

Dedication

To my parents, Doo-Hwan Kim(김 두환) and Ae-Soon Park (박 애순).

Abstract

This thesis focuses on the combination of a set of artificial immune algorithms and their application to intrusion detection. Three evolutionary algorithms are investigated, each based on a process from the human immune system. It is demonstrated that these three algorithms, negative selection, clonal selection and gene library evolution, lead to self-organisation in the artificial immune system (AIS). In addition, the attributes required for effective intrusion detection are analysed in depth. With the aim of intrusion detection in mind, novel variations of the algorithm are created and tested on different data sets, including real network traffic data.

This thesis makes the following eight main contributions. 1. The components of human immune systems that are crucial to the improvement of AIS for intrusion detection are identified. 2. A systematic framework for an AIS for network intrusion detection is introduced by combining three evolutionary stages: negative selection, clonal selection and gene library maintenance. It is demonstrated that this framework can fulfil the role of a network-based intrusion detection system. 3. It is demonstrated that the negative selection algorithm employed for the thesis has a severe scaling problem when applied in a real network environment. 4. It is demonstrated that a static clonal selection algorithm with a negative selection operator achieves efficient niche maintenance and acceptable self-tolerance. 5. A dynamic clonal selection algorithm that combines three evolutionary stages allows the AIS to be adaptable to dynamically changing antigen behaviours. 6. The effect of three parameters on the behaviour of the dynamic clonal selection algorithm is analysed. These parameters are: tolerisation period, activation threshold and life span. Satisfactory TP and FP rates are obtained by setting these parameters to appropriate values. 7. The extension of the dynamic clonal selection algorithm to employ deletion of memory detectors reduces high FP rates observed when previously observed normal behaviours no longer represent normal behaviours. 8. It is demonstrated that simulation of gene library evolution using hypermutation reduces the amount of costimulation (human intervention).

These contributions support the conclusion of this thesis: that an artificial immune model harnessing the three evolutionary stages demonstrates adaptability to continuously changing environments, dynamically learning the fluid patterns of ‘self’, and detecting new patterns of ‘non-self’.

Acknowledgements

There are many special people who have made it possible for me to complete this thesis. My very special thanks go to my supervisor, Peter Bentley, who consistently provided valuable advice, stimulating discussion and a close friendship sharing many enjoyable memories together. Peter has not only been an excellent supervisor, but also a good friend. He has criticised me, encouraged me, praised me, cheered me up, distracted me, guided me and pushed me. All of these together finally made me finish this work. I also would like to thank another supervisor, Philip Treleaven, who allowed me to start my research at UCL alongside many excellent researchers.

Other researchers in the AIS field who have provided valuable criticism also deserve my special thanks. My colleagues in the AIS-Forum, U.K. and attendees of ICARIS, GECCO and CEC have inspired me to continue this research.

Very special friends at UCL also made my long PhD period enjoyable, dynamic and colourful. They are Ian Brown, Ken Carlberg, Laura Dekker, Hyun-Sung Jeong, Min-Seok Kang, Nadia Kausar, Sanjeev Kumar, Bill Langdon, Hugh Mallinson, Seng-Gun Oh, Mazliza Othman, Maria Consuelo Ruiz, Tony Ruto, Amela Sadagic, Supiya Ujjin, Kanta Vekaria, Carol Webb, Paul White, In-Su Yu, Tina Yu, and many other friends whose names I have missed here.

I am very grateful to Arlene Ong and Richard Overill at KCL, who put up with me being distracted by PhD research whilst working with them on the CIFD project. I would also like to thank other friends at KCL who made me smile when I was getting very tired of never-ending writing. They are Nazareno M. Aguirre, Kelly Androustopoulos, Chris Hannon and Paul Sant.

I also owe a big debt to my ex-supervisor, Jong-Uk Choi, who enlightened me by convincing and supporting me to go abroad and experience a new world, and to undertake an interesting avenue of research. My friends in Korea have supported me for many years without getting anything in return from me. Among them, I am particularly thankful to Su-Jeong Kim, Soo-Young Lee, Hye-Lim Yu, Won-Jin Lee, Hyun-Ju Lee, the late Mun-Kyung Cho, and Ian King for their long and loyal friendship.

I also thank Kook-Hee Gill, with whom I have shared long hours of Korean chatting on the phone whenever we miss Korean food and other Korean things here in the UK, and to Kook-Hee's best friend, Ivan Yuen, who has visited me all the way from Edinburgh to cheer me up whenever I have been depressed. My best and first friend in the UK, Amanda Clare, who taught me how to speak and write in English and how to survive in the UK, deserves more than the word

“thank”.

My most heartfelt thanks should go to my family, who have supported me in all possible ways even when I am millions of miles away from them. Without their endless love and trust, I would not even dream of enjoying my little achievement today.

My final acknowledgement goes to Max Christian, who has been always with me for the last five years. When I was happy, when I was depressed, when I was annoying, when I had insomnia, when I felt hopeless, when I had to debug my systems, when I wanted to go on holiday, when I needed to work through every weekend, when I needed to ask for proof-reading of the thesis, he was always next to me.