Integrating time into majority-rule sorting models: application to the cyber-defense context

Arthur VALKO[1,2], David BROSSET[1], and Patrick MEYER[2]

[1]Chaire de cyber défense des systèmes navals, École navale, CC 600 29240 BREST CEDEX 9, France
[2]IMT Atlantique, Lab-STICC, Univ. Bretagne Loire, F-29238 Brest, France

ABSTRACT

On a day to day basis, we are confronted with decision problems, going from trivial decisions that we often make without even realizing, to more complex ones, characterized by multiple and often conflicting criteria. This latter class requires more attention and cognitive effort from the decision makers, and has therefore led to the development of the field of Multiple Criteria Decision Aiding (MCDA).

Integrating a temporal component with the evaluations of the decision alternatives, either in order to account for past states or foresee future ones, is a research question that has received very little attention in MCDA to the best of our knowledge. Nevertheless, in our research, we have been confronted to various application domains which require that a time component be included in the decision aiding process.

Let us consider a cyber-defense context, in which, actions needed to counter a cyber-attack can possibly impact the performance of the system under attack. The evaluation and planning of these countermeasures depend on the attack, the countermeasures themselves and their impact on the system over a given period of time. For example, performing a system update is a common and effective solution, but it could have a significant impact on the availability of some or all functions of the system during a given period of time in the future. The decision maker is therefore faced with the complex task of determining the best actions with respect to multiple criteria (risk for the system, performance of the system, ...) over various periods of time.

We therefore propose to take into account time in the evaluation of decision alternatives and their consequences on the multiple criteria. Motivated by the application domain of cyber-defence, we choose to study this integration in sorting algorithms, based on the outranking paradigm. The main motivations for this choice are the heterogeneity of the scales of the input data, which speaks for outranking methods, and the qualitative output required to evaluate the various countermeasures, or decision alternatives, which is in favor of the sorting problem. We chose to work on the MR-Sort sorting model, in order to preserve the flexibility and readability of the provided recommendations, as the output of MR-Sort leads to the construction of norms that can be reviewed independently by specialists of the cyber-defense domain.

The decision alternatives are here defined on criteria which can take multiple values with respect of time. Therefore these evaluation can be seen as discrete time series. As a consequence, this vision leads to a three-dimensional performance table : alternatives $\times$ criteria $\times$ time.

A first intuition would be to apply the classical MR-Sort model directly, by breaking down the time component and considering the evaluations of each criterion the various periods of time as a new criterion. However, this can lead to losing the readability of the model due to the explosion of the number of criteria in the final model. In order to simplify the interaction with the decision maker, we propose a hierarchical approach which decomposes the decision problem into sub problems, either criterion-wise first and then time-wise, or vice-versa. We associate this model with an inference approach that builds the entire hierarchical structure from holistic judgments of the decision-maker on the final classification of the decision alternatives. Additional input regarding the intermediate models could also help speed up this process and increase the interpretability of the final model. We detail the various algorithmic developments as well as several experimental results in order to explore their performance.