(Re-)configuration of large-scale surveillance systems

(argumentation in the Metis project)

Peter Novák (with Cees Witteveen)

Algorithmics, EEMCS, Delft University of Technology

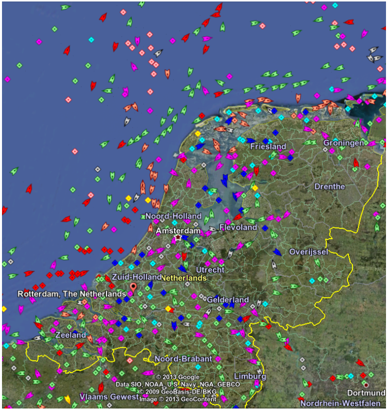
TU Delft Delft University of Technology

Challenge the future

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.

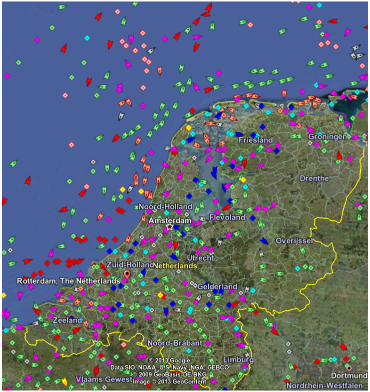
- thousands of vessels
- dozens of info-sources per ship

Problem

Scalability of the system!

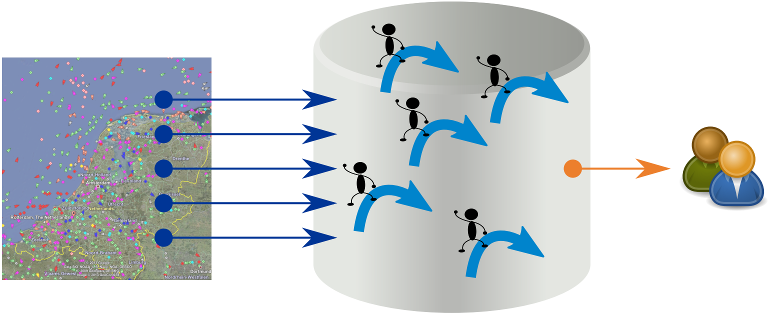
Solution idea

Run-time reconfiguration between vessel run-levels.



Talk outline

System scheme



Info-aggregation system

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

Database & environment

update of a database D by a configuration C

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

$$\rightsquigarrow \; C^*(D_0) = D^* = C(D^*)$$

Database & environment

update of a database D by a configuration C

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

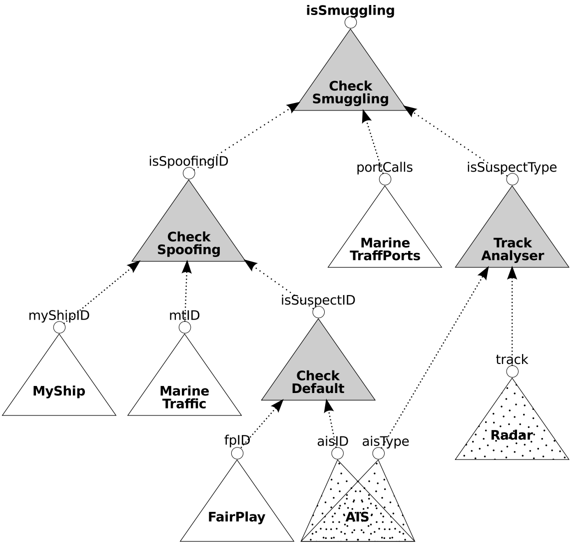
$$\rightsquigarrow \; C^*(D_0) = D^* = C(D^*)$$

Environment interface

information-source agents: no input variables/output variables are shared with the environment, $in_A = \emptyset$

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

Metis info-aggregation system



Research question

Which info-sources?

Which info-aggregators?

Detect malicious intents early and cost-efficiently!

Research question

Which info-sources?

Which info-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 $C \subseteq \mathcal{A}$

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

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'

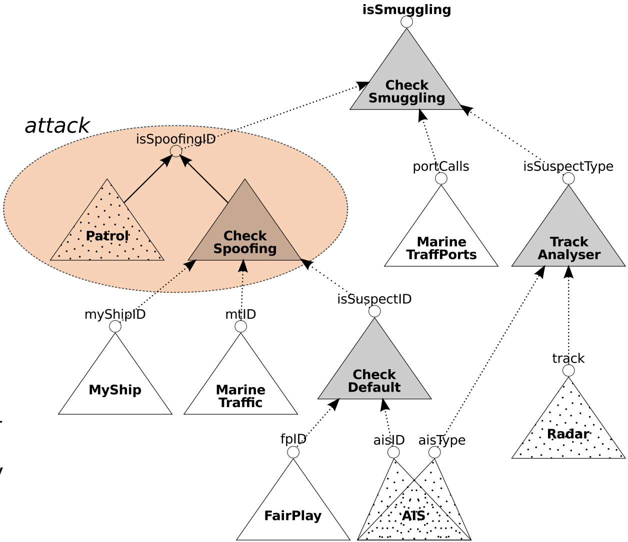
- asymmetric attack relation $\varnothing$ vs. crisp valuations

Acceptability:

valid arguments input is crisply valued and supported by C

Metis argumentation

Abstract argumentation - a natural fit!



arguments: heterogeneous complex reasoners

attacks: relatively simple structure

Sceptical argumentation

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

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

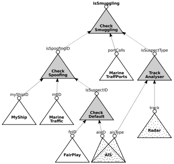
$$F_{CAF}(C) = \{A \mid A \in \mathcal{A} \text{ is acceptable to } C\}$$

advantage: preserves presumption of innocence!

issue: justification traceable to evidence

solution: acyclic/stratified systems

$\rightsquigarrow$ hierarchical (lattice) structure!

