

Simulating Network Robustness: Two Perspectives on Reality

Dr. Anthony Dekker

Defence Science and Technology Organisation, Canberra, Australia

dekker@ACM.org

Abstract. Two important recent trends in military and civilian communications have been the increasing tendency to base operations around an internal network, and the increasing threats to communications infrastructure. In the civilian sphere, the threat is from terrorist attacks, while in the military sphere this comes from the increasing tendency to view communications networks as high-value targets. This combination of factors makes it important to study the robustness of network topologies. The obvious measures of network robustness are the graph-theoretic concepts of node and link connectivity, and we argue that node connectivity is the best of these. We have developed a network analysis, design, and simulation package, called CAVALIER. We use the agent-based combat simulation feature of CAVALIER to explore the impact on performance of 300 randomly generated network topologies. Simulation results show that node connectivity correlates positively with performance, and is a better predictor of performance than other measures of network robustness. Furthermore, node connectivity provides the best complement to a previously developed measure of network efficiency (the intelligence coefficient). Together the two measures provide an excellent way of assessing network quality. We therefore have two perspectives on reality: our agent-based simulation, and the mathematics of graph theory, which provide the same answer, and therefore give greater assurance that node connectivity is indeed the best measure of network robustness in the face of potential node destruction.

1. INTRODUCTION

There have been two important recent trends in both military and civilian communications. The first is network-centric operation, which bases organizational activity strongly around an internal network. In the civilian sphere, this is called e-commerce. In the military sphere, this is called Network Centric Warfare (NCW). To quote Alberts *et al* [1]:

“We define NCW as an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.”

The second trend is the increasing threat to communications infrastructure. In the civilian sphere, the threat is from terrorist attacks, while in the military sphere this comes from the increasing tendency to view communications networks as high-value targets.

The first trend makes networks more important, while the second makes them more vulnerable. This dilemma makes it critically important to address network robustness, i.e. the continued ability of the network to perform its function in the face of attack.

Designers of communications networks must therefore assume that networks will be attacked, and that some of these attacks will result in damage. Robust networks will continue functioning in spite of such damage and outages.

In this paper, we specifically focus on the robustness of the network *topology*. We use *graph theory* to investigate which network topologies are the most robust. Graph theory provides two different measures of *connectivity*, which are possible ways of measuring robustness, and we argue that *node connectivity* is the most useful of these.

In order to further investigate these issues, we have developed a powerful network analysis and design tool called CAVALIER, and we have integrated into it an agent-based combat simulation for evaluating network architectures. Our simulation is Java-based, taking advantage of Java's object-oriented and dynamic instantiation capabilities. Experiments with the simulation confirm the usefulness of node connectivity as a robustness measure, thereby providing greater assurance that it is indeed best.

2. GRAPH CONNECTIVITY

A natural way to model the topology of a communications network is as an (undirected) *graph* consisting of *nodes* and *links*. For the purposes of analysing topology, we ignore any variation in the *type* of links. Robustness of the topology will come from the presence of *alternate paths*, which ensure that communication remains possible in spite of damage to the network.

If a graph has n nodes, then we say that the graph has *size* n . If a node has d outgoing links, we say that the node has *degree* d . The minimum degree d_{\min} of the graph is the smallest of the node degrees, and the maximum degree d_{\max} of the graph is the largest of the node degrees.

There are two generally accepted concepts of connectivity for a graph that can be used to model network robustness:

- 1) The *node connectivity* κ is the smallest number of nodes whose removal results in a disconnected or single-node graph.
- 2) The *link connectivity* λ is the smallest number of links whose removal results in a disconnected graph.

For example, K_n , the completely connected graph of size n , with each node connected to the $n-1$ others, has $\kappa = \lambda = n-1$.

It will always be the case that $\kappa \leq \lambda \leq d_{\min}$ [11]. According to Menger's Theorem [10], the above definition is equivalent to the following:

- 1) The node connectivity κ is the smallest number of node-distinct paths between any two nodes.
- 2) The link connectivity λ is the smallest number of link-distinct paths between any two nodes.

