Information & Security Volume 8, 2002

Agent-based Technologies

Edited by Petya Ivanova

Information & Security, Volume 8, Number 1

Information & Security, Volume 8, Number 2

Coalition Operations Planning and Negotiations

Agents in Resou Planning

I&S Monitor

I&S Research Centers

E-Comerce Laboratory, Plovdiv University, Bulgaria

Author: **Editorial**
Title: **Agent-based Technologies in Defense and Security**
Year of issuance: **2002**
Issue: **Information & Security. Volume 8, Number 1, 2002, pages 5-15**
Hard copy: **ISSN 1311-1493**

AGENT-BASED TECHNOLOGIES IN DEFENSE AND SECURITY

The field of autonomous agents and multi-agent systems is an exciting and rapidly expanding area of research and development. In the last few years, there has been a growing interest in the application of agent-based systems to various security-related and military domains. In this special issue of Information & Security we shall present the results achieved in this area, discuss the benefits (and drawbacks) that agent-based systems may bring to the military and the broader security community, and provide a list of research and practical challenges that should be tackled in the near future so that the full potential of agent-based systems is realized.

Published results reflect applications, or potential applications, of agent-based systems for situational assessment for submariners; agents that discover and alert on conflicts in air mobility plans; software agents that aid military intelligence efforts; cooperating agents that address the problem of discovering and prosecuting mobile, time-critical targets; multi-agent systems for mechanics' decision support during aircraft maintenance; software systems that support mission critical team decision-making; multi-agent systems that assist defense acquisition and contracting; integrated marine multi-agent C2 system providing "near" real-time situation awareness; multi-agent simulations for planning and executing joint operations, rehearsing dangerous tactical operations, noncombatant evacuation operation and logistics planning; multi-agent system for identifying and exploiting emergent collective behavior on the battlefield; agents that recognize aircraft maneuvers during simulated flight; intelligent agents for threat assessment in small unit operations; multi-agent intelligence analysis systems; Internet-based multi-agent systems for military training; robotic demining agents; multi-agent system that handle tank platoon movement.

During application researchers encounter a set of methodological and technical problems. For example, there are no universally accepted standard ontologies and semantic definition languages in the military; it is necessary to improve quality and efficiency of multi-agent simulations of operations; it is problematic to integrate agent technology in existing large-scale military simulation system; there is a need to develop robust agent behavior control mechanisms. Last but not least, is the challenge to prove to the military the utility and reliability of agents. Nevertheless, the trend is gradual transition from limited applications performing isolated functions to collaborative applications interacting with other systems and data sources to reach complex goals.

Objectives of the special issue

The purpose of this special issue is to present latest achievements and new ideas in applying agents

and multi-agent systems to the military and the broader security domain. The topics include but are not limited to:

- General and specific architectures of agents in different settings and environments
- Cooperation and competition; coordination and collaboration
- Negotiation, consensus development, conflict detection and resolution
- Communication protocols and languages (communication standards)
- Intelligent cognitive activities jointly realized by multiple agents, e.g., distributed problem solving, planning, learning, and decision making
- Emergent behavior and organizational intelligence
- Organizational structuring and dynamics
- Mobile agents as general-purpose framework for distributed applications
- Performance issues; security, reliability, and robustness
- Agents and the interoperability of heterogeneous systems
- Human-agent interaction and interfaces
- Architectures, environments and languages for mobile and secure information services
- Agent capability requirements in military applications
- Analysis of experience in implementing and operating agent-based systems

In particular, based on the accepted publications, we have decided to organize the special journal issue on Agent-based Technologies in two numbers. Volume 8, number 1 focuses on the following two groups of topics:

- Agent-based Defense Modeling and Simulation
- Security of Agent-based Systems.

Number 2 deals with:

- Coalition Operations Planning and Negotiations
- Agents in Resource Planning

Agent -based Defense Modeling and Simulation

Computer simulation is a valuable tool for complex decision-making, especially in military and civilian operations in the land, air or sea. Simulation has been used in the military domain for the evaluation of acquisitions, missions and force development options. Modeling and simulation for this

purpose is becoming increasingly complex as multi-role, multi-platform and multi-system aspects are taken into consideration. The complexity of this task is further increased by the difficulty in modeling human decision-making using conventional software approaches. Current implementations of computer generated forces have proven to be very useful, but do not model human reasoning and cannot easily model team behavior. Applications of intelligent agents in military simulations have proved highly effective. This is due to the capability of agents to represent individual reasoning and from the architectural advantages of that representation to the user due to the ease of setting up and modifying operational reasoning or tactics for various studies. In addition, intelligent agents extend the modeling of reasoning to explicitly model the communications and coordination of activities required for team behavior.

The aim of the first group of papers is to point out the importance of agent-based modeling and simulation, as a scientific concept and technological possibility, to enhance the potential of simulation in both civilian and defense applications.

Agent-based distillations represent an emerging technology within the field of combat modeling and simulation. They utilize agent-based methods to model combat as a complex adaptive system. Existing distillations have already shown the great promise of this approach in providing analysts with valuable insights into areas such as non-linearity, co-evolving landscapes and intangibles.

The paper by Michael Barlow and Adam Easton present a new multi-agent-based distillation known as CROCADILE – a Comprehensive, Research Oriented, Combat Agent Distillation Implemented in the Littoral Environment. This is a new distillation system that significantly extends the agent-based distillation field. CROCADILE has been designed as an open distillation harness and developed at the Australian Defense Force Academy.

Among the key new features that CROCADILE brings to agent-based distillations are the following: a true 3D world, probabilistic or projectile-physics combat resolution, extensible object-oriented design, multiple agent control paradigms, sophisticated command, mission, and communication structures for agents, higher fidelity combat resolution models that incorporate blast effects, round penetration, rates of fire, and line of site, and multi-team structure including neutrals and levels of enmity/alliance and communication between teams.

The paper details the object-oriented design together with the various efficiencies employed to deliver a real-time 3D implementation involving hundreds of agents. The system and its explanation are illustrated via a scenario examining a possible structure for the Australian Army's "Army after Next" concept.

The emphasis on timely, accurate information in modern warfare, and the availability of modern communications, has led to the development of increasingly complex command and control systems. It is important to understand the behavior of these systems under a variety of circumstances. However, as they are difficult to analyze manually, advanced modeling and simulation tools for command and control systems development are required. As we have already elaborated, the challenge in these systems is to model the reasoning associated with different roles in the hierarchy. Intelligent agents can represent the reasoning and command capabilities associated with their assigned roles in the

hierarchy, allowing different command and control strategies to be quickly evaluated under varying circumstances.

These intelligent agent simulation models are in the focus of the second paper. Such agent models consist of a number of entities which interact locally in order to produce global emergent behavior. In complex systems, elaborate and unpredictable properties arise from the interaction of the constituents. Examples of such emergent properties include how the system organizes itself, how it finds a balance between order and disorder, and how agents, both individually and collectively, evolve new behaviors in response to change. Some of the emergent behaviors can be surprising, and it is the aim of the work described by James Moffat and Susan Witty to produce a theory of such processes which helps to explain the types of behavior to be expected.

In a nutshell, understanding the behavior of such agent-based combat models is now becoming more important, especially as the agents gain intelligence and try to outsmart each other, producing potentially very complex behavior. The principal variables in these models can often be separated out from the rest of the model to produce a metamodel that is aimed at decreasing the run-time of the original model while still retaining the characteristics and arriving at the same final solution as the original model.

In their paper, James Moffat and Susan Witty discuss the development of such a metamodel of an intelligent agent simulation model. Their metamodel is a mathematical abstraction of such a simulation, composed of two parts. For the first part, the fractal dimension of a force is introduced as a parameter measuring the emergent ability of such forces to cluster locally, corresponding to local decision-making by individual agents. For the second part the authors consider the mathematics of Bayesian Decision-Making as a metamodel for top down decision processes in such simulation models.

Security of Agent-based Systems

A great deal of military applications is characterized by an environment that is distributed, heterogeneous, dynamic, unpredictable, insecure, and unreliable. More specifically, the latency and bandwidth of network connections varies enormously in space and time, especially with the growing demand for wireless networks, satellite connections, mobile devices (laptops and personal digital assistants), and other highly volatile communications networks. Therefore, computing paradigms that are robust in the presence of network volatility are largely needed. The applications in this environment must be able to adapt to different and changing conditions.

Mobile (transportable) agents are an excellent computing mechanism to realize such applications, especially when used in a wireless environment. These mobile agents have the potential to provide a convenient, efficient and robust programming paradigm for distributed applications. Mobile agency is also the paradigm that has been suggested for allowing efficient access to remote resources. It is particularly attractive in situations where the amount of information to be processed is large relative to the network bandwidth.

A mobile/transportable agent is an autonomous software program/entity that can migrate from host to

host in a heterogeneous network. The program chooses when and where to migrate. It can suspend its execution at any point, ship itself to a new location on a network, and continue execution on the new machine. On each host, the mobile agent interacts with stationary service agents and other resources to accomplish its task. Mobile agents are goal-oriented, can communicate with other agents, and can continue to operate even after the machine that launched them has been removed from the network.

Mobile agents have several advantages over the traditional client/server model. Experiments show that mobile agents can, among other things, lead to faster applications, reduced bandwidth demands, or less dependence on a reliable network connection. Although none of these benefits are unique to mobile agents, no competing technique shares all of them. The mobile-agent system provides a single general framework in which a wide range of distributed applications can be implemented in an efficient and easy manner.

Mobile agent applications are currently being developed by industry, government, and academia for use in such areas as telecommunications systems, personal digital assistants, information management, on-line booking, contract negotiation, air traffic control, parallel processing, and computer simulation.

However, the mobile agent computing paradigm poses several privacy and security challenges, which clearly are one of the main obstacles to the widespread use and adaptation of this new technology. Mobile agent security issues include: authentication, identification, secure messaging, certification, trusted third parties, non-repudiation, and resource control. Mobile agent frameworks must be able to counter new threats as agent hosts must be protected from malicious agents, agents must be protected from malicious hosts, and agents must be protected from malicious agents. Therefore, the next group of papers is directed towards evaluating existing mobile agent security mechanisms and developing new countermeasures for mobile agent security threats.

In the first paper in this group, Raj Gururajan studies security of transactions in mobile commerce. He argues that while most of the various security procedures are limited to corporate IT infrastructure, in mobile commerce issues concerned with transaction security appear to have extended beyond the corporate network to embrace the complete business process. Any lapse in procedures that maintain confidentiality of data or violation of privacy could affect corporate image. In addition to existing security problems in a wired commerce environment, the emergence of mobile devices has renewed calls for addressing security threats to financial transactions. These are the problems discussed in Gururajan’s paper as key issues in terms of organisation’s architectural and procedural approaches to security, reliability and availability of transactions.

Since all the information about a mobile agent is transported over the Internet, the security policies become very important. However, as Iuon-Chang Lin, Hsia-Hung Ou and Min-Shiang Hwang point out, the transportation security is usually neglected. Therefore, their paper proposes two secure transportation schemes for mobile agents. These new transportation mechanisms can prevent all possible attacks during the process of transporting agents. Furthermore, users can choose the best transportation scheme according to the system’s scale.

Coalition Operations Planning and Negotiations

Military coalitions are examples of large-scale, multi-faceted, virtual organizations, which sometimes need to be rapidly created and flexibly changed as circumstances change. The agent-based paradigm is a good mechanism of building complex software systems in general, and hence offers potential benefits in the coalition context.

The next group of papers in the special issue aims to show that multi agent systems are an effective way of dealing with the complexity of real-world problems, such as agile and robust coalition operations and enabling interoperability between heterogeneous components, including legacy and actual military systems.

In the first paper, Zakaria Maamar, Nabil Sahli, Bernard Moulin, and Paul Labbé present their software agent-based collaborative approach to humanitarian-assistance scenarios. Their research deals with the use of software agents as a support to collaboration. Collaboration can face different constraints, such as partner distribution and resource heterogeneity. To deal with these obstacles, the authors propose coordination strategies. They enable agents to avoid conflicts and, hence, to fulfill their activities efficiently. Their work is applied to medical evacuation scenario, in which different participants, such as non-governmental organizations, have to work together despite their individual differences. The authors demonstrate that the agent-based computing paradigm offers a promising new approach to dealing with the technical and non-technical issues in establishing a coherent collaboration environment in humanitarian assistance scenarios.

Coalitions exhibit the problems of integrating single-service and joint capabilities into a coherent force. Furthermore, the nature of a coalition context implies some need to rapidly configure own or foreign systems into a cohesive whole. Many problems in this environment can only be solved by organizational changes and by aligning doctrine, concepts of operations and procedures. Due to the absence of pre-existing coordinated systems, coalition scenarios require a rapid, flexible, on-the-fly approach that allows capabilities to be assembled at run-time. In ensuring interoperability, it is also crucial to address issues of security of data, control over semi-trusted software from other coalition partners, and robustness of the resulting system. Coalition operations are often characterized by data overload, lack of information, labor intensive collection and coordination of information, and standalone command and control systems that use incompatible data formats.

The paper by Zakaria Maamar and Paul Labbé shows that the agent-based computing paradigm offers a promising new approach to dealing with the described issues by embracing the distributed, heterogeneous, and dynamic nature of the coalition environment. The agent-based technologies aim at managing the coalition informational infrastructure, in terms of autonomy, adaptability, and scalability. To develop their agent-based approach to support of coalition operations, the authors identify different aspects of a coalition. These include the coalition structure; the roles and responsibilities held by people within the coalition; the flow of information within the coalition; the capabilities required or available within the coalition; and the context in which the coalition operates. For many of these aspects, software agents can be used. The authors have shown a number of disparate agent systems working together in a realistic coalition environment and indicated the value of the agent-based computing paradigm for rapidly creating such agent organizations. Their conclusion is that software agents, together with agent-based infrastructures and services could play a key role in supporting coalition operations. This technology will provide the ability to bring together

and integrate legacy or previously incompatible systems quickly to aid in all aspects of coalition operations, without sacrificing security and control. Thus an agent-enabled environment helps create shared understanding and improves the situational awareness of military commanders. Moreover, it could make a significant contribution to the aims of Network-Centric Warfare.

The issue of integrating information systems in coalition operations is further dwelled upon in the contribution by Marvin “Lenard” Simpson, Jr. The author from the US examines in detail the challenges of command and control in a coalition air operation under the presumption that the operation is led by the United States. Being far from standard, the arrangement of a Coalition Aerospace Operations Center, or CAOC, is still a subject of deliberation. We believe that the description in this article will provide to multi-agent researchers a glimpse at a potential testbed for implementation of advanced agent-based technologies.

Recently, there has been an increased interest in the application of the agent-based technology in negotiation. In their paper, Javier Carbo, José Molina and Jorge Davila present a scheme for multi-agent argumentative negotiation in the generic domain encompassing intelligence agencies and informers. The goal of the negotiation phase in their work is to persuade the other party by argumentative reasons. They have studied several typical arguments, which may be useful in this context, such as ultimatums, promises of future fidelity, past behaviour, and future proposals received. Their approach tries to make the negotiation dialogue more human through arguments commonly used in real-life negotiations. They have also studied how to prove certain knowledge without revealing the corresponding details, and how to preserve anonymity during negotiations when arguments such as past payoffs and offerings from other intelligence agencies are available. All this, according to the authors, can be accomplished through the exchange of arguments in counterproposal attributes and with the help of encryption techniques.

Agents in Resource Planning

Among the many appealing features of the multi-agent technology, its capabilities for collaboration and adaptation are particularly attractive to the military domain. Agents are capable of cooperating and collaborating with other agents and possibly human users to solve problems. Agents share information, knowledge, and tasks among themselves, and cooperate with each other to achieve common goals. The attractiveness of the multi-agent system is not only reflected by the intelligence of individual agents but also by the emergent behavior of the entire agent society.

The system developed by David Camacho, José M.Molina, Daniel Borrajo, and Ricardo Aler demonstrates many of the appealing features of the agent-based technology. Their paper presents MAPWeb (Multi-Agent Planning on the Web), a multi-agent system for cooperative work between different intelligent software agents that solve user planning problems using the information stored in the World Wide Web. MAPWeb is a heterogeneous system of intelligent agents whose main characteristics are cooperation, reasoning, and knowledge sharing. The architecture of MAPWeb uses four types of agents: user agents that are the bridge between the users and the system; control agents that are responsible for managing the rest of the agents; planning agents that are able to solve planning problems; and, finally, web agents whose objectives are to retrieve, represent, and share information obtained from the Web. MAPWeb solves planning problems by means of cooperation between

planning agents and web agents. Instead of using the planning agents to solve the whole planning problem, they focus on a less restricted problem and cooperate with the web agents to validate and complete abstract solutions. To enable efficient cooperation, the authors define a common language and data structures.

Military logistics planning involves the efficient coordination of supply requests and shares many features common to complex problem situations including information overload, uncertainty, and layers of time constraints. Decision makers coordinate supply orders and determine the availability of requested items, the location that will receive the items, and how the items will reach the appropriate location in the most efficient and timely manner.

The agent-based approach to military logistics planning suggested by Stanimir Stojanov, Roumen Venkov and Radi Radev allows their applications to react quickly to changing logistic requirements and offers technical solutions to complex problems. Their approach to system design incorporates collaborative agents with knowledge in specific domains. These agents create a partnership and collaborate with expert human staff members during the various stages of the logistic process. In addition to creating realistic and timely solutions, the system also monitors the execution of logistic plans and offers real-time decision solutions to complex problems. Their system, DIANA, is a software “tool kit” that can be adapted to the user, to the logistic support concept, and to the changing circumstances of a military contingency. This is an agent-based system that is based on the MALINA-technology. The goal of the authors has been to create a general technological framework for development of modern information systems for military logistics and e-commerce.

Finally, this special issue provides a comprehensive, up-to-date list with on-line resources on general multi-agent research and journals, security and defense oriented research, projects, and software tools, as well as some milestone publications.

Information & Security

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Authors: **Michael Barlow and Adam Easton**
Title: **CROCADILE - An Open, Extensible Agent-Based Distillation Engine**
Year of issuance: **2002**
Issue: **Information & Security. Volume 8, Number 1, 2002, pages 17-51**
Hard copy: **ISSN 1311-1493**

CROCADILE - AN OPEN, EXTENSIBLE AGENT-BASED DISTILLATION ENGINE

Michael BARLOW and Adam EASTON

Table Of Contents:

Introduction

Simulation continues to grow as a vital tool for modern military forces. As an example there are approximately 70 simulations that are used throughout the Australian Army alone.[1] These include Live, Virtual and Constructive simulations.

There is a diverse range of applications that simulation is applied to within the military. These include individual training, strategic planning, decision support, capability and force structure development, mission rehearsal, and operational analysis.

Constructive Simulation has been used in all of the above roles. Constructive Simulation can be defined as computer models that represent the actions of people and/or equipment.[2] Currently it is the most commonly used form of simulation within the Australian Army.

In order to assist in their application of simulations the Australian Army has proposed a hierarchy of simulation.[3] This hierarchy defines a layered approach to simulation where scenarios are first examined with less detailed models which are quick and easy to use. More detailed models then further examine the insights gained from these models. This process continues until finally the most detailed simulations can be used with a better understanding of what the critical parameters for a given scenario are. A conceptual diagram of this hierarchy is shown in Figure 1.

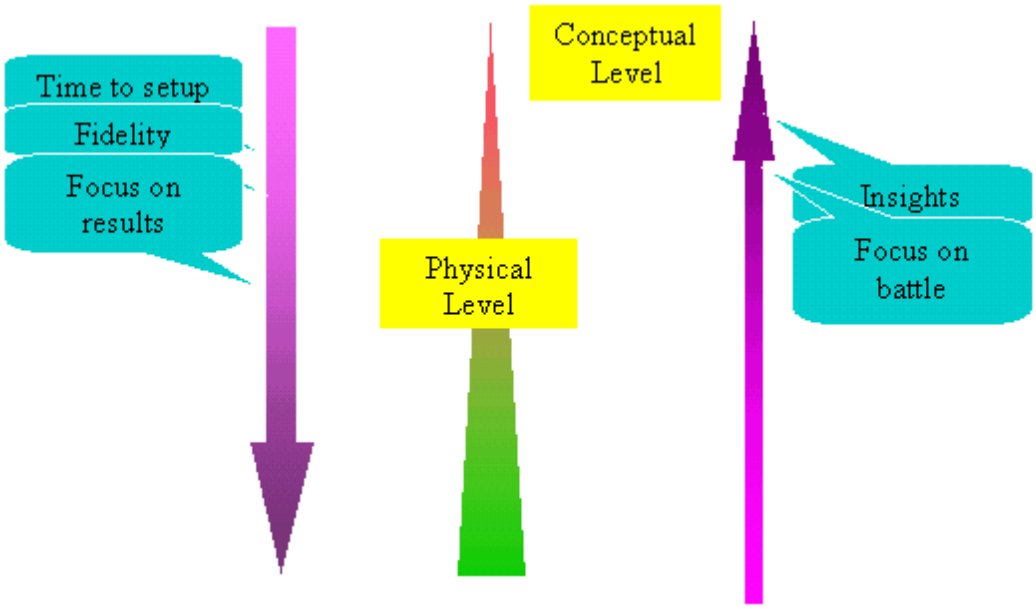


Figure 1: A diagrammatic representation of the Australian Army simulation hierarchy.

At the very top of this hierarchy are what can be considered 'conceptual level simulations.' [4] These are simulations that do not directly model physical entities on the battlefield such as tanks or soldiers; instead they model generic capabilities on the battlefield. This reduces the need to gather data on specific battlefield entities. This in turn allows a more rapid development of scenarios

While these simulations obviously do not produce results that can be directly applied to the real battlefield, they do provide an insight into what capabilities appear to be effective against the enemy and which do not.[5] However, a limitation of these systems is that they have minimal ability to explore and further develop the insights that they provide. Instead other simulations must be used. This transition is not smooth and unfortunately much of the value of the insights gained can be lost in the transition from the conceptual to the more realistic level.

The move towards a more holistic approach to combat simulation has not been confined to the Australian military, nor has it been confined to a linear progression from lower fidelity models to higher fidelity models. A key example of this is the work being conducted under the Project Albert [6] banner into a concept termed Operational Synthesis.

Project Albert was initiated by the United States Marine Corp with the mission of addressing three key weaknesses in existing simulation models. [7] The following features were not adequately addressed:

- non-linearity of combat – how small changes in given factors can produce much larger changes in the combat result;
- co-evolving landscapes – how forces are able to adapt to each others tactics and alter their own course of action accordingly; and
- the effect of intangibles – factors such as morale, training, aggression and fear.

All three of these concepts are extremely difficult to model with traditional constructive simulations that rely heavily on mathematical formulas and a black and white rule set. As a result, Project Albert is using Operational Synthesis in an attempt to address these concepts.

Operational Synthesis involves the concurrent use of a range of simulation tools in order to gain a more complete understanding of a combat scenario.[8] It recognises that all simulation tools have strengths and weaknesses, and attempts to use each tool in a capacity that draws from its strengths to mitigate the weaknesses of the other tools.

Within its operational synthesis framework, Project Albert has examined the use of a variety of tools allowing the use of human in the loop and automated systems, stochastic and deterministic models as well as a varying degree of fidelity.[9] Broadly, however, the tools that it has used can be divided into four categories. These are:

- War games;
- Deterministic equations;
- Simulations;

- Distillations.

Of these, the tools known as distillations have received the most attention by Project Albert members.[10] They represent an emerging area in the combat modelling body of knowledge and have shown great promise in providing analysts with insights into areas such as non-linearity, co-evolving landscapes and intangibles where other tools have been unable to provide meaningful results.

Perhaps the oldest form of combat simulation is through the technique of war gaming. This process involves utilising personnel, and their experience to brainstorm scenarios and develop courses of action. War-gaming in its primitive form can be traced back as early as 490 BC and has played a significant role in military planning through the history of conflict.[11] More recently computers have been integrated into the war-gaming process; however, the strength of war gaming still relies on the contributions of personnel involved in the process.[12]

During the early 20th century a more mathematically based approach toward combat simulation began to emerge. This occurred through the development of formulas and equations which attempted to model combat. These equations were predominantly attrition based and embraced the concept that the losses by one side in a conflict would be mathematically related to the size and strength of the opposition force. Perhaps the best-known pair of equations for combat simulation were the Lanchester Equations.[13]

The Lanchester Equations are a set of coupled differential equations that were first developed in 1914 by F.W. Lanchester. Similar to the predator/prey models, they describe a linear battle where the casualties of one side are dependent on the size and strength of the other. [14] These equations, while perhaps overly simplistic, were reasonably effective during early twentieth century warfare such as the trench warfare and artillery duels of World War One.[15] As the century progressed, however, warfare became a less linear relationship.

As the twentieth century progressed, the increasing power of computers paved the way for the development of computer based constructive simulation. Traditionally these computer based constructive simulations have been based upon mathematical attrition modes like the Lanchester Equations or derivations thereof. [16] In addition to this they have provided a way to integrate prescriptive rules and specific detail into models facilitating more detailed scenarios and consequently, the ability to investigate quite complex combat situations. These computer-based simulations are currently the most widely used tool for conducting combat simulation.

While these simulations are rich in detail and high in fidelity, they have several drawbacks. Probably the main one of these is that they are completely prescriptive. That is, behaviours of elements within the simulation are stringently specified. This makes it difficult to model all possible outcomes because of the level of detail and time required to set up an individual scenario run.

A second disadvantage of traditional simulations is that, to date, these simulations have been strongly equipment and firepower centric. [17] This is largely a result of their founding in attrition-based equations such as the Lanchester Equation. This basis means that all simulations, at their lowest levels, resolve combat as a mathematical relationship based on a purely attritionist model. As the nature of warfare changes, this is becoming an increasingly significant limitation.

The end of the twentieth century saw the emergence of Manoeuvre Warfare. This represented a fundamental shift in the way that warfare was fought. The Australian Army's definition of Manoeuvre Warfare is the application of combat power to defeat the enemy's will to fight. [18] It refers to the principle of a force applying its strength to an enemy's weak points so as to cause a disproportionate amount of damage to the enemy.

With this change in the nature of warfare, it can be argued that the Lanchester Equations and traditional constructive simulation techniques no longer provide as accurate a result as they have in the past. This in turn leads to the question of whether a paradigm exists which would better model modern warfare. Significant research has been conducted in this area over the last decade, and arising from it has been a strong argument that combat may perhaps best be modelled as a complex adaptive system.

Complexity is a concept that is strongly coupled with chaos. While chaos can be considered an investigation of how simple microscopic behaviours produce a complicated macroscopic behaviour, complexity is the investigation of how complex microscopic behaviours can produce simpler macroscopic behaviours.[19] A good example of complexity can be seen in the output of cellular automata models.[20]

Complex Adaptive Systems (CAS) can be described as systems composed of many nonlinearly interacting parts that continually adapt by changing their internal rules as both their environment and knowledge of that environment evolve over time.[21] Within these systems, while the system parts act independently based on localized rules, an overall macroscopic behaviour emerges which appears to have some sort of natural coordination.[22]

Further examination of these CAS, has allowed the following list of key properties to be developed:

- non-linear interaction;
- hierarchical structure;

- decentralised control;
- non-equilibrium order;
- adaptation.

When comparing each of these to combat, similarities begin to emerge – the non-linearity due to environment, equipment, and doctrine; the hierarchical rank and command structure; decentralised control due to the fact that individuals compose a force and modern commanders are given scope in achieving their goals; plus non-equilibrium and adaptation as fundamental aspects of combat. The presence of all of the abovementioned factors lends evidence to support the hypothesis that combat is indeed a CAS.

This hypothesis is also mathematically supported. Analysis of cellular automata models and other CAS have shown them to produce fractal distributions in comparison to traditional constructive simulations which do not. The fact that studies into real combat data have shown the presence of fractal distributions in historical combat again suggests that combat may indeed be a complex adaptive system.[23]

If this hypothesis is accepted it gives some direction in answering the question of what new paradigm should be used to model modern combat. If, as complexity suggests, the fundamental building blocks of a system are its sub-parts, a reasonable approach would seem to be modelling individual entities on the battlefield rather than attempting to develop mathematical models that approximate the outcome of force on force scenarios that contain many entities.

Agent-Based Simulations are systems in which the infrastructure of the simulation and the entities that participate within the simulation are logically separated.[24] This allows the agents to be easily added, removed or modified within a simulation.

Agent-based paradigms are a relatively new technology within the simulation domain. They emerged as an expansion from work on Cellular Automata [25] and initially focussed on the simulation of primitive insect colonies. [26] Multi-Agent systems have been used in a plethora of applications. These include modelling of nations, economic factors, businesses and neurons.

The military applications of agent-based technology are a recent development. The agents within these simulations range from simple agents that follow a basic set of rules, to highly detailed models with complex knowledge bases and rule sets. Their purposes are diverse including agents that control battlefield entities, command agents that act as high level commanders, air traffic controllers, information filtering agents and decision support agents.[27]

Broadly speaking, work on agent-based simulation has been in one of five areas. The first of these has been in creating more complex agent architectures. This work has been tightly coupled with work into creating higher fidelity simulation engines. As the complexity of the worlds in which the agents operate increase, it is necessary to increase the complexity of the agents' architecture so that they can relate to the world at this higher level of fidelity.

A somewhat related field of work to this has been the creation of team-based agent architectures. The majority of agent-based simulations currently model agents in relative isolation from each other. It can be argued, however, that as the military environment is fundamentally a team one, the inclusion for a team model in agent-based combat scenarios would be beneficial.[28] This argument has lead to work being conducted into team-based agent architectures that allow control over formations, agent connectivity and path planning.

Another area of work on agent-based simulations has been into integrating agent-based systems with distributed simulations. A principle component of this approach is the generation of Semi-Autonomous Forces. This is an inherently agent-based requirement that will require agents to be able to operate intelligently in a broad suite of applications.

Human-in-the loop simulation is another area that is being integrated with agent-based simulations. Through including humans within the simulation process, the effectiveness of the agents involved has been able to be better tested and consequently improved.[29]

The final, and most recent, development of agent-based technology has been in the development of simple agent-based distillations.[30] These distillations take a different approach to agent modelling, moving away from the traditional high fidelity approach towards a more compact agent architecture where the focus is on the interactions between agents and not so much on the agents themselves. This has allowed combat to be modelled in new ways and is providing promising results in representing combat as a complex adaptive system.

Distillation Systems

Broadly speaking, distillations can be defined as simulations that attempt to model warfare scenarios by implementing a small set of rules that allow agents to adapt within each scenario. Distillations represent a far closer modelling of CAS than any other constructive simulation paradigm.[31] Furthermore, distillation systems can be shown to be relevant to the conceptual end of the simulation hierarchy.

Distillations are far less detailed than traditional simulations and rely on sensible global behaviour to emerge naturally, unlike traditional

models that require this behaviour to be explicitly programmed. This simplicity gives distillations the characteristics of speed, transparency, ease of configuration and the ability to use the systems with minimal training.[32]

Unlike the traditional firepower and equipment centric simulations, distillations can be considered to be manoeuvre centric.[33] This means that insights are predominantly gained not through the numerical results of simulation runs, but rather from an understanding of how the agents adapt to each other's tactics.

Agent-based distillations provide a bottom-up approach to modelling combat scenarios.[34] Unlike traditional constructive simulations which specify an overall scenario, and then layer more and more levels of detail as they generate the components of that scenario, distillations require the analyst to develop the individual components and then observe the overall behaviour that emerges within the model.

There are currently several agent-based distillations that have contributed to this field of knowledge. The most commonly employed are: Irreducible Semi-Autonomous Agent Combat (ISAAC), Enhanced ISAAC Neural Simulation Toolkit (EINSTein), Map Aware Non-uniform Automata (MANA), and Socrates.

All of these systems contain common characteristics. These include a two-dimensional world, a kill probability combat resolution algorithm which is used to determine combat outcomes at the lowest level, and an attractor / repulsor agent control paradigm.[35] This attractor / repulsor method can be described as a set of weights that determine what direction, and how far, an agent will move at any given time. It can perhaps best be likened to the spring-embedder method of multi-dimensional distance resolution described by Battista.[36] While all extant combat distillations possess these properties, they are not necessarily a property of agent distillations in general. Rather they represent the design decisions that have been made within extant systems.

ISAAC was the first Multi-Agent System to be developed which treated combat as a complex system. It was developed as a proof of concept model. In this system, as with all of the models described below, agent behaviour is not pre-programmed. Instead, agents are given a set of instincts such as aggression, self-preservation and attraction to friendly forces. These instincts are weighed off against each other to determine a course of action for that agent at a given point in time.[37]

As the name "Enhanced ISAAC Neural Simulation Toolkit" suggests, EINSTein expanded upon the ISAAC model, retaining much of the ISAAC engine but adding additional visualisation tools, simulation log utilities as well as meta-personalities [38] for the agents. These meta-personalities allowed agents to change their behaviour when they were in a group of agents of a sufficient size. Therefore an agent acting on its own could be made to be less aggressive than an agent collocated with 20 other friendly agents.[39]

MANA is a system developed in New Zealand that further expands upon the concepts validated by ISAAC and EINSTein. Unlike these systems, however, it attempts to model squad level scenarios as opposed to the strategic large-scale scenarios modelled by the other systems. Another key factor in MANA is the introduction of Agent memory. This allows agents to build a picture of the world as the simulation progresses. Consequently an agent's actions are not based solely on the situation it is currently faced with, but rather the current situation plus the situations it has faced in the past.