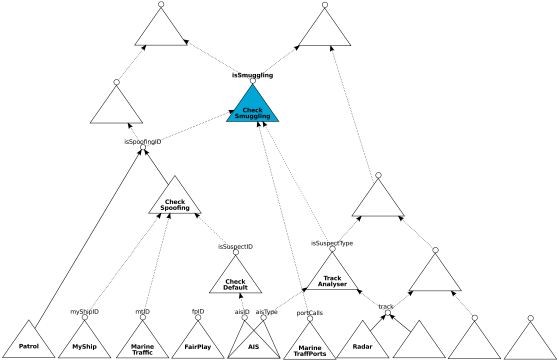


Theorem (config. problem $\mathfrak{C} = (\mathcal{S}, \phi, D)$, with stratified $\mathcal{S}$)

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

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

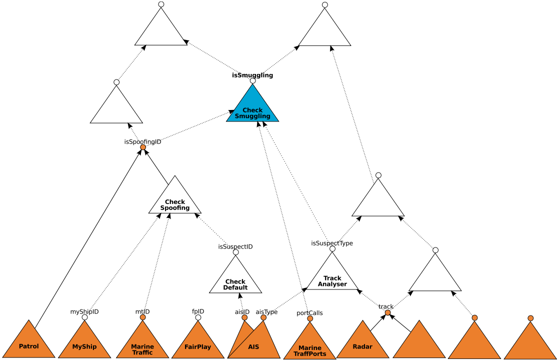
Naïve algorithm example



Naïve algorithm example

information sources

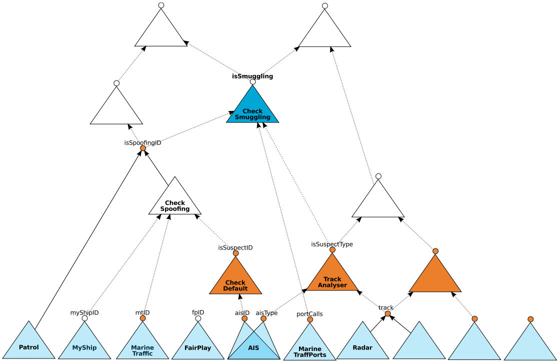
$\mathcal{A}_0$



Naïve algorithm example

inference propagation

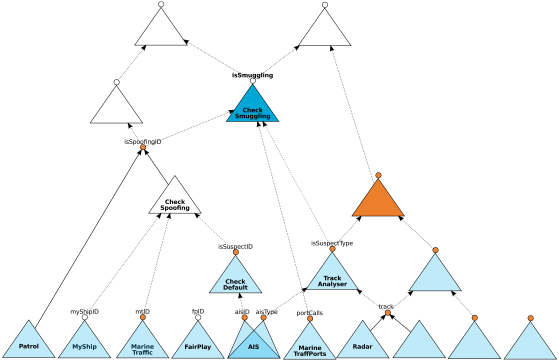
$\mathcal{A}_1$



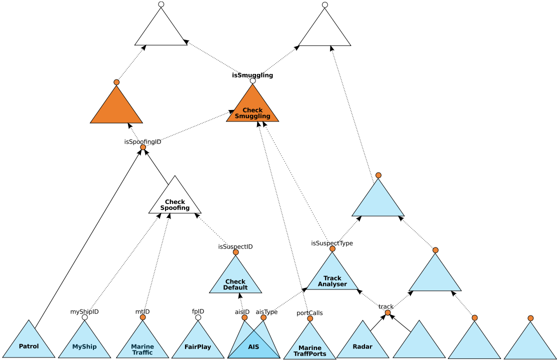
Naïve algorithm example

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

$\mathcal{A}_2$



Naïve algorithm example



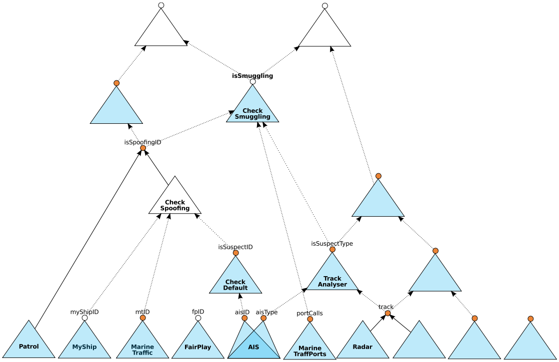
deferred exec of *isSpoofingID* query solution inferred, but $\emptyset$