This formulation clarifies the relationship between the connectivity measures and the presence of redundant paths. The node and link connectivity measures can be calculated using the maximum-flow algorithm [10], and we have developed a network design and analysis tool called CAVALIER that incorporates these calculations.

The CAVALIER tool also performs statistical and graph-theoretical network analyses, 2-dimensional and 3-dimensional visualisation [3], and has a simulation capability to assess network performance [5],[7]. All the figures in this paper were produced using the CAVALIER tool.

When modelling network robustness in the face of equipment failures (particularly for civilian networks) we would expect *link connectivity* to be the most useful. Random equipment failures, by affecting cables, interfaces, circuit boards, etc. would primarily put links out of action. On the other hand, when modelling network robustness of military networks in the face of combat (and indeed also of civilian networks in the face of terrorist activity), the major threat is the destruction of entire nodes (usually by explosive means). In this case, we would expect *node connectivity* to be the most useful in modelling robustness. Section 4 describes our combat simulation experiment which confirms that this is, in fact, the case. Furthermore, there is a statistically significant correlation between node connectivity and performance. Since simulation and theoretical reasoning give the same answer, this supports our choice of node connectivity as the appropriate metric.

The properties of the node and link connectivity measures are discussed in detail in [8]. If $\kappa = \lambda = d_{\min}$ for some graph, we say that the graph is *optimally*

connected, since the node and link connectivities are as high as possible, i.e. the network is as robust as it could be, given the value of d_{\min} . See [8] for a more detailed discussion of this concept, which is also related to the *symmetry* of a graph. Figure 1 shows two graphs with different kinds of symmetry. The graph in Figure 1(a) has $\kappa = \lambda = 1$, while the ‘‘soccer-ball’’ graph in Figure 1(b) has $\kappa = \lambda = 3$, and is therefore optimally connected.

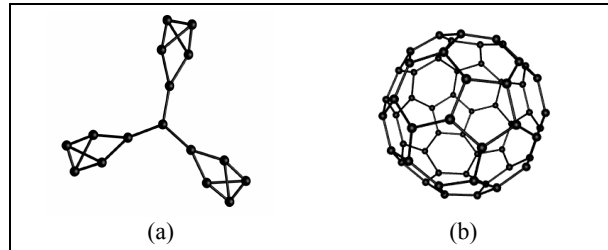


Figure 1: Two Graphs with Different Symmetry

3. RANDOM GRAPHS

There is interesting relationship between optimal connectivity and graphs that are created by making connections at random, i.e. with a fixed probability p of an edge between any pair of nodes (the Erdős-Rényi model). We generate 300 random graphs of this kind in our simulation experiment.

Bollobás [2] has proved that, with probability approaching 100%, such random graphs will be optimally connected (irrespective of the value of p). More precisely, for any randomly generated graph of size n , the probability that $\kappa = \lambda = d_{\min}$ approaches 1 as $n \rightarrow \infty$ (this suggests that such random graphs may be useful militarily for e.g. ‘‘swarms’’ of many low-cost unmanned aerial vehicles or UAVs [14], although the connections must be made genuinely at random, rather than depending on the physical distances between nodes).

Convergence here is surprisingly rapid. In a simple test of 200,000 random graphs with size n ranging from 7 to 30 and average degree \sqrt{n} , we found that the percentage of optimally connected graphs increased from 94.8% for $n=7$ to 99.98% for $n=30$. The percentages fitted very closely (with a correlation of 0.97) to the curve $100 - 20e^{-0.2n}$. This result is indicative only, but if extrapolation of this were valid, the percentage of optimally connected graphs for $n=100$ would be approximately 99.9999999%.

4. SIMULATION

In order to examine the usefulness of the connectivity measures κ and λ in a military combat environment, we utilised an agent-based simulation (or *distillation*) testbed that we have developed and integrated into CAVALIER for assessing NCW architectures [5],[7]. This testbed was one of the first agent-based distillations for exploring NCW, although Version 3 of

the MANA tool [13] now provides a more sophisticated tool for exploring NCW.

