*, with *Thales Nederland B.V.* as the carrying industrial partner.

▷ original image adapted for the title frame background by zulfinho via flickr.com (CC)