Integrating time into majority-rule sorting models

Application to the cyber-defense context

Arthur VALKO
Director : Patrick Meyer
Supervisors : Alexandru-Liviu Olteanu, David Brosset

26 septembre 2018

NAVAL GROUP - THALES - IMT ATLANTIQUE - REGION BRETAGNE
ECOLE NAVALE
CHAIRE DE CYBERDEFENSE DES SYSTEMES NAVALS

Sommaire

1 Context

- Cyber-defence and naval environment
- Decision problem
- Operational constraints
- MCDA choice

2 Time integration

- Hierarchical model
- Learning Process
- Experimentation
- Concluding remarks and future work

Cyber-defence in naval context

Naval Systems

Today's ships are mainly **controlled** by automatons and **information systems**.

Information system are everywhere in naval equipment both at sea and in harbours.

This equipment have lots of **connections** with other information systems inside and outside.

Potentially very long life.

Risk

Like every information system they **can be hacked** and need cyber-defence.

Expansion of connectivity increases the risk of cyber attacks.

PhD topic :
Decision aiding to help selecting **a reaction** to a cyber attack event on military ships

Problem

How to help a naval system administrator to make good decision to restore his ship's systems ?

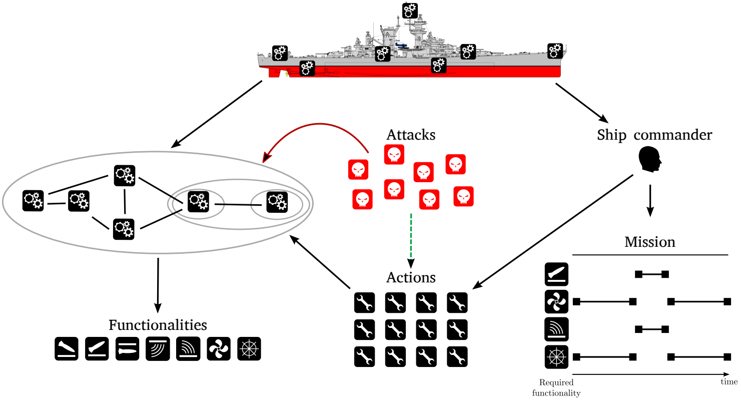
Specificity of **cyber-security** context

- Propagation of the attack in the connected systems.
- Effect of the attack on the system varies in time.
- Defence actions may take time.
- → Answers must take into account time.

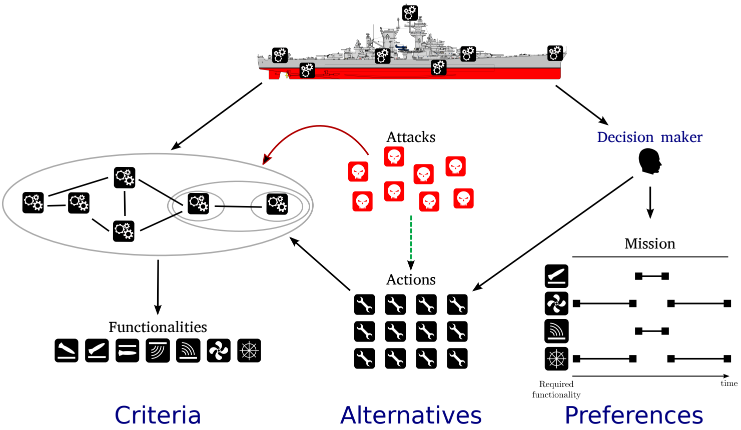
Specificity of **naval** context

- Physical (weather, position, ...) context of the ship has to be considered.
- Mission constraints and needs.
- "Distance" between the decision maker (captain of the ship) and the system experts.

