Building a Robust Distributed Artificial Immune System

Johan Kaers[1], **Richard Wheeler**[2] and **Herman Verrelst**[1]
[1]Data4s Future Technologies
Ambachtenlaan 13G, 3001 Heverlee, Belgium
{johan.kaers, herman.verrelst}@data4s.com
[2]Public Voice Lab
Opperngasse 24, Vienna, Austria, rew@pandora.be

Abstract

It is shown how to build and use large-scale networks of communicating Artificial Immune Systems that are robust against random failures or intentional attacks. The nodes of the network graph contain the immune systems while the edges are channels over which antibodies are circulated. Because there's a constant flow of antibodies through the nodes, the anomaly detection performance increases over time. This *Distributed Artificial Immune System* model (or DAIS) is introduced and analysed for networks with ring shaped, fully connected and finally arbitrary topologies. These results are combined with recent results from Complex Network Theory about the construction and robustness of random (Erdős-Rényi) and scale-free (Barbási-Albert) graphs. We show that by using these kinds of graphs, it can be guaranteed that the DAIS will degrade gracefully when nodes fail and will maintain a reliable detection performance, even under very high failure conditions. The mapping of the model onto a real-world software architecture and it's possible usages are also discussed.

1 Introduction

The *Artificial Immune System* (AIS) model introduced in [9] is an inherently distributed anomaly detection technique. The main reason for this is that a collection of independent and atomic detection particles or *antibodies* are used to determine whether the system under consideration has changed. It was soon observed [9] that this allows using a collection of artificial immune systems that each contain part of the antibodies. In [11] a similar type of AIS model is introduced (as ARTIS) and applied to network intrusion detection under the name LISYS. Again, the anomaly detection nodes form a distributed system, each containing part of the antibodies and observing the same environment (a LAN). [12] investigates a distributed Artificial Immune Model, also applied to network intrusion detection. There, the evolutionary processes that drive the model can trigger an exchange of antibodies between its sub-systems.

Here the detection performance of a network of Artificial Immune Systems is analysed while they exchange antibodies. The nodes of the network graph contain the immune systems while antibodies are circulated over the graph's edges. This greatly increases the number of unique antibodies encountered at any given node over time and hence also the detection performance. If the network graph is constructed well, soon all antibodies in the system will have passed through all nodes. It has the advantage that all anomaly detection knowledge is shared over the entire system. If an advanced immune response model is used, like in [10] or [12], products of the involved mechanism (e.g. memory detectors) could be communicated throughout the system with the same ease. The goal is to find a type of graph that is robust against random failure or intentional attack on it's nodes and at the same time reasonable in the amount of resources it consumes (e.g. the number of edges it has, the number of antibodies it holds). In section 2 the DAIS model is formally defined and analysed for the ring-shaped and fully-connected topologies. The fact that neither realize this goal, leads us to a consideration of *Complex Network Theory*.

Recently it has become clear that complex network theory, with roots in graph theory and statistical mechanics, can explain the behaviour of a wide variety of biological [16], physical [3], sociological [14] and technological systems [17], ranging from the World Wide Web [1] to movie actor collaboration networks.

In addition, it also shows how to build networks (graphs) that are robust against node failure or attacks. Combining the Distributed Artificial Immune System model with this holds the promise of building a large scale distributed pattern recognition system that degrades gracefully under failure conditions. As the analysis in section 3 will show, using this type of graph creates a system that satisfies both our design goals. It is robust against failure and attacks on the nodes because fragmentation of the graph does not occur unless under extremely high failure rates. And while reaching almost the same detection performance as a fully connected graph with the same number of nodes, it needs far less edges.

The possible applications of this model are discussed in section 5 as well as the mapping onto the software implementation we used for the experiment included in this report. Finally, some conclusions and possible tracks for future work are outlined.

2 The DAIS

Throughout the paper we use the Distributed Artificial Immune System model defined in this section. It extends the Artificial Immune System model first introduced in [9] by embedding a number of identical AISs in the nodes of a graph. The edges connecting the graph's nodes are communication channels over which antibodies are circulated. A discrete time dimension is added, at every time-step all nodes send a fraction of their antibodies to their neighbouring nodes in the graph. All nodes are identical in the sense that they share the same set of *self strings*, match-rule, size of the antibody set and antibody migration probability. Because of the randomness in the antibody generation algorithm that is used, the actual antibodies present in the nodes do differ. Also, the environment that is monitored and from which the *antigens* originate can be different at every node. During a series of time-steps the antigens are matched against all antibodies that pass through a node to determine if they differ from the pre-defined self set.