Socrates is the most recently developed agent-based distillation. Fairly similar to the systems described above, Socrates implements the instinctive based attractor / repulsor agent control paradigm, a 2D world and a probability based physics model. In comparison to the other models, however, Socrates provides a reasonably rich set of agent capabilities and behaviours.[41]

There is little doubt that the behaviours exhibited within the above systems often bear a resemblance to behaviour that we would intuitively expect on the battlefield.[42] Furthermore, while they take some time to learn, such systems are quick to use. Through the use of these systems a commander or analyst is able to gain understanding of the overall shape of a battle and what factors are more important than others in determining the outcome of a battle.

Despite these advantages, the question arises as to how effective these systems are in the larger simulation framework and whether they have attained the full potential that a distillation-based approach promises. This aspect of their role in the simulation hierarchy is currently problematic: the very abstraction that makes them an ideal tool for rapid exploration of the combat parameter space makes it difficult to link them and the insights they provide to higher fidelity simulation models. The difference in detail of representation is often too large to extrapolate from the distillation domain into the domain of higher fidelity simulations.

Secondly, current distillation systems have built-in a number of assumptions that serve as hard constraints on the battlespace domains that may be explored. These constraints, often tied to the origins of the systems in cellular automata, include amongst others the binding of agent behaviour and agent capability together, limitation to a flat 2D world, a single paradigm of behaviour for agents – the spring-embedder approach of weighted vector addition, and the lack of important modern military capabilities such as indirect fire, blast weapons, and round penetration. The constraints not only limit the range of scenarios that can be explored but also can significantly weaken the strength of the insights the distillations provide. For instance, how might an insight about the impact of a sensor overmatch on scenario outcome be altered by taking place in a 3D environment of hills and valleys, that impact detection ability, rather than in a flat

plain? Alternatively, in what way would the possession of blast weapons that affect an area alter the insights about manoeuvre tactics, in particular unit clustering and dispersion?

CROCADILE - Design of a New Distillation

In an attempt to address the perceived issues with distillation systems, a new system CROCACDILE—Conceptual Research Oriented Combat Agent Distillation Implemented in the Littoral Environment—has been designed and implemented.

The following subsections identify the design goals and key features of CROCADILE, discuss the Object Oriented design of the system, its major components in the form of the simulation engine and the agent interface, before concluding with the issues faced and overcome in the area of computational tractability and complexity management.

Design Goals

The previous section describing distillation systems identified two issues that CROCADILE was designed to address. Firstly, that the abstraction of the current distillations is both a strength and a weakness. Secondly, current systems also have a number of in-built limitations that hinder their generality and applicability to represent certain aspects of modern conflicts.

The means that CROCADILE employs to address these issues is generality and multi-fidelity resolution through a clear Object Oriented (OO) design. CROCADILE is designed as an open and expandable distillation engine. Not only does it support multiple levels of fidelity and conflict resolution—2D or 3D world, probabilistic or projectile-physics hit resolution—but it is also expandable by the user. Users can write their own agents and add them to the worlds simulated. Additionally, the various objects that compose the simulation can be extended to incorporate new types of functionality. This is a key lesson from observing the current distillation systems in usage. It is impossible to envisage all possible future applications of the system. A versatile and extensible core simulation engine and components are key to longevity and wide applicability.

CROCADILE follows a very strong object oriented design in all aspects. Its internal design and implementation is object oriented and, being written in the Java language, it will run on any hardware/OS platform. That OO design extends through to the simulation and the world itself that is seen by both the agents and the user. Agent behaviour is separated from agent capability, with capability being defined by individual weapon, sensor, communication, and movement objects with which that agent is equipped. Similarly, the world and the items that occupy it—agents, munitions, terrain features, objectives, etc.—are all objects with their own properties and capabilities.

This clear OO design, combined with the goal of not imposing any unnecessary constraints, has led to a number of key features in CROCADILE:

- 3D or 2D environment in which the agents interact;
- Probabilistic or Projectile-Physics combat resolution;
- Movement by Air and Water, as well as by Land;
- User extensible agent behaviours allowing users to code different control paradigms;
- Sophisticated Command, Mission, and Communication structures for agents;
- Higher fidelity combat resolution models that incorporate blast effects, round penetration, rates of fire, and line-of-sight;
- Database of world objects—agents, agent groups, behaviours, weapons, sensors, etc.—that can be saved individually and reused in subsequent scenario building;
- Comprehensive result logging including time-line and individual event information. Analysis possible via a visualisation tool part of the system, or commercial spreadsheet;
- Multi-team structure including neutrals and levels of enmity/alliance and communication between teams.

CROCADILE realises a 3D environment. This includes a location in 3D space for all physical objects such as agents and munitions. Further, digital terrain is supported and can be imported into any scenario meaning that agents can exist in a world of synthetic or actual (drawn from some part of the Earth's surface) terrain. Agents exist on that 3D landscape and their actions may be modified by that same landscape. Terrain affects movement, line-of-sight issues such as sensor detection, and hit resolution - the flight of projectiles and blast effects. Agents are also aware of that terrain, if employing their sensors, meaning that it becomes part of their decision process. Terrain features—water, vegetation, obstacles, and objectives—may also have a shape and location prescribed, once again enriching the environment in which the agents exist. However, simply by not incorporating these elements, such as digital terrain, in a particular scenario it is possible to simplify the simulation to a 2D world. Indeed, it is possible to start from a 2D scenario and progressively layer-in additional 3D aspects – enriching the environment and gauging how that modifies scenario outcomes. Scenario runs that are being visualised present a top-down view of the world in which terrain height is colour-coded. Figure 2 is a screenshot of a scenario taking

place on terrain in south-west New South Wales, Australia.

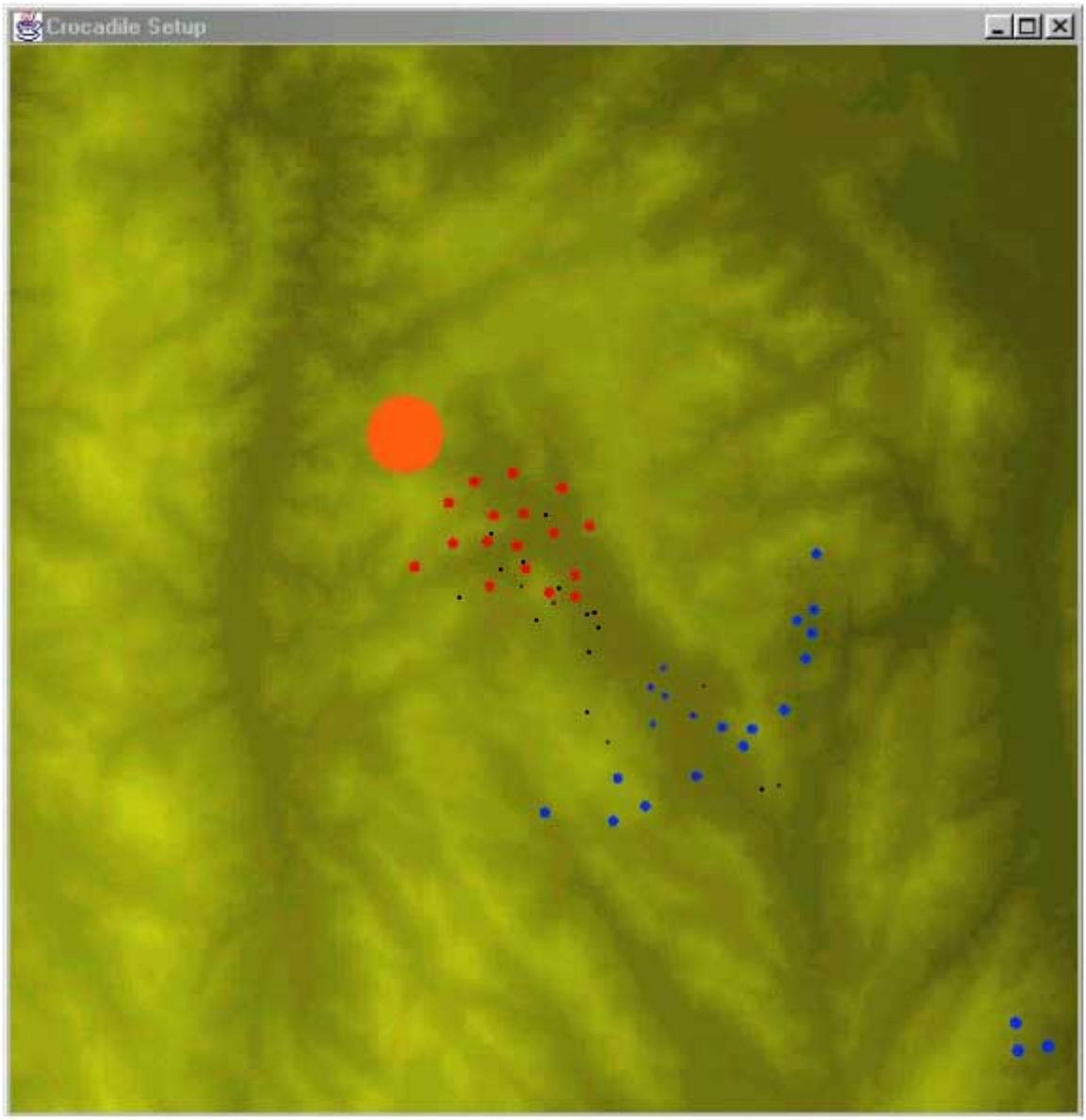


Figure 2: A screen-capture of CROCADILE while running. The conflict between red and blue occurs atop a 3D terrain that is colour-coded as to height - darker colours are lower. Agent munitions are also seen as the small black dots, while the large orange circle is an explosion.

Traditionally, distillation systems have employed a probabilistic model for hit resolution. Each weapon has certain chance of hitting any target regardless of factors such as target size, distance to target, or the terrain. CROCADILE supports this model but also incorporates a projectile-physics model. Munitions are fired with given speed and headings and 3D collision detection is used to detect when agents are hit or where explosions occur. Factors such as target size, speed, and distance away, together with the terrain itself become an important aspect of whether individual shots hit or not. Scenario runs that are being visualised show the projectiles. Figure 2 is a screen-capture of a CROCADILE run – munitions can be seen as the small black dots.

CROCADILE supports not only land-based movement but also air and sea. Movement capabilities can be defined to function in these domains also. Providing an agent with that capability then equips the agent to travel in that type of environment. This facilitates ‘joint operations’ style scenarios.

One means of viewing CROCADILE is as an agent test-harness – a means of contrasting different types of agents. CROCADILE defines an interface for its agents – their means of acting within a CROCADILE scenario. CROCADILE can load and run any agent which conforms with that interface. While CROCADILE incorporates an instinctual agent with behaviour resolution via weighted vector addition similar to that of other distillations, it is entirely possible for a user to write their own agent and add that to any CROCADILE

scenario. Thus Belief, Desire and Intention (BDI), learning, or user controlled agents can all be added to CROCADILE.

Recognising that the complexities of agent interaction provide the emergent behaviour of distillation systems, CROCADILE provides a rich set of command, mission, and communication structures. Hierarchies of command and communication can be established between groups of agents. Agents can issue orders to fulfil a mission to their subordinates, while subordinates have a propensity, or lack there of, to follow orders. Similarly, missions include not only the destruction of enemy agents but features of the environment itself, reaching a goal or destroying a static feature.

CROCADILE provides for a higher fidelity, though still abstracted, hit resolution than other distillation systems. Each agent has a health score that is reduced by the damage of the round that hit it. Each agent's initial health may be set differently. Further, each agent has a 7-point adjectival armour scale. Weapons are similarly rated for penetration. Only if the damage rating of a round that hits an agent exceeds the armour rating of that agent, will the round cause damage. This, for instance, can be used to stop small arms fire destroying heavily armoured vehicles in a scenario. Different weapons may have different rates of fire and number of rounds with which they are equipped. Terrain plays a part in hit resolution for explosions. Only if there is LoS (Line-of-Sight) between the centre of the blast area and the agent inside that area will the agent potentially suffer damage. If there is no LoS, then the agent is sheltered from the blast by the terrain.

CROCADILE provides the ability to save, as separate items, the individual components that form a scenario. Users may save terrain, agents, agent groups, agent behaviours, weapons, movement capabilities, sensors, command structures, and communication structures individually. These libraries of scenario components can then be employed in the rapid creation of new scenarios.

A rich range of data logging is built into CROCADILE. Each run results in a set of logs output to files. These logs include information about the state of the scenario at each timeframe – number of agents and health of each team. Further, they include a record of each significant event in the game. Each time an agent is hit, an objective hit or entered, or an agent is destroyed, the particulars of the event are recorded. These include the location, agent(s) and team(s) involved, damage etc. Logs are output as comma-separated-values, making them compatible with spreadsheet applications. CROCADILE also includes a data visualisation tool, allowing users to view various aspects of the run. CROCADILE can be run in an interactive or batch-mode thus facilitating extensive analysis of a scenario.

Finally, CROCADILE can support scenarios with any number of different teams involved. Relationships between pairs of teams can be friendly, neutral, or enemy allowing more complex situations to be designed. Communications for agents can be configured to occur at several levels, including whether to share information with friendly teams or not.

Major Components of the System

The CROCADILE design is split into two logically distinct sections. The first of these is the simulation itself, consisting of the simulation engine, specification of the world, agents, agents' capabilities, world objects and how they all inter-relate. The second of these is the instinctual agent control paradigm, which specifies how the agents behave within the world.

Both of these sub-parts can be further broken down to examine the major functionality groups within them. The simulation component of the system is by far the larger of the two sub-components. It is responsible for specifying all of the aspects of the system except for how the agents within the system 'think.' This cognitive simulation is carried out by the agent behaviour sub-component.

The overarching principle in the conceptual design of CROCADILE is to keep the two levels of separation as strong as possible. The first is the logical separation between the agents and the rest of the world, and the second is the separation between agent capabilities and agent behaviour.

Both of these divisions are largely established through the development of a set of classes that act as interfaces between the logically separated components. These classes are the agent's Capability Manager, Information Manager and Status Monitor. The agent control components of CROCADILE cannot access the agent that they are controlling directly, but can only gain information or affect this agent and the broader world through using these interfaces. Broadly speaking, the Capability Manager is responsible for allowing an agent to affect the world around it. The Information Manager is responsible for allowing an agent to gain knowledge on the world around it, and the Status Monitor is responsible for allowing an agent to gain knowledge about its own condition and status.

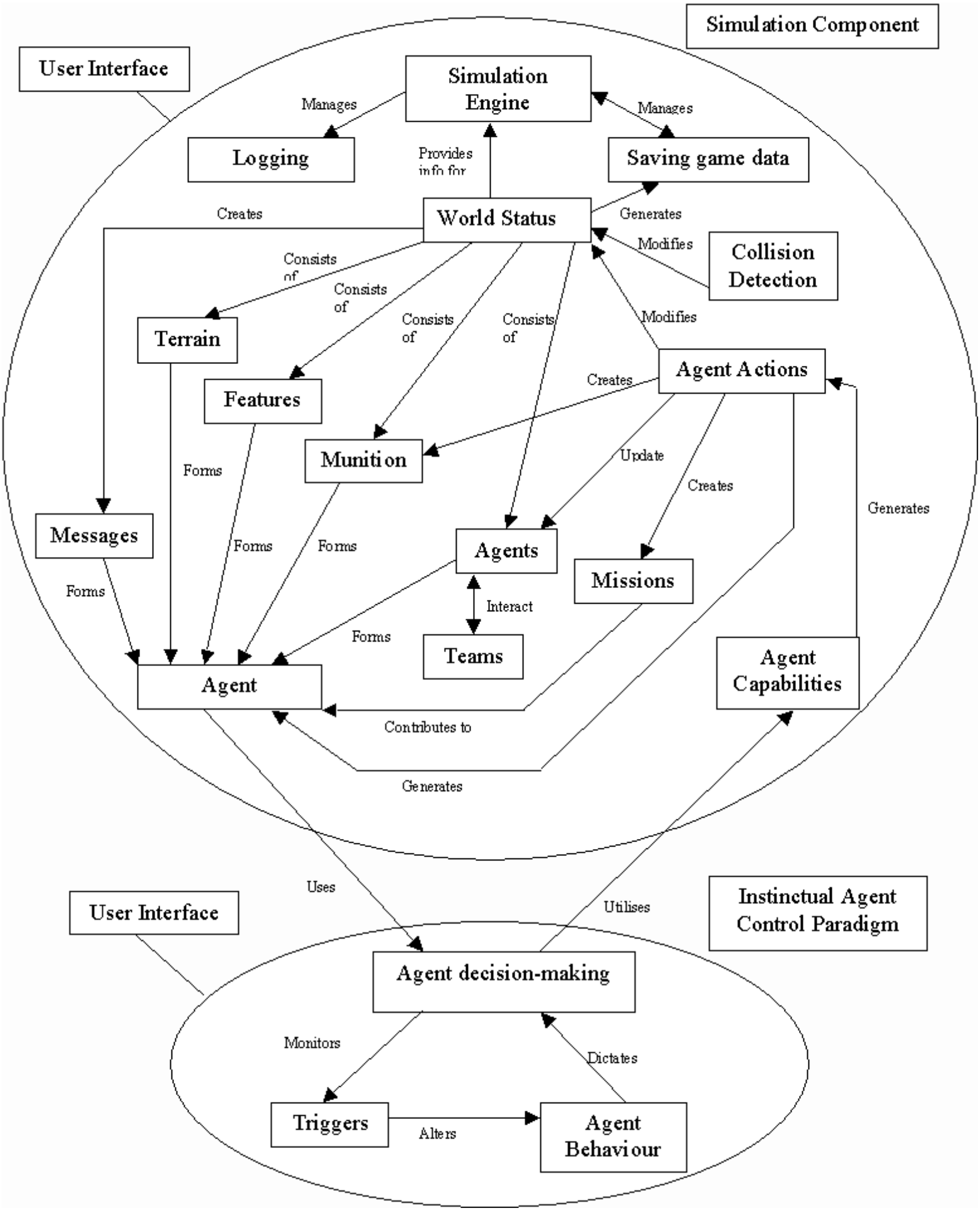


Figure 3: A conceptual representation of the CROACDILE distillation illustrating the major functional classes and their relationships.

A conceptual representation of the CROCADILE distillation is provided in Figure 3. This diagram shows the major functionality elements

within the system and how they relate to one another in greater detail than depicted in the logical diagrams included as Figures 4 and 5. The arrows within Figure 3 represent the directions of data flow within the system, and the labels describe the nature of the relationships that the major functional components have.

Because of the complexity and size of these two system components, it is necessary to break each one down into its major functionalities in order to better understand how the system works.

The Simulation Engine

The simulation component of CROCADILE is the core of the Agent Distillation. It is the component of the system that manages how objects interact, the status of all objects in the world, what data is recorded about a scenario, generally how the simulation runs, and when it stops.

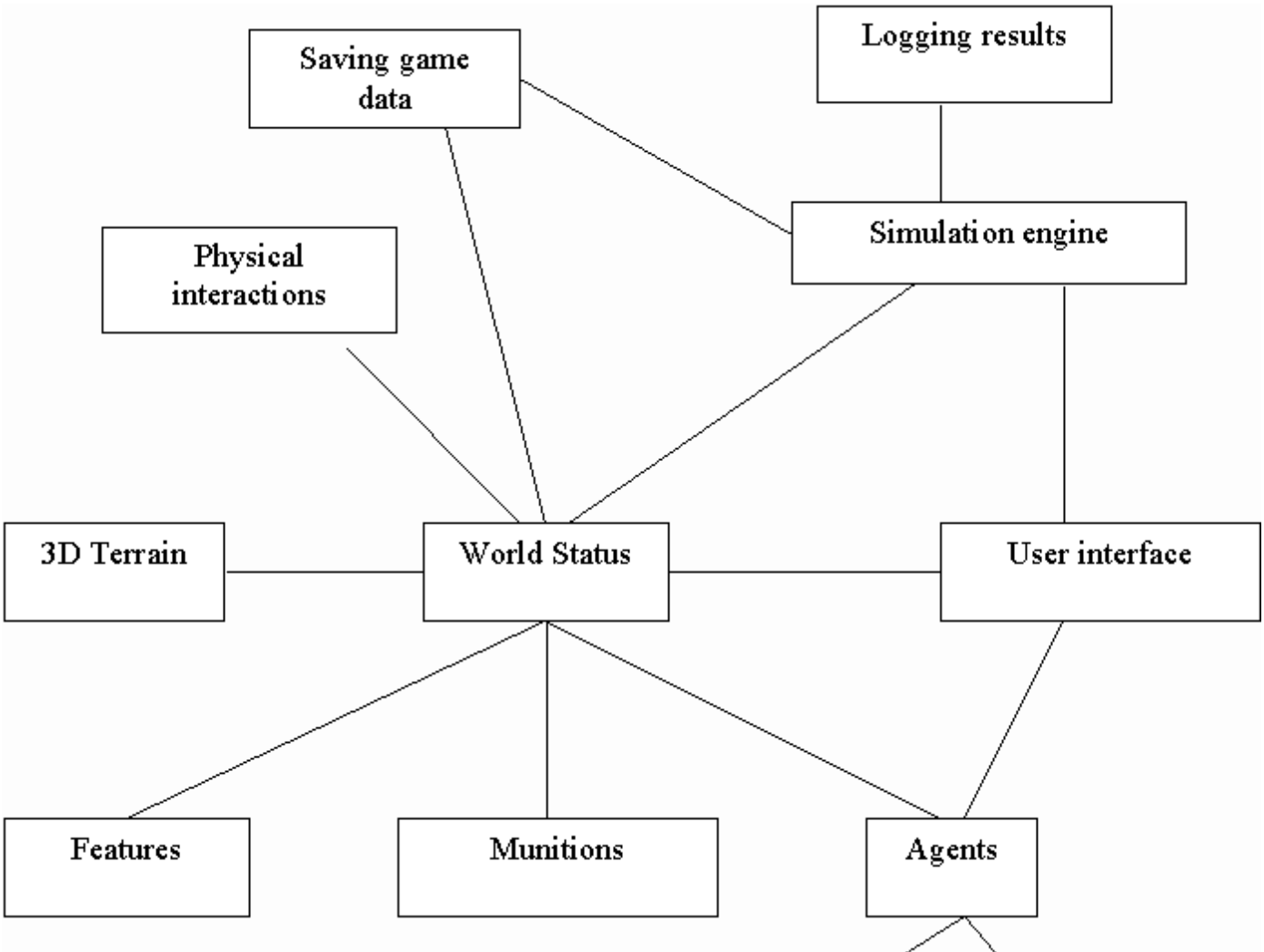
The object that is central to the simulation component is the World. It represents all of the rules that relate to the physical interaction of objects in the world as well as storing all of the objects present within it. The major elements that are present within the world are munitions such as explosions and weapon rounds, physical features such as vegetation and obstacles, the 3D terrain landscape, and the agents themselves. The physical interactions between all of these objects are resolved by the world's collision detection elements.

The World itself has no knowledge of the concept of a simulation run, which the simulation engine manages. This engine sits above the world and utilises the World's functionality to run the simulation. The simulation engine is responsible for managing the simulation sequence, recording data about the simulation run, and determining the success or stopping conditions of a simulated scenario.

The simulation component of CROCADILE also consists of a suite of library classes. These classes are responsible for saving components of the world such as agent capabilities, whole agents, other world objects or indeed, an entire world scenario.

Finally, the simulation component consists of a user interface component that is responsible for both displaying and allowing the user to modify the details that relate to the simulation or simulation scenario.

Figure 4 shows the major logical elements of the simulation component of CROCADILE, along with lines to represent relationships between these logical elements.



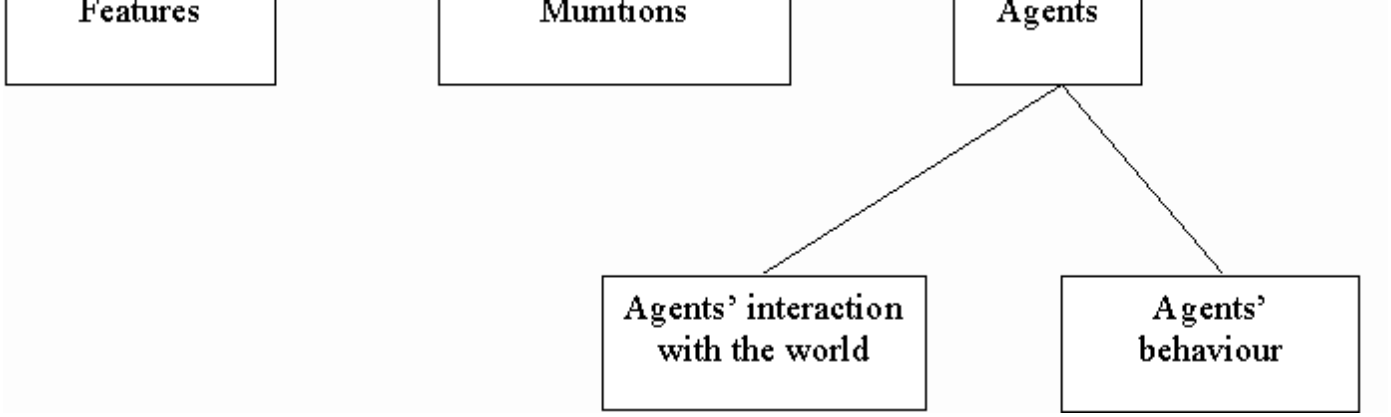


Figure 4: The major logical elements of the CROCADILE distillation.

The simulation engine is the core of CROCADILE. It contains the main simulation loop that controls the sequence in which the simulation is run. This core functionality is contained within the Simulator class. The Simulator sits on top of the world and manages when and how it applies its rules to the elements within it.

In addition to simply managing the simulation sequence, the simulation engine is also responsible for performing several key tasks. The first of these is the management of the agent behaviours that are used within the simulation. As any class that extends the AgentBrainClass and uses the correct methods to interact with the world, it can be used to control agents within CROCADILE. However, it is necessary to protect the rest of the system against poorly written or malicious agents that are being used within the simulation. The simulation engine manages this protection.

Another important attribute of the simulation is its ability to specify the time step used for a simulation run. Rather than updating the simulation for each time unit, it can be specified exactly how many times per time unit the world is updated, or conversely, how many time units should pass between each update of the world. When this value is changed, all corresponding velocities, forces and time factors are scaled accordingly. This allows a balance to be struck between the accuracy of the simulation and the time that it takes to run.

Other functions performed by the simulation engine are determining the stop conditions for a given simulation run, managing random number generation, and determining what hit resolution method is to be used for the given simulation run.

Agents and Agent Capabilities

The agent control component of CROCADILE specifies how the agents within the simulation behave, and can be seamlessly integrated with CROCADILE's simulation component. As described previously, any paradigm for controlling the behaviour of the agents can be used, providing that its inputs and outputs match those specified by the simulation component.

The default instinctual paradigm that is implemented incorporates a set of behavioural triggers which facilitate agent meta-personalities. The paradigm consists of four main elements. The first is the behaviour element that stores the set of weights that dictate how an agent will behave. The triggers within the paradigm are responsible for altering this behaviour according to the situation that the agent is currently in. The user through the user-interface element sets up both these triggers, and the behaviours, before run time.

The final element of this agent control component is the Agent decision-making element. This element contains no configurable local data but rather holds the methods that translate the behavioural weights stored within the behaviour element into a specified course of action. The decision-making element is also responsible for activating the trigger tests at appropriate times.

Agents in their capacity as cognitive entities interact with the world and each other in many ways other than through the process of collision detection that characterises the interaction between physical objects. A class diagram showing some of this interaction is found in Figure 6.

Agents are created as being part of an agent family and a team. Agents are able to identify whether other agents are part of their agent family and whether they are part of their team. This allows agents to react differently to other agents depending on their relationship to them.

Every agent within the world has a reference to an Agent Brain. This is the class that dictates how that agent should behave. This agent brain cannot access the agent itself but is rather given access to a set of tools, namely the Capability Manager, Information Manager and Status Monitor. Using these tools, Agent Brains are able to control the physical agent that they belong to, and interact with the world around them. Figure 5 shows the relationship of the AgentBrain class to other elements of the system.

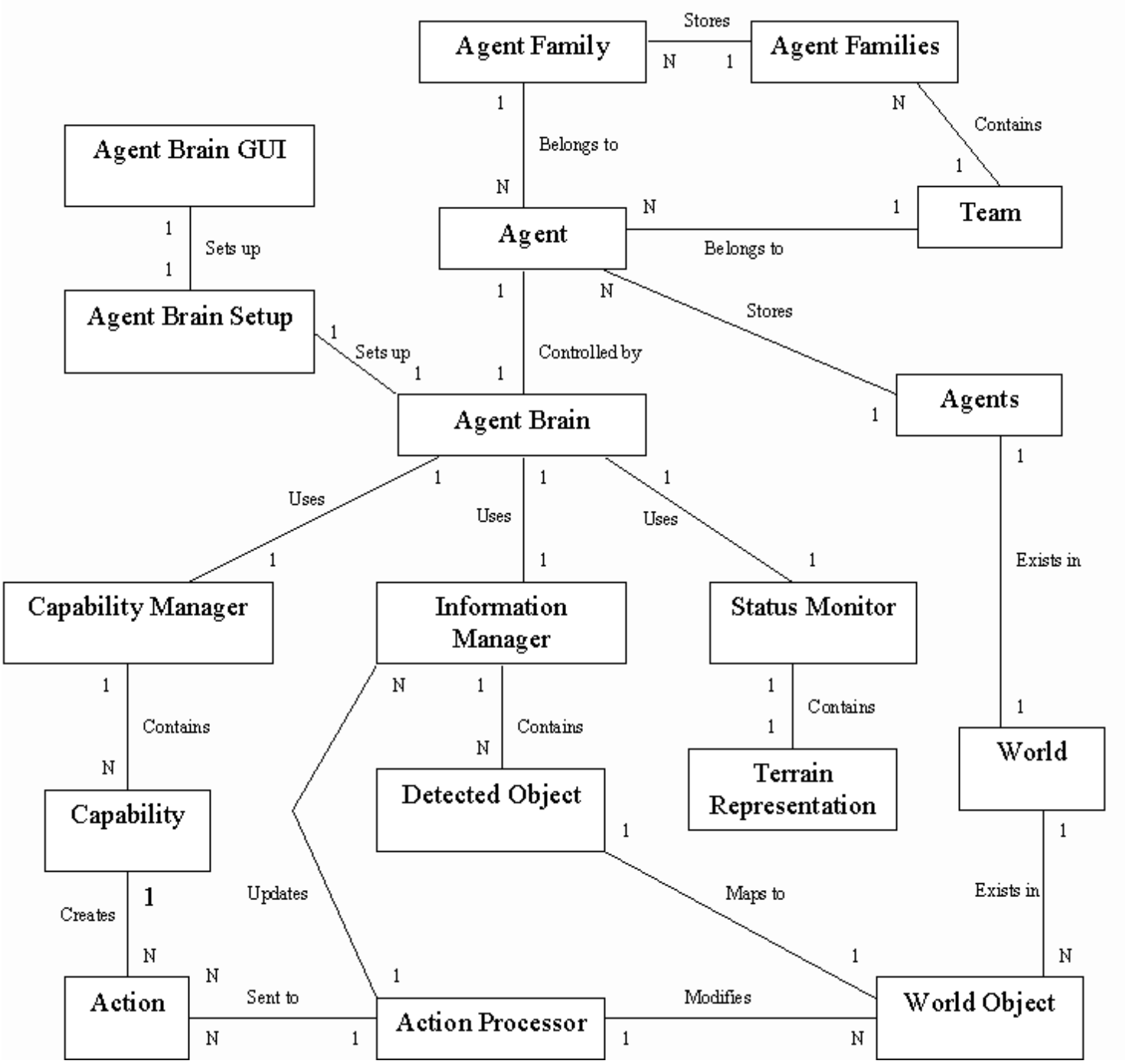


Figure 5: Relationship of the AgentBrain class to other aspects of the CROCADILE system.

As is the case with real life, perception often does not match reality. The fact that an agent observed another object several moments ago does not mean that its knowledge of that object automatically updates as the object changes. Rather, that detection was a snapshot of that object and will not be updated unless the object is detected again. CROCADILE caters for this divergence between perception and reality through creating a parallel set of classes for all physical objects within the world. These objects are termed DetectedObjects. The hierarchy of these detected objects can be seen in Figure 6.

As an agent becomes aware of objects within the world, a detected object is created from the real object. This detected object is then sent to the agent. The information contained within this detected object may be varied depending on the level of detail that the agent was able to determine from the physical object. This level of detail is a function of distance and can be assigned to each sensor during the set-up phase.

There are two fundamental aspects of an agent's knowledge. The first is the knowledge of the world around it and the second is of the agent itself. CROCADILE provides an agent brain with the tools to process both forms of information. These two tools are the Information Manager, which handles an agent's understanding of the broader world; and the Status Monitor, which allows an agent to

gain information on its own status.

The Information Manager is probably the most complex of these two tools. It is essentially a data store of all Missions, Messages and Detected Objects that an agent is aware of within the world at that given time. Of these three entities, the Detected Objects represent the largest volume of data that is processed by the Information Manager. The structure of the Detected Objects class hierarchy and their corresponding relationship to the Information Manager is shown within Figure 6.

