

# Co-operative Agents in Network Defence

**Robert Ghanea-Hercock**

BTexact Technologies

Adastral Park, B61,pp5, Martlesham, Suffolk, UK

Robert.Ghanea-Hercock@bt.com

## 1. Introduction

The question addressed in this paper is how can complex information networks survive hostile attacks and what mechanisms can increase survivability and defence in large-scale computing networks. As recent evidence indicates, firms, governments and other organisations urgently require better defensive strategies in cyberspace, (Anderson et al 1999, and Briney 2000). In particular, the ability of an information network to maintain itself in the face of continuous perturbation also raises more complex issues related to system metabolism, and network topology.

A multi-agent simulation model has been developed which demonstrates spontaneous group formation and the self-maintenance of group integrity. These system parameters are proposed as critical aspects in the defence of network systems. Each agent is susceptible to a modelled virus infection, passed between the agents. We then introduced an artificial immune system to each agent, which allows 'antibody' solutions to be exchanged between the agents within a social group.

The interest in this behaviour stems from the concept that by linking together the sensory and intelligence capabilities of a large number of agents distributed across a network we can *amplify* the ability of the network to resist attacks or intrusion. Specifically through social co-operation, agents can benefit from the combined defensive capabilities of their particular group.

## **2. Collective Defence**

### **2.1. Introduction**

The process of survival in natural agents is intimately linked with collaborative behaviour. Stereotypical examples include schooling in fish, and herding behaviour in land mammals. Natural systems have also widely employed distributed sensing and defensive processes, as in the social insects (Wilson 1971) and within multi-cellular organisms in the form of immune systems (e.g. Segel 1998). This paper therefore considers how to utilise social co-operation in software agents in order to achieve a group defensive capability.

### **2.2. The Problem**

There is an urgent demand within the computing industry for robust and secure systems and networks. Unfortunately the number of successful attacks is increasing via an increasing number of channels, e.g. email, worms, instant messaging, mobile devices, and wireless links. The almost religious belief in rigid corporate firewalls as a perfect defence is finally succumbing to the realisation that no static defence mechanism will ever suffice (Cohen 1997).

## **3. System Design**

The agent system presented in this paper models the secure transmission of useful pre-processed intrusion data through a large-scale computing network. The system is intended to operate as part of an intrusion detection system (IDS). Within proposed IDS (Cohen et al 1998), this approach is defined as "behavioural change detection".

In order to develop some understanding of the dynamics of agent interactions and group cohesion on the integrity of complex networks we created a multi-agent model as an experimental platform. Using this tool we investigated a range of behaviours which might influence the robustness and integrity of such a society of interacting agents. Within the agent group an attack on any one agent or host machine should be visible to other agents within the local domain of the agent. Hence warnings and defence solutions can be rapidly propagated throughout the network.

### **3.1. Metabolic Rate Sensors**

The key concept is to create an independent measure of the normal operational state of the network to be defended. By comparison with biological agents we need to create a measure of the *metabolic rate* of the services and data flow on the host network. This is achieved through each defence agent monitoring the flow of inter-agent traffic, in addition to monitoring any local host-specific intrusion sensors, such as port scanning alerts. By analogy with natural agents the first stage of most medical tests is to measure a few macro-scale variables, which are strong predicative indicators of the health of the organism, i.e. temperature, pulse and blood pressure.

## 4. Security Agents

Co-operative software agents have been frequently proposed as a tool for a variety of information processing tasks, i.e. e-commerce transactions (Maes et al. 1999), workflow modelling or as personal assistants (Etzioni 1996). However, relatively little research has considered their role as an element of network security, exceptions being (Crosbie & Spafford 1995, Helmer et al 1998).

### 4.1. Social Agent Models

The first question we need to address is what properties of a software agent make them suitable for inclusion in a security system. Software agents therefore possess a number of useful properties that would be beneficial in the construction of a distributed adaptive security system. In particular the ability to sense their environment and take proactive decisions against potential threats. The particular aspect of multi-agent systems that we have focused on is their ability to form dynamic social groups. The interest in this behaviour stems from the concept that by linking together the sensory and intelligence capabilities of a large number of agents distributed across a network we can *amplify* the ability of the network to resist attacks or intrusion. Specifically through social co-operation, agents can benefit from the combined defensive capabilities of their particular group.