2.1 The DAIS Model

More formally, the set $N = \{n_1, \ldots, n_{N_n}\}$ contains the nodes of the network graph. $E \subseteq N \times N$ contains the pairs of nodes that are connected. The graph $G_t =< N, E >$ defines the *network topology* of the DAIS. The set M_i contains the neighbours of the node n_i.

$$\forall i = 1 \ldots N_n : M_i = \{n_j \in N \mid (n_i, n_j) \in E\} \quad (1)$$

The *degree* k of a node is the number of neighbours it has, $k_i = |M_i|$

All nodes contain an identical artificial immune system with the following properties

- **Self Set**
  It detects changes in a *Self Set* S, consisting of N_s binary strings of l bits.
- **Match-Rule**
  The contiguous bit matching rule, with match-length r is used. The probability of a match between 2 random string is [9].

$$p_m \approx 2^{-r}((l - r)/2 + 1) \quad (2)$$

- **Antibody Set**
  An algorithm such as the ones found in [7] is used to generate an *Antibody Set* A with N_a *Antibodies*.
- **Antibody Migration**
  At every time-step an antibody has a probability p_{am} of migrating to a node neighbouring the one it is currently found in. The destination node is also selected at random.
- **Antigen Set** Every node has an *Antigen Set* that contains N_g binary string and captures the current state of the environment. In contrast to the self set, this set may differ from node to node. The antigens bit-string are matched over time against the antibodies passing through the node to determine if they differ from the Self Set bit-strings.

Using these notations we can determine the number of time-steps needed to ensure that an arbitrary non-self antigen will be detected with some predetermined probability. This depends on the total number of distinct antibodies that have been present in the node while the antigen was matched against them. Therefore, the key is to understand the *Antibody Migration* behaviour in the graph.

2.2 The Ring Shaped DAIS

As a first example, we instantiate the model for a ring-shaped network. In this topology, every node has exactly 1 neighbour, and they form the only cycle in the graph. So, $M_i = \{N_{i+1}\}$ for $i < N_n$ and $M_{N_n} = \{N_0\}$, $k_i = 1$.

The crucial observation is that the probability $p_d(t)$ for an antibody to migrate over d nodes in time t follows the *binomial distribution* with parameters t and p_{am}. Because at every time-step it has a chance p_{am}

of migrating to the next node and the time-steps are independent.

Using the notation

$$C_k^n = \left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!}$$

$$p_d(t) = C_d^t \; p_{am}^d \; (1 - p_{am})^{t-d} \qquad \forall t \geq d \qquad (3)$$

This means that for a random node in the ring, at time t, the number of antibodies that passed through it starting from the node d edges away is

$$N_a \sum_{j=d}^{t} C_j^t p_{am}^j (1 - p_{am})^{t-j} \qquad (4)$$

So, for the entire ring, the total number of distinct antibodies encountered at the node after time t is equal to

$$N_a(t) = N_a[1 + \sum_{i=1}^{N_n - 1} \sum_{j=i}^{t} C_j^t p_{am}^j (1 - p_{am})^{t-j}] \qquad (5)$$

Assuming a self-set of random binary string, the non-self detection performance is [9]

$$p_d \approx 1 - e^{-p_m N_a(t)} \qquad (6)$$

which is reached at time-step t where

$$N_a(t) \approx -\frac{\ln(1 - p_d)}{p_m} \qquad (7)$$

2.3 The Fully Connected DAIS

From the perspective of building a robust network, the ring-shaped topology example is far from optimal. With *robustness* we mean tolerance of the graph's topology and other properties against errors, be it the failure of nodes in the graph or the removal of edges between them. After only 2 nodes are removed, it breaks up in 2 disconnected parts. Removing even more nodes creates more disconnected chain-like graphs of rapidly decreasing size.

Going to the other extreme, instead of connecting every node to only 1 neighbour, we can connect all nodes to all other nodes. So, $M_i = N \backslash \{N_i\}$ and $k_i = N_n - 1$.