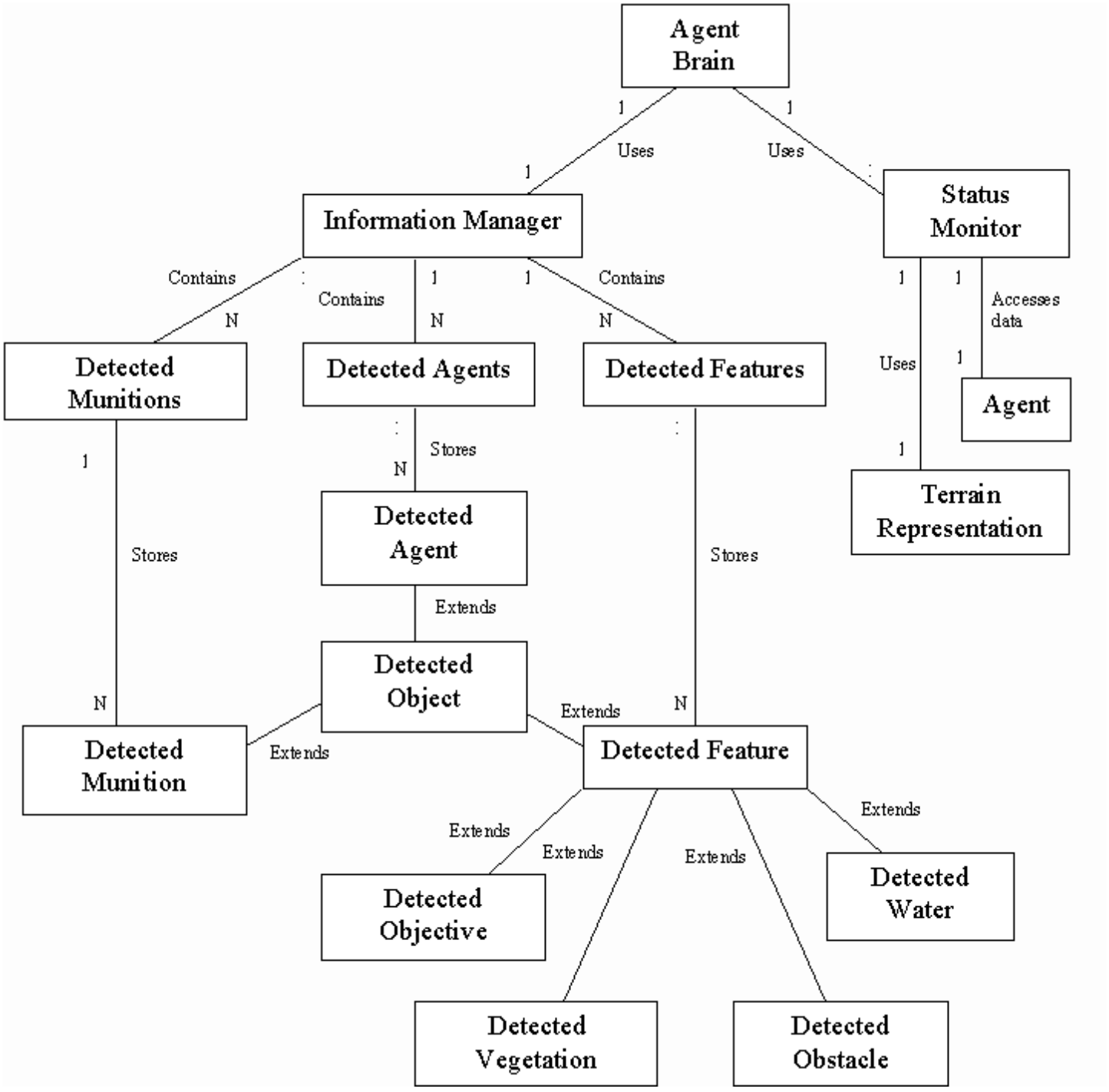


Figure 6: Knowledge representation classes employed by agents in CROCADILE.

As well as understanding the world, agents need a way to affect it in some capacity. They are able to do this through the use of the Capability Manager tool. This tool is a central repository for all of the capabilities owned by an agent. Agents are not restricted to one capability of any type. The Capability Manager contains a constant that specifies the maximum number of capabilities of a given type that an agent may posses, agents may have any number up to and including the value of this constant. Figure 7 shows a diagram of the classes related to capabilities and capability management in CROCADILE.

At this stage, it is necessary to describe how capabilities interact with the world. When a capability is exercised, the effect on the world is not immediate. Instead, an object called an Action is created. This action is added to a central world store of Actions called the Action Processor. Once all of the agents within the world have completed their turn, the simulation engine activates the Action Processor. This loops through all of the actions that have been created and transforms them into effects on the world. Through this process it can be ensured that the world does not change between agents' turns and consequently, that the order that the agents think in (their turn sequence) has minimal impact on the simulation.

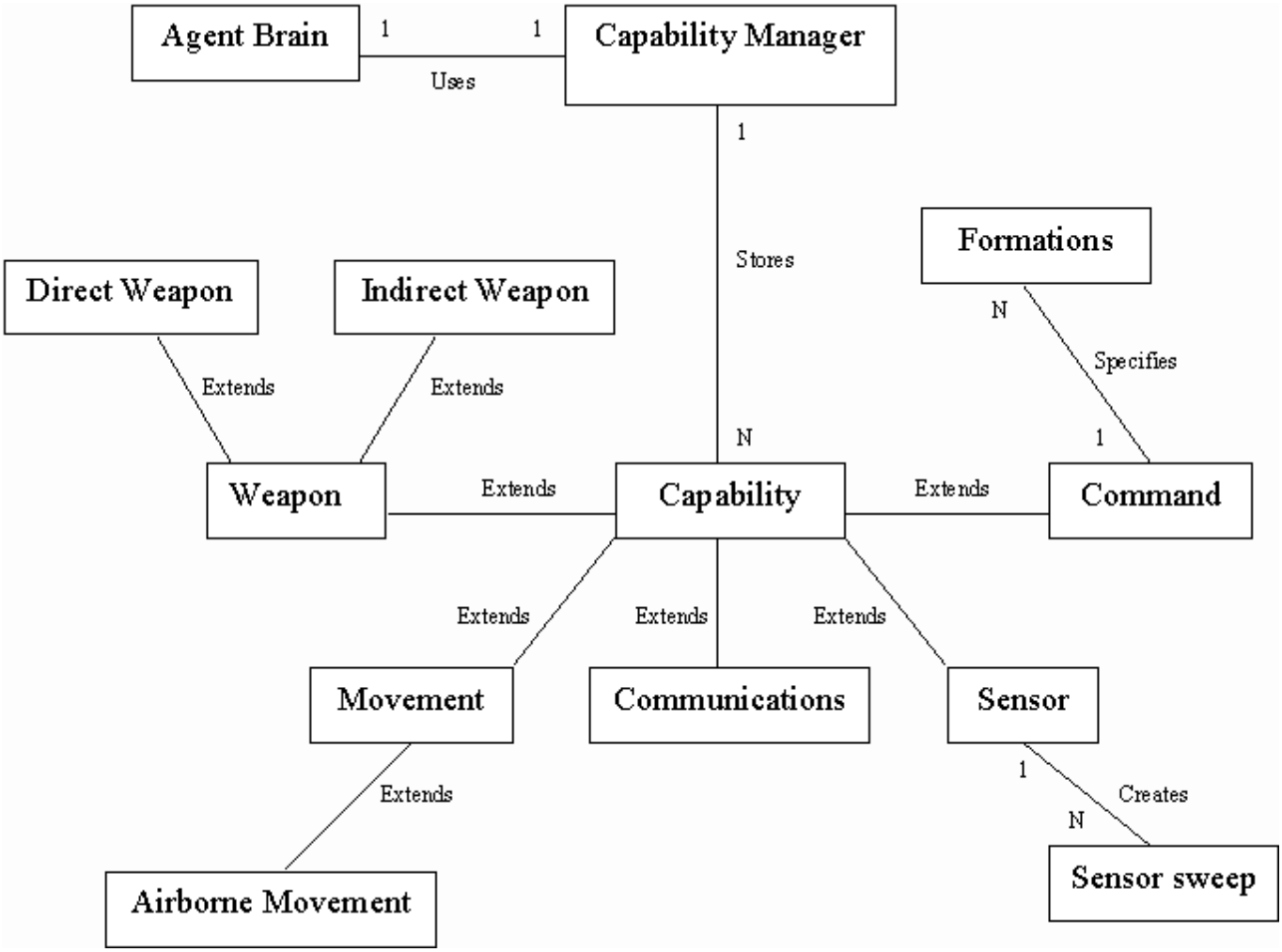


Figure 7: Capability management classes employed by agents.

Every capability has an associated action. The Weapon class creates a fire action, the Sensor class creates a scan action, the Movement class creates a Movement action, the Communications class creates a send action and the Command class creates an order action. The class diagram of these actions and how they relate is shown in Figure 8.

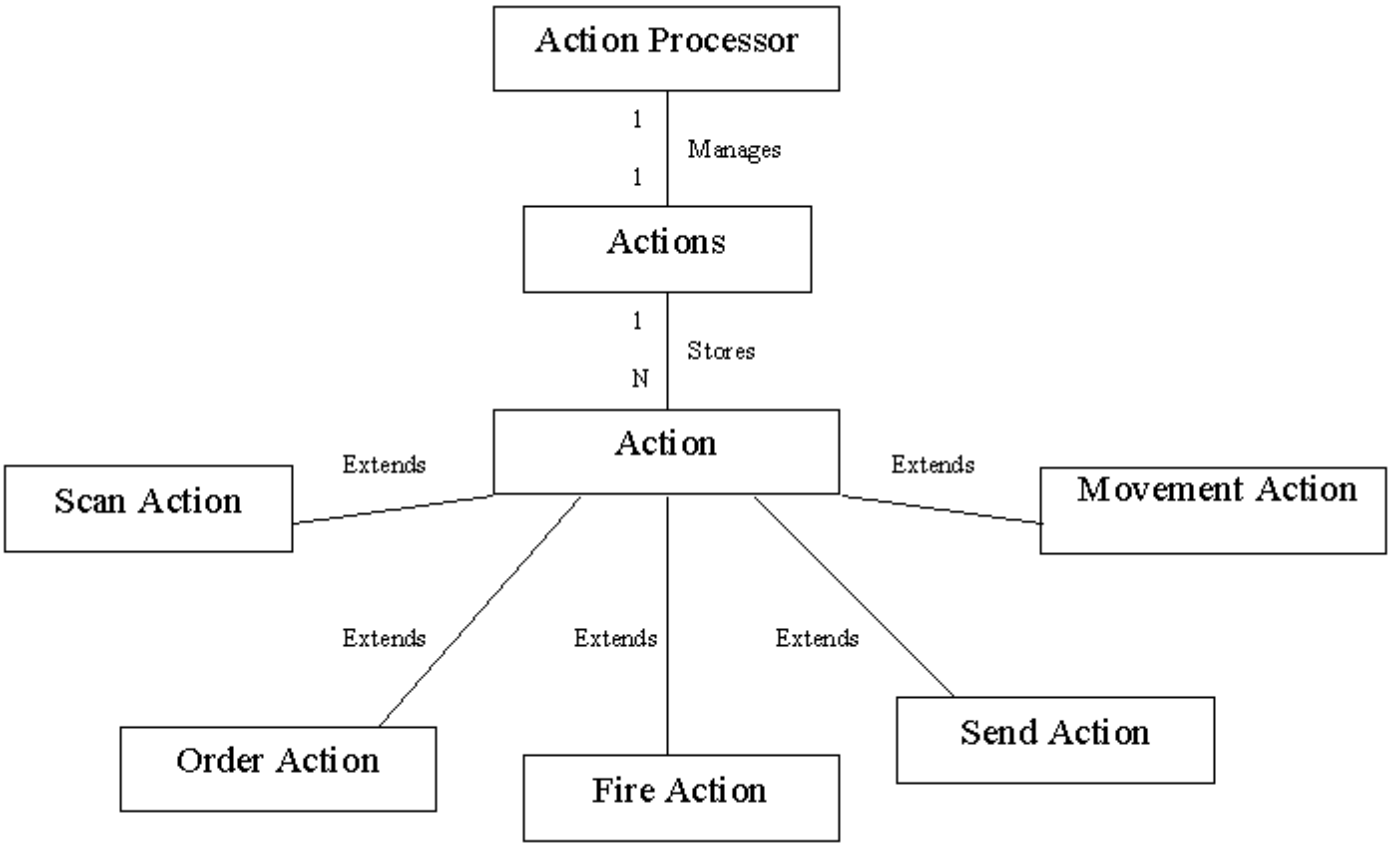


Figure 8: The action class hierarchy employed by CROCADILE.

Instinctual Agent

The three principal elements of the instinctual agent are the trigger mechanisms, the Instinctual agent itself and the behaviour templates that it uses. These elements and their related classes are shown in Figure 9.

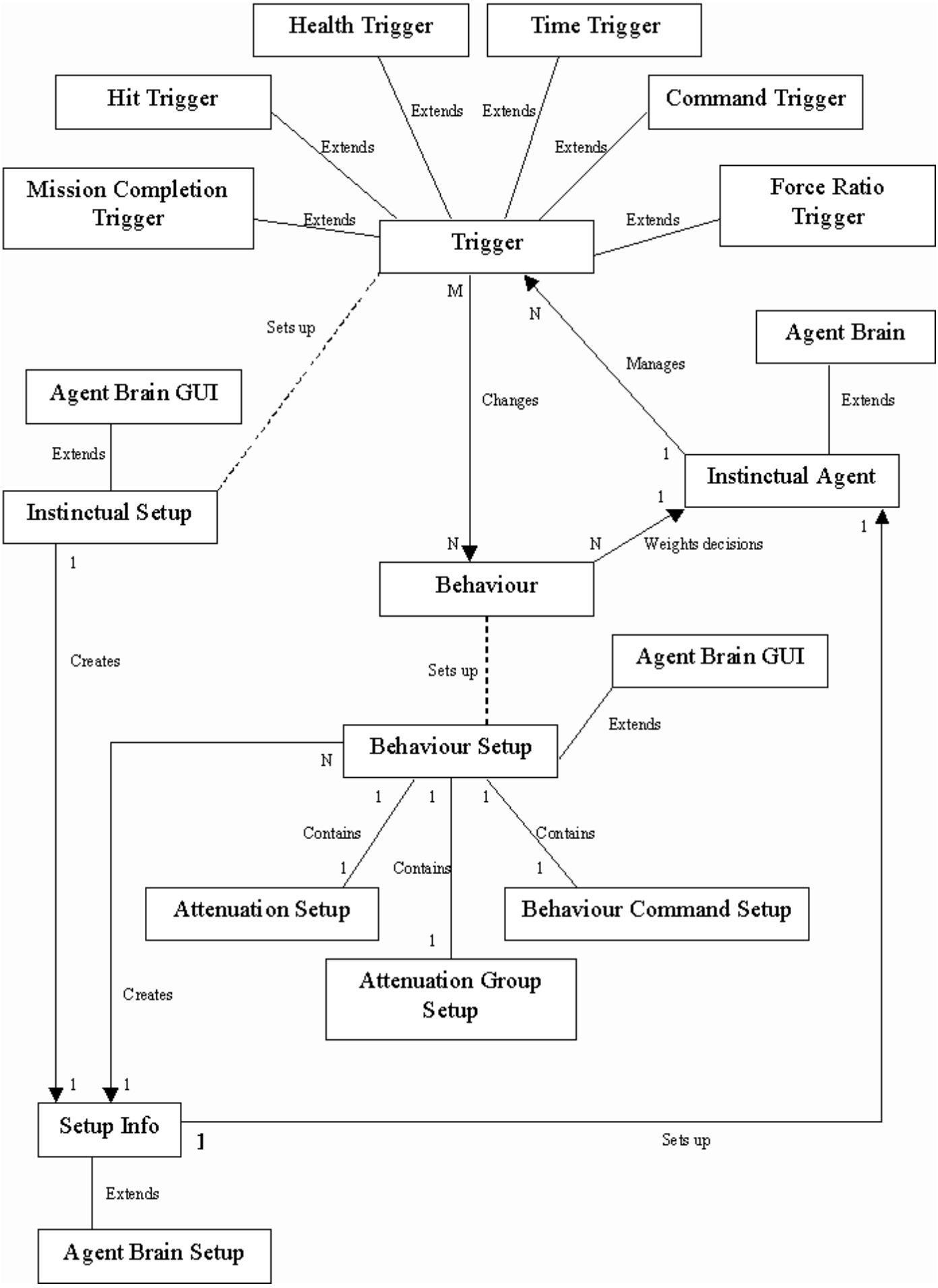


Figure 9: The instinctual agent class and mechanism. The instinctual agent is the default agent behaviour supplied with CROCADILE.

The Instinctual Agent class is the core of the instinctual agent. It is this class that extends the Agent Brain class. It is responsible for

determining the course of action that will be adopted at a given time. The information that it uses to make this decision is the data that it gains from the Information Manager and Status Monitor, and the relevant set of behavioural weights. These behavioural weights are stored in the Behaviour class.

The trigger mechanism allows these behavioural weights to be changed depending on the situation that an agent is immersed in. It is again the Instinctual Agent that manages how and when these triggers are checked. When a trigger fires, the currently selected collection of behavioural weights is swapped with the new set. This requires no change on behalf of the instinctual agent that continues using the new set of weights, unaware that a change has even occurred.

In addition to the core functionalities of the instinctual agent paradigm, Figure 9 also shows the mechanism used for setting up an instinctual agent. This happens through the InstinctualSetup class that allows a definition of the triggers within the world. From this class, dialogs can be invoked which allow individual behaviour weights to be specified.

Computational Efficiency and Usability Issues

CROCADILE presents a far more complex system than previous distillations due to a number of its features. That complexity presents a particular challenge in the areas of computation and usability. With its 3D physics model, continuous domain, and more involved hit resolution the computation requirements are potentially far higher than previous distillations. However real-time, interactive runs are a key feature in the usability of distillations. Similarly the range of additional functionalities afforded by CROCADILE could potentially overwhelm a user, again eliminating that ease-of-use that characterises distillations.

Considerable effort was spent in the design and implementation of CROCADILE to minimise the impact of these elements. The result is a distillation that runs in real-time even on older desktop PCs (e.g., Pentium II) for a projectile-physics resolved scenario involving over 60-agents on 3D terrain. Similarly, time for scenario design is of the same order as other distillations for similar complexity of scenario.

In terms of computational load, the collision detection required for a 3D world with projectile-physics combat resolution is a great burden. Every object – agents and munitions – must be checked for a collision with every other object and the terrain, every round of the simulation. Several strategies were implemented to ameliorate this computational load. Level-of-Detail (LoD) modelling was employed for the terrain at four separate levels with collision detection occurring at the minimum level of detail necessary to resolve the situation. Similarly, terrain features such as water or vegetation are defined in CROCADILE by arbitrarily complex polygons. In order to simplify checks for agents entering such features, bounding spheres around the features were employed as a first level of check. Finally, and most significantly, CROCADILE employs a tiling mechanism in order to reduce the number of redundant checks. The world is subdivided into a number of tiles with checks for collisions between objects only being made for objects, which occupy the same tile. For an n x n tiling scheme that reduces inter-object collision checks by a factor of n^2 (for an evenly spread group of objects).

The issue of complexity of usage is addressed in two ways by CROCADILE. Firstly, a hierarchical user-interface with sensible default values for a number of parameters is provided as a shield from the potential complexity. Users may then navigate the higher-level UI and employ the default set of values. Secondly, CROCADILE provides for a database of world objects – agents, weapons, agent groups, sensors, etc. This enables users to compile libraries of world objects. These objects can then be employed for the rapid creation of new scenarios.

A Future Land Force Scenario in CROCADILE

This section illustrates some of the features of CROCADILE by detailing the design of a scenario and the subsequent analysis of the results. A scenario representing one possible structure under the Australian Army's "Army After Next" concept is built. The batch processing facilities of CROCADILE were utilised to run the scenario 100 times, keeping a log of all results. Finally, those results were briefly analysed and are presented below.

It is worth noting that this is not an analysis of potential force structures – for that the parameter space of sensor, weapon, communication, and mobility would need to be explored, along with the relative worth of the three different force elements. Rather the following section presents possible analyses performed at one point in that multi-dimensional space.

The Scenario

The test case chosen was based on an examination of the force structure that could be used to combat a traditional armoured style battle group. The scenario consisted of two sides. The red side resembled a traditional tank group, characterised by high firepower, relatively slow mobility and an average sensor range. This group consisted of 40 agents that exhibited these characteristics.

These red agents were attempting to move from the top left of the world to the bottom right. Furthermore, they were aggressive and would attack and advance toward any enemy that they sensed.

In contrast, the blue side consisted of a three-tier force structure based on the Army After Next model. It had 15 agents which formed its recon element, 5 agents which formed its strike element and 3 agents which formed its reach back capability.

The recon elements exhibited poor firepower but moderate movement and good sensor capabilities. Their mission was to keep any detected red agents in sensor range without moving into the weapon range of the red agent. They also had a desire to stay dispersed in order to cover a larger area.

The strike element possessed a highly damaging, but short-range firepower capability, rapid movement and a limited sensor capability. These strike assets were intended to stay out of range of the enemy and then attack the enemy when vulnerability was detected.

Finally the reach-back element was static with a long-range area effect firepower capability, and limited sensor range. All elements of the blue force structure were able to communicate with each other. The agents that formed the reach-back element were intended to engage the enemy as soon as it was detected.

The scenario was framed as an encounter between Australian forces and an Enemy that was moving southerly from Sydney towards Canberra. Consequently, real world terrain data for this area was used in CROCADILE.

Terrain

Digital terrain data was obtained of the region of NSW between Canberra and Sydney. This was scaled into a 500x500 grid of points on which the simulation runs took place. Figure 10 shows one projection of that terrain.

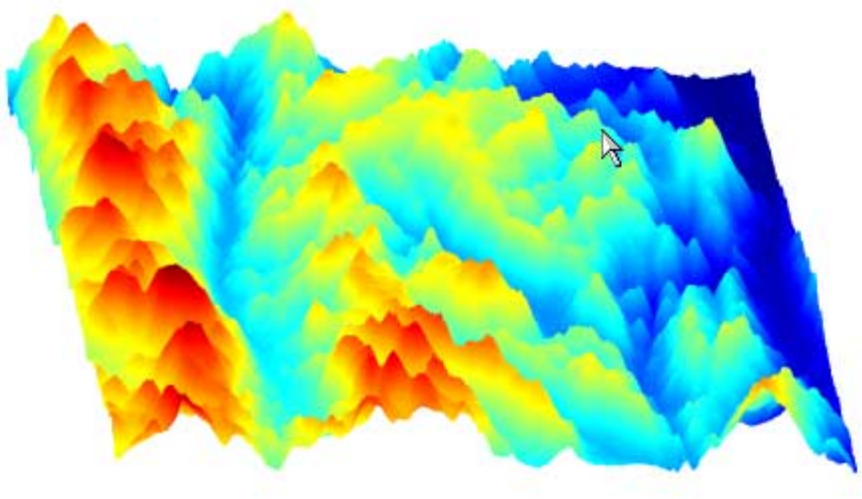


Figure 10: The 3D terrain on which the scenario runs took place. Red agents start the scenario in the top-left, while the static elements of blue begin in the bottom-right.

Agent Behaviours & Capabilities

Table 1 summarises the agents and their capabilities that form each side. Red is a homogenous single group of 40 agents, while blue is a heterogeneous group of three sub-groups – the most numerous light reconnaissance units, the fast strike units, and the long-range reach-back units with area effect weapons.

Table 1: Agent properties, capabilities, and behaviours as used in the example scenario of a conventional red force against a heterogeneous blue force.

	Red	Blue		
	Armour	Recon.	Strike	Reach Back

Physical	**Number**	40	15	5	3
	Health	100	100	100	100
	Initial Location	Top-Left	Middle	Bottom-right	Bottom-right
Capability	**Sensor Range**	250	250	250	250
	Comms Range	100	500	500	500
	Move Speed	4	4	10	0
	Weapon Range	150	120	150	special
	Weapon Damage	15	10	50	45
	Damage Type	kinetic	kinetic	kinetic	explosive (18 radius)
	Fire Rate	1/4	1/4	1/6	1/7
	Munition Rounds	100	100	20	6
Behaviour		Aggressive - close with blue, maintain friendly spacing	Passive - Keep at sensor range from enemy, maintain spacing, close with wounded enemy	Controlled aggression - Keep at weapon range from enemy	Fire at leading elements of enemy

Like all distillations the particular values are unitless, it is only their relative strength or weakness within the scenario that has meaning. Hence weapon damages range from 10 to 50 points – these points have no units and they have meaning only when considered relative to the health statistic of agents: 100. The reach back units of blue do not have a weapon range. Rather the weapon's muzzle velocity of 150 units/round is used in combination with the firing angle to calculate its munitions' parabolic path and, hence, where it strikes the terrain.

Analysis

As mentioned previously, one hundred runs of CROCADILE were made for the scenario as described above. This was done in order to capture the range of variability that is one of the features of distillation systems. The log-files were processed in order to analyse the scenario outcomes. For the purposes of this illustrative example the mean across was employed as a means of summarising the results of the one hundred runs.

Figure 11 shows the number of agents alive, and total team health as a function of time within each simulation run. Despite starting the scenario with superior numbers and superior health (both nearly 2:1), in the average case red is decimated, while blue fairs far better.

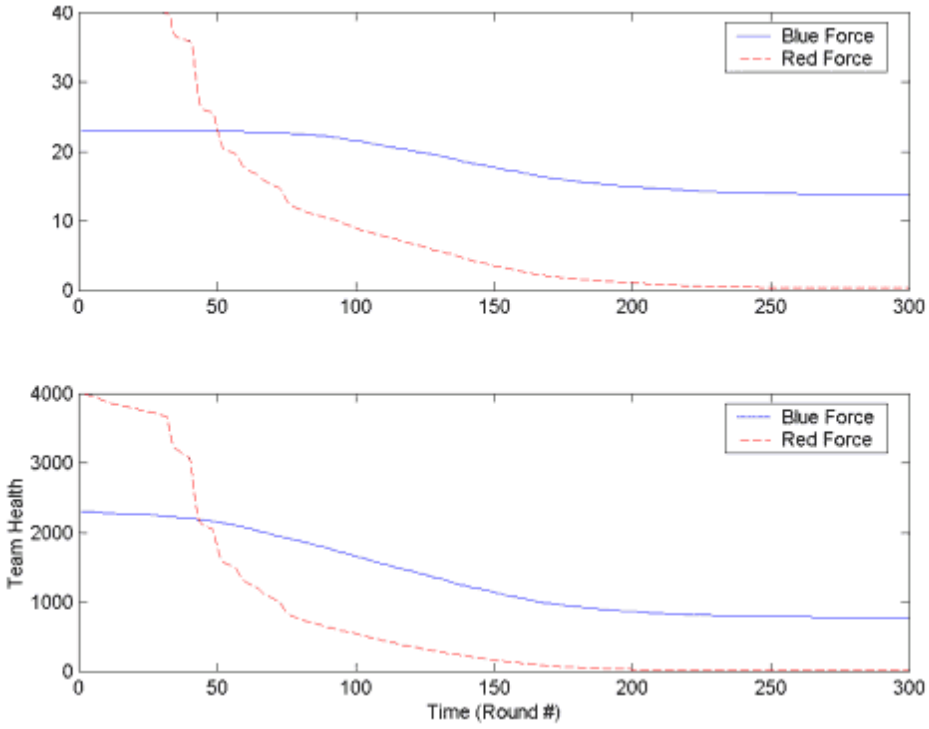


Figure 11: Number of red and blue agents alive (top) and total team health (bottom) as functions of time within the scenario. The plots represent the mean of 100 individual runs.

Red appears to suffer a large number of casualties and damage between rounds 40 and 75. Observing scenario runs it was noted that this appeared due to the indirect, explosive rounds of blue's "reach back" group. In order to check this hypothesis damage in the scenario was subdivided into explosive—fired by the reach-back units—and impact – fired by all other units and plotted as a function of time. Figure 12 is the result.

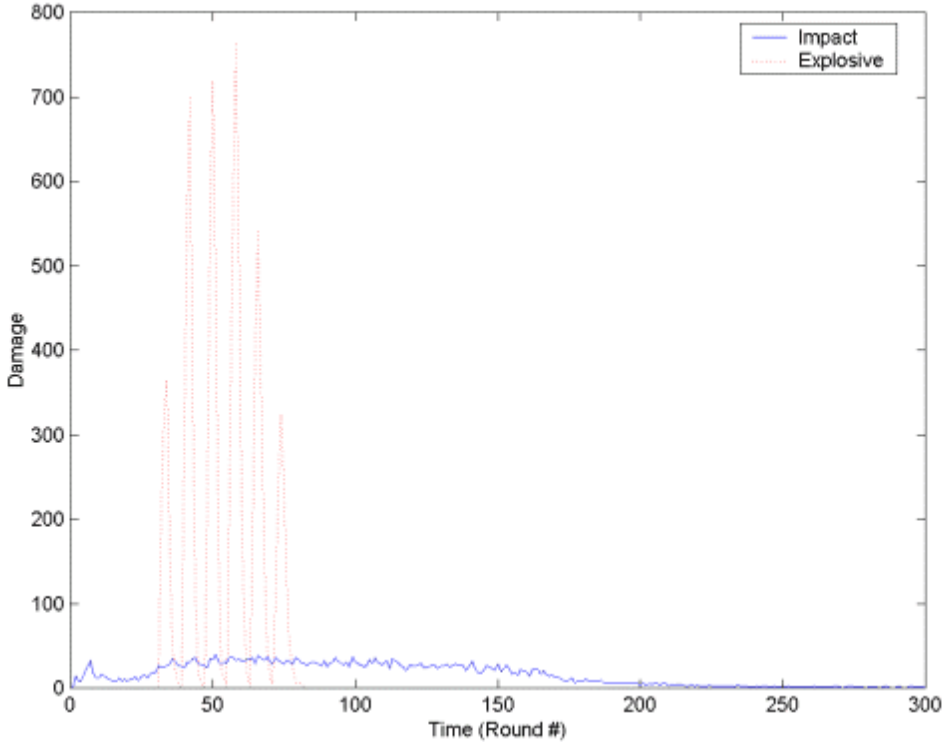


Figure 12: Damage within the scenario runs as a function of the time (round number) within the scenario. Damage is subdivided into impact (ballistic) and explosive rounds.

As is clearly seen from the figure, impact damage is spread rather evenly throughout the scenario, tailing off towards the end as the number of agents becomes small. On the other hand, explosive damage all occurs between roughly round 40 and 80. This is indeed the period when blue's indirect rounds fall amongst the red agents. Indeed those rounds are shown to be particularly devastating, causing very large amounts of damage. Observation of the log files showed that this was the result of the burst effect of the rounds – a single round might damage as many as five red agents. The explosive damage itself is confined to a relatively short time span. This is attributable to the limited number of rounds possessed by the reach back units. A final observation from the figure is the periodicity of the explosive damage – this is due to the fact that the reach-back units were constrained to only firing once every seven rounds.

As CROCADILE keeps a log of all major simulation events, such as every round that hits – that includes where the event took place, it is possible to spatially analyse the events of the simulation run.

Figures 13 and 14 provide such an analysis. Both are contour plots – showing the regions where hits occurred, where damage was taken, and where agents were destroyed. Figure 13 groups all, red and blue, agents together; while Figure 14 separates the red and blue agents, placing the respective representation side by side in two columns.

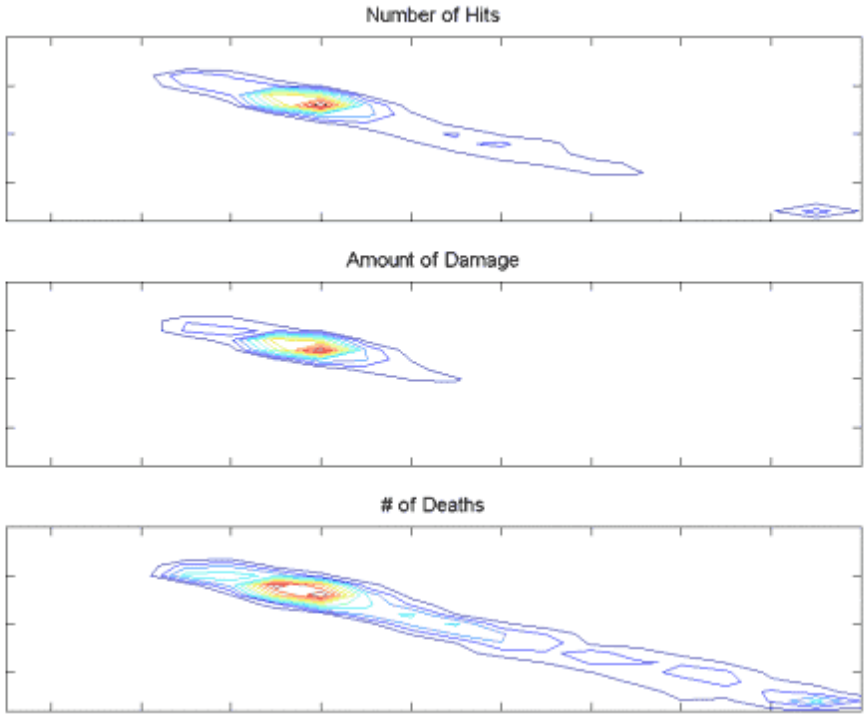


Figure 13: Distribution of hits, damage, and agent deaths across the physical landscape. Results are grouped across all agents, regardless of team. Red agents begin the scenario in the top-left of the world while blue's position is the bottom-right.

Several observations are possible from the figures. Firstly, just as red follows a simple approach of chasing blue units, while most blue retreat or are fixed in the bottom-right corner; so the course of the conflict is distributed along the diagonal from top-left to bottom-right. The non-linearity inserted by the reach-back units of blue means that most hits and damage occur where the munitions from those units fall. Because of munition flight-times and the delay in communication of information from the reconnaissance units to the reach-back units, most hits remain roughly at the same location across the runs – approximately one-third of the way from red's starting position to blue's static position.