## 5. Agent Defence Systems

Using a collective formation of smart software agents to form an adaptive immune-response structure within a network has been discussed in existing literature. Some preliminary work in this field has already demonstrated the effectiveness of such methods (Filman & Linden 1996, and Yialelis, Lupo & Sloman 1996). In particular work by Helmer et al (1998) demonstrates a multi-agent network defence system in which software agents monitor low-level network activity and report it to higher-level software agents for analysis. In the system proposed by Crosbie and Spafford (1995) a similar distributed set of agents monitors network traffic and machine activity, including CPU utilisation. The work by Carver et al (2000) demonstrates the use of a distributed heterogeneous group of agents as an IDS solution. The focus is on dynamic and adaptive response to varying levels of security threats. Work by Balasubramanian et al (1998) discusses a detailed design and methodology with common features to the proposed COSMOS system and model. The work by Qi He and Sycara (1998) demonstrates the use of encrypted KQML message exchange among a networked group of agents which is used for secure PKI certificate management. Parallel work on artificial immune systems has also been considered, (Forrest et al 1994, and Kephart 1994).

### 5.1 Comparison

The COSMOS project shares the concept of using a distributed set of co-operative software agents and adds the following novel feature:

Metabolic monitoring. COSMOS uses macro-scale changes in the behaviour and processes in a network in order to detect anomalous states, corresponding to attacks.

The system can then respond to any type of attack whether intrusions or viral attacks, unlike existing IDS systems.

## 5.2 Experiments

The agent simulation was developed using the REPAST agent toolkit from the University of Chicago (<http://repast.sourceforge.net/>). We first constructed a two-dimensional discrete spatial world model, in which a population of artificial agents could interact and move, based on the Sugarscape model (Epstein and Axtell 1996). This model was selected as it represents a suitable test case environment for investigating complex multi-agent simulations. The model is based on a population of agents, which are initialised randomly with the following set of variables:

- i) **Vision** – an agent can sense other agents and food objects within a specified radius from its own co-ordinates.
- ii) **Metabolism** – agents have an integer counter which represents their rate of energy consumption. Assigned randomly in a specified range. Increased whenever an agent is infected with a pathogen.
- iii) **Lifespan** – agents are initialised with a fixed lifespan, randomly assigned, typically between 20 – 200 time steps.
- iv) **Sugar** – agents require sugar to survive, which is an environmental resource. Sugar re-grows once consumed by an agent at some specified rate. Agents consume sugar by decrementing the value proportional to their metabolic rate. This would translate into an agents consumption of local CPU and machine resources.
- v) **Spice** – as described in the Epstein & Axtell model, a second commodity was introduced into the world which is only available from other agents, and is required for agent survival. Agents can only acquire spice when they engage in a trade interaction with another agent. The rules of trade are described in the following section.
- vi) **Immune system** – agents have an array of N characters, which represents a simplified immune system.
- vii) **Pathogens** – agents may be initialised with a dynamic array of viral infections, composed of short random character strings.

The simulation uses a tagging scheme on each agent in order to distinguish separate social groups of agents. The purpose of this design is to enable multiple groups of agents to coexist within the same physical Intranet environment and maintain independent operations and behaviours.

## 5.3 Experimental Objectives

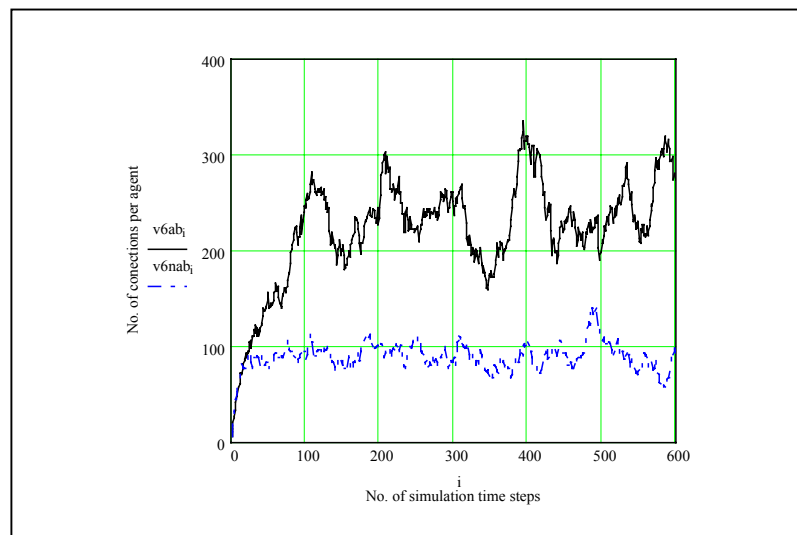
The first experiments were designed to study under what conditions socially co-operative groups of agents would spontaneously develop, using the defined model.