Agent-based simulations or distillations such as these provide an effective way of exploring “universal truths rather than situational specifics” [9], which is what we are attempting to do in this work.

In our testbed, a simulated networked friendly force of 10 units engaged in combat with a non-networked enemy force of 30 units. The combat took place on a 12×12 discrete grid containing obstacles. Simulation time was also discrete, occurring in distinct *timesteps*. Figure 2 shows an example combat session.

The agent-based simulation integrated into CAVALIER allows the specification of arbitrary network topologies, which can be edited using CAVALIER’s graphical editing capabilities. Each agent has a number of behaviour “slots” for sensors, movement, weapons, etc. These “slots” are filled by a reference to a Java class (satisfying an appropriate interface) and a list of parameter values, and these “slots” can also be edited using CAVALIER’s graphical editing capabilities. When the simulation begins, the relevant behaviour classes are dynamically loaded, which means that modified classes can be written and integrated very easily. The resulting modularity greatly simplifies experimentation.

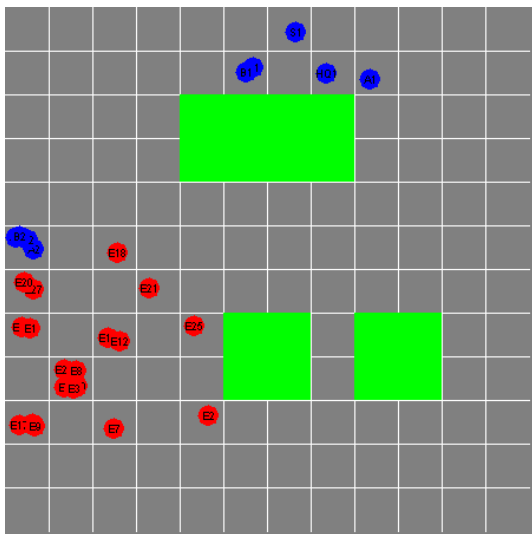


Figure 2: Example Combat Session

We conducted Monte Carlo simulations of combat (typically taking 30 to 70 timesteps) until one side was annihilated or a limit of 100 time steps was reached. The friendly force had the structure shown in Figure 3. There were two long-range sensors (*S1* and *S2*), two headquarters units (*HQ1* and *HQ2*), and six combat units in the friendly force.

The six combat units had on-board sensors capable of locating enemy units, but the range of their weapons was greater than the range of their sensors (sensor ranges were 8 grid squares for the long-range sensors, and 2 for combat units, while weapons ranges were all 4). Consequently, the friendly force was not fully effective unless it could effectively use the information

gathered by the two long-range sensors (and also the on-board sensors of other combat units).

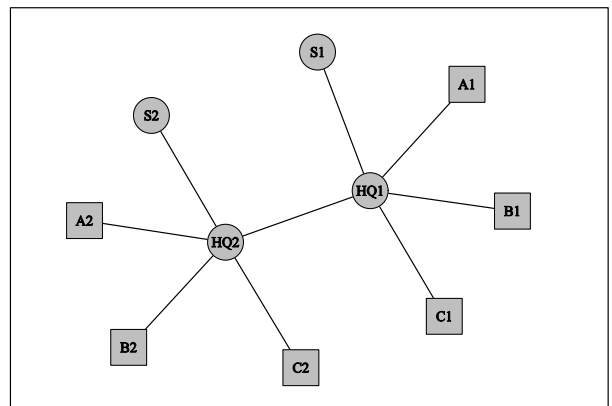


Figure 3: Structure of Networked Friendly Force

In addition, combat units had weapons systems with different characteristics, so that there was a benefit in using the network to work together. Combat units consisted of simulated infantry, ground attack aircraft (which could destroy multiple enemy units in a single grid square), and artillery (which had limited lethality but was very effective in suppressing enemy fire).

Messages sent along network links reported each unit’s situational awareness picture, similar to the use of messaging in MANA [13].