In this configuration, for any node, at any time-step, the chance that a random antibody will migrate to it is

$$p_n = \frac{p_{am}}{N_n - 1}$$

The probability that an antibody has visited a node k times at time-step t follows the binomial distribution with parameters p_n and t. So, at time-step t an antibody has been at a node once or more times with probability

$$\sum_{i=1}^{t} C_i^t p_n^i (1 - p_n)^{t-i}$$

And since all N_n nodes contain N_a antibodies, the total number of distinct antibodies encountered at any node after time t is equal to

$$N_a(t) = N_a[1 + (N_n - 1) \sum_{i=1}^{t} C_i^t p_n^i (1 - p_n)^{t-i}] \qquad (8)$$

Since all pairs of nodes are connected to each other, this kind of topology is maximally robust against node failures. But the number of edges grows quadratic in the number of nodes. This soon becomes unrealistic for large networks because in actual applications an edge corresponds to a communication channel that consumes resources of some kind (e.g. bandwidth on a LAN).

3 Complex Network Theory

Keeping the above examples in mind, we would like to find a type of graph that is tolerant against removal of nodes and at the same time, its number of edges shouldn't grow too fast with the number of nodes. Also, we would like to keep the ability present in the fully connected graph to travel between any 2 nodes in a small number of steps.

3.1 Graph Theory

Before using the graphs from complex network theory we need to state some concepts from graph theory.

- A graph is *connected* if there is a *path* between any two nodes, if there is at least one way to go from any node to any other node by following the edges of the graph.
- The *path length* between two nodes is the minimum number of edges that have to be followed between the nodes. The *diameter* of a graph is the maximum path length between any two nodes.
- A *small world* graph has, despite it's large number of nodes, a relatively short path between any two nodes.

- The *degree distribution* of a graph captures the spread in the number of edges a node has. The probability distribution function $P(k)$ gives the probability that a randomly selected node has exactly k edges.

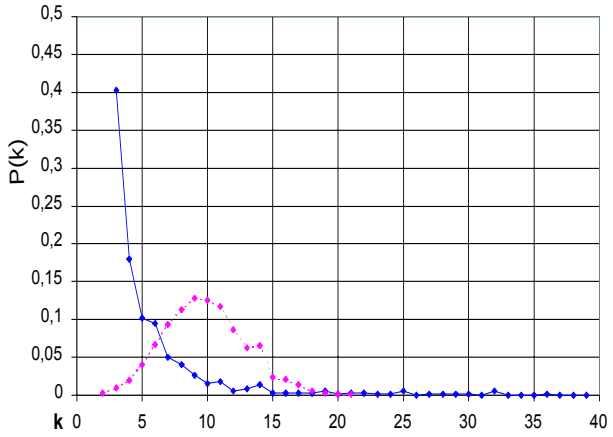

Figure 1: Degree Distribution of an Barabási-Albert (solid) graph of 1000 nodes with $m = 3$ and an Erdős-Rényi graph (dashed) with $p = 0.01$ and 1000 nodes.

3.2 Graph Models

The *Erdős-Rényi* or *ER* model was the first [8] *random graph* model. It is defined as follows: starting with N unconnected nodes, every pair of nodes is connected with probability p. Consequently, the total number of edges is a random variable with expectation value $E(n) = p\frac{N(N-1)}{2}$. A large number of interesting properties have been proven for this model, of which the following are important with respect to using it to embed a DAIS:

- If $p \geq \ln(N)/N$ the graph is totally connected.
- These graphs have the small world property. Their diameter scales logarithmically with the number of nodes and is concentrated around

$$d = \frac{\ln(N)}{\ln(pN)}$$

- The degree distribution follows a binomial distribution with parameters $N - 1$ and p. As figure 1 (dashed) shows, this means that the degrees of the nodes are concentrated around pN, resulting in a rather homogeneous graph.

The *Barabási-Albert* (*BA*) or *Scale-Free* model was first used in [2] to describe a wide variety of real-world networks that are all scale-free. That is, their degree distribution follows a power-law for large k : $P(k) \sim k^{-\gamma}$. Two ingredients are needed in the construction of such graphs :

- *Growth* Every node that is added to the graph links to m different nodes already present.
- *Preferential Attachment* The probability that a new node will link to node i depends on the degree k_i of node i as

$$\Pi(k_i) = \frac{k_i}{\sum_j k_j}$$

Following this procedure results in a graph with degree distribution $P(k) \sim k^{-3}$ for large k. Per definition, this kind of graph is connected. The number of edges is always equal to $2mN$ and it also has the small world property, the average path length increases approximately logarithmically with N. In contrast to the Erdős-Rényi model, the degree distribution always gives rise to a few nodes with very high degree (as e.g. in figure 1, solid line at $k = 32$). This makes the graph more heterogeneous, with a large majority of nodes having few connections but also some very highly connected ones. These nodes play an important role in the topology of the graph, as will become clear in section 4.