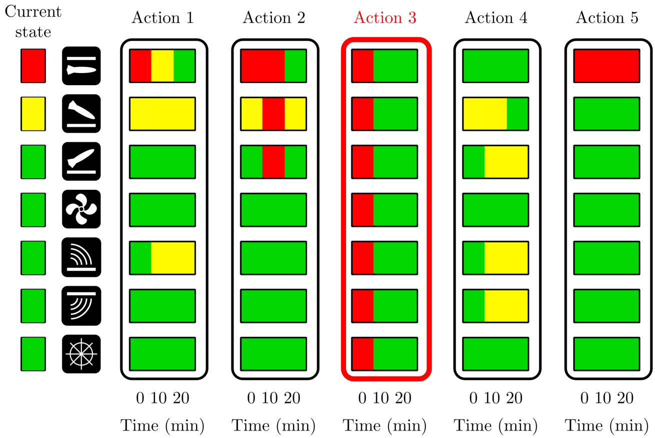
MCDA & cyber-defense : ship example



MCDA & cyber-defense : ship example



Dashboard for the decision maker



Mission requirements: critical important

Operational constraints

It is difficult for a decision maker in cyber-security to **evaluate** recovery actions
He / she does not necessarily look for the “best” action, but rather wishes to select among “**good**” ones
→ he / she wishes to have the final word !

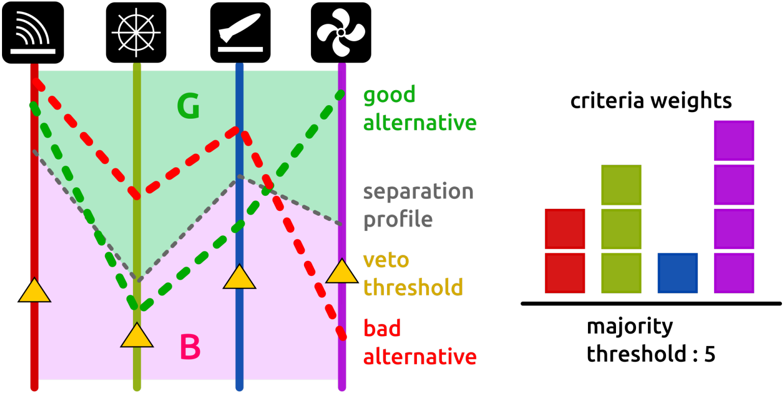
→ **sorting algorithm**

Evaluation scales of the criteria are **heterogeneous** and have a strong meaning for the decision maker
He / she (cyber defender) does not trust information systems (**black boxes**)
→ high readability of the decision recommendation required

→ **outranking method**

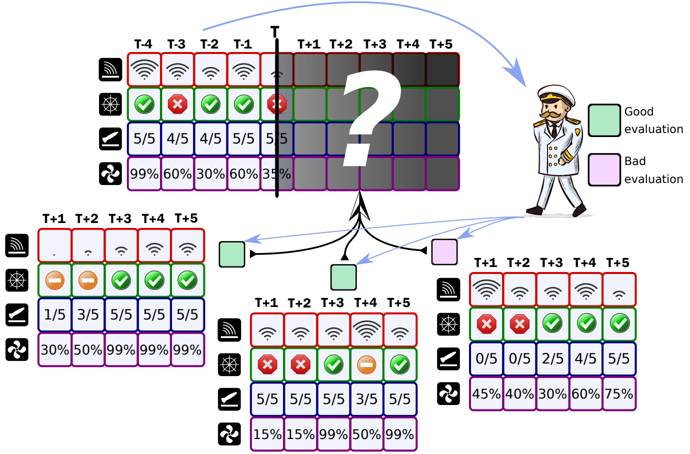
MR-Sort

- Sorting outranking model
- Various extensions possible to increase expressiveness (vetos, dictators, ...)
- Output easy to read and to explain
- Indirect learning process which is user friendly for the decision maker (from assignment examples)