The enemy force, on the other hand, consisted of 30 identical combat units without networking. Each of these units had short-range weapons and sensors, and was programmed to attack towards the friendly base at the top-left corner of the simulated world.

In order to investigate the impact of network connectivity, we randomly generated 300 networks, consisting of the links in Figure 3 together with up to 32 additional links. Consequently, the node connectivity κ and the link connectivity λ varied from 1 to 7. In order to compare these two definitions of connectivity, we ensured that 50% of the sample contained networks with $\kappa \neq \lambda$. In view of the result in Section 3, this required discarding several thousand networks with $\kappa = \lambda$. We also examined an additional factor: we varied the *quality* of individual links, with a communication delay ranging from 1 to 4 timesteps on each link. Our reason for this was to study possible interactions between link quality and network topology. For the purpose of analysis, we took the *value* of a link with delay δ to be $1/\delta$.

As a measure of effectiveness for the friendly force, we used the natural logarithm of the Adjusted Loss Exchange Ratio (ALER). To be precise, if C_e are enemy casualties (ranging from 0 to 30), and C_f are friendly casualties (ranging from 0 to 10), our effectiveness score is:

$$\text{score} = \ln \text{ALER} = \ln \left(\frac{1 + C_e}{1 + C_f} \right)$$

This measure of effectiveness has the advantage of being symmetric (inverting the ratio merely changes the sign of the result), and we have used it with success in previous studies [5],[7]. It avoids division by zero, and has better statistical properties than the more commonly used loss exchange ratio (C_e/C_f). Specifically, it has the advantage of being almost exactly normally distributed (values of skew and kurtosis are very small: -0.006 and -0.05 respectively). This allows us to use regression analysis to study variation in scores.

To reduce random noise, the score for each randomly generated network was averaged over 10 simulated combat sessions. These averages ranged from 0.7 to 2.6, with a mean of 1.7. The corresponding ALER values are 2 to 13, with the mean corresponding to an ALER of 5.3.

The data still contains a large random component, as indicated by the vertical axis of Figure 4. This is due mostly to a substantial “luck” factor, which is inevitable in simulating small unit engagements of this kind. For example, a lucky early hit by the enemy on a long-range sensor has a large impact on the end result. Agent-based simulations of this kind typically average over a much larger number of runs [9],[12], but this requires the use of supercomputing facilities to which we did not have access. Instead, we have used regression analysis to reveal patterns in the data.

We first examined the relationship between node (κ) and link (λ) connectivities and effectiveness scores. We also considered the average of the two connectivity measures: $(\kappa + \lambda)/2$. Table 1 shows the correlation coefficients, R^2 values (i.e. the squares of the correlation coefficients), and statistical significance (where p is the probability that the results could have been due to chance). The difference between these three metrics is small (but important) because κ and λ are themselves highly correlated for randomly generated graphs, as a consequence of the properties described in Section 3.

Table 1: Correlation between Connectivity Measures and Scores

Measure	Correlation Coefficient	R^2	Statistical Significance
κ	0.37	0.14	Extremely High ($p < 10^{-10}$)
$(\kappa + \lambda)/2$	0.35	0.12	Extremely High ($p < 10^{-9}$)
λ	0.33	0.11	Extremely High ($p < 10^{-8}$)

Clearly, node connectivity is the best predictor of the effectiveness score, although the correlation is weak (the regression equation is $0.066\kappa + 1.44$). The superiority of node connectivity confirms our expectation, since node connectivity best reflects the threat of node destruction in combat. The weakness of the correlation is due partly to randomness in the data,

and partly to the fact that the node connectivity κ does not reflect variation in link quality.

It is interesting to compare these results to those of [15], which studied evolutionary adaptation among networks restricted to node connectivity $\kappa = 1$ or 2 (but using a more complex definition of connectivity), and found that evolutionary processes produced a $\kappa = 2$ network (i.e. a ring) when robustness was important.