### *Immune System Development*

The second stage of the work involved adding an artificial immune model to the agents. During each trade interaction between two agents, the initiating agent is

passed a vector of  $N$  disease strings. Each string is a short sequence of characters, which the receiving agent then attempts to find a match for from its internal immune system, (a large array of character strings). Each string which the agents fails to match results in an increment to its metabolic rate. This results in a gradual degradation of an agent's ability to survive and a reduction in its lifespan. The agents can also undergo random mutation of elements in their immune system, in order to generate potentially novel "anti-body" solutions to current diseases in the population.

A second process was available in the simulation to allow agents to exchange a copy of the anti-bodies they have acquired, to each agent they trade with. Figure 1 illustrates the impact of allowing this co-operative inter-agent exchange to occur. The average number of social connections in the population more than doubles, indicating a significant increase in the agents state of health. This is also reflected in greater stability and lifespan of their social groups.



*Figure. 1. Graph of average number of connections per agent with 6 disease strings per agent. Upper trace shows the effect on the average health of the agents of allowing a co-operative exchange of anti-body vectors between agents during trading interactions.*

Figure 2 illustrates how sharing useful solutions to infections the agent population is able to eliminate the majority of infections in the case of a high degree of trust between the agents. The residual level is due to new agents joining the network and introducing new infections.

The metabolic conversions of such a cluster/group therefore contribute to defining its sense of self, (i.e. ability to recognise self-elements). Hence abnormal perturbations of the metabolic rate may be one method for agents to detect when attacks or intrusions are in progress.

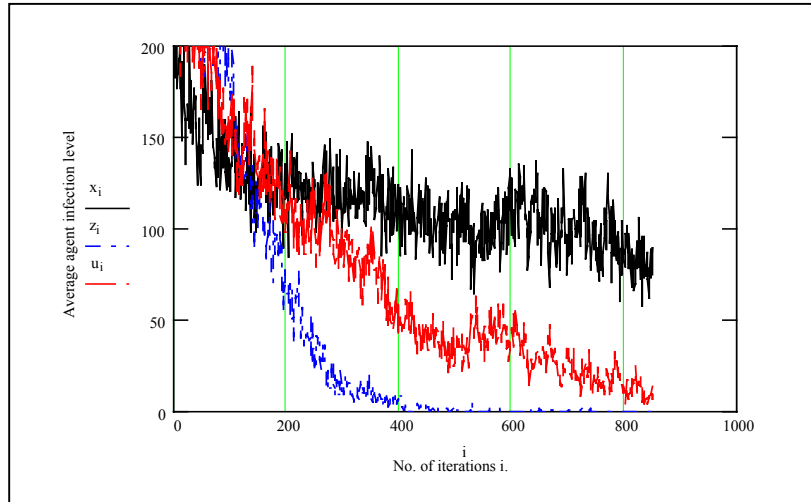


Figure 2. Graph showing decrease in average infection level with shared antibody process enabled between agents, (curve  $x_i$  trust level = 1 (low),  $u_i$  trust level = 4 (medium),  $z_i$  trust level = 9 (high) .

#### 5.4 Future Development

We are currently implementing a multi-agent IDS system across our local Intranet environment with the aim of detecting hostile behaviour and attacks in the network. This prototype is based on the FIPA JADE agent platform, which provides core messaging and agent visualisation services. In order to transport the artificial antibody signatures between the agents we have designed an encrypted XML formatted ACL message structure. A specific application domain for the project is in defending peer to peer (P2P) networks. In particular P2P class networks are currently difficult to secure using existing network security methods as they bypass traditional firewall mechanisms, and may span multiple corporate networks.

#### 6 Conclusions

This work indicates that a cohesive network of socially interacting agents can create a highly robust and adaptive defence system for information networks. The agent simulation we have developed demonstrates that it is possible to create a population of autonomous agents, which form self-healing social groups with greater resistance to attacks and perturbation than isolated agents. A key parameter of such co-operation is the degree of trust which is established between agents within the same domain, as increased levels of trust can assist in the rapid diffusion of anti-body solutions. (Although at the risk of corrupted agents exploiting such trust).