Further need

Consequences of actions might vary with time on the several criteria



	T-4	T-3	T-2	T-1	T	T+1	T+2	T+3	T+4	T+5
	📶	📶	📶	📶	📶					
	✓	✗	✓	✓	✗					
	5/5	4/5	4/5	5/5	5/5					
	99%	60%	30%	60%	35%					

🟩

	T+1	T+2	T+3	T+4	T+5
	📶	📶	📶	📶	📶
	⊖	⊖	✓	✓	✓
	1/5	3/5	5/5	5/5	5/5
	30%	50%	99%	99%	99%

🟩

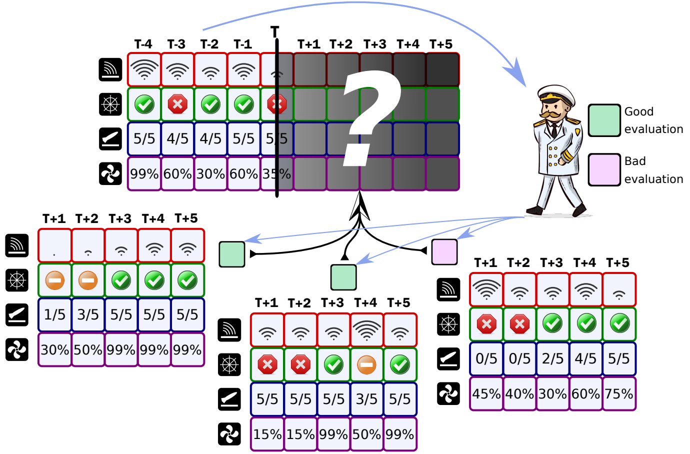
	T+1	T+2	T+3	T+4	T+5
	📶	📶	📶	📶	📶
	✗	✗	✓	⊖	✓
	5/5	5/5	5/5	3/5	5/5
	15%	15%	99%	50%	99%

🟪

	T+1	T+2	T+3	T+4	T+5
	📶	📶	📶	📶	📶
	✗	✗	✓	✓	✓
	0/5	0/5	2/5	4/5	5/5
	45%	40%	30%	60%	75%

Further need

Consequences of actions might vary with time on the various criteria



	T-4	T-3	T-2	T-1	T	T+1	T+2	T+3	T+4	T+5
📶	📶	📶	📶	📶	📶	?	?	?	?	?
☸	✓	✗	✓	✓	✗	?	?	?	?	?
✎	5/5	4/5	4/5	5/5	5/5	?	?	?	?	?
✇	99%	60%	30%	60%	35%	?	?	?	?	?

🟩

	T+1	T+2	T+3	T+4	T+5
📶	📶	📶	📶	📶	📶
☸	⊖	⊖	✓	✓	✓
✎	1/5	3/5	5/5	5/5	5/5
✇	30%	50%	99%	99%	99%

🟩

	T+1	T+2	T+3	T+4	T+5
📶	📶	📶	📶	📶	📶
☸	✗	✗	✓	⊖	✓
✎	5/5	5/5	5/5	3/5	5/5
✇	15%	15%	99%	50%	99%

🟪

	T+1	T+2	T+3	T+4	T+5
📶	📶	📶	📶	📶	📶
☸	✗	✗	✓	✓	✓
✎	0/5	0/5	2/5	4/5	5/5
✇	45%	40%	30%	60%	75%

🟩 Good evaluation

🟪 Bad evaluation

How to integrate time into MR-Sort models ?

Time integration

1 Context
- Cyber-defence and naval environment
- Decision problem
- Operational constraints
- MCDA choice

2 Time integration
- Hierarchical model
- Learning Process
- Experimentation
- Concluding remarks and future work

Time integration

Multiple options :

Increase the number of criteria

- One "time"-criterion per time step
- Loss of readability for DMs
- Difficulty of learning process for DMs