3.3 General Graph DAIS

To embed a DAIS in the above models, we need to derive the antibody migration behaviour. But in contrast to the ring and connected ones, the topologies of these models are not so trivial. The degree of their nodes can vary widely, having a large impact on the amount of communication between a node and it's neighbours. Nodes with more connections will receive more antibodies than ones with fewer connections and will sooner reach the number of antibodies necessary for the desired detection probability.

Therefore it makes sense to look at nodes with different degrees separately. A useful approximation to make is to regard a neighbouring node as totally average, with average number of antibodies N_a and average degree $\langle k \rangle$. Therefore, in a node with degree k, the number of antibodies entering at every time-step is equal to

$$in_k = \frac{N_a p_{am}}{\langle k \rangle} k \tag{9}$$

If we call $DN_a(k)$ the number of antibodies present at a node of degree k at time t, the amount of antibodies leaving each time-step is per definition $DN_a(k)p_{am}$.

The dynamics of this kind of system will converge to a state where the number of entering and leaving antibodies equals out. This happens when

$$DN_a(k)p_{am} = \frac{N_a p_{am}}{\langle k \rangle}\ k$$

So a node with degree k will converge to a state where it's number of antibodies is centred around

$$DN_a(k) = \frac{N_a}{\langle k \rangle}\ k \tag{10}$$

Figure 2 shows an illustration of this for a BA graph of 1000 nodes with $m = 5$. The figure shows plots of the average number of antibodies present in the nodes of degree 5 up to 15. All nodes initially have 100 antibodies. Depending on their degree they converge to a state where they have approximately $DN_a(k)$ antibodies.

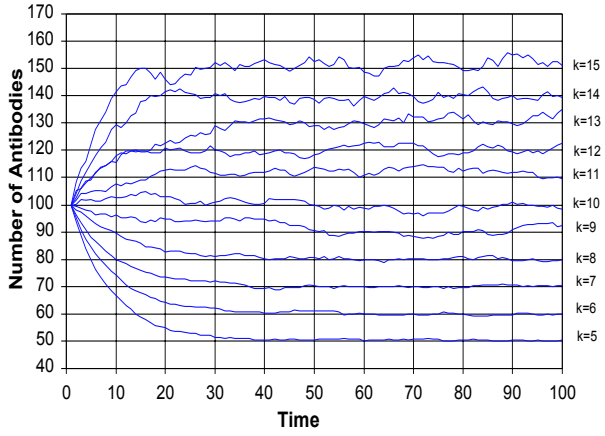

Figure 2: Average number of antibodies in nodes of degree k over time. In a BA graph of 1000 nodes with $m = 5$, $p_{am} = 0.1$, $N_a = 100$, $\langle k \rangle = 9.97$

So, for all nodes of degree k, at every time-step the chance that a random antibody will migrate to it is equal to

$$p_n(k) = \frac{in_k}{N_a N_n} = \frac{\frac{N_a p_{am}}{\langle k \rangle}\ k}{N_a N_n}$$

As before, the probability that an antibody has visited a node a number of times at time-step t follows the binomial distribution with parameters p_n and t. So, at time-step t an antibody has been in a node with degree k once or more times with probability

$$p_n(k)(t) = \sum_{i=1}^{t} C_i^t p_n(k)^i (1 - p_n(k))^{t-i} \tag{11}$$

Taking the weighted sum over the degree distribution of the graph, gives the final approximation of the antibody migration behaviour in an arbitrary graph

$$N_a(t) = N_a[1 + (N_n - 1)\sum_{i=1}^{N_n} P(i)p_n(i)(t)] \tag{12}$$

4 Error and Attack Tolerance

In the previous section we already noted that the ER and BA graph models contain far fewer edges (and hence consume less resources) than the fully-connected case, respectively $p\frac{N(N-1)}{2}$ and $2mN$ edges. In this section we use results from graph theory to show that, despite their relatively few edges, a DAIS embedded in these graphs can survive under high error rates and attacks. When nodes are removed from the graph, the performance will degrade gracefully until a critical threshold is reached and the graph suddenly collapses.