Contrasting between the two forces, as shown by Figure 14, it is once again clear that the red force suffers most of its damage and hits from the indirect explosive fire of the blue reach-back units that occurs in the first third of red's advance. On the other hand, the blue force suffers most of its hits, damage and casualties in the "second half" of the battle as red approaches blue's defensive position – blue looses room to manoeuvre, its stationary units come within reach of the advancing red units, and a number of blue units become more aggressive (the "fast strike" units have entered the conflict while the recon units become aggressive in response to wounded red units).

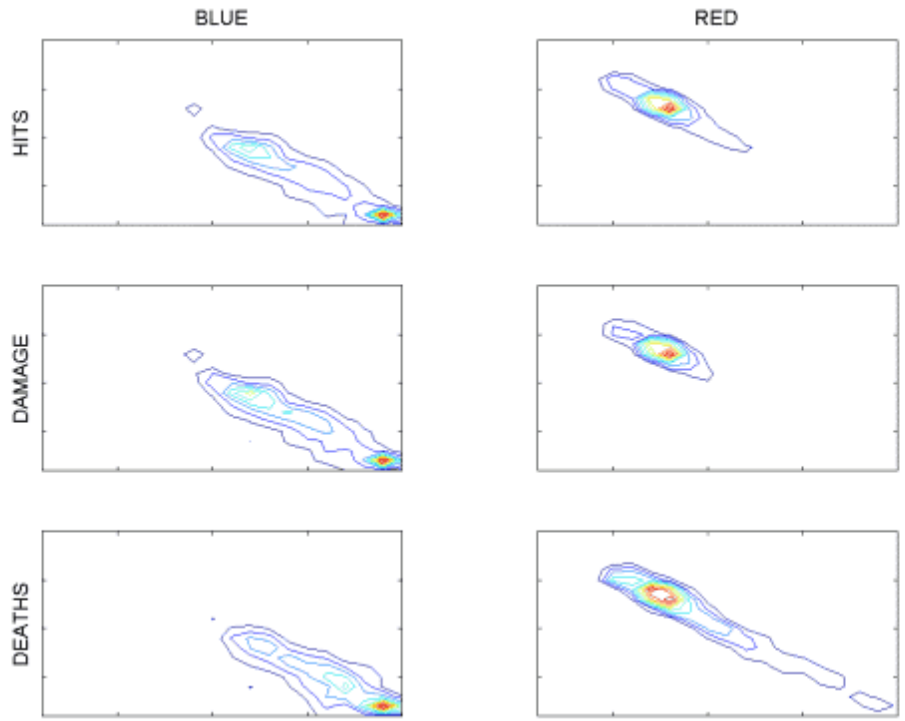


Figure 14: Distribution of hits, damage, and agent deaths across the physical landscape. Results are subdivided on the basis of team – blue in the left column and red in the right. Red agents begin the scenario in the top-left of the world while blue's position is the bottom-right.

Discussion

This paper has presented a new multi-agent-based combat distillation known as CROCADILE—Conceptual Research Oriented Combat Agent Distillation Implemented in the Littoral Environment—that has been developed at the Australian Defence Force Academy. The system is not intended to replace existing distillations such as MANA, EINSTein or Socrates; rather it complements them by building on their core features while incorporating several key new aspects. These key aspects have been previously summarised but lie in two areas. Higher fidelity models in the form of a 3D world, including 3D terrain; probabilistic or projectile hit resolution; more complex combat phenomenon – round penetration, continuous health, burst effects and indirect fire; and the ability to load user-written agents are all supported by the system. The conventional 2D world and instinctual agent behaviour is also supported, allowing users to select the level of fidelity they desire. This moves the realm of distillations closer to conventional constructive simulations, arguably making it easier to transfer insights gained in the distillation realm into more detailed simulations and thus supporting the operational synthesis, or holistic approach to simulation. Secondly, CROCADILE delivers an open, extensible simulation engine that can be extended simply and efficiently. This is directly attributable to the strong object-oriented approach that permeates all levels of CROCADILE. Just as it is possible for the user to design a new sensor with which to equip an agent, so also is it possible to write code for a new agent, or even extend the definition of the Communication capability within the simulation engine in order to support fallibility of communication equipment.

CROCADILE is a free system and its usage by the distillation, operation analysis, Alife and agent communities is welcomed. The web site http://www.cs.adfa.edu.au/VESL/Croc contains not only the latest version of CROCADILE but also supporting materials such as a user manual, more detailed technical information, together with a growing database of terrain files and pre-built scenarios, agents, and equipment.

CROCADILE is not a static system. While it is already being used to investigate agents that learn tactics, teamwork within a heterogeneous group of agents, the impact of asynchronous updates within a network of relationships, and the importance of intangibles such as morale or personality on conflict outcome; these are only a fraction of its potential applications. At the same time CROCADILE has a developmental future – a full 3D visualisation of running scenarios, alternate agent behaviour paradigms such as BDI, high-level real-time control of agents by a human, and a centralised database accessible over the network through CROCADILE itself are all planned. Resource availability will dictate how quickly these and other planned features are realised.

Notes:

1. Trevor Colton, “The Army Synthetic Environment,” in *SimTecT Proceedings 2001* (Canberra, Australia, 2001), pp. 305-308.
2. Simon Mepham, “Synthetic Environments – Delivering Real Benefits to UK Defence,” *SimTecT Proceedings 1998* (Adelaide, Australia, 1998).
3. Trevor Colton, Private communication (2001).
4. Conceptual level simulations model conflict at an abstract level, modelling generic capabilities and effects rather than specific entities and weapons.
5. Andy Illachinski, *Towards a Science of Experimental Complexity: An Artificial Life Approach to Modelling Warfare*, Research Memorandum CRM 99-61 (Center for Naval Analyses, 1999).
6. The United States Marine Corps established project Albert in 1995 with the mission of examining new sciences to provide quantitative answers to important military questions. Since then Project Albert has become an international project with participants from Australia, New Zealand, Sweden, Germany and Canada all actively involved with research in this domain.
7. Gary Horne, “Beyond Point Estimates: Operational Synthesis and Data Farming,” in *Maneuver Warfare Science 2001*, ed. Gary Horne and Mary Leonardi (US Marine Corps, 2001).
8. Alfred Brandstein, “Operational Synthesis: Applying Science to Military Science,” *Phalanx* 32, 4 (1999): 1, 30-31.
9. Horne, “Beyond Point Estimates: Operational Synthesis and Data Farming.”
10. Alfred Brandstein, *Introduction to Project Albert*, Briefing slides to 4th Project Albert International Workshop (2001).
11. J. Clavell, *The Art of War By Sun Tzu* (London, England: Hodder and Stoughton, 1981).
12. Alfred Brandstein, “Foreword,” in *Maneuver Warfare Science 2001*, ed. Gary Horne and Mary Leonardi (US Marine Corps, 2001).
13. F. W. Lanchester, *Aircraft in Warfare* (London, England: Constable & Co, 1916).
14. Taylor thereof conducted a detailed mathematical analysis of the Lanchester Equations and derivations in 1983. – J. G. Taylor, *Lanchester Models of Warfare* (USA, Operations Research Society of America, 1983).
15. Andy Illachinski, *Irreducible Semi-Autonomous Adaptive Combat (ISAAC): An Artificial Life Approach to Land Warfare*, Research Memorandum CRM 97-61 (Center for Naval Analyses, 1997).
16. Illachinski, *Irreducible Semi-Autonomous Adaptive Combat*.
17. Michael Lauren, *Complexity Theory and Land Warfare*, Briefing slides for the 4th Project Albert International Workshop (2001).
18. Land Warfare Doctrine 1: *Fundamentals of Land Warfare* (Canberra, Australia: Defence Publishing Service, 2000).
19. Andy Illachinski, *Land Warfare and Complexity, Part 1: Mathematical Background and Technical Sourcebook*, Information Manual CIM-461 (Alexandria, VA: Center for Naval Analyses, 1996); Andy Illachinski, *Land Warfare and Complexity, Part 2: An Assessment of the Applicability of Nonlinear Dynamics and Complex Systems Theory to the Study of Land Warfare*, Research Memorandum CRM-68 (Alexandria, VA: Center for Naval Analyses, 1996).
20. Michael Lauren, *Characterising the Difference between Complex Adaptive and Conventional Combat Models* (Auckland, New Zealand: Defence Operational Technology Support Establishment, 1999).
21. Illachinski, *Land Warfare and Complexity.*
22. Illachinski, *Land Warfare and Complexity*.
23. Michael Lauren, *Beyond Lanchester: A Fractal-Based Approach to Equations of Attrition* (Auckland, New Zealand: Defence Technology Agency, 2001).
24. Stan Franklin and Art Graesser, “Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents,” *Third International Workshop on Agents, Theories, Architectures and Languages ATAL* (1996).
25. A Cellular Automata is a regular spatial lattice of cells, where each cell may have any one of a finite number of states at a given time step, and where the state of each cell is updated according to a local rule which may depend on the state of the cell and its neighbors at the previous time step.
26. Nino Boccara, O. Roblin and M. Roger, “Automata network predator-prey model with pursuit and evasion,” *Physical Review E* 50, 6 (1994): 4531-4541.
27. Gil Tidhar C. Heinze, Simon Goss, G. Murray, D. Appla, and I. Lloyd, *Using Intelligent Agents in Military Simulation or “Using Agents Intelligently”* (Australia: Defence Science and Technology Organisation, 2000).
28. Andrew Lucas, *et.al.*, “Towards Complex Team Behaviour in Multi-Agent Systems,” *SimTecT Proceedings 2001* (Canberra, Australia, 2001), 89-92.
29. Kerry Bennett, T. Josefsson, Simon Goss, M. Cross, S. Waugh, and T. Truong, “An Application of DSTO’s Battle Model using Agents and Humans-in-the Loop,” *SimTecT Proceedings 2001* (Canberra, Australia, 2001), 99-110.
30. Lauren, *Complexity Theory and Land Warfare.*
31. Brandstein, “Operational Synthesis: Applying Science to Military Science.”
32. Horne, “Beyond Point Estimates: Operational Synthesis and Data Farming.”
33. Lauren, *Beyond Lanchester: A Fractal-Based Approach to Equations of Attrition.*
34. Lauren, *Characterising the Difference between Complex Adaptive and Conventional Combat Models.*
35. An agent control paradigm is the algorithm or technique that is used to control an agent’s behaviour.
36. G. Battista, *et.al.*, “Algorithms for Drawing Graphs: An Annotated Bibliography,” *Computer Geometry and Theory Application* 4 (1994): 235-282.
37. Illachinski, *Irreducible Semi-Autonomous Adaptive Combat (ISAAC): An Artificial Life Approach to Land Warfare.*
38. Meta-personalities refer to the ability of an agent to exhibit alternative behaviours depending upon the situation that it is immersed in at a given time.
39. Illachinski, *Towards a Science of Experimental Complexity.*
40. R. Stephen, *Maui Agent-Based Combat Model*, Briefing slides, Project Albert 3rd International Workshop (Auckland, New Zealand, 2001).
41. N. Bent, *Socrates v1.1 User Manual* (USA: Emergent Information Technologies Inc., 2001).
42. Illachinski, *Towards a Science of Experimental Complexity.*

Dr. MICHAEL BARLOW is a senior lecturer within the School of Computer Science at the University of New South Wales, at the Australian Defence Force Academy (ADFA). He is also the founding director of the Virtual Environments and Simulation Laboratory (VESL) at ADFA. Dr. Barlow has published over thirty papers in the areas of speech and speaker recognition, visualisation, virtual environments, agents and cellular automata. He is also co-author of a book covering the media APIs of Java to be published by Sam's Publishing in mid 2002. Dr. Barlow's interests cover agent technologies, automatic speech understanding and speaker recognition systems, virtual environments and visualisation, and educational technology. Mail Address: Dr. Michael Barlow, School of Computer Science, University of NSW / ADFA, Northcott Drive ACT 2600, Australia. Email: spike@adfa.edu.au.

ADAM EASTON is a lieutenant in the Australian Army. Adam Easton is a new researcher with one prior publication. Adam Easton's interests cover agents, graphics, and simulation engine technologies.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

CROCADILE - An Open, Extensible Agent-Based Distillation Engine

Michael Barlow and Adam Easton

Keywords: CROCADILE, Conceptual Research Oriented Combat Agent Distillation Implemented in the Littoral Environment, multi-agent based distillation system, 3D or 2D simulation engine, projectile or probabilistic hit resolution.

Abstract: This paper describes a new multi-agent based distillation system known as CROCADILE – Conceptual Research Oriented Combat Agent Distillation Implemented in the Littoral Environment. CROCADILE shares the common features of other distillations such as MANA or EINSTein – an abstracted representation of the capabilities and behaviour of the conflict participants, from the interactions of those participants combat behaviour is seen to emerge. CROCADILE extends the realm of distillation systems in a number of novel and powerful ways delivering an open, extensible distillation engine realised in a 3D world and with variable levels of fidelity. In particular some of the key aspects that differentiate CROCADILE are: a 3D or 2D simulation engine; projectile or probabilistic hit resolution; units that can move by land, sea or air; support for multiple agent behaviour paradigms and user written agents; a high fidelity combat model that incorporates indirect fire, line of sight, round penetration and burst effects; sophisticated configurable command, mission, communication, and team structures; comprehensive logging of simulation results; and a database system for saving and loading world objects. CROCADILE follows an object-oriented approach in its design and realisation at all levels, making it easily extensible. Written in the Java language it is platform independent and freely available. The paper first covers the design philosophy and implementation of CROCADILE. A scenario concerning a potential future force structure for the Australian Army is then employed as a means of illustrating some of the features of the system. A number of runs of the system for the given scenario are analysed as to outcome for the teams of agents, weapon effectiveness, and the distribution of hits, damage and agent deaths within the physical combat space .

full text

Authors: **James Moffat and Susan Witty**
Title: **Phase changes in Meta-modelling using the Fractal Dimension**
Year of issuance: **2002**
Issue: **Information & Security. Volume 8, Number 1, 2002, pages 52-67**
Hard copy: **ISSN 1311-1493**

PHASE CHANGES IN META-MODELLING USING THE FRACTAL DIMENSION

James MOFFAT and Susan WITTY

Table Of Contents:

Introduction

In this paper we are concerned with intelligent agent simulation models which can be used to investigate some of the new aspects of “information-age” conflict. Such models consist of a number of agents which interact locally in order to produce global emergent behaviour. One of the simplest, yet very relevant, examples of such a model is ISAAC, developed by the US Marine Corps Combat Development Centre under the “Project Albert” initiative. [1,2] In this case, modification to the behavioural characteristics of the agents produces significantly different emergent behaviour in terms of the flow of battle and casualties suffered. Some of these behaviours can be surprising, and it is the aim of our work to produce a theory of such processes which helps to explain the types of behaviour to be expected.

In short, understanding the behaviour of such agent based combat models is now becoming more important, especially as the agents gain intelligence and try to outsmart each other, producing potentially very complex behaviour. The principal variables in these models can often be separated out from the rest of the model to produce a meta-model which is aimed at decreasing the run-time of the original model while still retaining the characteristics and arriving at the same final solution as the original model.

As an example, in developing a meta-model we consider the relationship between a key outcome of

the model, *a*, and a set of input variables as follows:

$$a = f(a_1, \ldots a_k, b_1) \qquad (1)$$

(This is easily generalised to an arbitrary number of *b*'s).

The meta-model function can then be shown to have the property: [3]

$$a = f(a_1, \ldots, a_k, b_1) = a_1^{p} \ldots a_k^{r} \Phi\left(\frac{b_1}{a_1^{p_1} \ldots a_k^{r_1}}\right) \qquad (2)$$

In some cases the function Φ can be further simplified using a re-normalisation group.[4] This approach directs us to search for evidence of power law relationships, re-normalisation groups, and normalised distributions of the form Φ. Such expressions arise naturally in certain types of complex system, particularly where fractal structures are involved, and are referred to as "scaling" relationships, since they have no preferred gauge. Moffat and Passman show that there is clear evidence for such assumptions.[5] In particular it turns out that the attrition rate for one side in such an agent-based model is correlated to the fractal dimension of the opponent.[6,7] This fractal dimension is a measure of the ability of a side to cluster and collaborate locally (to produce locally advantageous force ratios).

As an example of how these apparently abstract ideas can give us immediate insight, we illustrate the problem of relating local force clustering and collaboration to the ability of the whole force to control an Area of Operations. Control is defined here in terms of the ability to prevent the opposing force or some third party from being able to move freely across the Area of Operations.

Let a single unit be able to control a patch of the Area of Operations (AO) corresponding to a square of side length *l*. We assume that the force (from our previous discussions) is clustered fractally with fractal dimension *D*. It follows from the definition of *D* that if we cut up the AO into squares of side length *l*, then the number of occupied squares is

$$N(0) = l^{-D} \qquad (3)$$

Thus the probability of a square being under control is given by

$$p = \frac{l^{2-D}}{A}, \qquad (4)$$

where *A* is the area of the AO. This is in fact a standard measure of fractal clustering, and hence is a good measure of the ability of the force to locally cluster and collaborate.[8]

We now apply a re-normalisation group approach. By considering configurations in which 1,2, 3 or 4 of the cells of side *l* are controlled sub-regions of the square of side 2*l*, and assuming that control requires a span of controlled cells stretching from side to side and top to bottom (to prevent flow through the region in any direction), we have the following relationship:

$$p(2l) = 4p^3(1-p) + p^4, \qquad (5)$$

where *p(2l)* is the probability of control of a square of side 2*l*. By continually increasing the area considered in this way, through re-normalisation, we have the general iterative relationship for the probability of control at increasing levels of span of the AO:

$$\begin{aligned} p_{n+1} &= 4p_n^3(1-p_n) + p_n^4 \\ &= p_n^3(4-3p_n) \end{aligned} \qquad (6)$$

The stable points in this recursive relation then correspond to the intersection between the function

$$g(x) = x^3(4-3x) \qquad (7)$$

and the line *y=x* for values of *x* in the region between 0 and 1. In this region, *g(x)* is *S* – shaped and it

thus has three intersections with the line $y=x$. Two of these are stable, at the extreme values 0 and 1, and there is one unstable intermediate point.

Interacting force units should thus polarise to either a very high level of control or a very low level of control. Any particular clustering of the force (corresponding to a particular unit probability of control p) should thus give rise to a level of control which is attracted (by re-normalisation to larger areas of the AO) towards one of the two extremes.

Top Down Planning

All of the above analysis indicates that Fractal Dimension is a key indicator of behaviour in agent based models of conflict. However, it is very much a "bottom up" generated emergent behaviour of the model based on inherent assumptions about local clustering and collaboration. In order to complete the description of a meta-model, we also have to represent the "top down" perspective of a high level plan, and how this interacts with such emergent behaviour generated from below. To do this we have adopted the structure of Bayesian Decision Making, which assumes there is some overall goal or objective (or more generally a set of such objectives) to which the system as a whole evolves, and there is a loss of utility involved in not meeting such objectives. In agent based modelling terms we consider then a set of such desired end states or "attractors" to which the model evolves. We have an understanding of the set of outturns from the simulation model, and an understanding of the loss of utility relating to the gap between each outturn and the set of goals. We then consider the Expected Utility function, which combines together the distribution of outturn, and the associated utility. It turns out that the mathematics of such functions is congruent with that of elementary catastrophe surfaces, and this is discussed below.

In the first of these investigations we look at the robustness of each start point in relation to the end points of the model run. This is in the context of many possible different end states or goals. The second looks at the problem with only a small number of end states or goals.

Robustness Analysis with Many Possible Goals

In a given system, it is possible to divide the parameter space into regions of probability of each end state. In this case the parameter is the fractal dimension of one of the forces at the beginning of a model run. We assume that the probability of any start point of fractal dimension resulting in a particular end state can be approximated by a scaled Normal distribution with a mean value μ_i and variance V_i locally. The probability can be written as:

$$f(D|i) = \frac{h}{\sqrt{2\pi V_i}} \exp\left[\frac{-(D-\mu_i)^2}{2V_i}\right] \quad (8)$$

where, for a two-dimensional problem, $0 \leq D \leq 2$.

However, for any start point *D*, there is not just a single attractor which the system could move to as its end state. At each fractal dimension there exist *j* different attractors which the system could possibly choose as its end state. At this chosen fractal dimension *D*, each of these end states has a probability $p_j = f(D|j)$. At any given fractal dimension, the sum of the probabilities of reaching all end states must be 1, i.e. $\sum_j f(D|j) = 1$.

Each of the possible end states has a utility attached to it. In this way, some end states or attractors are considered to be "better" outcomes than others. For each fractal dimension value *D*, with respect to a single end state *i*, a utility function $U(i, D)$ is assumed, according to the utility of each end state based on the fractal dimension.

To calculate the expected utility for each end state over all possible values of the fractal dimension *D*, the probability function and the utility function are multiplied together and integrated over all possible values of the fractal dimension:

$$E(i) = \int_{\forall D} f(D|i)U(i, D)\mathrm{d}D \qquad (9)$$

This indicates the expected utility of end state *i*. It is a measure of how robust each of the end states is over the range of all possible start points. Alternatively the utility of the point *D* as a start point can be calculated as a sum over all possible end states:

$$E(D) = \sum_i f(D|i)U(i, D) \qquad (10)$$

This is a measure of which fractal dimension to start from to attain the maximum expected utility of outcome.

Catastrophe Theory Approach

In the above discussion, there was no explicit decision to make. The decision was implicitly, "which start point do I choose based on the prior knowledge I have of the model?" or "what is the best end state to aim for based on my prior beliefs?" based on maximum expected utility. By making this

decision explicit, it is possible to utilise Bayesian decision theory and the resultant mathematics of catastrophe theory to help in making the decision of which start point to choose for the model. The question we shall ask is: "I want my end state to be attractor *i*. Which is the best fractal dimension to choose for the start point of the force?"

A probability distribution for the prior belief of the best possible starting values of the fractal dimension can be written down to achieve the end state *i*.[9]

$$f(D|) = \frac{h}{\sqrt{2\pi V_i}} \exp\left[\frac{-(D-\mu_i)^2}{2V_i}\right], \qquad (11)$$

where the mean of the distribution is μ_i and the variance V_i. The next question we ask is "what would happen if we move the fractal dimension by a mean amount d in an attempt to improve the likelihood of achieving end state *i*?" We assume that the probability of each fractal dimension giving the end state *i* is now given by

$$f(D|,\delta) = \frac{h}{\sqrt{2\pi V}_i(\delta)} \exp\left[\frac{-(D-(\mu_i+\delta))^2}{2V_i(\delta)}\right] \qquad (12)$$

By changing the starting fractal dimension of the force, we are assuming that the change to the start point will increase the success in outcome in relation to end state *i*. However, if the starting point is changed from the mean μ_i to the value $\delta + \mu_i$, the benefit of that starting point in terms of achieving goal or end state *i* is less certain and the variance must increase. Therefore, the variance $V_i(\delta)$ depends on the decision d made (we assume) according to:

$$V_i(\delta) = \left\{V_i + A\delta^2\right\}^{1/2} \qquad (13)$$

A is a scaling factor which relates how much effect the decision d has on the variance of the distribution. A high value of *A* means that the user has very little information on what the effect of changing the start point will have on the outcome of the combat model other than the information he has on the original belief of the start point; thus a change will make a large increase to the variance.

It is assumed that there exists a preferred fractal dimension denoted by D_0 . This may be that determined by the doctrine of the force. Alternatively, it may indicate that there is high utility in the end state being achieved relative to some other measure, for example that the goal should be achieved with a high level of control of the battlespace. Therefore, the fractal dimension of D_0 should be the "best" fractal dimension for any desired outcome or end state and the utility of any starting point can be written as:

$$U(i,D) = U(D) = \exp\left[\frac{-(D-D_0)^2}{2k(\delta)}\right] \quad \forall i \qquad (14)$$

Just as the variance of the prior belief function changes with greater decisions, the variance $k(\delta)$ of the utility function can too. As the change d to the starting value of the fractal dimension is increased, it becomes more important that the starting value of the fractal dimension *D* is closer to the value D_0, since it is uncertain what effect other values of *D* will have on the outcome or end state. So *k* can be written as

$$k(\delta) = \left(\eta + B\delta^2\right)^{-1/2} \qquad (15)$$

Here, h is the largest possible variance the utility function may take. *B* is a scaling factor which represents the effect of a change to the mean fractal dimension value μ_i .

If $U(D)$ and $f(D|_i,\delta)$ are multiplied together and integrated over all possible changes to the prior belief, the maximum value corresponds to that decision which will give the highest expected utility to that force given the aim of achieving end state *i*.

$$E_i(\delta) = \int_{vD} U(D) f(D|, \delta)$$

$$= h\left(\frac{1}{1 + (\eta + B\delta^2)^{1/4}(V_i + A\delta^2)^{1/4}}\right)^{1/4} \exp\left\{\frac{-(\delta + \mu_i - D_0)^2}{2\left(\frac{1}{(\eta + B\delta^2)^{1/4}} + (V_i + A\delta^2)^{1/4}\right)}\right\} \quad (16)$$

To find the points of maximal utility, this function must be differentiated with respect to the decision d and the points at which $E_i'(\delta) = 0$ are the points of maximum (and minimum) expected utility.

To examine these turning points, we thus plot the function $E_i(\delta)$, the expected utility of the start point given the aim of achieving end state *i*. For different values of m , *h* , *V*, *A* and *B*, different plots are obtained. The following three figures (1, 2 and 3) show the behaviour and the best start point of fractal dimension for increasing values of the parameter *A*.

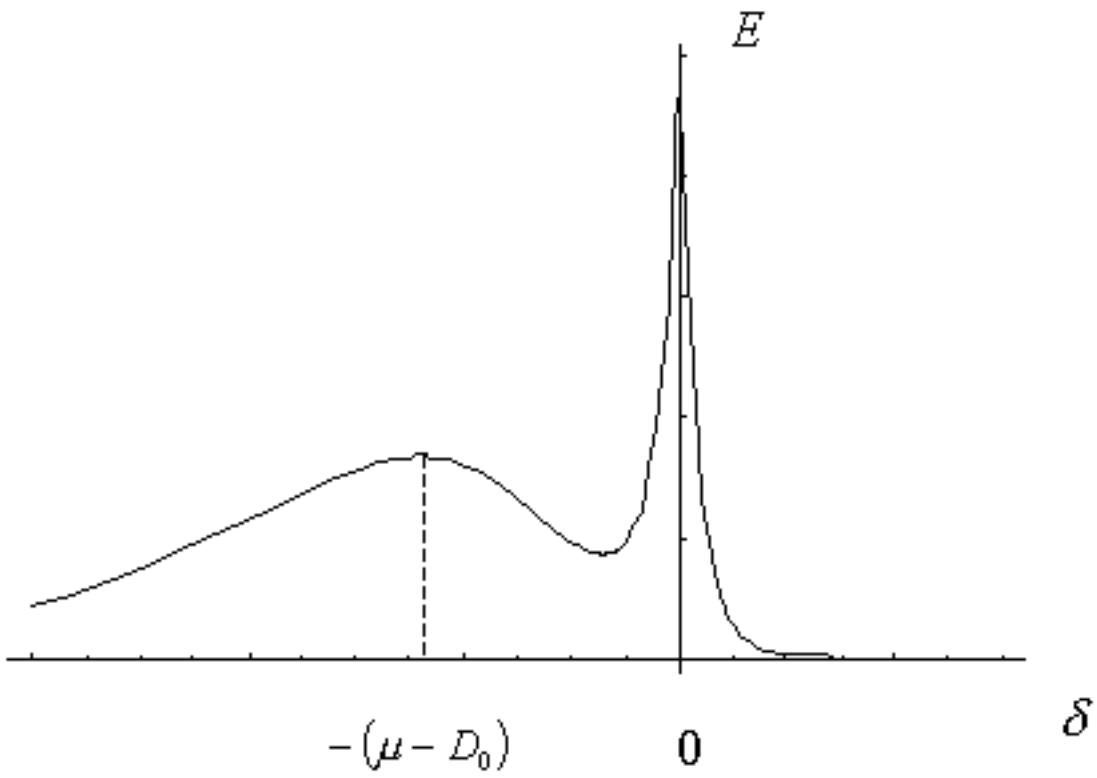


Figure 1: Behaviour of the expected utility for increasing values of A.

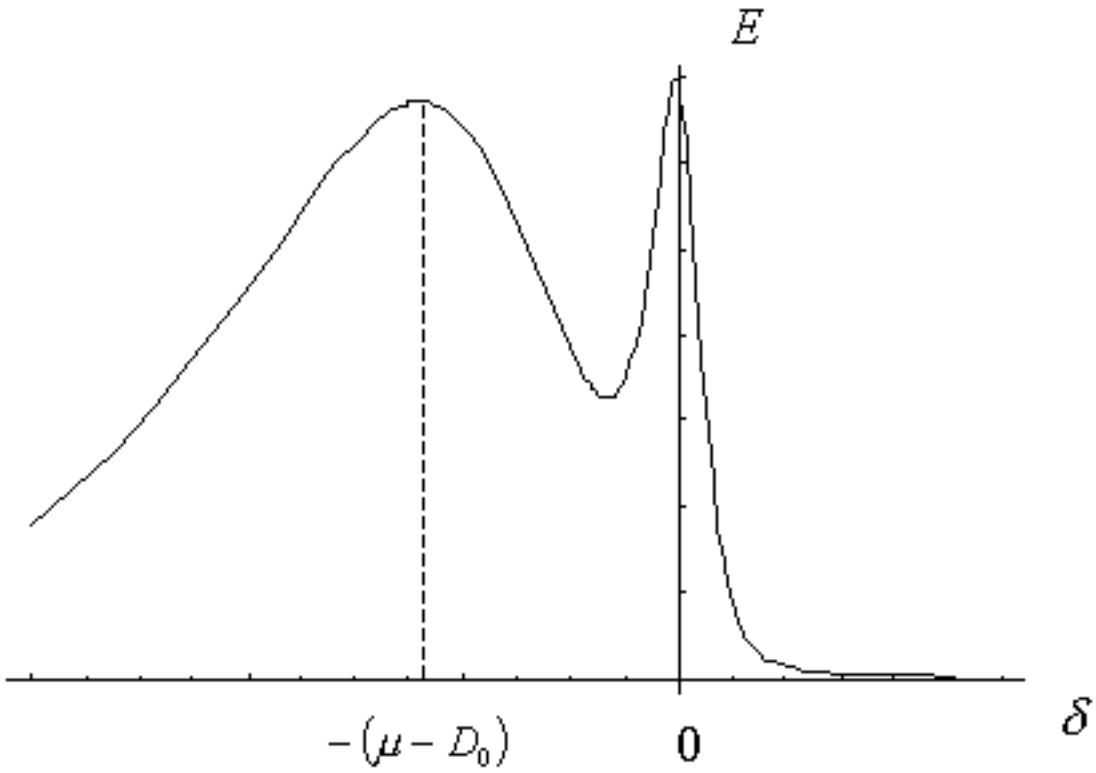


Figure 2: Behaviour of the expected utility for increasing values of A.

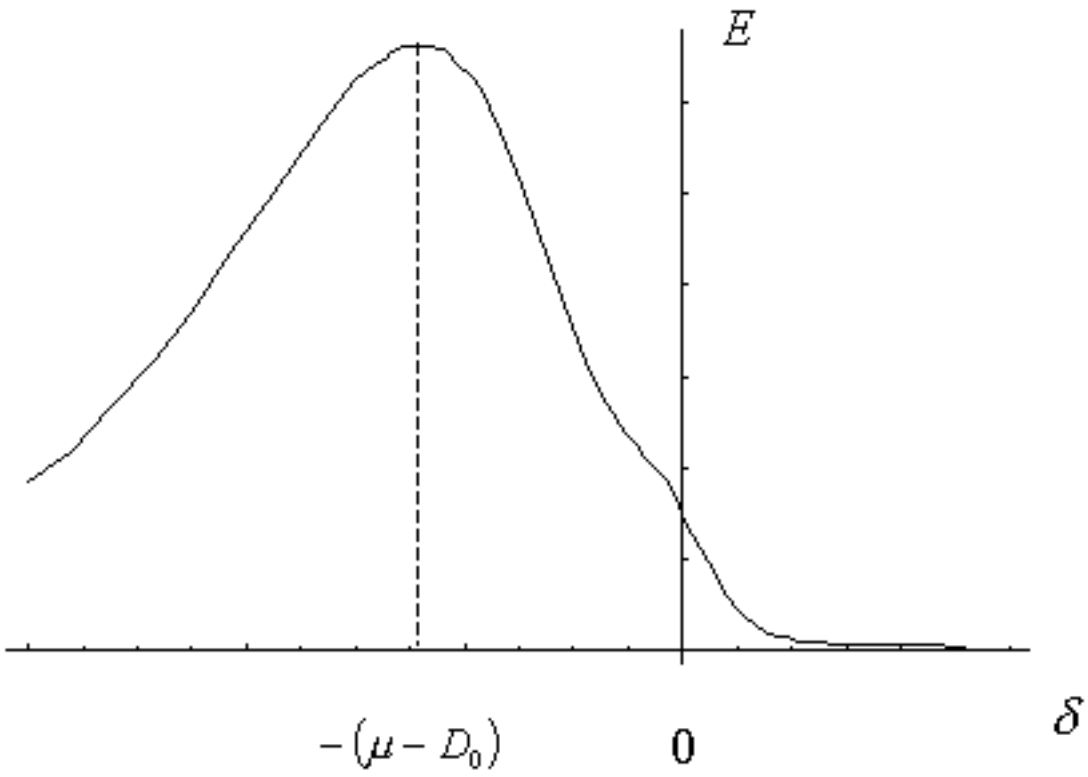


Figure 3: Behaviour of the expected utility for increasing values of A.