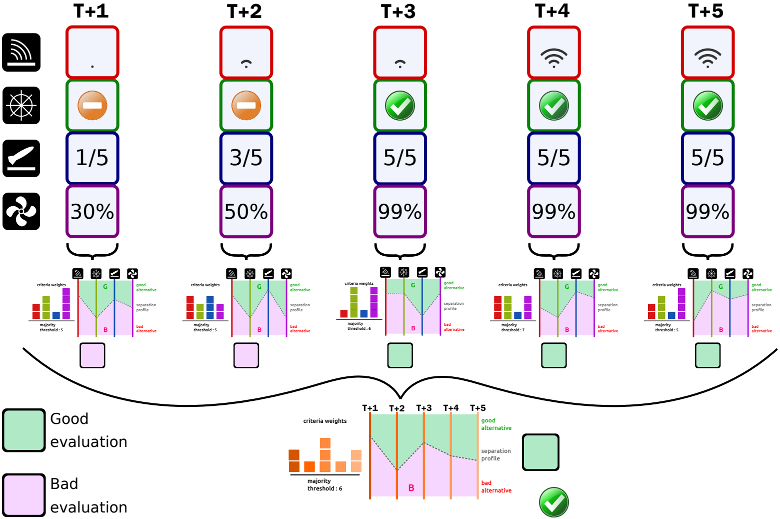
Time aggregation

- Loss of information (intra- and inter-criterion)

Our proposal : hierarchical approach

- Time structure conservation
- Better readability for DMs
- Easier learning for DMs

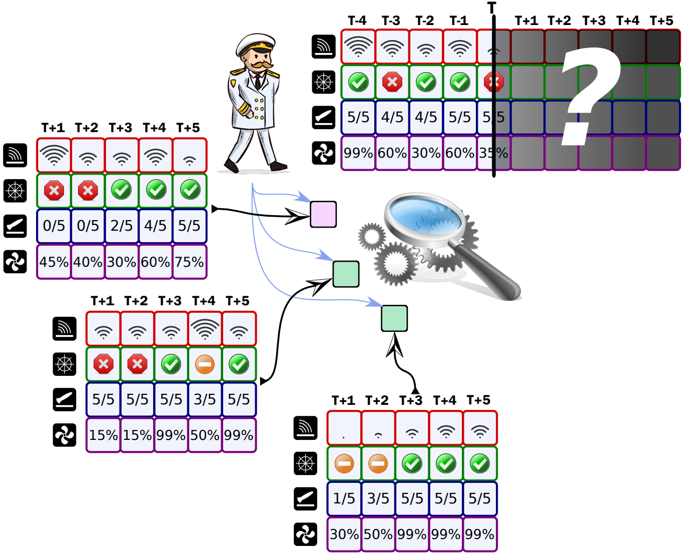
Hierarchical model



🟩 Good evaluation

🟪 Bad evaluation

Learning process



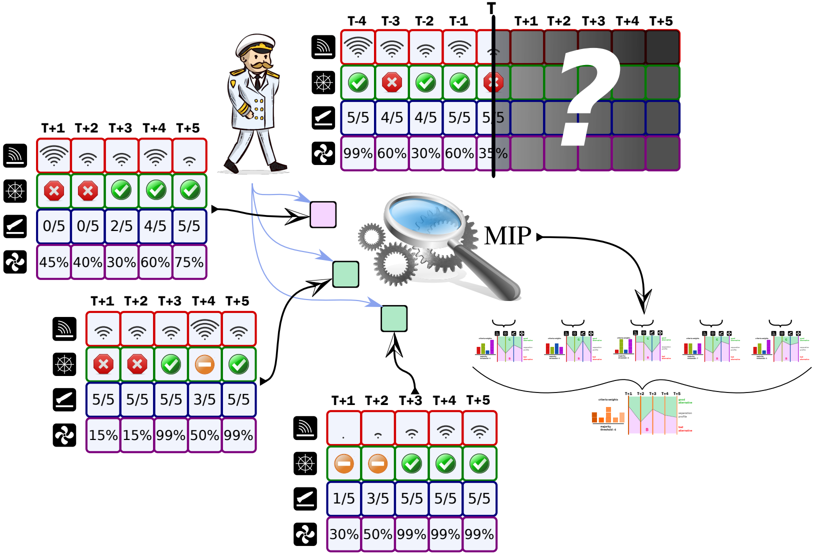
	T-4	T-3	T-2	T-1	T	T+1	T+2	T+3	T+4	T+5
	📶	📶	📶	📶	📶	?	?	?	?	?
	✓	✗	✓	✓	✗	?	?	?	?	?
	5/5	4/5	4/5	5/5	5/5	?	?	?	?	?
	99%	60%	30%	60%	35%	?	?	?	?	?