In the following, two types of node removal are looked at. *Error tolerance* is simulated by removing randomly selected nodes from the graph, corresponding to the random failure of nodes. In *Attack tolerance* the most connected nodes are removed, simulating a pre-determined attack with as much disruptive effect is possible.

4.1 Largest Cluster Size

Looking at the general antibody migration equation 12, it is clear that there are 2 values that determine how well a DAIS survives under error or attack conditions : the number of nodes N_n and $p_n(k)$. We will concentrate on the N_n factor. If the graph breaks up into 2 or more parts, or *clusters*, the set of nodes with which a node in the DAIS can communicate are suddenly limited to the ones in it's cluster. Since $N_a(t)$ scales linearly with the number of nodes (N_n), this greatly affects the detection performance.

The relative size of the largest cluster (i.e. the fraction of all nodes contained in the largest cluster) is an indicator of the state of fragmentation of the graph [1]. Figures 3 and 4 show plots of this measure for the ER and BA models, under both the error (solid lines) and attack (dashed lines) conditions. The ideal shape for the plots is the diagonal line, since it corresponds to the situation where the largest cluster contains all nodes that are still left in the graph.

4.2 Error Tolerance

Cohen *et al.* [5] and Callaway *et al.* [4] first studied the fragmentation of random and scale-free graphs under

random node failures. For both models, they conclude that there exists a *critical threshold* f_c for fragmentation at which the graph breaks down into tiny clusters. For ER graphs

$$f_c = 1 - \frac{1}{pN}$$

indicating that the larger the original average degree of the network, the larger the damage it can survive.

For Scale Free graphs with $\gamma > 3$

$$f_c = 1 - \frac{1}{\frac{\gamma-2}{\gamma-3}m - 1}$$

If $\gamma \leq 3$ however (as in the BA model used here, or the Internet), this critical threshold does not exist for infinite systems. For finite systems, a critical threshold is presents although at a very high node removal fraction > 0.99.

Figures 3 and 4 (solid lines), show a numerical simulation for a ER and BA graph under random node removal. As predicted, at $1 - pN = 1 - (0.006 \,.\, 500) = 0.7$ the ER graph starts to fragment into small clusters, while the BA graph shows no sudden fragmentation threshold. In summary, both models exhibit a very high degree of error tolerance, degrading gracefully up until a very high degree of node failure.

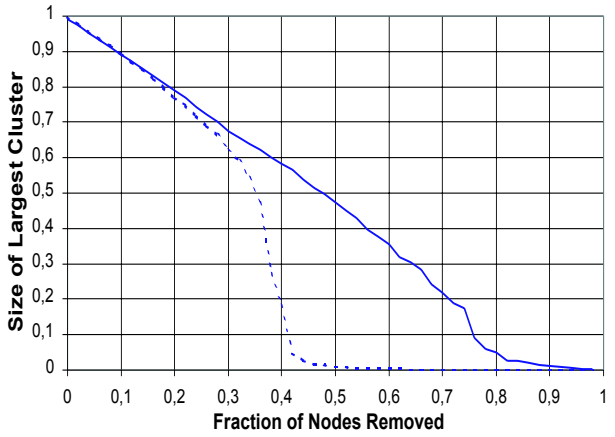

Figure 3: Relative Size of Largest Cluster in a ER graph with $N = 500$, $p = 0.006$ and hence $\langle k \rangle \approx 3$ under Error (solid) and Attack (dashed) conditions.

4.3 Attack Tolerance

As for attack tolerance, the results reached in the condensed matter physics community are not so clear yet. For both graph models, a sudden breakdown in the graph occurs when a critical fraction of nodes are removed. The figures illustrate this clearly. The BA

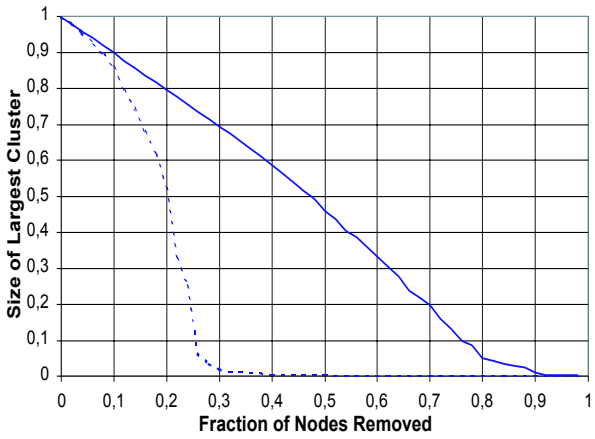

Figure 4: Relative Size of Largest Cluster in a BA graph with $N = 500$, and $\langle k \rangle \approx 3$ under Error (solid) and Attack (dashed) conditions.