The above three figures show that the change d with the highest utility switches suddenly from 0 to approximately $-(\mu - D_0)$ as the *A*, the dependence of the variance of the prior belief on the decision change, increases. A value of d = 0 means the expected starting value of fractal dimension should be μ_i. If d = $-(\mu_i - D_0)$, this means that the most appropriate expected initial fractal dimension value is that of D_0. Similar behaviour can be seen when the value of the parameter μ_i is increased.

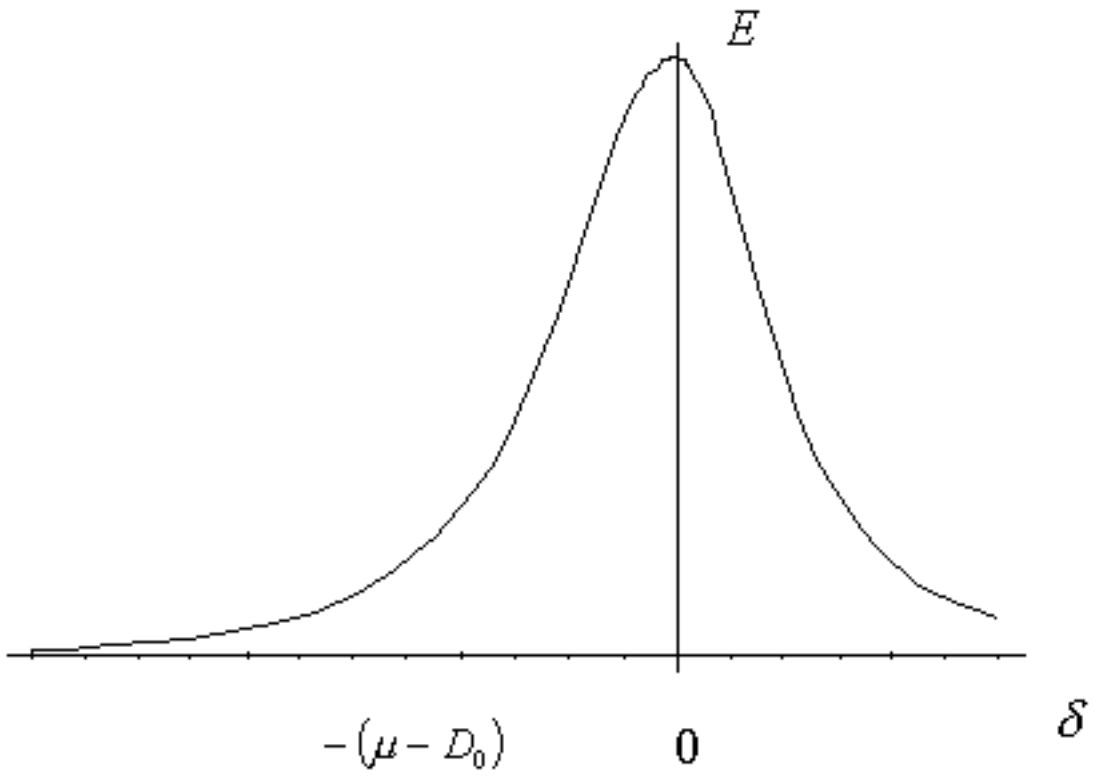


Figure 4: Behaviour of the expected utility for increasing values of μ.

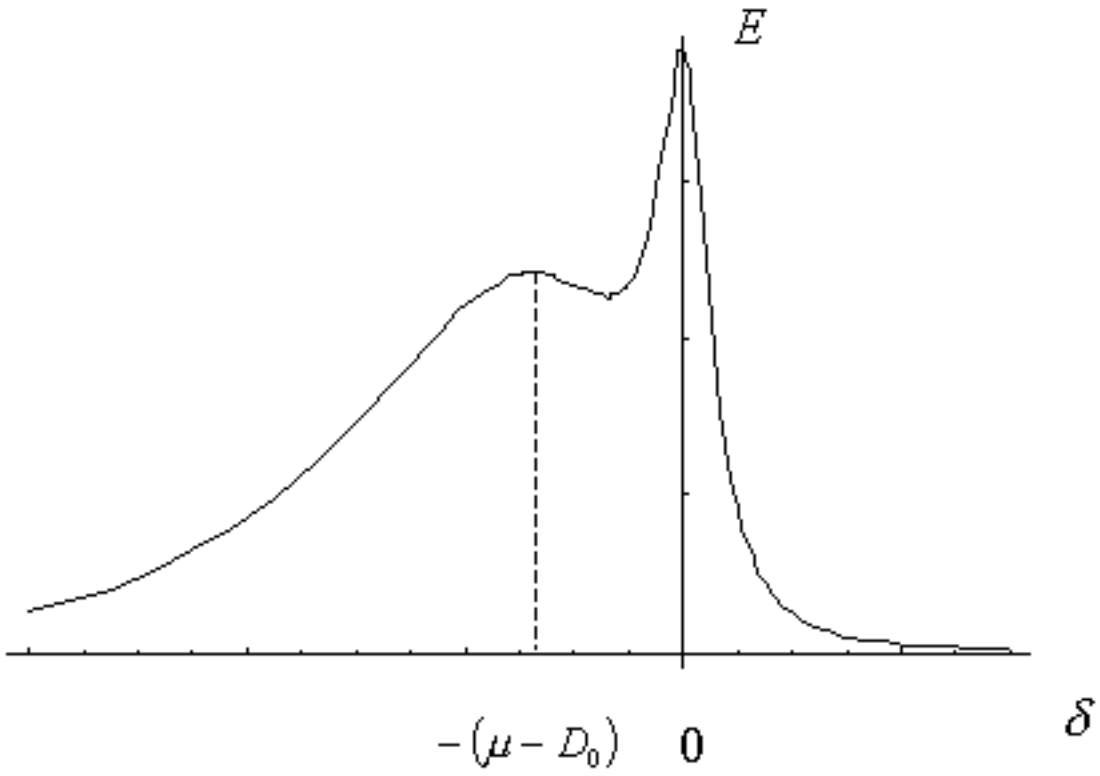


Figure 5: Behaviour of the expected utility for increasing values of μ.

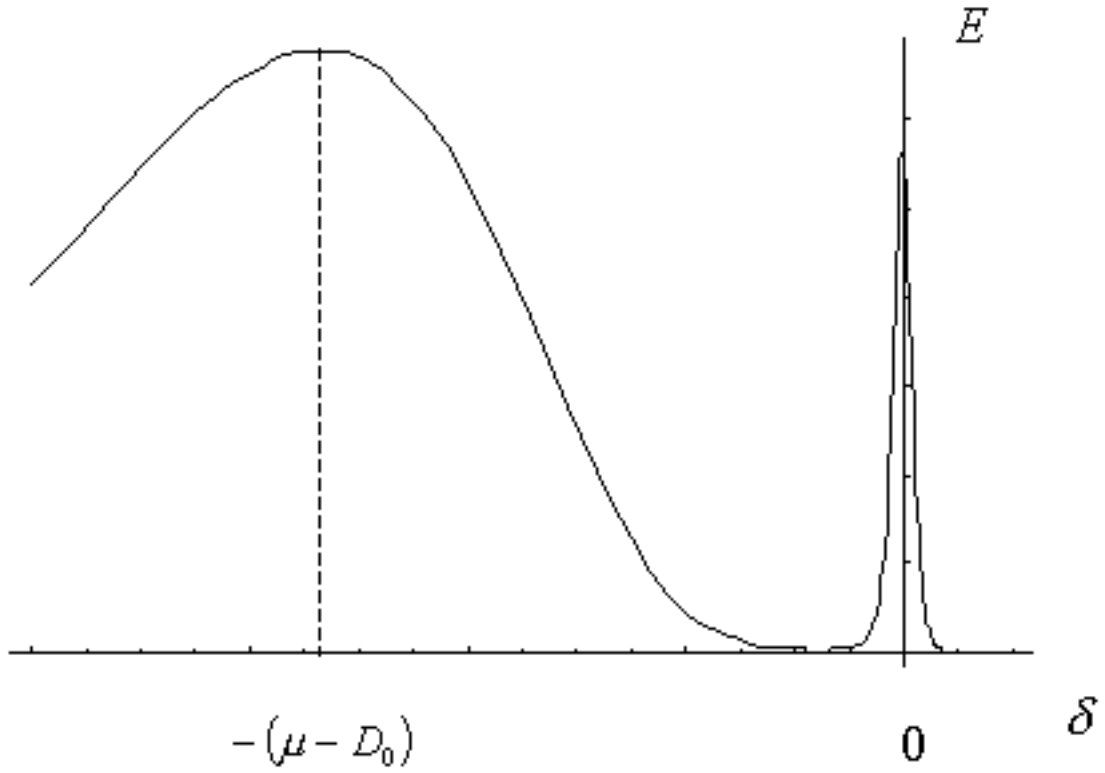


Figure 6: Behaviour of the expected utility for increasing values of μ.

These plots thus show a change of phase in expected starting fractal dimension based on small changes to the model parameters. The solution set is restricted to either “no change” (d = *0*) or a significant move to an expected value of D_0. If we plot the maxima of the expected utility function using just the mean μ and *A* as variables and keeping all other parameters constant, it is possible to build a cusp catastrophe surface of the maxima of the expected utility function as in Figure 7.

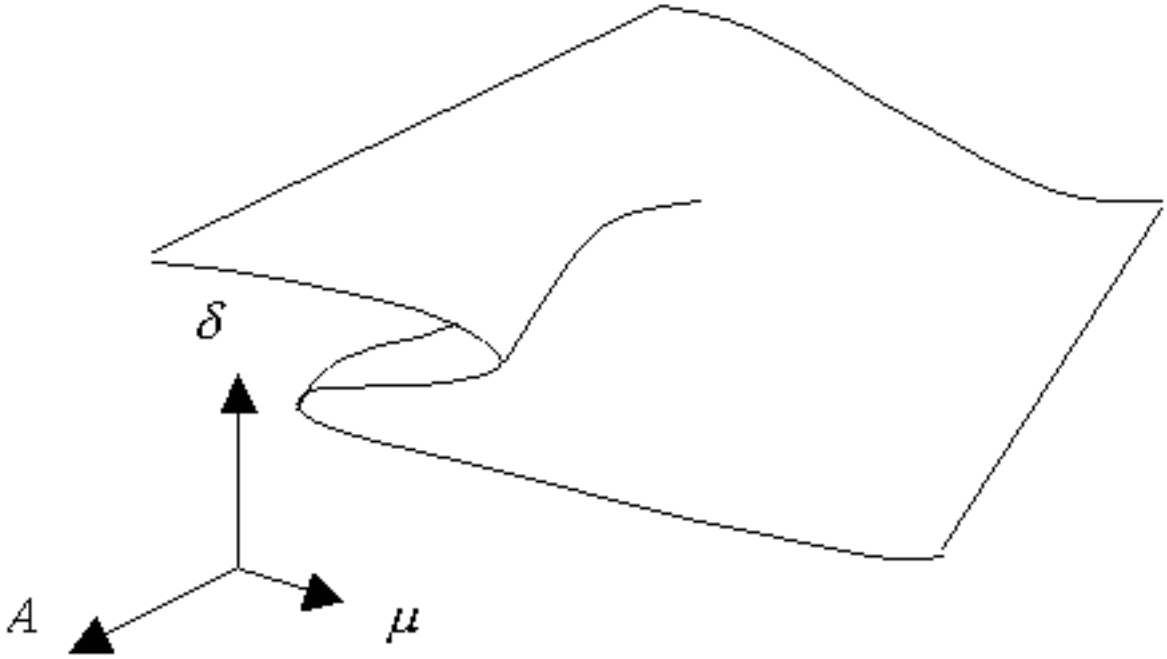


Figure 7: A cusp catastrophe surface

The different “sheets” of the surface correspond to different “best” starting points for the force in terms of the fractal dimension. In the region of the fold, there is more than one maximum for the expected utility function and therefore, at these values of *A* and m the global maximum of the expected utility function must be taken. If the other parameters h , *V* and *B* are varied, the cusp catastrophe becomes a higher order catastrophe surface in five dimensions.

Small Number of End States

During a single simulation combat model run, the value the fractal dimension takes varies slightly and throughout the run, the fractal dimension takes a range of values. At any point in time in the model run, the probability of the fractal dimension taking a particular value can be approximated by a Normal distribution centred on a mean value of m with a variance of *V* as indicated by the equation

$$f(D) = \frac{1}{\sqrt{2\pi V}} \exp\left[\frac{-(D-\mu)}{2V}\right] \qquad (17)$$

Changing the starting value of the fractal dimension by an amount d means that the probability

distribution for the fractal dimension throughout the model run can also be approximated by a Normal distribution as in Equation 18. However, in this analysis, the variance of the belief of the fractal dimensions the force takes during the model run will not increase with a change in start point. This is because it is assumed that the small deviations to the initial fractal dimension value are always of the same magnitude no matter what the starting value is. Therefore, the new probability of each fractal dimension occurring during a model run when the start point is changed is written as:

$$f(D|\bar{s}) = \frac{1}{\sqrt{2\pi V}} \exp\left[\frac{-(D-(\mu+\delta))^2}{2V}\right] \qquad (18)$$

In the previous discussion, we assumed that the number of end states or attractors in a system was relatively large. If the set of attractors in the system is small, it is possible to state at each value of the fractal dimension, what the probability of achieving each end state is and that end state's utility. Each end state has a fixed distribution of utility over the fractal dimension and we assume this utility can be approximated as a mixture of Normal distributions. Assuming that there are only two possible end states, the utility function can be written as:

$$U(D) = X \exp\left[\frac{-(D-\mu_1)^2}{2\sigma_1^2}\right] + (1-X)\exp\left[\frac{-(D-\mu_2)^2}{2\sigma_2^2}\right], \qquad (19)$$

where μ_1, μ_2 are the means and σ_1^2, σ_2^2 the variances of each Normal distribution making up the mixture distribution of utilities relating to each of the end states.

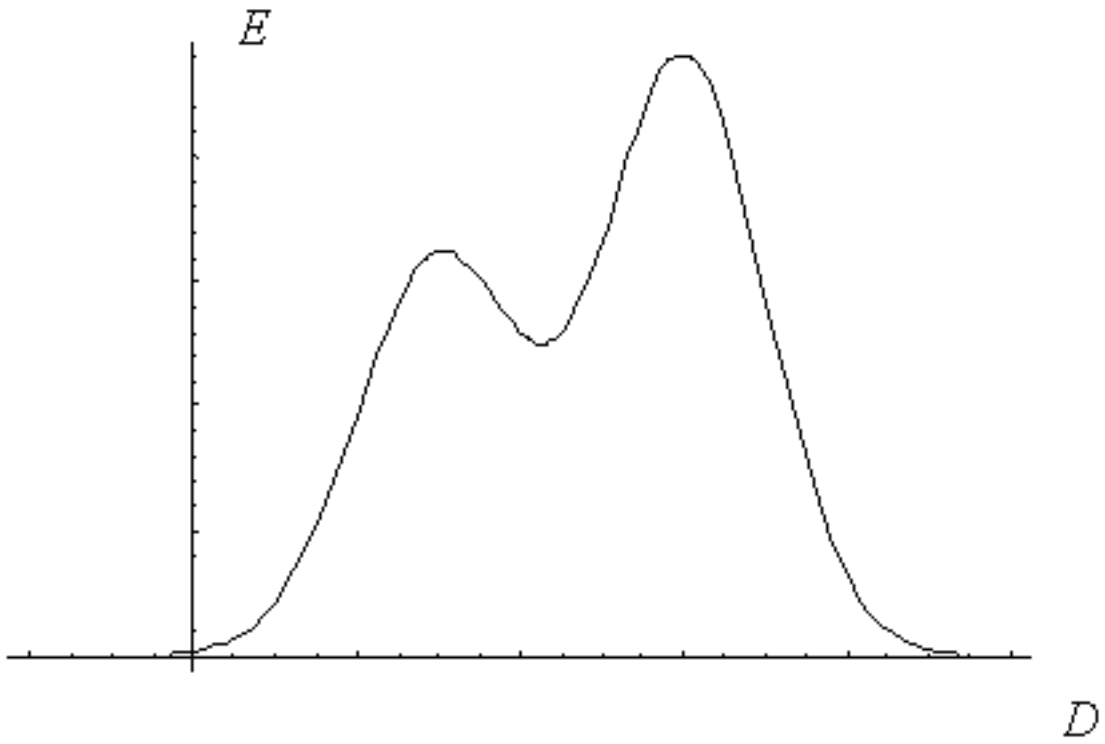


Figure 8: A mixture utility function

Figure 8 shows an example of a mixture utility function. The expected utility $E(\delta)$ from each decision and so starting fractal dimension can be calculated from, as before,

$$E(\delta) = \int_{\forall D} f(D|\delta)U(D)dD =$$

$$\int_{\forall D}\left(\frac{1}{\sqrt{2\pi V}}\exp\left[\frac{-(D-(\mu+\delta))^2}{2V}\right]\right)\left(X\exp\left[\frac{-(D-\mu_1)^2}{2\sigma_1^2}\right]+(1-X)\exp\left[\frac{-(D-\mu_2)^2}{2\sigma_2^2}\right]\right)dD \qquad (20)$$

$$= X\sqrt{\frac{\sigma_1^2}{\sigma_1^2+V}}\exp\left[\frac{-(\delta-(\mu_1-\mu))^2}{2(\sigma_1^2+V)}\right]+(1-X)\sqrt{\frac{\sigma_2^2}{\sigma_2^2+V}}\exp\left[\frac{-(\delta-(\mu_2-\mu))^2}{2(\sigma_2^2+V)}\right]$$

Maximising this function gives the "best" starting points of the fractal dimension relative to the prior knowledge of the model's behaviour. It can be shown that the function $E(\delta)$ exhibits a catastrophe with a cusp point which can be determined analytically.[10] The global maximum value of the expected utility function depends on the values of μ_1, μ_2, σ_1^2, σ_2^2 and the relative weight, *X*, of the utilities.

At certain points of these parameters, there will only be one local maximum of the expected utility function corresponding to one or other of the utility maxima. At others there will exist two local maxima, for which cases, the best starting value of the fractal dimension will correspond to the global maximum. The following figures show the effect of increasing the relative utilities of each end state.

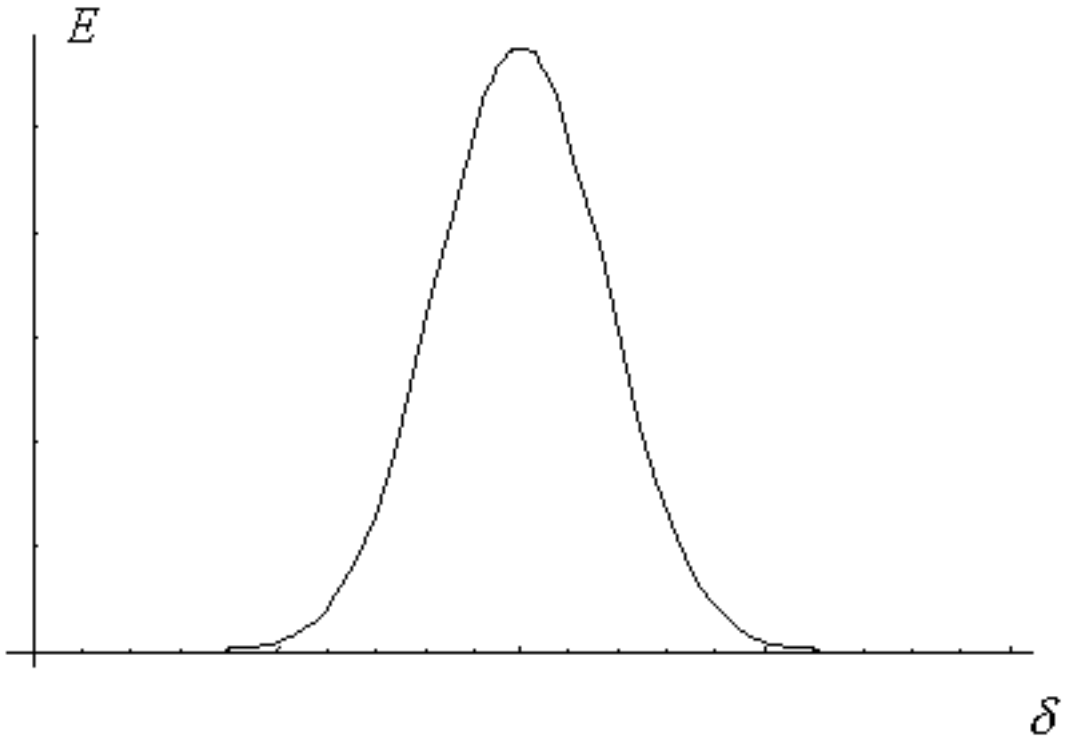


Figure 9: Goal utility – changing μ

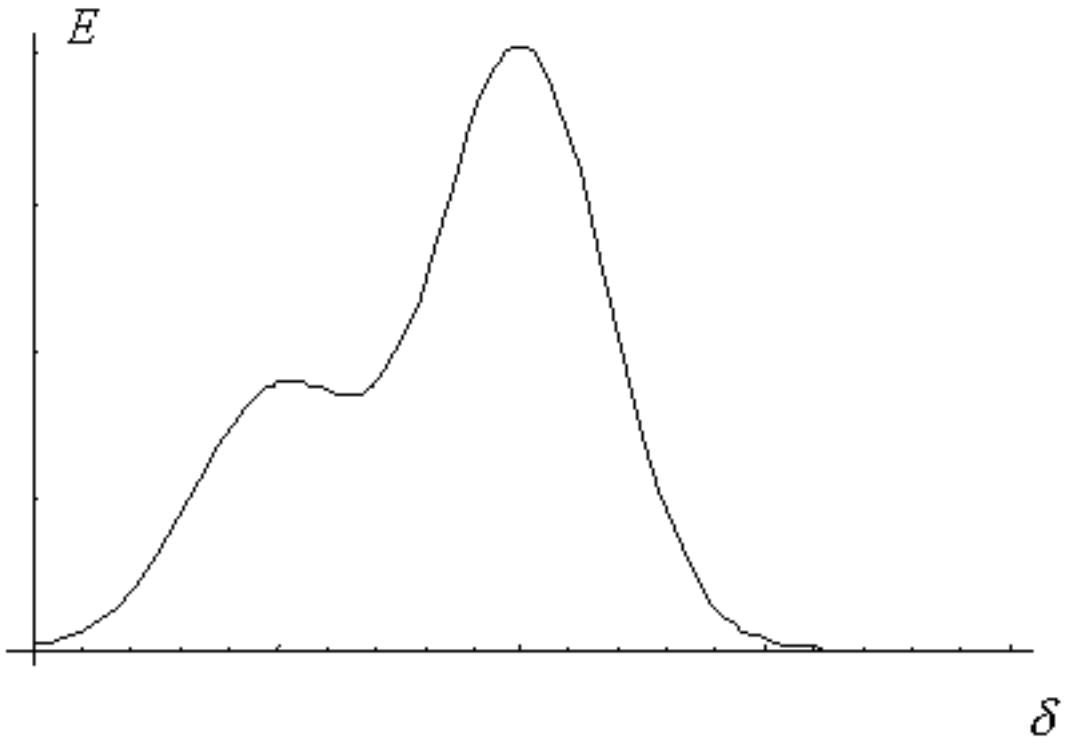


Figure 10: Goal utility – changing μ

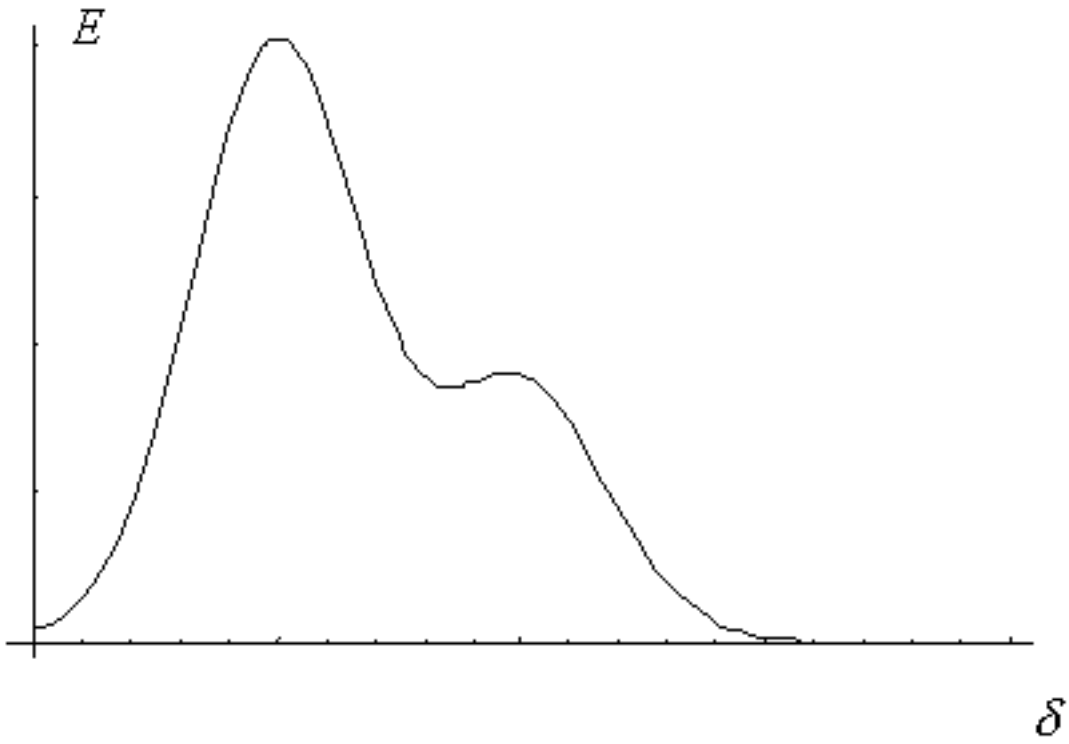


Figure 11: Goal utility – changing μ_i

The fractal dimensions with greatest utility are always either μ_1 or μ_2. Similar effects can be seen with changes to the values of the utility variance, σ_1^2 and σ_2^2. Keeping σ_2^2 fixed and changing σ_1^2 gives the following plots.

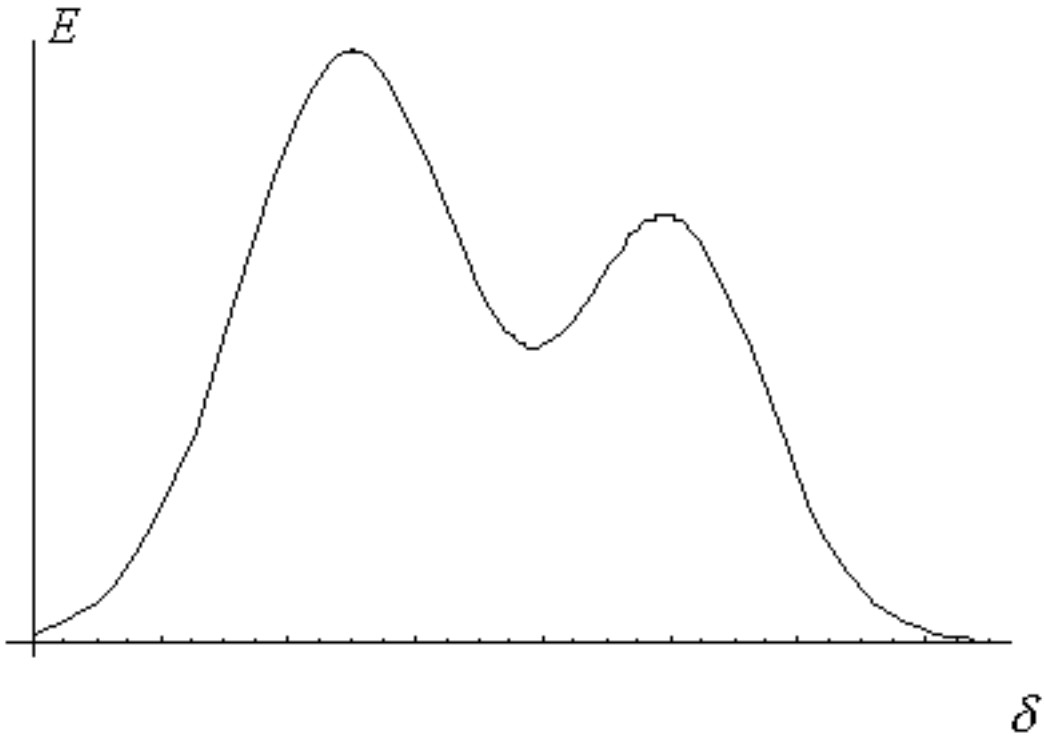


Figure 12: Goal utility – changing utility variance

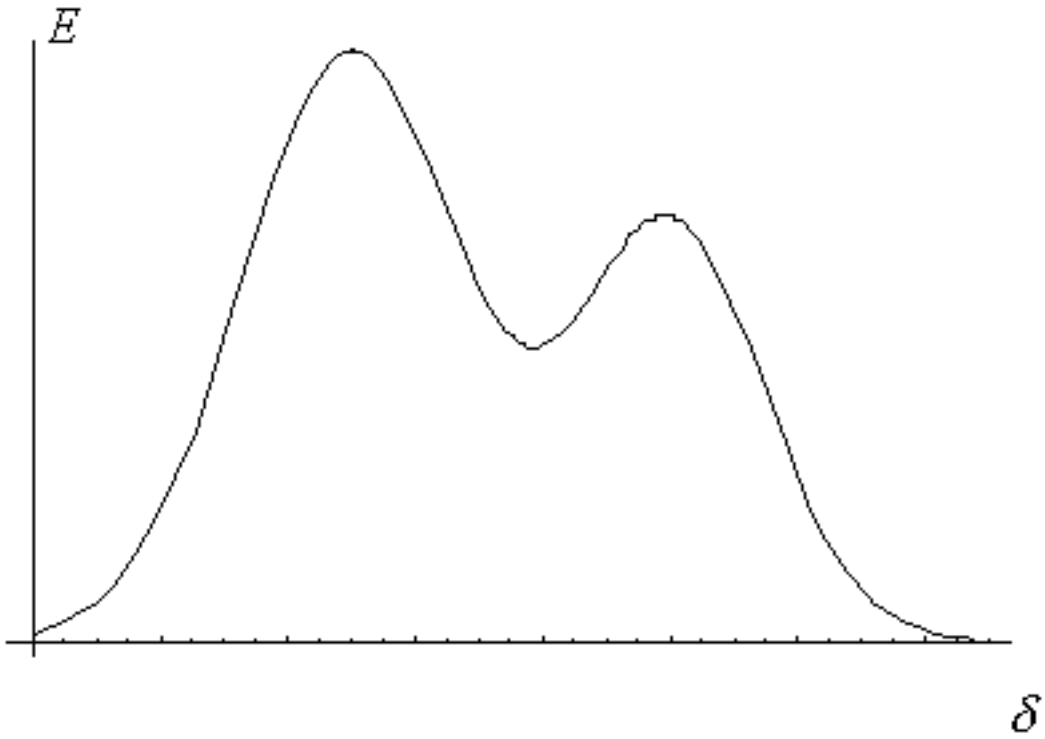


Figure 13: Goal utility – changing utility variance

Again, the only two points of maximum utility (either local or global) are the means μ_1 or μ_2 in the mixture of Normal distributions making up the utility function. The regions of the parameter space ($\mu_1, \mu_2, \sigma_1^2, \sigma_2^2$, *X, V)* can then be classified according to the starting value of the fractal dimension of the model run with the highest expected utility. This will produce a higher order catastrophe surface.

By including more than two Normal distributions in the mixture making up the utility function, it is possible to examine the effects of more than two end states, or end states which have a more complicated relationship to the starting fractal dimension of the force.

Notes:

1. Andy Illachinski, "Irreducible Semi-Autonomous Adaptive Combat (ISAAC): An Artificial Life Approach to Land Warfare," *Research Memorandum CRM 97-61* (Center for Naval Analyses, June 1997).
2. <www.cna.org/isaac> (June 2002)
3. G.I. Barenblatt, *Scaling, Self Similarity and Intermediate Asymptotics*, Cambridge Texts in Applied Mathematics, (Cambridge University Press, 1996).
4. Barenblatt, *Scaling, Self Similarity and Intermediate Asymptotics.*

5. Jim Moffat, M. Passman, “Metamodels and Emergent Behaviour in Models of Conflict,” in *OR Society Simulation Study Group Workshop Proceedings*, (The Operational Research Society, UK, March 2002).
6. Jim Moffat, “Command and Control in the Information Age – Representing its Impact,” in press, (The Stationery Office, UK, 2002).
7. M. Lauren, “Firepower Concentration in Cellular Automata Models – An Alternative to the Lanchester Approach”, *DOTSE New Zealand Report 172 NR 1350 ISSN 1174-3387,* (2000).
8. D.L. Turcotte, *Fractals and Chaos in Geology and Geophysics* (Cambridge, UK: Cambridge University Press, 2nd edition, 1997).
9. J.Q. Smith, P.J. Harrison, E.C. Zeeman, “The Analysis of Some Discontinuous Decision Processes,” *European Journal of Operational Research*, 7 (1981): 30-43.
10. J.Q. Smith, “Mixture Catastrophes and Bayes’ Decision Theory,” *Mathematical Proceedings of the Cambridge Philosophical Society*, 86 (1979): pp.91-101.

Professor **JIM MOFFAT** is a Fellow at the Defence Science and Technology Laboratory, UK, a Fellow of Operational Research and a visiting Professor at Cranfield University, UK. He was awarded the President’s medal of the Operational Research Society for the year 2000. He holds a first class honours degree in Mathematics and a PhD in Mathematics, and was awarded the Napier medal in Mathematics by the University of Edinburgh. He has worked for the past 20 years on defence related operational analysis problems and aerospace technology research. His current research interest is in building analysis tools and models which capture the key effects of human decision making and the other aspects of C4ISR.