	T+1	T+2	T+3	T+4	T+5
	📶	📶	📶	📶	📶
	✗	✗	✓	✓	✓
	0/5	0/5	2/5	4/5	5/5
	45%	40%	30%	60%	75%

	T+1	T+2	T+3	T+4	T+5
	📶	📶	📶	📶	📶
	✗	✗	✓	⊖	✓
	5/5	5/5	5/5	3/5	5/5
	15%	15%	99%	50%	99%

	T+1	T+2	T+3	T+4	T+5
	.	📶	📶	📶	📶
	⊖	⊖	✓	✓	✓
	1/5	3/5	5/5	5/5	5/5
	30%	50%	99%	99%	99%

Learning process



T-4	T-3	T-2	T-1	T	T+1	T+2	T+3	T+4	T+5
📶	📶	📶	📶	📶					
✓	✗	✓	✓	✗					
5/5	4/5	4/5	5/5	5/5					
99%	60%	30%	60%	35%					

T+1	T+2	T+3	T+4	T+5
📶	📶	📶	📶	📶
✗	✗	✓	✓	✓
0/5	0/5	2/5	4/5	5/5
45%	40%	30%	60%	75%

T+1	T+2	T+3	T+4	T+5
📶	📶	📶	📶	📶
✗	✗	✓	⊖	✓
5/5	5/5	5/5	3/5	5/5
15%	15%	99%	50%	99%

T+1	T+2	T+3	T+4	T+5
📶	📶	📶	📶	📶
⊖	⊖	✓	✓	✓
1/5	3/5	5/5	5/5	5/5
30%	50%	99%	99%	99%

Learning algorithm questions

Complexity

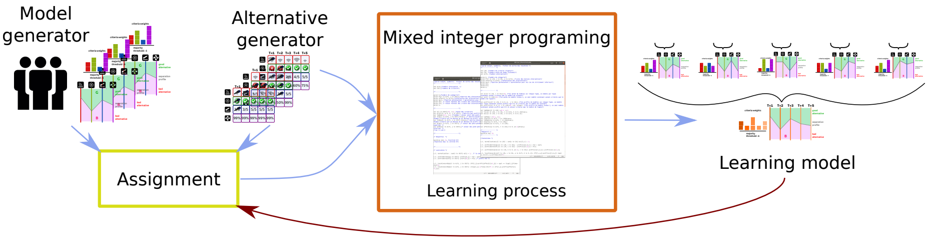
- Computation time for the learning process compared to classical MR-Sort

Elicitation

- Size of assignment examples to determine a good-enough representation of the decision maker's preferences
- Expressiveness of hierarchical MR-Sort model versus a classical one taking into account all criteria and time steps at once.

Experimentation

Test platform



Ongoing tests :

- Learning time as a function of problem size
- Inferred model quality as a function of problem size
- Cross-analysis of classical and hierarchical MR-Sort models

Concluding remarks and future work

Hierarchical model :

- Adds a time component into the decision-making process.
- Adds an additional structural layer to the analysis of the decision problem.

Apply the model in a **real-world case** :

- Ship protection system
- Cyber-defence data hypervisor, dashboard management
- Security Operational Centre

Future work :

- Meta-heuristic learning method
- Automatic explanation of recommendations

Thank you for your attention.
Any questions ?