Editorial
Special issue on artificial immune systems

10.1007/s12065-008-0007-7

Uwe Aickelin, School of Computer Science, University of Nottingham, Nottingham, UK

Email: uwe.aickelin@nottingham.ac.uk
URL: http://www.aickelin.com

Artificial Immune Systems (AISs) are a relatively new area of research at the interdisciplinary interface between Computer Science, Engineering and Life Sciences [1]. Like other similar endeavours, for instance genetic algorithms or neural networks, their basic premise is to look at the way the natural system works, extract models and algorithms and then apply these to real-world problems.

Early AIS algorithms mainly borrowed from three immunological concepts: Clonal Expansion, Negative Selection and Idiotypic networks. Clonal Expansion is a process taking place in the lymph nodes whereby useful immune cells undergo rapid expansion in numbers to counter an ongoing attack on the immune system. The closer immune cells match the threat, the more they are copied and the less they match the more likely they will be mutated. Although these concepts sound quite different from other nature inspired techniques, in practice the implementation of this algorithm is rather similar to an evolutionary strategy or simple genetic algorithm where the fitness function is replaced with a 'matching' function. As a result, Clonal algorithms were similarly successful to genetic algorithms in areas such as clustering or data mining.

Idiotypic network algorithms were based on a theory proposed 30 years ago by NK Jerne. He proposed that antibodies do not only interact with antigen, but also with each other. Thus they form a network that results in mutual stimulation and suppression that might explain concepts such as immunological memory. Unfortunately, to date no consistent experimental evidence for the existence of such networks has been found and thus the majority of immunologists do not believe they exist. Nevertheless, algorithmic implementations of these networks show interesting properties and have been useful in areas such as robotic control or data clustering. Like the Clonal algorithms, the idiotypic concepts might sound novel, but their practical implementations have been shown to share many similarities with neural networks. Neural nodes equate antibodies and network weights are the equivalent of antibody concentrations.

Arguably the most novel immune inspired algorithm is Negative Selection which describes a process in the Thymus that eliminates self-reacting T-cells that otherwise might lead to auto-immune problems. The algorithm works by randomly creating bit strings. In an initial training phase these strings are then matched against 'self' and any matching strings are deleted. Eventually one is left with a set of all those strings that did not match, the so called 'detector set'. This set is then used to analyze the real data and any resultant matches are reported as 'non-self', i.e., anomalies.

The Negative Selection algorithms have been applied mainly to anomaly detection problems in areas such as computer security or prediction of machine failures. Although these algorithms showed early promise, even after 10 years of refinement they were unable to solve complex real-world problems and as a result have never been accepted by outside communities like computer security experts. More recently, the AIS community itself has further investigated these algorithms and theoretical proofs have been established regarding their performance: Due to the need to create random detectors Negative Selection systems can never scale to cover real-world multi-dimensional data sufficiently without too many 'holes' in the coverage.

As one might expect from the above summary of the field, the AIS community reached somewhat of an impasse a few years ago: The novel algorithms were shown not to work that well and the ones that did work were not really different enough from other fields. It was at this point that some people in the community realized that so far AISs had only scratched the surface of what immunology had to offer: Partly due to the previous background of AIS researchers in genetic algorithms and neural networks and partially due to a poor understanding of immunology based on outdated text books, the community had focused on a few simplistic immune mechanisms. The questions is, what else had the immune system to offer?

Amongst the first to address this issue were those working on the 'Danger Project' [2]. This project featured intense and direct collaboration between computer scientists and wet lab immunologists, leading to a much better understanding of what the immune system does. Apart from inventing some new computer algorithms, such as the Dendritic Cell Algorithm featured in some of the special issue papers, the project also served as a shot in the arm of the AIS community. After initial scepticism, there was a flurry of new ideas and new, direct collaboration with both experimental and theoretical immunologists. Nowadays, the field is more healthy than ever, with numerous exciting ideas in the pipeline.

Presented in this issue are a selection of some of the first such second generation AISs. They differentiate themselves from previous attempts not only through their novelty, but also through their grounding in sound, up-to-date immunology and ultimately through their success in solving problems better than other established algorithms. The future looks bright for AIS as with the ever closer links with immunology fascinating research awaits!

References

[1] http://www.artificial-immune-systems.org/
[2] http://www.dangertheory.com/