It is possible to turn each connectivity measure into an “overall” measure of network quality by incorporating a measure of link value (recall that we took the value of a link with delay δ to be $1/\delta$). We considered four combined measures: multiplying the three connectivity measures in Table 1 by the average link value α , and also the average weighted degree d_{ave} , calculated by:

$$d_{ave} = \frac{1}{n} \sum_{ij} w_{ij}$$

where w_{ij} is the link value from node i to node j , or 0 if there is no link.

These measures were highly skewed, and so regression analysis required taking the logarithm of these values, to obtain an approximately normal distribution. Table 2 shows the results of regression analysis.

Table 2: Correlation between Adjusted Connectivity Measures and Scores

Adjusted Measure	Correlation Coefficient	R^2	Statistical Significance
$\ln \alpha\kappa$	0.46	0.21	Extremely High ($p < 10^{-16}$)
$\ln \frac{1}{2}\alpha(\kappa + \lambda)$	0.44	0.20	Extremely High ($p < 10^{-15}$)
$\ln \alpha\lambda$	0.43	0.18	Extremely High ($p < 10^{-13}$)
$\ln d_{ave}$	0.45	0.21	Extremely High ($p < 10^{-15}$)

We can see that $\alpha\kappa$, the node connectivity multiplied by the average link value, provides the best predictor of the effectiveness of the networked force for this scenario.

We could use this measure as a quick “back of the envelope” assessment of network quality. In previous work [4],[5] we have examined several such measures for assessing network quality, and have found a measure that we call the *intelligence coefficient* to be the most consistently useful over a range of different scenarios.

The intelligence coefficient I is obtained by summing (over all combat nodes and all relevant sensors for that node) the quotient of sensor quality and total path delay, i.e.

$$I = \sum_{ij} \frac{q_i}{\Delta_{ij}}$$

where Δ_{ij} is the total path delay from sensor node i to combat node j (or ∞ if there is no connection), and q_i is the quality of sensor i . Essentially the intelligence coefficient measures the ability of the network to effectively move sensor information to the point where it is needed.

In this experiment, we took the sensor quality to be the area covered by each sensor (i.e. very large for the long-range sensors, and less for the on-board sensors on combat units). Again, the high degree of skew in intelligence coefficient values required us to take logarithms.

Values of I ranged from 31 to 218, and so $\ln I$ ranged from 3.4 to 5.4. The correlation between $\ln I$ and scores was 0.42 ($R^2 = 0.17$), and the statistical significance was extremely high ($p < 10^{-13}$).

This correlation is less than for $\ln \alpha\kappa$ since the intelligence coefficient I incorporates no information about network robustness. Since the intelligence coefficient I has proven itself useful in several different scenarios, we therefore ask: which of the seven measures that we have examined best adds additional value to it?

Table 3 shows the correlation and R^2 values for two-variable linear models (of the form $a \ln I + b x + c$), and the statistical significance for the second variable.

Table 3: Correlation for Two-Variable Models using Intelligence Coefficient

Second Variable	Correlation Coefficient	R^2	Significance of 2 nd Variable
κ	0.47	0.22	Very High ($p < 0.0002$)
$(\kappa+\lambda)/2$	0.46	0.21	High ($p < 0.001$)
λ	0.45	0.21	High ($p < 0.002$)
$\ln \alpha\kappa$	0.46	0.21	Poor ($0.02 < p < 0.05$)
$\ln \frac{1}{2}\alpha(\kappa+\lambda)$	0.45	0.20	Very Poor ($0.05 < p < 0.1$)
$\ln \alpha\lambda$	0.44	0.19	Not significant ($p > 0.1$)
$\ln d_{ave}$	0.46	0.21	Not significant ($p > 0.1$)

Table 3 shows that, of the seven measures examined, the node connectivity κ adds the most value to the intelligence coefficient I . This is because it best expresses what is missing from the intelligence coefficient: the impact of node destruction. The other measures also combine robustness with other network characteristics, but less well than the combination of the intelligence coefficient I and the node connectivity κ .