SUSAN WITTY has an honours degree in Mathematics and a PhD in aero-acoustics research. She has been an analyst in the Defence Science and Technology Laboratory for about three years. Her current research interests are complexity science and Bayesian networks applied to high level data fusion.

BACK TO TOP

Phase changes in Meta-modelling using the Fractal Dimension

James Moffat and Susan Witty

Keywords: meta-model, intelligent agent simulation model, Fractal Dimension, decision-making, Bayesian Decision-Making.

Abstract: We discuss in this paper the development of a meta-model of an intelligent agent simulation model. Such intelligent agent models consist of a number of entities called agents, which interact with each other. The nature of such interactions creates emergent behaviour. In conflict or peacekeeping situations, these agents correspond to the actors in the situation (the different force elements, for example). A meta-model is thus a mathematical abstraction of such a simulation, composed of two parts. For the first part, the fractal dimension of a force is introduced as a parameter measuring the emergent ability of such forces to cluster locally, corresponding to local decision-making by individual agents. For the second part we consider the mathematics of Bayesian Decision-Making as a meta-model for top down decision processes in such simulation models.

full text

Author: **Raj Gururajan**
Title: **New Financial Transaction Security Concerns in Mobile Commerce**
Year of issuance: **2002**
Issue: **Information & Security. Volume 8, Number 1, 2002, pages 71-86**
Hard copy: **ISSN 1311-1493**

NEW FINANCIAL TRANSACTION SECURITY CONCERNS IN MOBILE COMMERCE

Raj GURURAJAN

Table Of Contents:

Introduction

In the past, the majority of the computer security officers had difficulty in convincing management to allocate financial resources for IT security. However, with the emergence of electronic commerce and varied legislation, organisations appear to have understood the necessity for computer security, especially data security.[1] Currently, in most organisations, security officers focus on IT security – namely – hardware security, software security and access security.[2] The access security involves both physical access and logical access. What appears to be missing from these security procedures is proper integration of business transactions. Ghosh states that while various security measures have been taken independently from business transaction, electronic commerce and the emerging mobile commerce have changed the perception that independent IT infrastructure security alone can protect an organisation in terms of its business needs.[3] To support Ghosh's statement, Deise [4] has identified a shift in the focus of IT security in organisations, resulting in new security policies to focus on reliable, available and trusted business transactions of organisations.

In this paper, new security threats arising from mobile commerce are initially highlighted. These threats are then linked to financial transactions in order to highlight the potential loss or damage to organisations' revenue. Then the organisations' IT requirements are assessed with a view to provide support to financial transactions in a mobile commerce environment. Organisational support is then formed into "architecture" and the architecture is discussed in terms of IT in an organisation, how IT supports an organisation and what does IT do to support the business processes of financial transactions. This architecture is then elaborated in terms of action items so that transaction security in an organisation can be guaranteed. It is believed that these action items would then enable organisations to tighten their security measures.

Security Threats Arising from Mobile Commerce

Security threats in mobile commerce can range from passively eavesdropping into others' message to actively stealing user's data.[5] In a radio frequency operated mobile commerce, with minimum difficulty it is possible to listen to one's conversation. This has an impact for consumers because they are concerned about their data and voice messages from unauthorised access. On the other end of the problem is the inherent security risk involved in transferring information over the networks. This

problem consists of two components: *identification integrity* and *message integrity*. The identification integrity refers to the signature elements found in the messages in order to establish where the message is originating. The message integrity refers to details to establish that the message is received as sent and no third party has attempted to open, modify or alter the contents. According to Zhang and Lee, these two items appear to cause a lot of concern to both sender and receiver.[6] While the sender risks theft or misuse of their personnel information such as account and bank details, the receiver (usually a merchant) risks repudiation of the transaction and resultant non-payment.

In addition to the above two, other security concerns in mobile commerce arise due to the new development in technology itself. [7] The mobile technology is envisaged in such a way that the services offered will eventually warrant payment for the type of services offered. This is already emerging in the domain of mobile telephones. For instance, when mobile telephone users access other network carriers, a special charge is levied on the users. Therefore, it is safe to assume that there will not be any “free services” in the future. The technology is developing in such a way that the payment for such services will be through some form of “smart cards.” The details stored in the smart cards need to be transmitted via the networks for validation and verification in order to determine service levels. If these networks are not fully secure, security breaches may occur.

One major security breach that can happen in mobile commerce is when the user details are transferred from one mobile network to another.[8] When this transformation occurs, any encrypted data needs to be decrypted for transparency. In mobile commerce, when mobile devices make requests to web pages of a network server, a four-stage process is followed. First, the requests arise from the originating Wireless Transport Security Layer (WTSL) protocol. Second, the requests are translated at the originating Wireless Application Protocol (WAP) gateway. Third, they are sent to the standard Session Security Layer (SSL) protocol of the destination network. Fourth, the translated information reaches the Hyper Text Transfer Protocol (HTTP) modules in the new network in order for the requests to be processed. In the process of translating one protocol to another, the data is decrypted and then re-encrypted. This process is commonly known as the “WAP Gap.” If an attacker can gain access to the mobile network at this point, then simply capturing the data when it is decrypted can compromise the security of the session.

Data in the Mobile Commerce environment is secured using encryption technology. According to Ghosh, it has already been proven that the technology is vulnerable to attacks.[9] Hackers have broken some of the existing algorithms for encryption. So, there is nothing like a complete security. Further, there is no international regulatory framework available to enforce certain security related problems. For example, in the current climate, no individual organisation or government can guarantee security to consumers. When the security breach appears in an international transaction, no one country will be able to assume responsibility to prosecute the vandals. While these problems have been recognised and solutions are being proposed, organisations tend to loose consumer confidence. This will potentially impact organisation’s revenue.

Trust is central to any commercial transaction and more so in the case of mobile commerce.[10] Trust is normally generated through relationships between transacting parties, familiarity with procedures, or redress mechanisms. In the case of mobile commerce, the need for creating the trust in the consumer assumes extreme importance because of its virtual nature. It hinges on assuring consumers and businesses that their use of network services is secure and reliable, that their transactions are safe, that they will be able to verify important information about transactions and transacting parties such as origin, receipt and integrity of information, and identification of parties dealt with. Therefore the challenge is not to make mobile Commerce fool proof but to make the system reliable enough so that the value greatly exceeds the risk.

Any new development in technology in today’s consumer minds creates both curiosity as well as reluctance. The informality and lack of overall control creates the perception that the Internet is inherently insecure.[11] This inherent perception can trigger business risks and technological risks.[12] Business risks involve products and services, inadequate legal provisions, reliability of trading partners, behaviour of staff and demise of Internet service provider. Technological risks involve hacker attacks, computer viruses, data interception and misrepresentation. To achieve satisfactory levels of trust, organisations have to think about managing both business and technological risks. Currently Mobile Commerce relies mostly on knowledge-based trust that is useful for Business-to-Business commerce.[13] However, there is a big surge in the identification-based trust to satisfy consumer concerns about their transaction details. In addition, current architectures for mobile communications do not provide full security measures in terms of transaction integrity. Some of the models envisaged for mobile commerce are based on smart-cards oriented approach and hence the issue of financial transaction security needs greater examination in mobile commerce.

Security Threats That Can Impact Financial Transactions

Security risks in a mobile commerce environment associated with financial transactions can be categorised into traditional risks

and non-traditional risks.[14] Traditional risks usually involve loss or damage to tangible physical assets and resulting economic loss. For example, loss of computer hardware may have an impact on incomplete transaction. Alternatively, a data disk, which is not fully protected from theft, can place an organisation into some form of risk. Treatment of traditional risks is usually addressed in risk management policies. Protecting tangible assets from traditional perils, even when those assets are devoted to mobile commerce, does not involve new and different techniques. These security treats are beyond the scope of this paper.

Non-traditional risks involve sustaining damage to organisations' computer systems and electronic data. [15] These risks can fall under the category of stolen information, damages to web sites by hackers, hijack of web sites and viruses. An attack may be perpetrated for any of a number of reasons including financial gain involving credit card fraud, curiosity with no specific intent of harm, espionage by domestic or foreign competitors, or by foreign governments, revenge by a terminated employee with the intent to wipe out files, disclosure of personal data to unauthorised institutions as in health related cases, thrill seeking, disruption to stop critical activities, and extortion for financial or political reasons. Any attack, internal or external, on a computer system is at minimum disruptive and forces the administrator to shut down the system resulting in revenue loss.

Non-traditional security breaches also include any unauthorised access or use of a company's computer system and data by an outsider or insider.[16] For example, a hacker could break into a company's computer system and steal or destroy data. Widespread use of mobile commerce enhances the possibility of an outsider invading an organisation's computer system. Due to businesses reliance on computers for their daily operations, breaches of a company's computer or information security system are a risk to almost all functional components of businesses. Use of software to encrypt and, thus, safeguard communications provides some protection, but also adds a risk that a virus or other bug could damage equipment or data. Further, according to Dang,[17] theft of information such as critical electronic files that include financial data, customer information, marketing and new product data, trade secrets, and personnel data may provide competitors with a strategic advantage, criminals with the means to commit fraud, and others the opportunity to disparage the company. Dornan states that the use of misappropriated information may harm third parties such as customers, employees, and business partners.[18] The theft of information may undermine an acquisition or cause a public relations problem and hence potential loss of revenue.

Security breaches may be very costly to an organisation.[19] When unauthorised access to the computer is gained for the purposes of committing a crime or fraud, reputation is also at stake. Other security issues include the prohibition against the use of high-level encryption technology by domestic or foreign governments so that agencies can break the codes if necessary for defence or law enforcement, changes in international standards, and loss of recovery of encryption key.

A Closer Look at Fraud and Crime Risks in Mobile Commerce

The scope of computer fraud and crime is immense in mobile commerce. Among the most common crimes are malicious mischief, such as the insertion of viruses or Trojan horses into one or more computer systems; the fraudulent transfer of money to personal accounts; the use of forged electronic signatures; the theft of credit card information and credit card fraud; Medicare and Medicaid fraud; the theft of intellectual property; illegal use of software; stock and commodity market manipulations; and similar illegal activities. Most losses are insurable, but premiums will be relatively exorbitant if security measures are not appropriately enacted.[20]

A hacker may use a number of methods such as insertion of viruses, spamming and web snatching to access computer systems and data and cause resulting damage. Damage may occur at data centres or to transmission networks, routers, and power sources. Virus attacks may also come from innocent parties who pass on an infection without knowing that the system is contaminated, usually by e-mail.

Using another technique called a *distributed denial of service* hackers attacked some of the most well-known and highly secured web sites in the world, including Yahoo.com, eBay.com, and amazon.com. This technique hijacks numerous computers on the Internet and instructs each one to flood a target site with phoney data. The target site trying to accommodate the phoney data becomes overworked and soon begins to lose memory. The result is effectively slowing or shutting down the entire site to real customers.

Web snatching is a practice in which one party plants a virus in another party's Web site that automatically moves the viewer from the selected site to a site run by the web snatcher. This is done without the permission of the selected Web site owner or the site visitor. In many instances, the viewer is unable to get out of the unwanted site, short of turning off the computer, and is held hostage to the new site. The diverted-from and diverted-to sites usually have nothing in common with each other.

Financial institutions and companies that have inadequate electronic security protection are likely to suffer losses of money, information, or other corporate assets. Surveys have shown that most companies and institutions have incurred losses, and a substantial number have no idea whether they have come under electronic attack or not. Insiders or former insiders have committed most of the electronic crime and fraud, but there are also many examples of third-party fraud and theft.

Mobile commerce can only be conducted if all parties believe there is adequate security. The majority of those who use the Internet, on which current mobile commerce technologies are built, are very concerned about security.[21] Some forty percent of Internet consumers give false information when they use the Web because they do not trust the Internet's security.[22] Other users refuse to register at sites that require what the consumer believes to be personal information.[23] Many persons want the government to legislate security on the Internet, as they are not confident businesses will do the job on their own.[24] Therefore, it is critical that businesses enhance both their security and their security image to combat fraud and crime on the Internet as well as to increase customer confidence and participation to realise secured transactions.

Security Risks in Mobile Commerce Emerging from Reliance on Third Parties

Today, most organisations rely on computers for their daily operations. Traditional risks and non-traditional security risks can interrupt a business or literally shut it down. For example, a security breach by a hacker can severely disrupt a business and those that depend on it. Most businesses in mobile commerce are dependent in several ways on the continued reliability and operation of computer controlled systems not within their control such as the telephone network managed and controlled by computers. Businesses are dependent on their financial institutions that are also managed and controlled by computers. In mobile commerce, to accommodate home users, organisations are dependent on their Internet service providers. Suppliers and customers depend on each other's electronic data systems and on mutual systems, such as a third-party commodity exchange. When one system fails, it may cause the other systems to fail as well. Failure may be a slowdown in the dependent system, also called the "brownout," or a total denial of service, also called the "blackout." [25]

The risks described above can result in many different types of losses.[26] The losses that arise from reliance on a third party can generally be grouped into: (1) loss or damage to property, both tangible and intangible, (2) business interruption, and (3) extra expense. Property losses occur when loss or damage is suffered to a firm's own tangible property or to property for which the firm is responsible. Traditionally, this meant damage to a building or other business property, including computer equipment. In the mobile commerce world, the focus is on damage to computer networks and, more importantly, data. An important issue is whether data is considered tangible property under a typical property insurance policy. It appears that insurers will begin to address the issue of what is defined as covered property under these policies. More likely, courts will have to decide this issue.

Property losses can also occur when an organisation's intangible or intellectual property is infringed or violated. Copyrighted materials can be copied without permission, trademarks can be infringed upon or diluted, and patented property or ideas can be stolen. Today, a firm's intellectual property may be its most valuable asset.[27] Organisations need to protect their intellectual property from hackers, crackers, competitors, and others, as well as make sure they do not infringe on the intellectual property rights of third parties. This could potentially expose a firm to third-party liability.

Time element losses typically include business interruption (BI) losses and service interruption losses. BI loss is the economic loss resulting from the interruption of business activities. Business interruption losses may result from the inability to access data, the theft of data, or a threat to the integrity of the database. For example, a security breach of a credit card database may cause the database owner to curtail activity on the system until a damage assessment is completed and the system integrity is re-established. Not only is there a disruption of the database operations, there is also a consequential effect on all third-party users of the system.

Service interruption losses include economic losses associated with the interruption of utilities. A service interruption incident can occur from an "off-site" exposure or event. There have been many incidents of communication cables inadvertently being cut. Long-distance telecommunication companies have experienced software problems in data routing that effectively crippled their networks for several days.

In addition to the business losses and service losses, mobile commerce gives rise to new implications about doing business and being protected from interruptions in doing business.[28] Businesses suffering losses related to server outages face the risk of losing customers for extended periods of time. In mobile commerce, the increased reliance on suppliers is also exposing businesses to new risks for financial losses. These range from suppliers of goods (such as raw materials) to suppliers of services (such as server usage, delivery services, electricity, and telephones).

Business interruption may have several consequences, e.g., loss of income; extra expenses to recover; loss of customer, partner, and shareholder confidence; and, ultimately, reduced market capitalisation. Third parties harmed by the denial of service may sue, adding liability losses to first-party damages. In some cases, business interruption may constitute a breach of contract.

According to Lee, service denial may cause a customer business interruption, network suspension, or a disruption in or delay of services.[29] Service denials may result in damage claims or lawsuits for breach of contract.

Expense Incurred by Organisations Due to Business Interruptions

In the event of an interruption, a business may incur extraordinary expenses to resume operations as quickly as possible. Extra expense coverage is for those costs incurred by the policyholder in excess of the normal costs that would have been incurred to conduct business during the same period had no loss or damage occurred. An example of extra expense might be increased freight charges incurred to meet a customer's demand for an order due to delays in the production process associated with a loss event.

In the mobile commerce area, there are new types of costs that may need to be considered in the context of risk and insurance, including additional costs of operating Web sites from alternative servers, costs of operating Web sites through alternative providers, costs to repair Web sites damaged by hackers or equipment failures, and costs of rebuilding other lost information.[30] Thus, various security risks arising from a combination of issues warrants a closer scrutiny for assessment of an organisation's IT requirements in order to facilitate a secured financial transaction.

Assessment of Organisation's IT Requirements

In order to guarantee security of transactions in mobile commerce, initial assessment of an organisation's IT requirement is essential for a number of reasons.[31] These include the ever-changing customer requirements, changing hardware and software platforms, dynamically changing user needs and user experiences gained from the innovative IT products. Therefore, such an assessment involves four key components of mobile commerce. These are:

(1) Embedded computers in many everyday objects;[32]

(2) Next generation wireless networks;[33]

(3) Interfacing technologies for bi-directional communications;[34] and

(4) Design of application that satisfy user needs.[35]

The first key component arises from the need that there are going to be more wireless devices by 2005 and the prediction is that by 2005, mobile devices will outnumber wired devices.[36] These mobile devices would consist of some form of embedded systems in them and hence the allocation of priority. The next component follows from the first one which highlights the need for networks to go wireless in order to support the concept of mobility and hence mobile devices. Users communicate via a number of different mobile devices and hence the bi-directional communication aspect is essential for an organisation to ensure that transactions are reliable and secure. Finally, to accommodate diversity of user needs, applications assume a key component role in mobile commerce.

With these four key components in mind, when organisations' IT requirements are assessed, importance should also be given to "user experience." In mobile commerce environment, these user experiences typically involve cameras, music and other emerging innovative technologies such as positioning systems and, hence, organisations should find a way to accommodate these ever changing user experiences. Organisations would then be tempted to add additional hardware and software resources to their existing infrastructure but this will increase the financial burden of an organisation. One emerging suggestion appears to be the consideration of "interface" facilities to enable sharing other third-party resources. This requires address and connectivity mechanisms that do not exist today. While recent newspaper articles forecast such capabilities are emerging, the bigger challenge for organisations is to create applications that truly have this multi-modal, multi-channel character because it is believed that the immediacy of wireless technology is great.

With this scope in mind, if we analyse an organisations' IT infrastructure, then we would be able to bundle business needs to

support secure transactions into four main groups. They are:

1. Technical infrastructure that can identify what is IT made up of in an organisation;

2. Physical components of IT that can identify how these components support various workflow requirements in an organisation;

3. Logical components that can identify how IT components support various business processes; and

4. Real time measurement and control of security and service levels in real time.

While the first three points provide essential components of an application architecture in an organisation, the fourth point provides the control and maintenance components of the application architecture. This real time control is essential in mobile commerce because of the difficulty in describing complete security architecture to ensure security of transactions.

The Architecture

Figure 1 represents the proposed architecture that attempts to address various new security concerns. The architecture consists of 10 levels, starting from level 0. Level 0 is where all security policies to ensure transaction security are dealt with. This is a management component and it is independent of organisation's IT infrastructure. This is because in the mobile commerce environment, due to changing user needs, it is difficult for the security officer alone to ensure reliability of transaction. Since business managers know the various processes involved in conducting financial transactions, it is essential that they assume the overall responsibility, while security officers provide the necessary infrastructure. This view is quite different from the current electronic commerce environment where security officers are responsible for data and information security. This may be possible in a wired environment; however, due to the importance given to the information and the origin of it in a mobile commerce environment, the view is totally different. This new view will also enable organisations to align their business processes with proper security policies as it will be difficult to track users in a mobile commerce environment due to the possibility of "roaming."

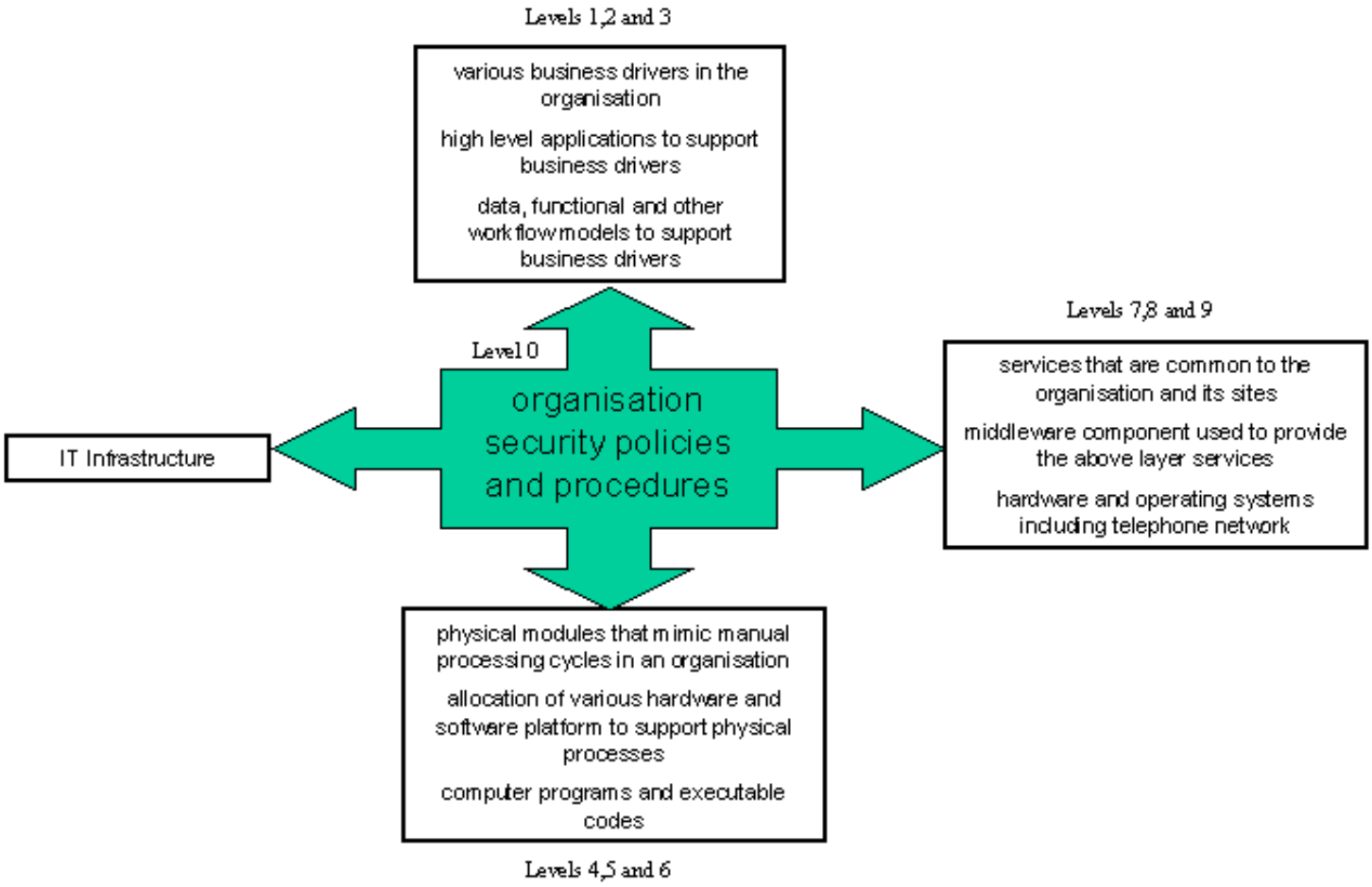


Figure 1: The Architecture

Further, in mobile commerce environment, users, systems and transactions change rapidly and unpredictably. This requires organisations to accommodate these needs and yet provide reliable and secured transactions. The current static authentication and authorisation is becoming out of use in mobile commerce while the new dynamic privilege management is becoming an essential component. Therefore, risk management associated with organisations' IT security also needs to be dynamic and in real time to react to incidents and also to address potential threats more pro-actively. In essence, level 0 of the architecture will ensure that customers, business partners, and other stakeholders of a transaction such as banks and governments interact directly with these business applications and their IT environments, especially mobile environments. This level 0 architecture will ensure that the transaction environment is up and running, reliable and secure.

Levels 1 to 3 put the customer first and they are specific to business needs. At this level, several independent business activities are integrated through IT applications in order to ensure that data, functions and workflow modules of various business needs in an organisation are synchronised. Due to increasing demands from customers, the visibility and interaction across the supply chain to the customer is essential in mobile commerce. Therefore, manual sub-transactions usually found in a traditional transaction (including weaker electronic commerce models) need to disappear and levels 1-3 will ensure that this happens in an organisation.

Levels 4-6 consist of the various physical modules to support the workflow. These levels also consist of "code" needed to support workflow and integration of workflow. These levels are of extreme importance to business because this is where the integration of multiple segments of a business, such as Customer Relationship Management (CRM) and Supply Chain Management (SCM), takes place. Further, due to the physical nature of IT components, this is where the existing resources are integrated with new resources. To establish financial security, levels 4-6 need to be maintained properly because the transaction is split into multiple components at these levels before the transaction is processed. Further, when the transaction is split into component sub-transactions, each of the sub-transactions may run on varied systems with different infrastructures. Organisations should focus their "security" at this level for successful mobile-commerce.

The last three levels comprise of IT components in order to realise various combinations of business needs. At this level, IT components such as a computer are added to the existing infrastructure. While the previous levels (4-6) facilitate business needs, levels 7-9 actually implement them. Issues such as network speed, transaction completion time are essential characteristics at these levels. While the business performance is measured at the previous levels, response time measurement is conducted at the last three levels (7-9). These three levels are vulnerable to attack and implementation of security procedures starts at these levels.

Discussion

When a financial transaction is facilitated in a mobile commerce environment, usually the consumer accesses the organisation's computer to search for appropriate details. Once the consumer is satisfied with his/her order, an order is placed. The consumer places an order using the infrastructure provided by the Internet storefront and using his or her payment method of choice. Once the order reaches the organisation, the transaction is processed. A number of security issues such as verifying the credentials of the consumer arise at this point. Provision for real-time security and connectivity to authorise payment via the Internet or wireless medium forms an integral component of the transaction. The organisation involved in the transaction channels the transaction through various financial networks such as banks, ensuring that customers are authorised to make their purchase.

While security issues are applied onto a transaction, usually client/server architecture is used to perform transaction processing. The client is installed on the organisation's merchant site by the third-party providing user authentication for financial details and this client is integrated with mobile commerce application. The client is usually pre-integrated with store management systems, such as those for management reporting purposes.

For the purposes of transaction authorisation, the client software establishes a secure link with the processing server over the Internet using an SSL connection, and transmits the encrypted transaction request. The server, which is a multi-threaded processing environment, receives the request and transmits it over a private network to the appropriate financial processing

network.

Depending upon the consumer's financial status, the transaction is approved or denied. When the authorisation response is received from the financial network, the response is returned via the same session to the client on your site. The client completes the transaction session by transparently sending a transaction receipt acknowledgement to the server before disconnecting the session.

The whole transaction is accomplished in few seconds, including confirmation back to the customer and the organisation. If the transaction is approved, funds will be transferred to the organisation's account. Once the transaction is confirmed, the transaction will be securely routed and processed. As proof of a securely processed transaction, both the customer and the organisation will receive a transaction confirmation number.

The transaction processing cycle is presented on Figure 2.

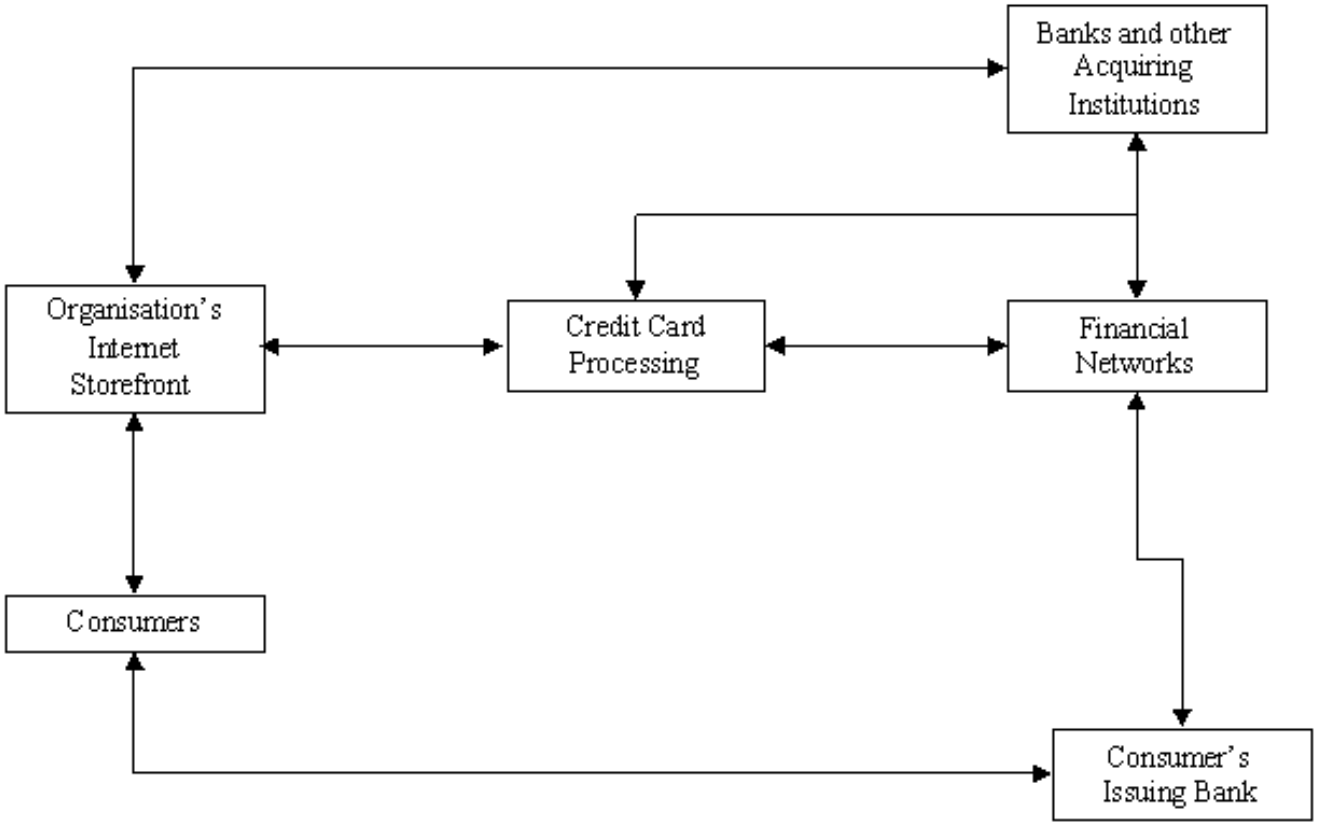


Figure 2: Transaction Processing Cycle

The architecture described in this paper supports almost all the elements of the transaction that can be conducted in the organisation. The security aspects not only involve the organisational IT infrastructure but also third-party security levels in order to approve a financial transaction. It should be remembered that consumers expect the organisation to facilitate a reliable and secure transaction and it is in the interest of the organisation that third parties involved in the transaction are reliable and capable of providing necessary security to consumer's transactional details.

While the above diagram portrays a complete financial transaction system, the following two diagrams portray the component that needs to be supported by an organisation. Components such as office systems form the levels 7-9 in the architecture outlined in this paper. Components such as databases would form the levels 4-6 in the architecture described above. Other components such as Business Logic Components form levels 1-3 of the architecture. The business processing for facilitation of

transaction is also highlighted in the diagram on Figure 3.

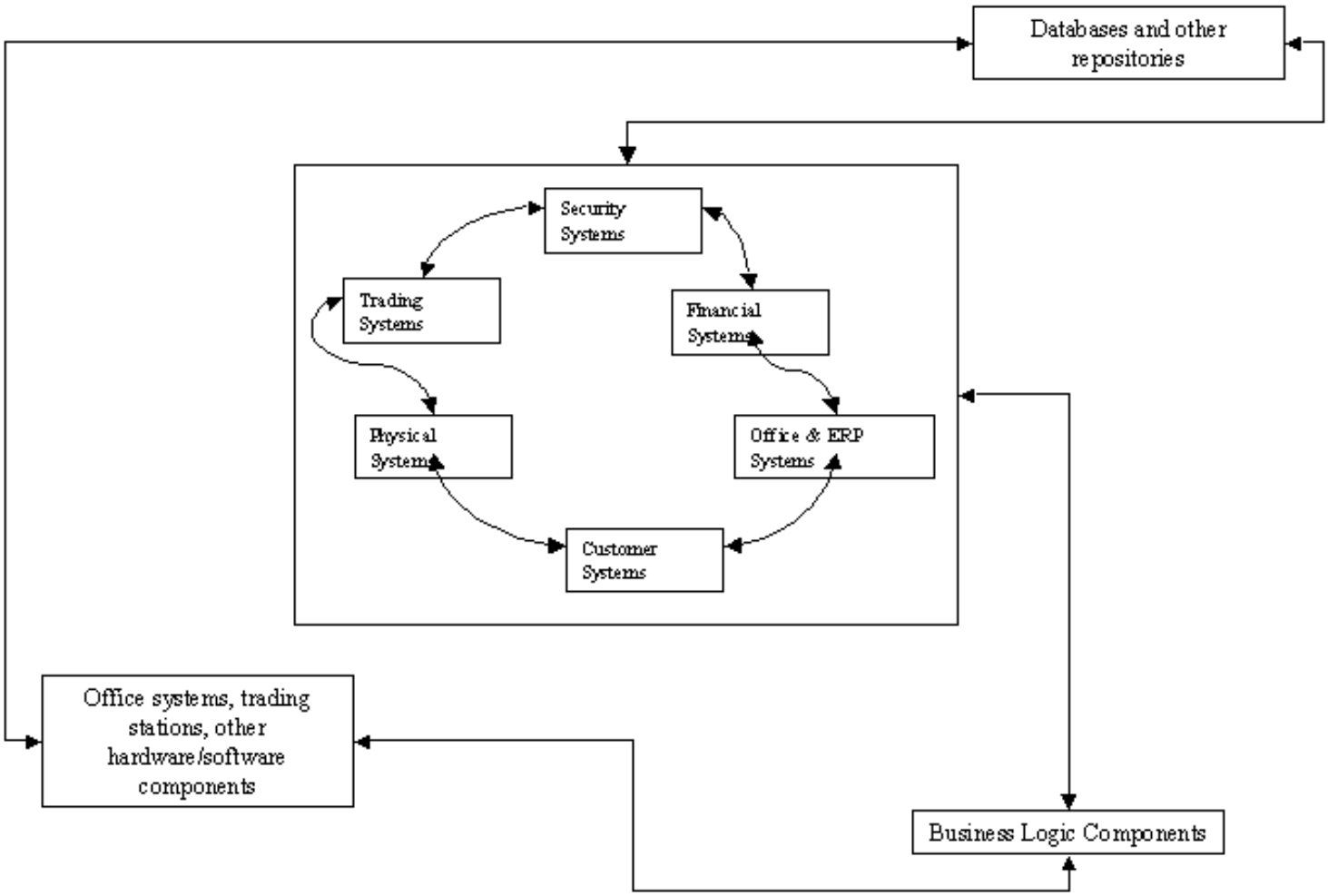


Figure 3: Business Processing Facilitating Mobile Commerce Transaction

Conclusion

The architecture presented in this paper addresses various new security concerns in the emerging mobile commerce. The architecture is derived in order to accommodate various business processes as an integral component and security management encompassing these business processes. It is believed that this architecture will assist in avoiding issues such as loss of transaction authenticity because the business process is integrated with the security procedures in the architecture. Further, the business processes are kept in the centre of the architecture to enable transaction confidentiality and integrity from an organisational point of view. Further, the interdependence of various systems within the architecture is expected to provide much needed real-time reaction to any causes of transaction unavailability in mobile commerce.