model is much more sensitive to this kind of node removal because it contains a few, very important nodes with a very high degree that play an important role in the graph's topology. When these are progressively removed, the graph soon collapses. One recent result [5] concludes that for scale-free graphs with $\gamma > 2$ such a critical fraction exists. Since the ER model's critical threshold is higher than the BA model's, it should be used if tolerance against attacks is desired.

5 Possible Applications

As such, the above model and analysis can be applied to a large number of domains, not necessarily related to Artificial Immune Systems. In fact, all large scale communication networks containing a probabilistic element in the initiation of information exchanges can use it as a model. But here we will limit ourselves to some possible applications closely related to the original scope of this paper.

5.1 Applications

The first way of using it is as a plain parallelization of the standard AIS. The computational and memory complexity is distributed over the nodes in the graph, each taking on a part of the antibody generation and anomaly detection process. While the antibodies circulate, all nodes communicate back to one 'master' node which collects and synthesizes their result into one decision. More interesting is a truly distribution application. The nodes can be computers connected over a computer network (a LAN, or the Internet) running the same application (e.g. a Web Server). The

self-set consists of the normal data and/or instruction flow patterns of the application. These can be captured by monitoring the system-level calls or, when using Java technology, by hooking a custom-built code profiler into the Java Virtual Machine. The real difficulty here is in finding a suitable encoding for the large set of memory and instruction reference patterns that make up the normal behaviour of a large modern application. Alternatively, during the design or refactoring of a software product, this aspect can be taken into account and the program itself can be made to automatically output diagnostic behaviour to the DAIS. Other possibilities could be combining the ideas of this paper with the adaptive computer virus immune system introduced in [13] or the network intrusion detection models of [12] or [10]. Finally, applications where the robustness of the model is it's most important aspect can also be imagined. As shown above, given the right choice of graph, it degrades gracefully under failure or attack conditions.

5.2 Implementation

All simulations were generated using a Java implementation of the AIS and Graph Theory algorithms. The AIS package uses the standard bit-string representation or a generalized fuzzy set theory based one. For both representations, it includes the exponential time (from [9]) and greedy (from [6]) antibody generation algorithms, it can determine the optimal antibody morphology using an inductive algorithm and includes immune response models that use genetic antibody cloning. It has been tested on benchmark machine-learning datasets related to cancer diagnosis, the risk assessment of malaria cases and on a distributed physically security system using advanced video motion detection algorithms to encode the self-set. A visual front-end has been built that allows the user to connect to structured files or databases, visualize the data in 3D and acquire the self-set. All aspects of the AIS can be tuned via a GUI and it's behaviour can be monitored on new incoming data. To generate the results from the figures, several similar applications were linked together using the integrated support for the DAIS model described here.

6 Conclusion and Future Directions

6.1 Conclusion

We have shown how to construct large scale robust networks of communicating Artificial Immune Systems. A new model for a Distributed Artificial Immune Systems was introduced. We analysed the flow of antibodies in this DAIS model for the ring-shaped, fully connected and arbitrary graph topologies in order to arrive at a prediction for the detection performance over time in the nodes. The advantages and disadvantages of these topologies with respect to resource consummation and node failure tolerance were discussed using results from graph- and complex network theory. The ring-shaped and fully connected graphs were not robust against node failures or consumed too many resources. The ER and BA graphs on the other hand behaved excellent under node failure conditions, degrading gracefully up until very high failure rates. The authors feel that the primary contribution of the research is that we have shown how to predict the detection performance in a DAIS using these types of topologies. This result makes it possible to build large scale robust networks of artificial immune systems.

6.2 Future Directions

The DAIS model as well as it's implementation are currently being extended on several fronts. Work is underway to decentralize the graph building process. The graph topology construction algorithm in it's current state uses one central node that knows the entire graph structure to incrementally build the graph. This is unrealistic for very large scale networks and dangerous because it introduces a single point of failure. Due to the small-world properties of the graphs, it is possible to embed in every node the ability to add new nodes or even a self-healing graph construction algorithm that restores it's original topology's properties (e.g. degree distribution) after nodes have been removed.