$\mathcal{A}_3$

Naïve algorithm example

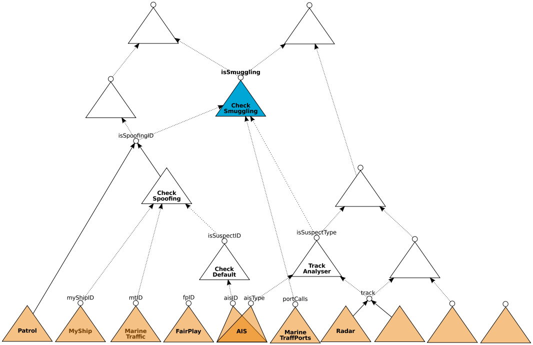
no more acceptable agents

$\mathcal{A}_4$



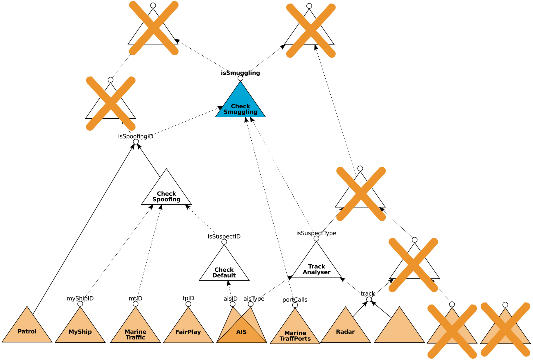
the attack relation is **a priori unknown**!

Naïve algorithm: issues



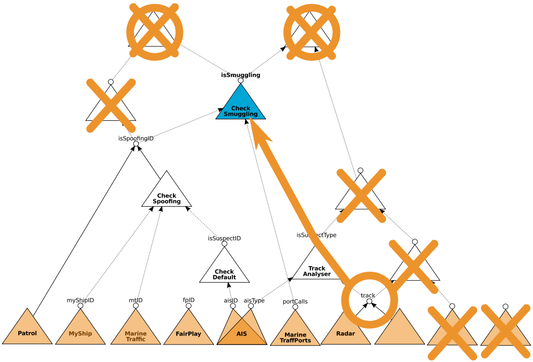
1 considers **all information sources**

Naïve algorithm: issues



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

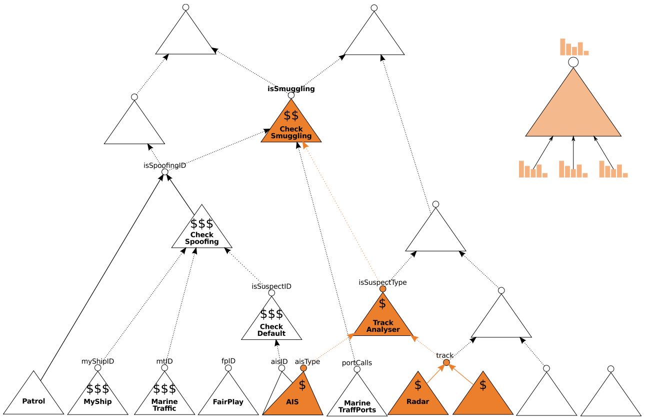
Naïve algorithm: issues



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

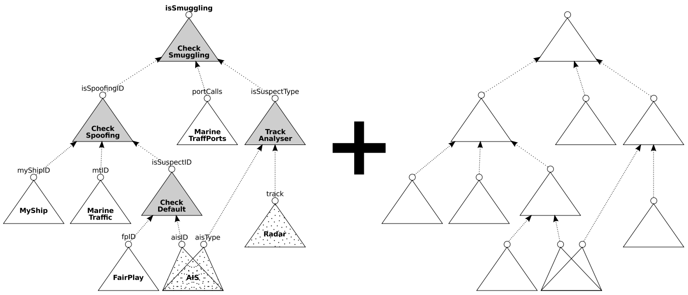
Outlook: argumentation

1. explanations of conclusions
2. budget-constrained argumentation
3. probabilistic argumentation

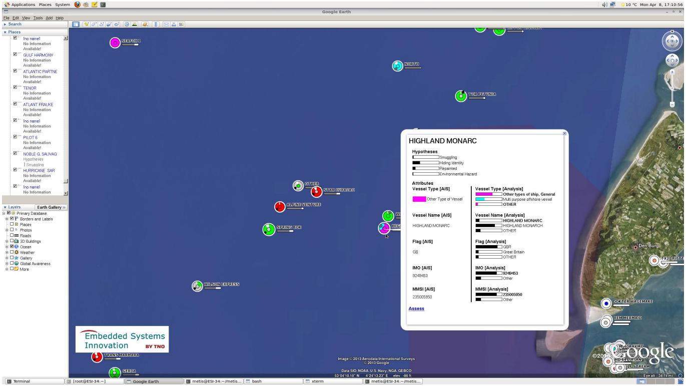


Outlook: (belief) change

1. evolving database
   - recalculation
2. evolving knowledge base
   - AF structure change
   - modularity, elaboration tolerance



THANK YOU FOR YOUR ATTENTION.



▷ 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)