While the architecture is only a conception, the inclusion of business process along with IT security is expected to provide tight controls to management in terms of financial transactions. This is rapidly becoming essential in the competitive world of mobile commerce where the volume of transactions ensure healthy revenue to organisations. Therefore, the focus was set on transaction security. It is hoped that this architecture will help organisations to get a head start to review their security procedures and establish a better control on financial transactions.

Notes:

1. A.V. Dang, *E-Business raises transaction security concerns* (Gartner Advisory, 2000).

2. Dang, *E-Business raises transaction security concerns.*

3. A.K. Ghosh, *Security and Privacy for E-Business* (New York: Wiley, 2001).

4. M.V. Deise, et al., *Executive's Guide to e-Business: From Tactics to Strategy* (New York: John Wiley & Sons, Inc., 2000).

5. M. Loney, "M-Commerce safety fears," in *IT Week* (2000), p. 6.

6. Y. Zhang, and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *ACM/IEEE MobiCom* (2000).

7. Zhang and Lee, "Intrusion detection in wireless ad-hoc networks."

8. G. Hulme, "Services Seeks to Bring e-Business to Small Businesses," in *Informationweek.com* (2000), p. 21.

9. Ghosh, *Security and Privacy for E-Business.*

10. D. Fink, "Developing trust for Electronic Commerce," in *Internet and Intranet: Security and Management: Risks and Solutions,* ed. L. Janczewski (Idea Group Publishing, 2000), p. 44-86.

11. J. Schiller, *Mobile Communications* (New York: Addison-Wesley, 2000).

12. S. Shroeder, *Wired for business.* Risk Management, 1999(March): p. 12-22.

13. Fink, "Developing trust for Electronic Commerce."

14. P. Judge, "Little guys still say NO to the net," *Business Week* (1998): 134.

15. D. Young, "Handicapping M-Commerce: Getting ready for wireless e-commerce," *Wireless Review* (August 2000): 24-30.

16. Deise, et al., *Executive's Guide to e-Business: From Tactics to Strategy.*

17. A.V. Dang, *Four action items for E-Business: Transaction Security* (Gartner Advisory, 2000).

18. R. Dornan, *The essential guide to wireless communication applications* (Upper Saddle River, NJ: Prentice Hall PTR, 2001).

19. M. Gerrard, *Organising for E-Business: Getting it right* (Gartner Advisory, 2000).

20. G. Hulme, "Services Seeks to Bring e-Business to Small Businesses."

21. Ghosh, *Security and Privacy for E-Business.*

22. J. Craig, and D. Julta, *e-Business Readyiness: A Customer Focused Framework* (Boston: Addison Wesley, 2001).

23. Anonymous, *E-Commerce is growing,* in *The Australian* (2000).

24. B. Stowe, "Wireless networking looks attractive, but what about the cost of keeping it secure?," *Infoworld* (May 2000): 92.

25. Ghosh, *Security and Privacy for E-Business.*

26. R. Dornan, *The essential guide to wireless communication applications;* D. Smith and W. Andrews, *Exploring Instant Messaging* (Gartner Research and Advisory Services, 2001); Anonymous, *Wireless technology reaches behind the firewall.*

27. M.V. Deise, et al., *Executive's Guide to e-Business: From Tactics to Strategy.*

28. A. Arena, "Asian Internet start-ups invests heavily in dot.coms," *Australian communications* (February 2000): 15-18.

29. A. Lee, "Small firms must take Internet plunge or risk being sidelined," *The Engineer* 10, (November 2000): 10.

30. T. Lewis, "Ubinet: The ubiquitous Internet will be wireless," *IEEE Computer* 32, (1999): 10.

31. N. Langley, “Get moving on m-commerce,” in *Computer Weekly* (2000): p. 68.

32. S. Hayward, et al., *Beyond the Internet: The Supranet* (Gartner Advisory, 2000).

33. M. Gerrard, *Organising for E-Business: Getting it right* (Gartner Advisory, 2000).

34. Dang, *E-Business raises transaction security concerns.*

35. Dang, *Four action items for E-Business: Transaction Security*.

36. L. Koller, “Banks flirting with wireless billing,” in *Bank Technology News* (2000), p. 25.

RAJ GURURAJAN is a Senior Lecturer in the School of IT at Murdoch University. He is the program chair for the Bachelor of Applied Technology program at Murdoch University. He has been appointed as the Director for the Centre for Electronic Commerce and Internet Studies for the two-year period 2002 - 2003. He has over 12 years of academic experience and 5 years of industry experience. During his tenure in academia, he has published over 50 refereed papers, a text book in Computer Science, 7 book chapters and has conducted management consulting in the South West Region of Western Australia. His teaching and research interests include advance topic in electronic commerce, software costing and management, computer security and mobile and wireless computing. *Address for correspondence:* School of Information Technology, Murdoch University, South Street, Murdoch Perth, Western Australia – 6150. *E-mail:* r.gururajan@murdoch.edu.au.

BACK TO TOP

New Financial Transaction Security Concerns in Mobile Commerce

Raj Gururajan

Keywords: mobile commerce, IT security, financial transactions, business risk, technological risk, security threats.

Abstract: Security of transactions in Mobile Commerce is moving away from an IT concern to a Business concern because of potential loss of revenue to businesses due to lack of privacy, integrity or confidentiality, system slowdown or downtime. While most of the various security procedures are limited to corporate IT infrastructure, in mobile commerce issues concerned with transaction security appear to have extended beyond the corporate network to embrace the complete business process. Any lapse in procedures that maintain confidentiality of data or violation of privacy could affect corporate image and hence would impact customer relationships. Any adverse effect on customer relationship would negatively impact business revenue. In addition to existing security problems in a wired commerce environment, the emergence of mobile devices has renewed calls for addressing security threats to financial transactions. These problems are discussed in this paper as key issues in terms of organisation's architectural and procedural approaches to security, reliability and availability of business transactionss.

full text

Author: **Iuon-Chang Lin, Hsia-Hung Ou and Min-Shiang Hwang**
Title: **Two Secure Transportation Schemes for Mobile Agents**
Year of issuance: **2002**
Issue: **Information & Security. Volume 8, Number 1, 2002, pages 87-97**
Hard copy: **ISSN 1311-1493**

TWO SECURE TRANSPORTATION SCHEMES FOR MOBILE AGENTS

Iuon-Chang LIN, Hsia-Hung OU and Min-Shiang HWANG

Table Of Contents:

1. Introduction

Mobile agents have been the focus of a great number of research studies. All the experts in this domain aim to study the relevant technologies and thus enhance business activities.[1,2] In the information era, the Internet is widespread; it is both open and general.

Mobile agent technology has been proposed for use on the Internet. The mobile agent is a software program that acts on behalf of a user or software. It has the following features: (1) it is autonomous; (2) it has one or more objectives; (3) it has a scope of competence; and (4) it may, or may not, collaborate and communicate with other software and users.[3] In order to perform its job, it is able to migrate from a source host to a target host on a network under its own control.[4] However, this may lead to a great deal of security threats and attacks. When a mobile agent moves between a series of hosts, it may happen to encounter either trust-worthy or malicious hosts. A mobile agent must be capable of authenticating legal hosts and other agents to avoid malicious attacks. Ideally, a mobile agent should be versatile, robust, and secure in changing environments. Therefore, the security issue when dealing with mobile agents becomes essential. So far, the research on mobile agent security has been focused on the following topics:[5]

1. Protecting hosts from access by unauthorized parties;
2. Protecting hosts from attacks by malicious agents;
3. Protecting agents from attacks by other agents;
4. Protecting agents from attacks by malicious hosts.

However, only a few research studies have been focused on transportation security, which is in fact a very important topic in mobile agent systems, especially when it comes to business. When a user makes a request for a work to be performed, the request may be tampered with during the transportation, which causes trouble when the user is unwilling to disclose the information as to what agents are to be dispatched and where the destination should be. In this paper, we address the transportation security for mobile agents. When the mobile agent is transported between distributed hosts, there are several security issues that we have to carefully account for: [6,7,8]

- *Confidentiality:* In order to protect the privacy from being violated, all of the transported messages are encrypted. No malicious attacker can wiretap the transported contents.

- *Integrity:* No malicious attacker can modify any message being transferred. If a transported message has been modified, the receiver can easily detect it.
- *Authentication:* The identities of the source hosts and the mobile agents must be identified. Such identification can stop the attacks from malicious users and agents.
- *Non-repudiation:* The system provides the property of non-repudiation. It can prevent the user from denying having sent the request for launching the mobile agent. The property can be applied in many business applications.
- *Audit*: The system should be able to easily launch an audit process in order to find anything exceptional.

In the next section, we shall present a basic framework for the proposed scheme. Then, we shall give the details of the scheme and perform security analysis in Sections 3 and 4, respectively. Finally, we shall give our conclusions in Section 5.

2. A Basic Framework of the Proposed Scheme

This section introduces the basic framework of the proposed protocol. Our method is based on trusted third party and cryptography. The framework is shown in Figure 1.

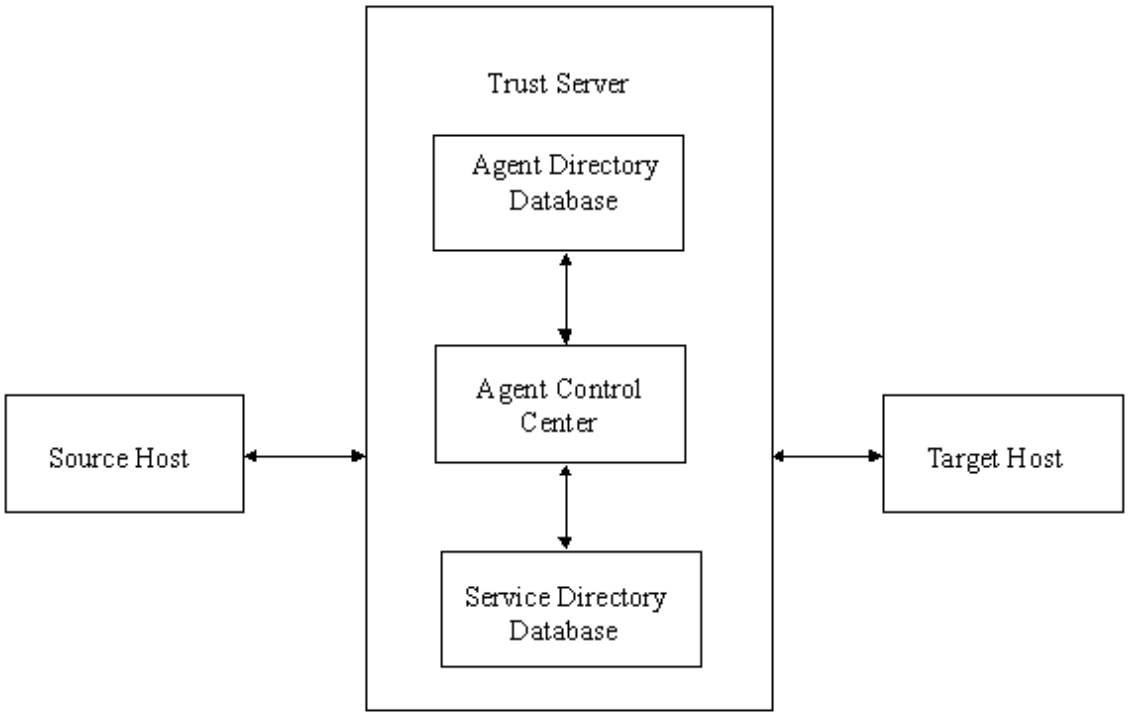


Figure 1: The basic framework

The framework includes the Source Host (SH), the Trust Server (TS), and the Target Host (TH), whose functions are described as follows:

1. *Source Host*:

   It is a host that owns mobile agents and sends requests for performing jobs to the trust server.

2. *Trust Server*:

   It is a trusted third party. It supports all requests for secure transportation between source hosts and target hosts. When TS receives request for an agent, it verifies the validity of the request and then dispatches the requested agent to a given target host. There are three modules in the trust server:

   (a) Agent Directory Database:
   This is a database that records the agent functions, source hosts, and historical records. When a target host is forced to accept a visit from a source host, the agent directory database is used to verify the agent.

   (b) Agent Control Center:

It supports all control functions of the agents. It searches the applicable data from either the agent directory database or service directory database and controls all the messages transferred via agents.

(c) Service Directory Database:
This is a database that records all the supported target hosts. When an agent is appointed to take a work request, the trust server uses the service directory database to search all the applicable hosts.

3. *Target Host*:

It is a host that an agent is sent to in order for the job to be completed.

We use the trust server to solve several security problems in mobile agents. Both the source hosts and the target hosts transact through the trust server. All agents must register and leave the records in the agent directory before starting the mobile agent. The agent directory records information such as: which agents belong to which hosts, what the agents' objectives are, and what the agents' source codes or certificates are. Then, all hosts which provide services must register with the service directory. The service directory records all the target host addresses and the services they provide.

3. Two Secure Transportation Schemes for Mobile Agent

In this section, two secure transportation schemes for mobile agents are proposed. The two schemes are designed to set up the transportation protocols for agent delivery between the source and target hosts.

In order to simplify the description of our schemes, we define some notations here.

TS:	Trust Server;
SH:	Source Host;
TH:	Target Host;
A:	An agent;
ID_i:	The identity of an entity *i*;
$E_{PK\,i}[\ldots]$:	An encryption function or a signature verification function using asymmetric crypto-systems, such as RSA, with the entity *i*'s public key being PK_i;
$D_{SK\,i}[\ldots]$:	A decryption function or digital signature product function using asymmetric crypto-systems, such as RSA, with the entity *i*'s private key being SK_i;
$F_{K\,j}[\ldots]$:	The encryption function using symmetric crypto-systems, such as DES, with the *j*-th session key being K_j, which is also used in the decryption function;
Response:	A target host's response, Yes or No.
$Noise_n$:	A unique serial number.

Scheme One:

In this scheme, we use cryptography techniques to accomplish our goals. Initially, each agent must register with the trust server and send the agent code to the trust server. The trust server will verify the agent to ensure the agent is secure and then store the data in the agent directory of the trust server. The scheme is shown in Figure 2.

The procedure of our first scheme looks as follows:

Step 1. SH sends a request for performing jobs to TS. The request includes TS's ID, SH's ID, the agent's ID, $Noise_1$, session key (K_1), and the signature of these messages. In order to provide confidentiality of communication, the request must be encrypted using TS's public key PK_{TS}. The main purpose of this step is SH to inform TS which agent will be launched.

Step 2. Upon receiving the above messages, TS decrypts them and verifies the signature by using SH's public key PK_{SH}. If the verification result is positive, TS records $Noise_1$ and its corresponding K_1 and locates the agent's function in the Agent Directory

Database. Then, TS searches the Service Directory Database for a suitable TH and generates a new session key K_2 with this TH. Next, TS sends TS's ID, SH's ID, agent's ID, $Noise_2$, K_2, and the signature of these messages, which are encrypted with TH's public key PK_{TH}, to TH. Here, TS checks whether the target host provides the requested services.

Step 3. The target host verifies the validity of the received messages and records $Noise_2$ and its corresponding K_2. Then, it sends a reply to the trust server. The messages containing answers are encrypted using a symmetric encryption function F with session key K_2.

Step 4. The trust server receives the answers from the target host. According to $Noise_2$, TS can find the corresponding session key K_2 to decrypt the message. If the reply is "Yes", the trust server will send the agent to the target host. The agent is stored in the agent directory of the trust server at the time when the agent registers. If the reply is "No", then the transportation process is stopped.

Step 5. The trust server notifies the source host which target hosts the agent will be sent to. These messages are encrypted with the session key K_1. Therefore, the content cannot leak out when it is passed over the Internet, and SH can be sure that the messages are sent from TS.

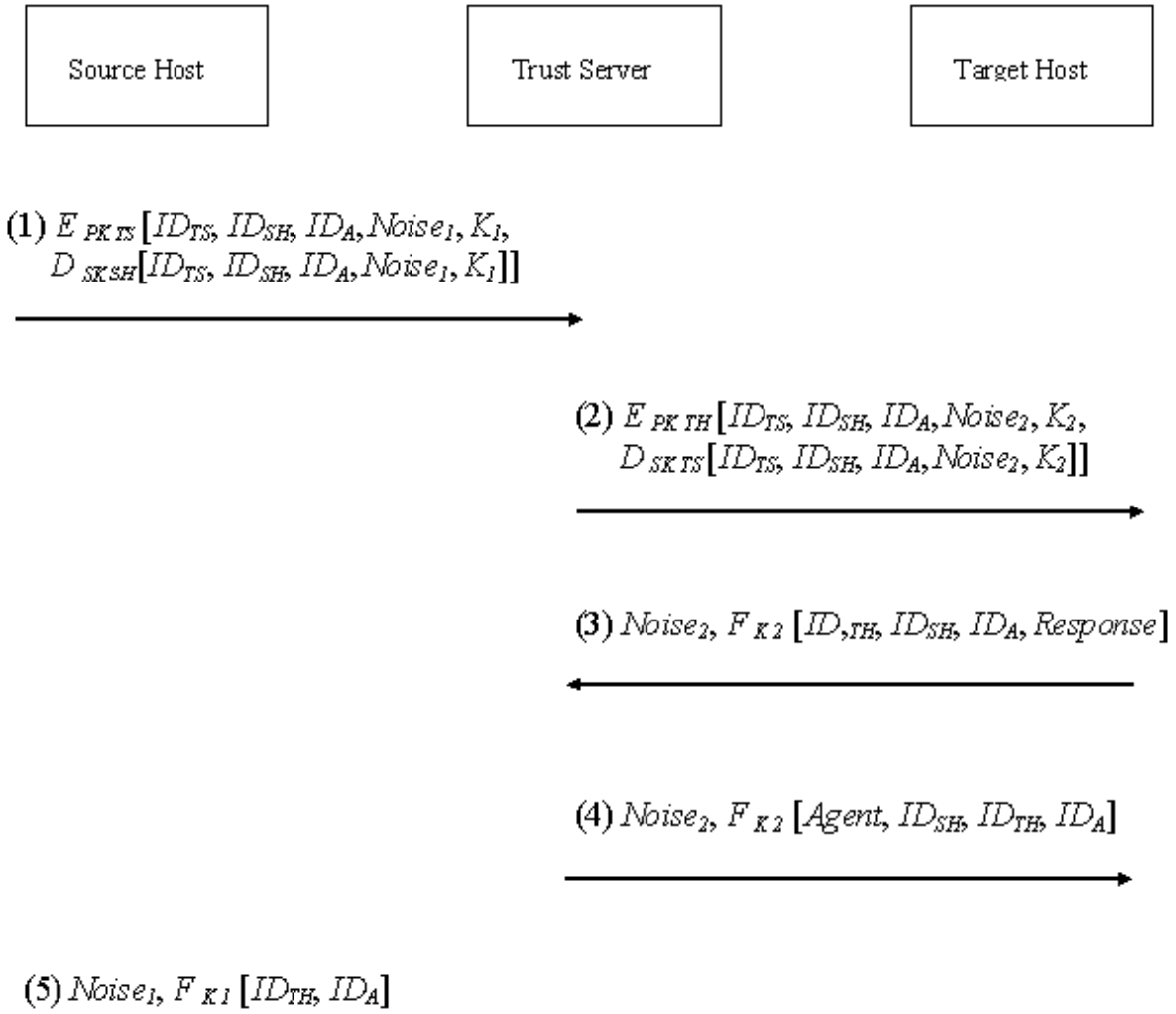


Figure 2: The first secure transportation scheme for mobile agents

In our first scheme, we use both symmetric cryptography and public key cryptography to achieve data protection. The public key cryptography is used only in the first two transactions to achieve confidentiality and integrity. Since the performance of symmetric cryptography is better than that of public key cryptography, we use symmetric cryptography instead of public key cryptography to achieve the same goals. In this schema, all of the transaction messages must go through the trust server. It has the advantage that the trust server can record all the messages for trail audit if any disagreement occurs in the transaction. However, the shortcoming is that there is a heavy load at the trust server. Therefore, we propose another scheme. In the second scheme, the agents do not need to be stored in the agent directory. When an agent registers, the trust server sends a certificate (*Cert*) to the source host. The certificate is composed of $D_{SK\,TS}(H(Agent) \oplus ID_{SH})$. The certificate can then be used to verify that the agent is a legitimate agent.

Scheme Two (Based on certificate):

We use the above mentioned certificate to improve our first scheme. The procedure of our second scheme is described below:

Step 1. This step is the same as the first step in our previous scheme. The main purpose of this step is SH to inform TS which agent will be launched.

Step 2. This step also coincides with the corresponding step from the first scheme. TS checks whether the target host provides the requested services.

Step 3. The target host verifies the validity of the received messages. Then, it sends a reply to the trust server. If the answer is "Yes", it appends $Noise_3$ and its corresponding session key K_3, which are encrypted and signed with PK_{SH} and SK_{TH}, respectively. Then TH encrypts the messages with the session key K_2 and sends $Noise_2$ and the encrypted messages to the TS.

Step 4. The trust server receives the messages containing the answers from the target host. According to $Noise_2$, TS can find the corresponding session key K_2 to decrypt the messages. If the reply is "Yes", then the TS notifies the SH which TH the agent will be sent to. These messages are then encrypted with the session key K_1, which includes ID_{TH}, ID_A and $E_{PK\,SH}[Noise_3, K_3, D_{SK\,TH}[Noise_3, K_3]]$. If the reply is "No", then the transaction is stopped. The objective is to let the SH know where the agent will be delivered and which session key will be used to protect the confidentiality in the next step.

Step 5. SH's ID, A's ID, agent, and certificate are encrypted with the session key K_3. Then SH sends $Noise_3$ and the encrypted messages to the TH.

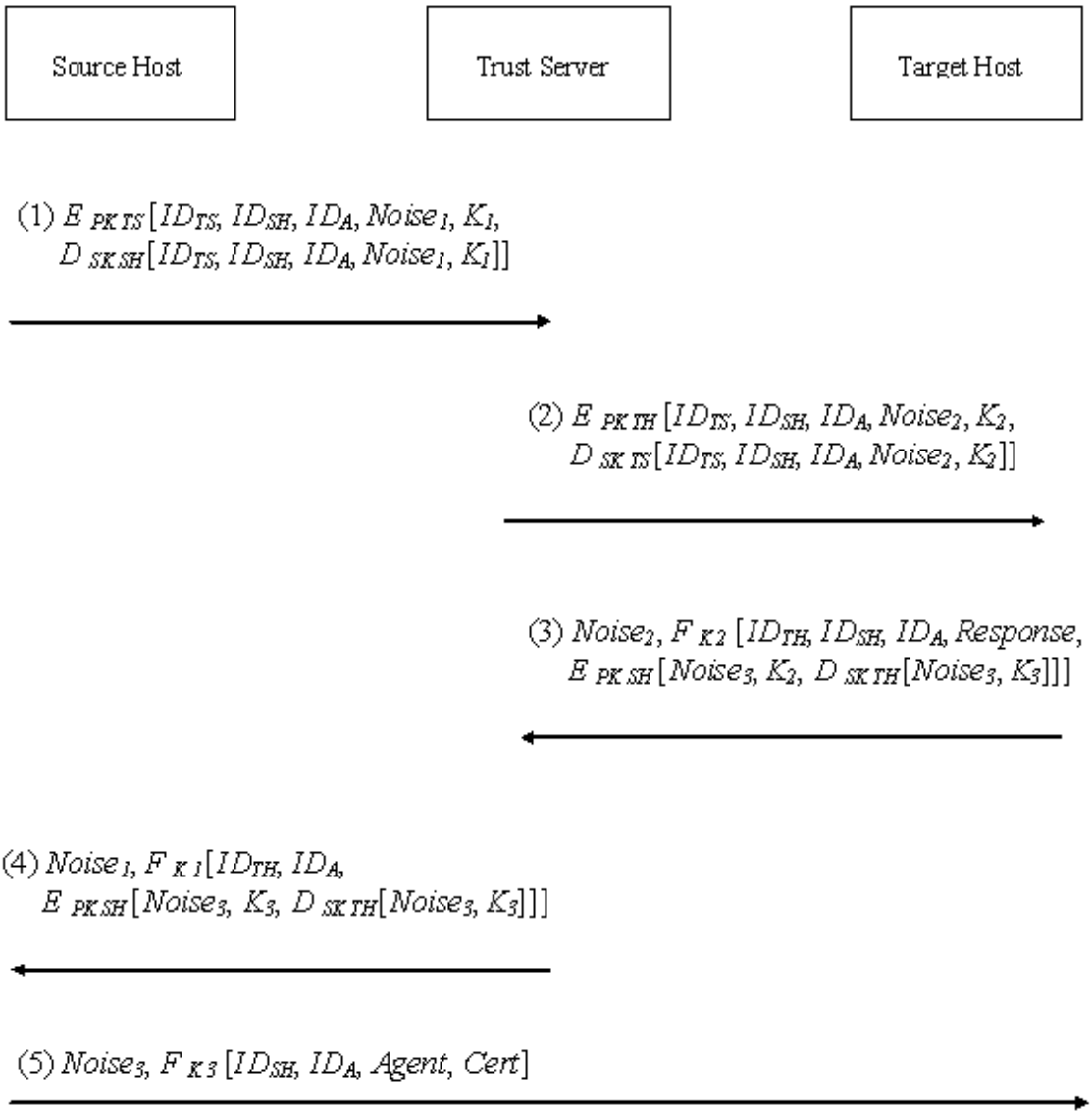


Figure 3: The second secure transportation scheme for mobile agents

Most of the procedures of protocol 2 are the same as those of protocol 1. Furthermore, if a target host wants to verify an agent's legitimacy, it proceeds as follows:

1. Hash the agent code and then take it along with the source host's ID to perform XOR.

2. Decrypt the certificate using TS's public key.
3. Compare results of step 1 and step 2, and the target host will verify the correctness.

Comparison

The first scheme is a general method, and the focus is on the trust server. All messages between the source host and the target host must go through the trust server where the agent's code is stored. The trust server is not only a third party. It also transmits the messages. So, the trust server is important, and it takes a heavy load. For this reason, we have proposed a second scheme to reduce the load on the trust server. In the second scheme, the role of the trust server is to be a successful transactor. There are both authentication and target search. To promote transaction, the source host directly delivers the agent's code to the target host. That can reduce the load on the trust server.

The point here is that the two schemes we propose in the same area are brought out to offer choices for different situations with different requirements. For local networks or a few agents, the first scheme is the better choice. Otherwise, the second scheme can support the heavy load in a large-scale network.

Both of the two proposed schemes can achieve our objective of offering secure transportation for the mobile agent delivered between distributed hosts. Security issues are discussed in detail in the next section.

4. Security Analysis

In Section 3 we have proposed and discussed two transportation schemes for mobile agents. Here, we intend to examine the security issues related to the proposed schemes.

Preventing the confidential information from leaking out

All the transported messages are encrypted in the proposed schemes. Hence, without the decryption key, it will not be possible for any malicious attacker to wiretap the transported contents. Any confidential information, such as what agent will be dispatched or where the agent works, will not leak out. The confidentiality is not a problem at all.

Attaining integrity and authentication

In the proposed schemes, asymmetric cryptography (i.e., RSA) is used to produce a signature of the transported message in the preceding steps. It is a powerful tool to authenticate the sender of the message and to ensure the integrity of the transported message. Because only the owner knows the private key, no attacker can acquire the correct signature. If a malicious attacker wants to forge a transported message or modify the content of the message, the receiver can check it out. In the preceding steps, we use symmetric cryptography to encrypt the transported message. Authentication and integrity can both be attained, because only the valid sender knows the session key. If the received message can be decrypted and turned back to be the meaningful message by using the same session key, the receiver can ensure the validity of the received message. Furthermore, the agent code is previously stored on the trust server. The trust server has to manage its authentication.

In the second scheme, the agent authentication is done through a certificate. The certificate is issued by the trust server and signed with the trust server's private key. Therefore, integrity and authentication can be guaranteed.

Resisting the replay attack

To resist the replay attack, the *Noise* and session key for a certain point of time are different from those for the next moment in our schemes. When an attacker replays previously intercepted message, the attack will not work because the receiver can detect that the *Noise* and session key were used before. Therefore, the proposed schemes are secure against the replay attack.

Providing the property of Non-repudiation

Non-repudiation is an important property when the mobile agent is used in business applications. In order to ensure this property, we use digital signature to achieve the objective. In the digital signature scheme, only the owner knows the private key and thus can produce a correct signature. Therefore, the user cannot deny sending the request for launching the mobile agent. Furthermore, all of the transferred messages must go through the trust server so that the trust server can record their message contexts to provide non-repudiation.

Ensuring host's security

In the first scheme, the agent is verified and encrypted by the trust server before arriving at the target host. In the second scheme, the target host can check its legitimacy by verifying the certificate. Furthermore, the agent transfer process is encrypted using the session key. No

malicious attackers can attack the agent during the transferring process. Therefore, the host does not have to worry about any attack. On the other hand, the trust server can trail the audit to find anything suspicious. These policies can ensure the security of the hosts.

5. Conclusions and Future Work

In this paper, two secure transportation schemes for mobile agents have been proposed. In the first of the proposed schemes, we use both symmetric and asymmetric cryptography to accomplish our goal. It is very efficient, but the trust server has to bear a heavy load. In the second scheme, we use the certificate technique to accomplish the same goal. It reduces the load on the trust server but is less efficient. The tradeoff should be made according to the system's requirements. For small networks or few agents, the first scheme is a better choice. Otherwise, the second scheme will be superior. Furthermore, according to the security analysis that has been presented, we have found our protocols useful in mobile agent communication and agent code delivery. However, there are more security problems that have to be addressed. In the future, we will continue the efforts in this domain, especially in electronic commerce and enterprise information management.

Acknowledgment. The authors wish to thank the anonymous referees for their suggestions to improve this paper. This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-005.

Notes:

1. P. Jorge, L.M. Silva, and J.G. Silva, "Security mechanisms for using mobile agents in electronic commerce," in *Proceedings of the 18th IEEE symposium on Reliable Distributed Systems* (1999): 378-383.
2. P. Maes, R. Guttman, and A. Moukas, "Agents that buy and sell," *Communications of the ACM* 42 (March 1999): 81-91.
3. M.S. Greenberg, J.C. Byington, and D.G. Harper, "Mobile agents and security," *IEEE Communications Magazine* 36 (July 1995): 76-85.
4. Ahmed Karmouch, "Guest editorial: Mobile software agents for telecommunications," *IEEE Communications Magazine* (July 1998).
5. F. Hohl, "A model of attacks malicious hosts against mobile agents," in *Proceedings of the 4th Workshop on Mobile Object Systems: Secure Internet Mobile Computations* (1998).
6. Min-Shiang Hwang and W.P. Yang, "Conference key distribution protocols for digital mobile communication systems," *IEEE Journal on Selected Areas in Communications* 13 (February 1995): 416-420.
7. M.S. Hwang, I.C. Lin, and Eric J.L. Lu, "A secure nonrepudiable threshold proxy signature scheme with known signers," *International Journal of Informatica* 11, 2 (2000): 1-8.
8. Min-Shiang Hwang and Chii-Hwa Lee, "Secure access schemes in mobile database systems," *European Transactions on Telecommunications* 12, 4 (2001): 303-310.

I.-C. LIN received a B.Sc. degree in Computer and Information Sciences from the Tung Hai University, Taichung, Taiwan, Republic of China, in 1998; a M.Sc.degree in Information Management from the Chaoyang University of Technology, Taiwan, in 2000. He is currently pursuing his Ph.D. in Computer Science and Information Engineering from the National Chung Cheng University. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

H.-H. OU received his B.Sc. and M.Sc. degrees in Information Management from the Chaoyang University of Technology, Taiwan, Republic of China, in 1999 and 2001 respectively. His current research interests include mobile agent, information security, and cryptography.