The equation of best fit was:

$$\text{score} = \ln \text{ALER} \approx 0.24 \ln I + 0.042 \kappa + 0.51$$

and is illustrated graphically in Figure 4 (data points in Figure 4 are labelled with the value of κ , and vertical and horizontal lines indicate the means and standard deviations). This regression equation corresponds approximately to:

$$\text{ALER} \approx 1.6 \sqrt[4]{I} (1.043)^\kappa$$

Given the range of values present in the data, varying I from minimum to maximum adds 0.46 to the score (equivalent to increasing the ALER by 60%), and varying κ from 1 to 7 adds 0.25 to the score (equivalent to increasing the ALER by 30%). Varying I and κ simultaneously adds 0.71 to the score (equivalent to doubling the ALER).

The power of 0.24 for the intelligence coefficient I in this regression equation is consistent with the re-analysis of our previous simulation studies [4],[5],[7] summarised in Table 4 (these studies did not consider connectivity). The power for the intelligence coefficient I in these previous studies ranged from 0.27 to 0.33. Correlation and R^2 values for these studies are higher, either because there was averaging over more runs, or because the simulation was simpler and less susceptible to random events. Since these studies were quite different from the study reported here, we have tentative support for a general principle that performance of a C3I network is related to the cube root or fourth root of the intelligence coefficient.

Table 4: Correlation between Intelligence Coefficient and Performance in Previous Studies

Study	Power of I	R^2	Corr. Coeff.
SCUD Hunt [4] (after adjusting for tempo)	0.27	0.59	0.77
Target search in land environment [5]	0.33	0.95	0.97
Cultural difference study [7]	0.31	0.66	0.81

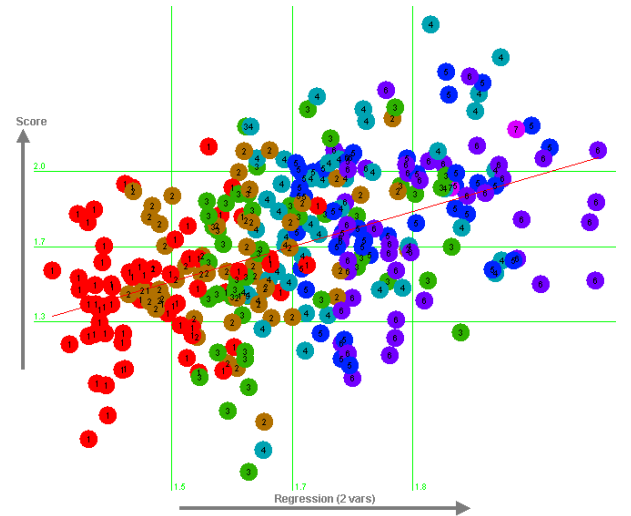


Figure 4: Scatter Diagram for Best Two-Variable Regression Equation against Effectiveness Score

5. CONCLUSIONS

Our experiment has thus demonstrated that node connectivity κ is, as expected, the best measure of network robustness in a military combat environment. It has a higher correlation with the effectiveness score than the link connectivity λ , and it adds the greatest value to our pre-existing measure of network quality (the intelligence coefficient I). Together these two measures provide an excellent way of assessing network quality, and Figure 4 shows the ability of these two measures together to predict performance. Naturally, performance in a combat situation also has a substantial random component.

Since both theoretical reasoning using graph theory, and agent-based simulation using CAVALIER, have predicted the usefulness of the node connectivity κ in predicting performance (in the face of potential node destruction), we have considerable assurance in our assertion that node connectivity is indeed the best measure of network robustness.

Our experiment has also demonstrated the usefulness of integrating analytical and simulation tools within the same package, as is done in CAVALIER. Such an integrated package permits easy comparison between analytical results and simulation results on the same set of networks.

In a more realistic simulation, we would of course also need to examine node robustness: the resistance of each individual node to attack. The robustness of a real-world network in the face of node destruction is a combination of network robustness (best modelled by κ , as we have seen), and the vulnerability of individual nodes to attack. In general, we can improve real-world network robustness by “hardening” individual nodes as well as by increasing the node connectivity. However, this does not detract from the importance of designing military communication networks to have high values of κ .