The process of continuous inter-agent meme transfer enables the agents to maintain a measure of group identity, which is essential to the process of distinguishing self from non-self. In addition the cooperative exchange of recognised patterns for hostile pathogens/viruses greatly improves the immune response of such an agent community.

## REFERENCES

Anderson R., Feldman P., Gerwehr S., Houghton B., Mesic R., Pinder J, Rothenberg J., and Chiesa J. (1999). "Securing the U.S. Defense Information Infrastructure: A Proposed Approach." MR-993-OSD/NSA/DARPA. [www.rand.org/publications/electronic/info.html](http://www.rand.org/publications/electronic/info.html)

Balasubramaniyan J., Jose Omar Garcia-Fernandez, Spafford E., and Zamboni D. "An Architecture for Intrusion Detection using Autonomous Agents". Department of Computer Sciences, Purdue University; Coast TR 98-05; 1998.

Briney A., "Security Focused", Online report on Information system security, from <http://www.infosecuritymag.com> 2000.

Carver C.A., Hill J.M, Surdu J.R., and Pooch U.W., "A Methodology for using Intelligent Agents to provide Automated Intrusion Response," IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop, West Point, NY, June 6-7 2000, pp. 110-116.

Cohen F., " 50 Ways to Defeat your Intrusion Detection System", onlien paper at <http://all.net/journal/netsec/1997-12.html>.

Crosbie M. and Spafford E. "Defending a Computer System using Autonomous Agents", In 18th National Information Systems Security Conference, oct 1995. <http://www.cs.purdue.edu/homes/mcrosbie/research/NISSC95.ps>.

Dittrich D., " The "Tribe Flood Network" distributed denial of service attack tool ", online report at <http://staff.washington.edu/dittrich/misc/tfn.analysis.txt>.

Epstein J., Axtell R., "Growing Artificial Societies: Social Science from the Bottom Up", MIT Press, 1996.

Etzioni O., "Moving up the information food chain: Deploying softbots on the world-wide web". In Proceedings of the Thirteenth National Conference on Artificial Intelligence (AAAI96) , Portland, OR, 1996.

Filman R., and Linden T., "Communicating Security Agents", Proc. WET ICE 1996.

Forrest S., Perelson S., Allen L., and Cherukuri R., "Self-Nonself Discrimination in a Computer". In Proceedings of IEEE Symposium on Research in Security and Privacy, pages 202-- 212, Oakland, CA, 16-18 May 1994.

Helmer G.G., Wong J.S., Honavar V., and Miller L. "Intelligent agents for intrusion detection". In Proceedings, IEEE Information Technology Conference, pages 121--124, Syracuse, NY, September 1998.

Kephart J.O., " A Biologically Inspired Immune System for Computers", Artificial Life IV, Proceedings of the Fourth International Workshop on Synthesis and Simulation of Living Systems, Rodney A. Brooks and Pattie Maes, eds., MIT Press, Cambridge, Massachusetts, 1994, pp. 130-139

Maes P., Guttman R. and Moukas A., "Agents that Buy and Sell: Transforming Commerce as we Know It." Communications of the ACM, Mar 1999 Issue, available online from [http://ecommerce.media.mit.edu /Kasbah/](http://ecommerce.media.mit.edu/Kasbah/).

MAFTIA "Malicious and Accidental Fault Tolerance for Internet Applications", IST Programme RTD Research project, 2001, <http://www.newcastle.research.ec.org/maftia/summary.html>

Moody J. & White R.D., "Social Cohesion and Embeddedness: A Hierarchical Conception of Social Groups", Submitted to American Journal of Sociology 2000.

Segel, A., and R. Lev Bar-Or. "Immunology Viewed as the Study of an Autonomous Decentralized System." In Artificial Immune Systems and Their Applications, edited by D. Dasgupta, 65-88. Berlin: SpringerVerlag, 1998.

Watts, D. & Strogatz S. "Collective Dynamics of 'small-world' networks", Nature 393, 440-442 (1998).

Wilikens M., Jackson T. "Survivability of Networked Information Systems and Infrastructures", EU DG III/F, Deliverable report on Survivability, Joint research Centre Italy, 1997.

Wilson, E.O. (1971) The insect societies. Harvard University Press.