Another track aims to heighten the detection performance by extending the immune system metaphor. In the biological immune system, molecules of the *Major Histocompatibility Complex* play the role of *antigen presentation* agents [15]. They bind to antigens and present them at the cell surface to the immune system's T cells. Each individual has a different set of MHC types, resulting in a slightly different resilience against antigens. This introduces a positive *population level* effect on the overall immunity of a species. This effect could be incorporated in the DAIS model as suggested in [11] by installing a random permutation mask on the self strings. This reduces the amount of holes [6] in the antibody space, especially near self-strings, heightening the detection probability of the system.

Not only antibodies could be circulated throughout the DAIS. An immune response model or antibody lifecycle model [11] can be included in the nodes. It could e.g. use genetic operators to clone successful

antibodies. This way, information about anomalies is automatically and rapidly distributed throughout the entire system.

The authors are now in the process of integrating these ideas into the DAIS model and adapting the implementation accordingly.

7 Acknowledgments

This work has been supported by Data4s Future Technologies, Leuven, Belgium and Starlab Research, Brussels, Belgium. Johan Kaers would like to thank Pedro Rosas for the helpful suggestions about the manuscript. Richard Wheeler would like to thank Prof. Peter Ross and Prof. Donald Michie for their support.

References

[1] R. Albert and A.-L. Barabási, *Statistic Mechanics of Complex Networks*, in Reviews of Modern Physics 74, 47, 2002.

[2] A.-L. Barabási, R. Albert, *Emergence of Scaling in Random Networks*, Science 286, 509-511.

[3] G. Bianconi, A.-L. Barabási, *Bose-Einstein condensation in complex networks*, e-print arXiv:cond-mat/011224 13 November 2000

[4] D. S. Callaway, M. E. J. Newman, S. H. Strogatz and D. J. Watts, *Network robustness and fragility : Percolation on random graphs*, e-print arXiv:cond-mat/0007300v2 19 October 2000

[5] R. Cohen, K. Erez, D. ben-Avraham, S. Havlin, *Resilience of the Internet to random breakdowns*, e-print arXiv:cond-mat/0007048v2 19 October 2000

[6] P. D'haeseleer, S. Forrest, P. Helman. *An immunological approach to change detection : Algorithms, analysis and implications*, in Proceedings of the 1996 IEEE Symposium on Research in Security and Privacy, pages 110-119, IEEE Computer Society Press, Piscataway, New Jersey.

[7] P. D'haeseleer, *Further efficient algorithms for generating antibody strings*, Technical Report CS95-3, The University of New Mexico, Albuquerque, NM, 1995.

[8] P. Erdős, A. Rényi, 1959, Publ. Math. Debrecen **6**, 290.

[9] S. Forrest, A. S. Perelson, L. Allen, R. Cherukuri, *Self-nonself discrimination in a computer.*, in Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy, Los Alamitos, CA : IEEE Computing Society Press, 1994.

[10] S.A. Hofmeyr, *An Immunological Model of Distributed Detection and its Application to Computer Security*, Ph.D. Thesis, University of New Mexico, May 1999

[11] S. A. Hofmeyr, S. Forrest, *Architecture for an Artificial Immune System*, in Evolutionary Compation 8(4): 443-473, 2000

[12] J. Kim, P. Bentley, *An Artificial Immune Model for Network Intrusion Detection*, Proceedings of the 7th European Congress on Intelligent Techniques - Soft Computing (EUFIT'99). Aachen, Germany. September 13-19, 1999.

[13] Gary B. Lamont, R. E. Marmelstein, D. A. Van Veldhuizen, *A Distributed Architecture for a Self-Adaptive Computer Virus Immune System*, Chapter 11 in New Ideas in Optimization. Ed., Corne, Dorigo, and Glover, McGraw Hill, 1999

[14] M. E. J. Newman, *Ego-Centered networks and the ripple effect -or- Why all your friends are weird*, e-print arXiv:cond-mat/0111070v1, 5 November 2001

[15] P. Parham, *The Immune System*, Garland Publishing/Elsevier Science, 2000

[16] R. Pastor-Satorras, A. Vespignani, *Optimal Immunisation of Complex Networks*, e-print arXiv:cond-mat/0107267, 30 July 2001

[17] S. H. Strogatz, *Exploring Complex Networks*, Nature, Vol 410, p268-276, Macmillan Magazines Ltd., 8 March 2001