6. ACKNOWLEDGEMENTS

The author is indebted to Bernard Colbert and three anonymous referees for comments on earlier versions of this paper. Figure 1 was produced by interfacing CAVALIER to the Persistence of Vision™ ray-tracing package.

REFERENCES

1. Alberts, D., Garstka, J., & Stein, F. (1999) *Network Centric Warfare: Developing and Leveraging Information Superiority*, C4ISR Cooperative Research Program Publications Series, Department of Defense, USA. Available electronically at www.dodccrp.org/Publications/pdf/new_2nd.pdf
2. Bollobás, B. (2001) *Random Graphs*, 2nd edition. Cambridge University Press.
3. Dekker, A. (2001) “Visualisation of Social Networks using CAVALIER,” *Proc. Australian Symposium on Information Visualisation*, Conferences in Research and Practice in Information Technology vol. 9, Eades, P. & Pattison, T., Eds, Sydney, Australia, pp 49-55. Available at <http://crpit.com/confpapers/CRPITV9Dekker.pdf>
4. Dekker, A. (2002a) C4ISR Architectures, Social Network Analysis and the FINC Methodology: an Experiment in Military Organisational Structure, DSTO Report DSTO-GD-0313, January. Available at www.dsto.defence.gov.au/corporate/reports/DSTO-GD-0313.pdf
5. Dekker, A. (2002b) Applying the FINC (Force, Intelligence, Networking and C2) Methodology to the Land Environment, DSTO Report DSTO-GD-0341, October. Available electronically at www.dsto.defence.gov.au/corporate/reports/DSTO-GD-0341.pdf
6. Dekker, A. (2003a) “Centralisation and Decentralisation in Network Centric Warfare,” *Journal of Battlefield Technology*, vol. 6, no. 2, July, pp 23-28.
7. Dekker, A. (2003b) “Using Agent-Based Modelling to Study Organisational Performance and Cultural Differences,” *Proc. MODSIM 2003 International Congress on Modelling and Simulation*, Townsville, Queensland, pp 1793-1798. Available electronically at <http://mssanz.org.au/modsim03/Media/Articles/Vol%204%20Articles/1793-1798.pdf>
8. Dekker, A. & Colbert, B. (2004) “Network Robustness and Graph Topology,” *Proc. 27th Australasian Computer Science Conference*, Conferences in Research and Practice in Information Technology vol. 26, Estivill-Castro, V., Ed, Dunedin, NZ. Available at <http://crpit.com/confpapers/CRPITV26Dekker.pdf>
9. Fry, A. & Forsyth, A. (2002) “The Australian Army and Project Albert: Pursuing the Leading Edge of Military Thinking and Technological Development,” *Maneuver Warfare Science*, Horne, G. & Johnson, S. eds.
10. Gibbons, A. (1985) *Algorithmic Graph Theory*. Cambridge University Press.
11. Harary, F. (1969) *Graph Theory*. Addison-Wesley.
12. Horne, G., Johnson, S., & Meyer, T. (2000) “Project Albert: Overview,” *Military Operations Research Society Workshop on Advancing C4ISR Assessment*, Army War College, Carlisle, Pennsylvania, October.
13. Lauren, M., Engleback, N., Stephen, R., & Anderson, M. (2002) “Modeling Precision Maneuver Using Mana,” *Maneuver Warfare Science*, Horne, G. & Johnson, S. eds.
14. Parunak, H., Purcell, M., & O’Connell, R. (2002) “Digital Pheromones for Autonomous Coordination of Swarming UAV’s,” *American Institute of Aeronautics and Astronautics (AIAA) First Technical Conference and Workshop on Unmanned Aerospace Vehicles, Systems, and Operations*.
15. Venkatasubramanian, V., Katare, S., Patkar, P., & Mu, F. (2004) “Spontaneous Emergence of Complex Optimal Networks through Evolutionary Adaptation,” *Computers and Chemical Engineering* (in press). Available at <http://xxx.lanl.gov/abs/nlin.AO/0402046>