M.-S. HWANG received a B.Sc. in Electronic Engineering from the National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; a M.Sc. degree in Industrial Engineering from the National Tsing Hua University, Taiwan, in 1988; and a Ph.D. in Computer and Information Science from the National Chiao Tung University, Taiwan, in 1995. He has also studied Applied Mathematics at the National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in the field "Electronic Engineer" in 1988. He has also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor and chairman of the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications. For correspondence: Prof. Min-Shiang Hwang, Department of Information Management, Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C., Fax: 886-4-3742337. E-mail: mshwang@mail.cyut.edu.tw.

BACK TO TOP

---

e-mail: infosec@mbox.digsys.bg

Two Secure Transportation Schemes for Mobile Agents

Iuon-Chang Lin, Hsia-Hung Ou and Min-Shiang Hwang

Keywords: Mobile agents, privacy, security, secure transportation.

Abstract: Mobile agents are a new emerging popular research topic. Nowadays, the mobile agents are widely spread and implemented on the Internet. Application areas of mobile agents include electronic commerce, electronic marketing, enterprise information systems, etc. Since all the information about a mobile agent is transported over the Internet, the security policies become very important. However, the transportation security is usually neglected. In this paper, we propose two secure transportation schemes for mobile agents. They can prevent all possible attacks during the process of transporting agents. Furthermore, users can choose the best transportation scheme according to the system's scale.

full text

Author: **Information & Security**
Title: **I&S Internet Sources**
Year of issuance: **2002**
Issue: **Information & Security. Volume 8, Number 1, 2002, pages 101-120**
Hard copy: **ISSN 1311-1493**

MULTI-AGENT SYSTEMS RESEARCH

General research – on-line resources

This is a collection of potentially useful sources of information about Multi-Agent Systems (MAS).

MultiAgent.com

http://www.multiagent.com/

This is a very good page on multi-agent technology with information about companies, conferences, courses, laboratories, organizations, software, people and publications.

Directory of European Projects

http://www.agentlink.org/

AgentLink Project Database

http://www.agentlink.org/resources/agentprojects-db.html

Agent software

http://www.agentlink.org/resources/agent-software.html

The Intelligent Software Agents Lab at Carnegie Mellon University

http://www-2.cs.cmu.edu/~softagents/

Agents at Dartmouth College

http://agent.cs.dartmouth.edu/

Swarm.org

http://www.swarm.org/index.html

The Swarm Development Group (SDG) is a not-for-profit organization dedicated to advancing the state-of-the-art in multi agent based simulation through the continued advancement of the Swarm Simulation System and support of the Swarm user community.

The Robust Agent-based Systems at the CHCC

http://www.cse.ogi.edu/CHCC/Agents/main.html

The Center for Human-Computer Communication (CHCC) is a research center in the Department of Computer Science & Engineering within the OGI School of Science & Engineering at the Oregon Health & Science University.

UMBC Agent Web

http://agents.umbc.edu/

AgentLand

http://www.agentland.com/

News and information on intelligent software agents and bots

Intelligent Agents

http://www.primenet.com/~terry/New_Home_Page/ai_info/intelligent_agents.html

A good site with information and links to other resources on intelligent agents

The Software Agents Mailing List FAQ

http://dent.ii.fmph.uniba.sk/ui/faqs/agent_faq.html

Stanford Next-Link Project

http://www-cdr.stanford.edu/NextLink/NextLink.html

The Next-Link project objective is to learn the principles of coordination that will enable computational agents to facilitate distributed design and engineering.

The Software Agents group of the MIT Media Laboratory

http://agents.media.mit.edu/index.html

MAGMA Multi-agent Systems Research Group at Institute IMAG, Grenoble, France

http://cosmos.imag.fr/MAGMA/home-fr.html

Agent-Based Systems

http://www.agentbase.com/survey.html

Author: Sverker Janson, Swedish Institute of Computer Science

A good page with information on integration, coordination, mobility, believable agents, readings, standards, conferences, mailing lists, bibliographies, companies

---

MULTI-AGENT SYSTEMS RESEARCH

Multi-agent systems: journals

Autonomous Agents and Multi-Agent Systems

http://www.kluweronline.com/issn/1387-2532

Provides a free online sample copy of the first issue, with articles by Jennings, Lesser, and others.

Journal of Artificial Societies and Social Simulation (JASSS)

http://jasss.soc.surrey.ac.uk/JASSS.html

An inter-disciplinary journal for the exploration and understanding of social processes by means of computer simulation.

MULTI-AGENT SYSTEMS IN DEFENSE AND SECURITY

Research projects, systems, and tools

The Control of Agent-Based Systems (CoABS) program

http://coabs.globalinfotek.com/

This is the technical coordination site for DARPA's project on software agents (http://www.darpa.mil/ito/research/coabs/index.html). It has pointers to the many MAS research projects it funds, as well as some publications and other information. CoABS is a program of the U.S. Defense Advanced Research Projects Agency (DARPA) to develop and demonstrate techniques to safely control, coordinate, and manage large systems of autonomous software agents. The Control of Agent-Based Systems (CoABS) program aims to develop and evaluate a wide variety of alternative agent control and coordination strategies to determine the most effective strategies for achieving the benefits of agent-based systems, while assuring that self-organizing agent systems will maintain acceptable performance and security protections. CoABS is investigating the use of agent technology to improve military command, control, communication, and intelligence gathering.

Integrated Marine Multi-Agent Command and Control System (IMMACCS)

http://www.cadrc.calpoly.edu/frame_text/text_projects_immaccs.html

Organization: Collaborative Agent Design Research Center (CADRC), California Polytechnic State University, San Luis Obispo, CA

The site contains research material (Brochure, Object Models and Immacs software) pertaining to IMMACCS, a Decision-Support System for the US Marine Corps Sea Dragon Program. IMMACCS was built by CDM Technologies at San Luis Obespo, CA under a contract from the Office of Naval Research. The Integrated Marine Multi-Agent Command and Control System (IMMACCS) provides an objectified picture of the battlespace to aid in exploiting opportunities and accelerating tempo. IMMACCS assists military commanders and crisis management teams under battle-like conditions when dynamic information changes, complex relationships, and time pressures tend to stress the cognitive abilities of decision makers and their staff. As a trailblazing fires and maneuver system, IMMACCS disciplines the information environment and highlights factors affecting the commander's key concerns. In order to accomplish this support, IMMACCS incorporates agents that have reasoning and similarly intelligent

capabilities. It is the core of the Capable Warrior C4I decision-support system (http://www.globalsecurity.org/military/ops/capable-warrior.htm), providing “near” real-time situation awareness (i.e., updated several times per second) at all C2 access nodes.

Reusable Environment for Task Structured Intelligent Network Agents (RETSINA)

http://www-2.cs.cmu.edu/~softagents/retsina.html

http://www.ri.cmu.edu/projects/project_76_text.html

Head: Katia Sycara, Robotics Institute, School of Computer Science, Carnegie Mellon University

These sites contain project and personnel information, publications and sub-projects. RETSINA is an open multi-agent system (MAS) that supports communities of heterogeneous agents. The RETSINA system has been implemented on the premise that agents in a system should form a community of peers that engage in peer to peer interactions. Any coordination structure in the community of agents should emerge from the relations between agents, rather than as a result of the imposed constraints of the infrastructure itself. In accordance with this premise, RETSINA does not employ centralized control within the MAS; rather, it implements distributed infrastructural services that facilitate the interactions between agents, as opposed to managing them. The RETSINA multiagent infrastructure consists of a system of reusable agent types that can be adapted to address a variety of different domain-specific problems. Each RETSINA agent draws upon a sophisticated reasoning architecture that consists of four reusable modules for communication, planning, scheduling and execution monitoring.

Agent Storm

http://www-2.cs.cmu.edu/~softagents/agent_storm.html

http://www.ri.cmu.edu/projects/project_442.html

Organization: Robotics Institute, School of Computer Science, Carnegie Mellon University

Agent Storm is a RETSINA agent scenario where agents autonomously coordinate their team-oriented roles and actions while executing a mission in the ModSAF (Modular Semi-Automated Forces) simulation environment. The goal of Agent Storm is to increase the effectiveness of decision-making teams through the incorporation of agent technology in domains that are distributed, open and subject to time and other environmental contingencies. The AgentStorm system is composed of 25+ communicating software components developed with the RETSINA agent architecture. Agent Storm is one of seven winners of the “Innovative Enterprise Decision Support System” award in the Department of Navy Knowledge Fair 2000.

MokSAF

http://www-2.cs.cmu.edu/~softagents/moksaf.html

Organization: Robotics Institute, School of Computer Science, Carnegie Mellon University

MokSAF is a software system that supports mission critical team decision-making, and provides a virtual environment for route planning and team coordination. It allows commanders to register new agent teams and design new scenarios, plan individual routes to a common rendevous point, communicate synchronously across great distances, negotiate the selection of platoon units, and plan joint missions via a shared virtual environment

TIE-3 Demo: Interoperability of Multi-agent Systems to Support an Escalating Noncombatant Evacuation Operation (NEO)

http://www-2.cs.cmu.edu/~softagents/tie3.html

Organization: Robotics Institute, School of Computer Science, Carnegie Mellon University

The NEO Tie-3 Demo is a demonstration of agent technology in a Noncombatant Evacuation Operation (NEO). In TIE-3, RETSINA and Open Agent Architecture (OAA) agent systems are coordinated and their agents are used to evaluate a crisis situation, form an evacuation plan, follow an evolving context, monitor activity, and dynamically re-plan. TIE-3 demonstrates the interoperability and use of two disparate agent systems for aiding humans (officers and Ambassador) to effectively monitor the scenario, retrieve and fuse information for immediate use, and to plan and re-plan an emergency evacuation.

The Aircraft Maintenance System

http://www-2.cs.cmu.edu/~softagents/aircraft.html

Organization: Robotics Institute, School of Computer Science, Carnegie Mellon University

The Aircraft Maintenance System is wearable software that uses RETSINA agents to assist in the process of documenting and making repairs to aircraft.

RETSINA Demining

http://www-2.cs.cmu.edu/~softagents/demining.html

Organization: Robotics Institute, School of Computer Science, Carnegie Mellon University

This is a robotic demining system, part of AgentStorm. The robotic demining agents cooperatively clear paths, enabling simulated forces to breach minefields. Within the demining domain, the researchers explore different multi-robot cooperation and communication strategies.

SEAWAY: Joint Decsion-Support System for Sea Base Logistics Planning and Coordination

http://www.cadrc.calpoly.edu/frameset_info/info_projects_seaway.html

Organization: Collaborative Agent Design Research Center (CADRC), California Polytechnic State University, San Luis Obispo, CA

The site contains information on SEAWAY, a decision-support system designed to satisfy the focused logistic demand of Joint Vision 2020 (U.S. Department of Defense). The SEAWAY's approach to system design incorporates collaborative agents with knowledge in specific domains such as cargo visibility, cargo operations, mission planning, mission tracking, and mission execution. These agents create a partnership and collaborate with expert human staff members during the various stages of the logistic process. SEAWAY is expected to play an integral part in the naval and joint sea base logistic program. SEAWAY is an agent-based system that assists sea base operations by providing total theater visibility of all shipborne asset items en route to onshore objectives.

LOGGY: Joint Decision-Support System for Tactical Logistic Planning and Coordination

http://www.cadrc.calpoly.edu/frameset_info/info_projects_loggy.html

Organization: Collaborative Agent Design Research Center (CADRC), California Polytechnic State University, San Luis Obispo, CA.

LOGGY is a decision-support system designed to satisfy the focused tactical logistic demands of Joint Vision 2020 (U.S. Department of Defense). LOGGY demonstrates how agent-based tools can assist commanders in rapidly developing schemes of maneuver and the correlating logistic requirements that support the warfighter in the field.

FALCON: Future Army Leaders Command Operations Network

http://www.cadrc.calpoly.edu/frameset_info/info_projects_falcon.html

Organization: Collaborative Agent Design Research Center (CADRC), California Polytechnic State University, San Luis Obispo, CA

The project FALCON is designed to provide an expandable intelligent agent tool kit as a client to the DaVinci system currently under development by the US Army Communications and Electronics Command (CECOM), under the Command Post XXI Advanced Technology Demonstration (ATD) program, at Fort Monmouth, New Jersey. FALCON utilizes CDM's Integrated Cooperative Decision Making framework and includes agents to address the following military command and control objectives: execution monitoring, scaled distributed situation awareness, inferences and implications, focused overwatch, and allocation of both combat and combat service-support assets.

ISAAC/EINSTein: An Artificial-Life Approach to Land Combat

http://www.cna.org/isaac/

http://www.cna.org/isaac/einstein_test_version.htm

The site contains research material (papers, briefs and beta-test software) pertaining to an ongoing project that involves applying complexity theory to land warfare. ISAAC and EINSTein are "toy model" agent-based models of

combat. ISAAC is a simple multiagent-based model of land combat that was developed to illustrate how certain aspects of land combat can be viewed as emergent phenomena resulting from the collective, nonlinear, decentralized interactions among notional combatants. ISAAC takes a bottom-up, synthesist approach to the modeling of combat and represents a first step toward developing a complex systems theoretic analyst's toolbox for identifying, exploring, and possibly exploiting emergent collective patterns of behavior on the battlefield. Originally developed for the US Marine Corps, EINSTein's continued development is sponsored, in part, by the Office of Naval Research.

The CoAX Project (Coalition Agents eXperiment)

http://www.aiai.ed.ac.uk/project/coax/

This is an international collaborative effort that aims to demonstrate that the agent-based computing paradigm is a promising new approach to dealing with the technical issues of establishing coherent command and control (C2) in a coalition organization. This effort is a Technology Integration Experiment under the auspices of DARPA's Control of Agent Based Systems (CoABS) program.

The ActComm Project

http://actcomm.thayer.dartmouth.edu/

Project Personnel: George Cybenko, Bob Gray, David Kotz, and Daniela Rus at Dartmouth College, H. T. Kung and Brad Karp at Harvard University, Ken Vastola and Major Lisa Shay at Rensselaer Polytechnic Institute, P. R. Kumar, Tamer Basar and Gul Agha at the University of Illinois, Ken Whitebread and Sue McGrath at Lockheed Martin, and Eileen Entin at ALPHATECH. Contact information of all the participants can be found at the project's site.

This project focuses on transportable agents and wireless networks. The project's goal is to develop technologies that will maximize the usability of complex, global computer and communications networks for modern command-and-control applications. The concept of an *active communications system* is major technical innovation of the project. Active elements will be coordinated by a novel architecture that uses advanced agents to manage network, computer and information assets delivering high confidence communications and computing.The ActComm project is funded by the Air Force Office Of Scientific Research through a Department of Defense Multidisciplinary University Research Initiative (MURI) grant.

Decision-Theoretic Multi-Agent Sensor Planning

http://www-cse.uta.edu/~holder/research/ugv.html

Investigators: Diane J. Cook, Piotr Gmytrasiewicz and Lawrence B. Holder, University of Texas at Arlington, Department of Computer Science and Engineering

The project focuses on a decision-theoretic approach to cooperative sensor planning between multiple autonomous vehicles with specific applications for executing military missions. During the deployment of autonomous vehicles, intelligent cooperative reasoning must be used to select optimal vehicle viewing locations and select optimal camera pan and tilt angles throughout the mission. Decisions can be made in order to maximize the value of information

gained by the sensors while maintaining vehicle stealth. Changes in the battlefield over time can be used to learn patterns of enemy movement and improve estimation of future utility for sensor placement alternatives. Because military missions involve multiple vehicles, cooperation can be used to balance the work load and to increase information gain. The approach is being applied within DARPA's Unmanned Ground Vehicle program.

Littoral Warfare Modeling and Simulation

http://www.ncsc.navy.mil/Capabilities_and_Facilities/Capabilities/Littoral_Warfare_Modeling_and_Simulation.htm

Organization: Coastal Systems Station

The Coastal Warfare Evaluation Systems (CWES) office provides end-to-end simulation support to meet analysis, training, and acquisition needs for the littoral warfare (LITWAR) community, including mine countermeasures (MCM), minefield operations and planning, amphibious assaults, naval fires support, and naval special warfare.

Robust Agent-based Systems Incorporating Teams of Communicating Agents

http://www.cse.ogi.edu/CHCC/Agents/main.html

Organization: Center for Human-Computer Communication (CHCC) in the Department of Computer Science & Engineering within the OGI School of Science & Engineering at the Oregon Health & Science University

This is another project sponsored by the Defense Advanced Research Projects Agency under the CoABS (Control of Agent Based Systems) Program. The concept of *teamwork* is central to this project and the goal is to support robust teams of humans and robots in the long run. The project is comprised of the following three research areas and deliverables:

- Adaptive Agent Architecture (AAA): Based on the theory of teamwork, the researchers have built a fault tolerant multi-agent system, AAA, and deployed it in support of TIE1 (helicopter evacuation). The research has also contributed a theory of persistent teams and maintenance goals, and a formal representation of fault-tolerant behavior in logic. The AAA library is developed in Java and is available for download by the DARPA CoABS and the research community.
- Agent-Talk: This research investigates the design of an agent communication language with well-founded communicative acts and provably correct dialogue protocols. The researchers at CHCC have proposed a framework for group communication semantics that meets a broad range of desired requirements.
- STAPLE: This research aims to design, specify and implement an agent oriented programming language called STAPLE (Social & Team Agents Programming Language) by building upon a formal theory of multi-agent systems (Belief, Desire, Intention, Teamwork, Persistent Teams, Maintenance Goals), a formal agent communication language based on speech act theory with provably correct semantics (Agent-Talk), and agent architectures that use some incarnation of BDI logic as formal specification of their behavior.

VIPAR Multi-Agent Intelligence Analysis System

http://www.csm.ornl.gov/~v8q/Homepage/Projects/projects.htm

Contact: Dr. Thomas E. Potok, Group Leader - Collaborative Technologies, Computer Science & Mathematics Division, Oak Ridge National Laboratory

The goal of VIPAR (Virtual Information Process Research Agent) has been to develop intelligent software agents that address challenges facing the intelligence community in quickly gathering and organizing massive amounts of information, then distill that information into a form directly and explicitly amenable for use by an intelligence analyst in his decision making process. The Oak Ridge National Laboratory has successfully implemented this technology for the US Pacific Command.

SURGE - Spare Part Grouping

http://www.csm.ornl.gov/~v8q/Homepage/Projects/projects.htm

Contact: Dr. Thomas E. Potok, Group Leader - Collaborative Technologies, Computer Science & Mathematics Division, Oak Ridge National Laboratory

The goal of SURGE (Supplier Utilization through Responsive Grouped Enterprises) has been to develop an agent based manufacturing system that groups aircraft parts into families so that efficiencies can be gained. The system has been successfully developed for the Defense Logistics Administration.

TeamLeader: An Approach to Mixed-Initiative Agent Team Management and Evaluation

http://openmap.bbn.com/~burstein/coabs/

Investigators: Dr. Mark H. Burstein, Principal Investigator, BBN Technologies (Cambridge), and Prof. Drew V. McDermott, Department of Computer Science,Yale University

This is a project within the Control of Agent Based Systems Program of DARPA supported by the Air Force Research Laboratory at Rome, NY. The TeamLeader project is taking an experimental, prototype driven approach to developing strategies and mechanisms for humans to control and manage collections of software agents acting as teams within mixed human/agent organizations. A major focus and driving force for the research in this project has been the role of BBN Technologies as lead for a collaborative effort to develop a large scale demonstration of command and control in mixed human/agent organizations. The Mixed-initiative Agent Team Administration (MIATA) system has demonstrated how six people representing various military officers could control over 100 agents as they executed, in simulation, a recreation of the U.S. relief effort in response to the Hurricane Mitch disaster.

Agent-Based Modeling and Behavioral Representation

http://www.afrlhorizons.com/Briefs/0006/HE0009.html

Organization: AFRL’s Human Effectiveness Directorate, Deployment and Sustainment Division, Sustainment Logistics Branch, Wright-Patterson AFB OH

To satisfy the needs for more sophisticated modeling approaches that will enhance the modeling and simulation capability of the Air Force, scientists at the Human Effectiveness Directorate are conducting research to discover efficient ways to simulate intelligent behavior in existing and new models. In particular, they are developing and demonstrating agent-based approaches to emulate intelligence. The first technology demonstration project has been to create an agent-based intelligent mission controller node (IMCN) to link the Theater Battle Management Core System (TBMCS) to several Air Force simulations, including the current simulation used to support CPXs (Air War Simulation) and the new simulation environment under development (National Air and Space Model). The second demonstration focuses on improving the behavior of some of the autonomous models that make up a CPX, for example, individual aircraft that fly missions under the control of role players. A role-playing intelligent controller node (RPICN) is being created, which will be an autonomous agent-based model capable of “seeing” changes to the battlefield and reporting them back to the role player.

Enabling agent perception in multi-agent air mission simulation

http://www.cs.mu.oz.au/~pearce/

http://www.cs.mu.oz.au/~pearce/research.html

Co-Chief Investigators: Dr A Pearce & Prof T Caelli. DSTO: Dr. S. Goss1996-7: 2 year Postdoc (Dr. A. Pearce), Air Operations Division (AOD) 1998-9: Contract Research Grant for deliverable (2) with Prof S.Venkatesh.

This project has developed in collaboration with Air Operations Division, DSTO, (http://www.dsto.defence.gov.au/) real-time matching and learning techniques that enable agents to recognize aeroplane manoeuvres during operational flight simulation. Outcomes: used for integrating valid pilot competencies into computer controlled agents, earmarked for future use in answering specific questions about expensive equipment requisitions, component capabilities and rehearsing dangerous tactical operations.

Situation description language (SDL) and situation assessment processor (SAP)

http://www.cs.mu.oz.au/~pearce/

Co-Chief Investigators: Dr A Pearce & Prof S Venkatesh. DSTO: Dr. C. Davies 1998-2001 3 year Postdoc (Dr S Greenhill), Maritime Operations Division (MOD)

The project involves development of methods for acquiring and describing plans and mission details for submariners. In collaboration with Maritime Operations Division, DSTO (http://www.dsto.defence.gov.au/).The project addresses a basic deficiency in maritime simulations, in that there has been no explicit way of representing the kind of situational assessments (tactical or operational) that experts think in terms of when describing responses to situations. The project utilizes temporal and interval logic, spatial analysis, procedural and multi-agent reasoning and Bayesian uncertainty techniques. The technology has value in the area of improving the quality and efficiency of multi-agent simulations of procedural and tactical operations. Natural language situation descriptions improve the credibility of simulations by allowing stakeholders to easily appreciate the logic controlling the action in a simulation.

C2: Agent-oriented software engineering

http://www.cs.mu.oz.au/~pearce/

Principle Investigator: Dr A Pearce. ADI Limited: Dr N. Lewins

This project aims to apply agent-oriented software engineering methods by transferring agents, normally used in operational simulations, for visualization in desktop command & control systems. In collaboration with ADI Limited (http://www.adi-limited.com.au/).

Future Combat System - Joint Vision Battlelab Generative Analysis Project

http://www.lanl.gov/orgs/d/d5/projects/FCSJVBGAn/FCSJVBGAn.htm

Organization: Military Systems Analysis and Simulations Group (D-5) at Los Alamos National Laboratory

Generative Analysis (GAn) is the use of evolutionary and other heuristic learning algorithms to search and assess technology, force structure, and doctrinal spaces of a new or future system using simulations that portray the system in the environments that it is expected to operate.

MULTI-AGENT SYSTEMS IN DEFENSE AND SECURITY

Software tools

The Darpa Agent Markup Language (DAML)

http://www.daml.org/

This is the DARPA Agent Markup Language program homepage. The goal of the DAML effort is to develop a language and tools to facilitate the concept of the semantic web. It is a language for writing ontologies. They also now offer DAML-S, a language for describing web services.

The CoABS Grid

http://coabs.globalinfotek.com/

The CoABS Grid is an important output from DARPA's CoABS — a middleware layer based on Java / Jini technology that provides the computing infrastructure to enable the dynamic interoperability of distributed, heterogeneous, objects, services, and multi-agent systems. It is being used to produce militarily relevant technical

integration experiments where legacy systems and multi-agent systems developed by CoABS researchers are integrated to solve real-world problems. The CoABS Grid features flexible run-time communications and dynamic registration and discovery of relevant participants. It is adaptive and robust, with the system evolving to meet changing requirements without reconfiguring the network.

D'Agents

http://www.cs.dartmouth.edu/~agent

Organization: Dartmouth College

D'Agents is a mobile-agent system. The ultimate goal of D'Agents is to support applications that require the retrieval, organization and presentation of distributed information in arbitrary networks. D'Agents focuses on support for multiple languages, security, fault tolerance, performance, and the ability to operate effectively in volatile, wireless networks. It will be the middle layer of the ActComm infrastructure, sitting on top of the network services but below the planning, learning, resource discovery, and information-retrieval services.

Generative Analysis Project - Integrated Virtual Environment for Simulation (IVES)

http://www.lanl.gov/orgs/d/d5/projects/IVES/GAnIVES.htm#IVES

Organization: Military Systems Analysis and Simulations Group (D-5) at Los Alamos National Laboratory

The Integrated Virtual Environment for Simulation (IVES) is a Java implementation of simulation concepts developed by personnel within the Military Systems Analysis and Simulations Group (D-5) at Los Alamos National Laboratory. IVES is a composition-centered framework to develop discrete event simulations based on a regulated aggregate-component view of simulation. A simulation is viewed as a top-level aggregate comprised of a collection of components, i.e., simulation entities, that interact with each other and an optional simulation environment. A component can be realized as an actor, an agent, or any entity that can generate events that affect itself, other components, or the state of the system.

The Swarm Simulation System:A Toolkit for Building Multi-agent Simulations

http://www.santafe.edu/projects/swarm/

http://www.swarm.org/index.html

Authors: Nelson Minar, Roger Burkhart, Chris Langton, Manor Askenazi

Swarm is a multi-agent software platform for the simulation of complex adaptive systems. In the Swarm system the basic unit of simulation is the swarm, a collection of agents executing a schedule of actions. Swarm supports hierarchical modeling approaches whereby agents can be composed of swarms of other agents in nested structures. Swarm provides object oriented libraries of reusable components for building models and analyzing, displaying, and controlling experiments on those models. Swarm is currently available as a beta version in full, free source code

form. It requires the GNU C Compiler, Unix, and X Windows. For more Swarm information, software, user community information and publications, visit: http://www.swarm.org/index.html

The Agent-Based Configurable (ABC) Testbed

http://www.bbn.com/mst/abc.html

Authors: **The BBN Technologies**

The ABC Testbed combines modeling and simulation with innovative visualization, providing a simulation and analysis environment for understanding large distributed heterogeneous systems. It allows researchers to: model system components at suitable levels of fidelity, to execute those models in a controlled environment and to analyze the resulting data set.

MULTI-AGENT SYSTEMS

Selected reading

Coalition Agents Experiment: Multi-Agent Co-operation in an International Coalition Setting

http://www.aiai.ed.ac.uk/~arpi/COALITION/KSCO/ksco-2002/pdf-parts/B-ksco-2002-paper-08-allsopp.pdf

Authors: David N. Allsopp, Patrick Beautement, Jeffrey M. Bradshaw, Edmund H. Durfee, Michael Kirton, Craig A. Knoblock, Niranjan Suri, Austin Tate, Craig W. Thompson

Multi Agent System: A Nonlinear Framework for Machine Learning and Emerging Strategic Behavior

http://www.cs.northwestern.edu/~wolff/aicg99/jbrzezinski.html

Author: Jacek Brzezinski, DePaul University, Institute for Applied Artificial Intelligence, School of Computer Science, Telecommunications and Information Systems

The Potential For Intelligent Software Agents in Defence Simulation

http://www.eleceng.adelaide.edu.au/ieee/idc99/abstracts/lucas1.html

Authors: Andrew Lucas and Simon Goss

D'Agent tutorials on mobile agents

http://agent.cs.dartmouth.edu/tutorials/index.html

- Bob Gray - Introduction to Mobile Agents: Performance, Security and Programming Examples
- Bob Gray - Agent Mobility: Performance, Security and a Case Study
- David Kotz - Agents, Mobile Agents, and D'Agents
- George Cybenko and Bob Gray - Mobile Agents in Distributed Computing

D'Agent papers on mobile agents

http://agent.cs.dartmouth.edu/papers/index.html

This page contains papers on mobile agents, mobile agents security, hypothesis tracking, mobile agents in information retrieval, network sensing, learning and planning, network routing and quality-of-service, visual agent construction, functional validation.

Selected titles:

- Mobile Agents: The Next Generation in Distributed Computing.
- Mobile agents: Motivations and State of the Art.
- Mobile-Agent versus Client/Server Performance: Scalability in an Information-Retrieval Task.
- D'Agents: Applications and Performance of a Mobile-Agent System.
- Write Once, Move Anywhere: Toward Dynamic Interoperability of Mobile Agent Systems.
- Mobile Agents for Mobile Computing.
- Future Directions for Mobile-Agent Research.
- Mobile Code: The Future of the Internet.
- Mobile Agents and the Future of the Internet.
- Performance Analysis of Mobile Agents for Filtering Data Streams on Wireless Networks.
- Scheduling Multi-task Multi-agent Systems.
- A Comparison of Mobile Agent Migration Mechanisms.
- D'Agents: Security in a multiple-language, mobile-agent system.
- A Game-Theoretic Formulation of Multi-Agent Resource Allocation.
- Mobile-Agent Planning in a Market-Oriented Environment.
- Trading Risk in Mobile-Agent Computational Markets.

- Multiple Hypothesis Text-based Tracking of Land Vehicles.
- The Foundations of Information Push and Pull.
- Mobile Agents for Distributed Information Retrieval.
- Network Awareness and Mobile Agent Systems.
- Q-Learning: A tutorial and extensions.
- Networking Reconfigurable Smart Sensors.
- Matching Conflicts: Functional Validation of Agents.
- Information theoretic principles of agents.

Publications of Katia Sycara

Home page: http://www.ri.cmu.edu/people/sycara_katia.html

http://www.ri.cmu.edu/people/person_304_pubs.html

A very good site with more than 160 publications on multi-agent systems theory and applications, majority available for download.

Selected titles:

- Communicating Agents in Open Multi-Agent Systems
- Facilitating Message Exchange through Middle Agents
- Algorithms for combinatorial coalition formation and payoff division in an electronic marketplace
- Conversational Case-Based Planning for Agent Team Coordination
- Configuration Management for Multi-Agent Systems
- Multi-agent reinforcement learning for planning and scheduling multiple goals
- Multiple negotiations among agents for a distributed meeting scheduler
- Agent Interoperation Across Multagent System Boundaries
- Agent-Based Support for Human/Agent Teams
- Agent-Based Team Aiding in a Time Critical Task
- Interleaving Planning and Execution in a Multiagent Team Planning Environment
- Agent-based aiding for individual and team planning tasks
- Evolution of Goal-Directed Behavior Using Limited Information in a Complex Environment
- Adding Security and Trust to Multi-Agent Systems
- Agent aided aircraft maintenance
- Interoperability among Heterogeneous Software Agents on the Internet

- A Roadmap of Agent Research and Development
- Agent Cloning: An Approach to Agent Mobility and Resource Allocation
- Calibrating trust to integrate intelligent agents into human teams
- Argumentation in Negotiation: A Formal Model and Implementation
- Personal Security Agent: KQML-Based PKI
- Intelligent Adaptive Information Agents
- Distributed Intelligent Agents
- Executing Decision-theoretic Plans in Multi-agent Environments
- Unified Information and Control Flow in Hierarchical Task Networks
- How Does an Agent Learn to Negotiate
- Multi-Agent Integration of Information Gathering and Decision Support
- Designing a Multi-Agent Portfolio Management System
- Cooperative Intelligent Software Agents
- Modeling teams of specialists
- Distributed Problem Solving through Coordination in a Society of Agents
- Informed Decision Making in Multi-Specialist Cooperation
- Machine Learning for Intelligent Support of Conflict Resolution
- Negotiation Planning: An AI Approach
- Persuasive Argumentation in Negotiation

Clint's publications

http://members.optushome.com.au/clintspapers/aamas-01.htm

A good site with publications on military modeling and simulation using intelligent agents

Selected titles:

- Developing Agents for Military Simulation: From Knowledge Acquisition to Deployment
- Interchanging Agents and Humans in Military Simulation
- Modelling Command, Control, and Communication in Intelligent Agents
- Interactions Between Real and Virtual Entities in Synthetic Environments
- Intelligent Agents in the Analysis of Air Operations
- Scalability Issues in Military Multi-Agent Simulation
- Enabling perception for plan recognition in multi-agent air mission simulations

- A Military Air Mission Planning Tool: An RMA Initiative
- Plan Recognition in Military Simulation: Incorporating Machine Learning with Intelligent Agents Recognition of Intention
- Intelligent Computer-generated Forces
- Using Intelligent Agents in Military Simulation or "Using Agents Intelligently"
- Flying Together: Modelling Air Mission Teams
- Thinking Quickly: Agents for Modeling Air Warfare
- The Battle Model
- Towards Credible Computer Generated Forces
- Air Defence Operational Analysis Using the SWARMM Model
- Modelling Decision Making in an Air-Combat Environment
- Air Combat Tactics in the Smart Whole AiR Mission Model
- The Challenge of Whole Air Mission Modelling
- Modelling Teams and Team Tactics in Whole Air Mission Modelling.
- FFG-7 Class Frigate Airwake Viewer

Collaborative Interface Agents

http://agents.www.media.mit.edu/groups/agents/publications/aaai-ymp/aaai.html

Authors: Yezdi Lashkari, Max Metral, Pattie Maes MIT Media Laboratory, Cambridge, MA

Strategic Negotiation in Multiagent Environments

http://mitpress.mit.edu/0262112647

Author: Sarit Kraus

The MIT Press

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg