2009

Simulations in 3D tactics, interdiction and multi-agent modelling

A. R. Green
University of New South Wales, a.green@unsw.edu.au

I. C. Piper
University of Wollongong, ian@uow.edu.au

D. Keep
University of Wollongong, d.keep@uow.edu.au

C. J. Flaherty
Archer Ball Consulting, c.flaherty@archerball.com

Publication Details

This conference paper was originally published as Green, AR, Piper, IC, Keep, D & Flaherty, CJ, Simulations in 3D tactics, interdiction and multi-agent modelling, SimTecT, Adelaide Convention Centre, Australia, 15-19 June, 2009. Original conference information available here

Simulations in 3D tactics, interdiction and multi-agent modelling

Abstract
The analysis of vulnerabilities in large complex spaces is fundamentally problematic. The lack of capacity to generate a threat assessment merely exacerbates this problem. Lacking as well, in current literature is a developed methodology. To overcome this problem, we propose an approach using multi-agent modelling, which is also melded with three dimensional (3D) tactical understandings. Our approach builds on a microsimulation decision support tool, which was developed for a behavioural simulation of CBRN events. Microsimulation is based on the individual; who as an individual has a number of attributes, and which are stochastic (when repeated within an attribute). This approach is then enveloped. The simulations approach is intended for simulation of global and social controls and is designed to deal effectively with separate population groups. Each group has rules based on the group's behaviour and attributes, and complex scenarios can be built very simply. This therefore, enables analysis of emergent group behaviours and patterns. Our approach is akin to chemical or fire spread quantification. It views particle spread analysis as synonymous with complex movement (or stationary location) of many active agents within a complex 3D environment. This approach, we believe is needed to 'solve' the counter terrorism problem presented by scenarios such as the 2007 Haymarket attack; such as, how to analyse such events, as well as develop effective interdiction. A discrete behaviour model approach is suggested. This approach through repeated simulation (within the same parameters) should build up a statistical pattern of domain behaviour. As well, information on the outcome of changing behaviour can also be logged. Therefore, individual outcomes can be matched against real-time data to give best prediction of eventual outcomes, and the range of future strategies based on closest approach to reality. Taking this approach, potential targets could then be given random attributes including movement, size, speed, destination, and degree of deception being used in behaviour. Superimposing targets from known information and still building in random attributes about what is not known, will allow forward prediction with back-correction over time as information becomes more available. As well, failure rates and other assumptions could also be gradually relaxed, and this will allow for continuous assessment of assumptions as real data becomes available.

Keywords
simulation, modelling, terrorism

Disciplines
Numerical Analysis and Scientific Computing | Other Computer Sciences | Other Legal Studies | Physical Sciences and Mathematics

Publication Details
This conference paper was originally published as Green, AR, Piper, IC, Keep, D & Flaherty, CJ, Simulations in 3D tactics, interdiction and multi-agent modelling, SimTecT, Adelaide Convention Centre, Australia, 15-19 June, 2009. Original conference information available here

SIMULATIONS IN 3D TACTICS, INTERDICTION AND MULTI-AGENT MODELLING

Anthony R. Green
The University of New South Wales.
a.green@unsw.edu.au
Ian C. Piper, Daniel Keep
University of Wollongong
ian@uow.edu.au, d.keep@unw.edu.au
Christopher J. Flaherty
Visiting Fellow, School of Risk and Safety Sciences. The University of New South Wales.
Technical Lead, Archer Ball Consulting.
E-mail: c.flaherty@archerball.com

Abstract. The analysis of vulnerabilities in large complex spaces is fundamentally problematic. The lack of capacity to generate a threat assessment merely exacerbates this problem. Lacking as well, in current literature is a developed methodology. To overcome this problem, we propose an approach using multi-agent modelling, which is also melded with three dimensional (3D) tactical understandings. Our approach builds on a microsimulation decision support tool, which was developed for a behavioural simulation of CBRN events. Microsimulation is based on the individual; who as an individual has a number of attributes, and which are stochastic (when repeated within an attribute). This approach is then enveloped. The simulations approach is intended for simulation of global and social controls and is designed to deal effectively with separate population groups. Each group has rules based on the group's behaviour and attributes, and complex scenarios can be built very simply. This therefore, enables analysis of emergent group behaviours and patterns. Our approach is akin to chemical or fire spread quantification. It views particle spread analysis as synonymous with complex movement (or stationary location) of many active agents within a complex 3D environment. This approach, we believe is needed to 'solve' the counter terrorism problem presented by scenarios such as the 2007 Haymarket attack; such as, how to analyse such events, as well as develop effective interdiction. A discrete behaviour model approach is suggested. This approach through repeated simulation (within the same parameters) should build up a statistical pattern of domain behaviour. As well, information on the outcome of changing behaviour can also be logged. Therefore, individual outcomes can be matched against real-time data to give best prediction of eventual outcomes, and the range of future strategies based on closest approach to reality. Taking this approach, potential targets could then be given random attributes including movement, size, speed, destination, and degree of deception being used in behaviour. Superimposing targets from known information and still building in random attributes about what is not known, will allow forward prediction with back-correction over time as information becomes more available. As well, failure rates and other assumptions could also be gradually relaxed, and this will allow for continuous assessment of assumptions as real data becomes available.

1. INTRODUCTION

The very nature of large complex spaces, and the dynamic of many free agents – people, traffic etc., produces a confused environment. In classical military theory, this is identified as generating the fog of war, this nullifying battlefield transparency [1]. The key problem is that events transpire simultaneously, as an undivided and continuous set of events/actions, which occur at the same time. Overcoming these conceptual difficulties, we have developed in our more recent work on 3D tactics the formulation –

"3D tactics is premised on 'area analyses' where the entire space surrounding a target is subject to continuous simultaneous review, constantly seeking out multidimensional attack." [1] [2]

This paper develops the current research in the area of 3D vulnerabilities modelling, linking this to modelling multiagent movement and interdiction.

2. SUMMARY OF THE 3-D TACTICS ANALYSIS CONCEPT

We have previously proposed a line model to demonstrate the 3D tactics concept which is reproduced in Figure 1. [4] This example develops a 'look-around' analysis; encouraging thinking tactically in three dimensions, and simultaneously watching multidimensional actions. Using tools such as these, we can begin to identify within complex spaces, and among seemingly diffuse vulnerabilities and opportunities, clear target and defence patterns. We have previously found that accommodating the full context of a complex space, seeking to identify the clustering of vulnerabilities and targets in 3D spaces is near – impossible [2] [4]. For instance, in the case of the 2007 Haymarket attack, it was the vigilance of ambulance crews and parking staff who noticed the vehicles. However, it was purely happenstance that these weapons were identified at all. The use of vehicles, carrying improvised explosive devices (IEDs), of a type

typically seen parked there, at a time when no one would potentially notice, explains the success of the perpetrators. Successful, because they were able to exploit the inherent information deception attributes of this space, and deploys these IEDs in the first place [2]. Figure 1 demonstrates these dynamic, between opportunities (O), vulnerabilities (V) and targets, in complex or 3D tactical environments [3].

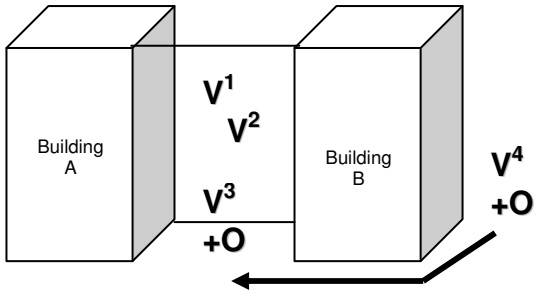

Figure 1. 3D Tactical Environment: Identifying where Opportunities (O) and Vulnerabilities (V) link.

This model identifies an open space between two built areas (identified as buildings 'A' and 'B'). Demonstrated are the links between attack opportunities and vulnerabilities, such as found in multi-level buildings, large transit spaces, covered rail stations, plazas, commercial precincts and malls. The basic 3D tactics concept, articulated here is that within the building and space, there are many vulnerabilities (represented V^1 to V^4), illustrative of dynamic multiagent moving or stationary within the environment. However, only certain vulnerabilities are paired with opportunities. These paired '*V+O*' are usually linear linked by some common line of transport (i.e. a road). This allows these to be targeted. The line of targets presents an attacker with multiple opportunities. Using a potential problem (opportunity analysis) approach to the scenario described in Figure 1 identifies the direction, risks, and myriad of other things that can give an advantage. The key question is how in a multiagent environment, do we develop effective interdiction?

3. INTERDICTION THEORY

Maritime interdiction and land-air Interdiction operations have developed some of the key concepts. Land-air interdiction theory regards as essential, that when affecting interdiction, achieves a 'significant volume of space free from an adversary's interference'. [7] As well, one of the adversaries needs to be able to deny his opponent 'entry to a significant volume of airspace, yet allow friendly forces freedom of manoeuvre.' [7] The second essential concept identified important is that interdiction, to be successful – it has to 'destroy, neutralize, or delay the enemy's military potential before it can be brought to bear effectively against friendly forces, at such distance from friendly forces' [6]

Fundamentally, any movement in space by an agent will travel along a path, while the direction, speed and height will be determined by factors such as mode of movement, and influenced by taking the line of least resistance avoiding contact or collision with other agents, or obstacles located along the movement line. Interdiction seeks to anticipate the line of approach of an agent, and either intercept before it reaches its target or as close as possible to its place of origin [3]. Little however, has been developed in regard to modelling capacity. For instance, dynamic queuing modelling has been advocated – this methodology: "consists of a set of things arriving at a system and seeking service (or to avoid service), a number of servers seeking to provide (impose) service, and a set of behaviour guidelines for arrivals and servers." [5]

Problematically, the queuing approach seeks to develop an ordering, and it is therefore heavily dependent on the scenario(s) chosen and introduces a constraint on the analysis. As sensing through intelligence and surveillance is at the centre of this method, then judicial used of this data with forecasting and backcastng models would be a more realistic approach to this interception problem. Difficulties also arise from considering the real chaotic environment. The challenge is authenticating many dynamic agents simultaneously. We propose a different approach akin to chemical or fire spread mathematical quantification; here, the complex movement of many active agents through a 3D environment offers insight into how to develop tactics. This mathematical approach will be reviewed next.

4. MULTIAGENCY MODELLING

The alternative approach to interception is the use of a random or chaotic model of individual behaviour that captures the elements of reality and avoids the major pitfall of steady state approaches, which subsumes important dynamic factors by aggregation and hence these are effectively forgotten about. This is similar to analysis of catastrophic accidents, where the time element on the factors that lead to the accident is effectively lost.

Microsimulation is a discrete simulation technique which allows for the modelling of the behaviour of single individuals in a complex system [1] [8]. It was originally devised for financial and economic modelling [11] [9], but is generally applicable to a wide range of scenarios. In the current research project, we have created a modular, scalable microsimulation package, called *Simulacron*, which allows for the rapid creation of microsimulations involving large numbers of people interacting with each other and their environment. A new simulation module has been integrated with the existing components. This new module, the "TPC" system, will allow the modelling of three distinct groups with differing behaviours as follows:

- Terrorists (the 'T' group): These are individuals who move through the environment until, at a predetermined moment in time, they attack, causing the 'deaths' of any individuals sharing their location. Each terrorist has, in addition to standard

model parameters, a 'camouflage factor' (F_c) which determines how effective they are at concealing themselves from law enforcement.

- Police (the 'P' group): These are individuals who move through the environment attempting to detect terrorist presence. If a police officer detects a terrorist, then that terrorist is 'killed' (and removed from the simulation). Each police officer has, in addition to standard model parameters, a 'perception factor' (F_p) which determines how effective they are at spotting the bad guys.

- Citizens (the 'C' group): These are the remaining individuals in the environment. They do not participate in the simulation except in the sense that they could be killed at any moment.

Detection is deemed to have occurred if, in any simulated period of time in which a terrorist and a police officer are collocated, a randomly determined value falls below the detection threshold defined by F_p $(1 - F_c)$. Similarly the terrorist has a probability option to blow themselves upon detection. This basic model may be varied by changing properties in a logical manner. For example, replacing the instantaneous lethality of the terrorist attack with a probabilistic one (a smaller bomb) or replacing it with a conventional infective state, simulating the release of a biological agent. Because of the flexibility of the program, police behaviours can range from completely random to precisely specified. The latter, allowing the investigation and validation of predetermined interdiction strategies such as those derived from game-theoretic modelling [10].

As an example of this approach Figure 2 shows the outcome for ten repeated simulations within a 'model' community of 400 houses; and 940 people; with one or two terrorists; and with 930 workplaces of various types.

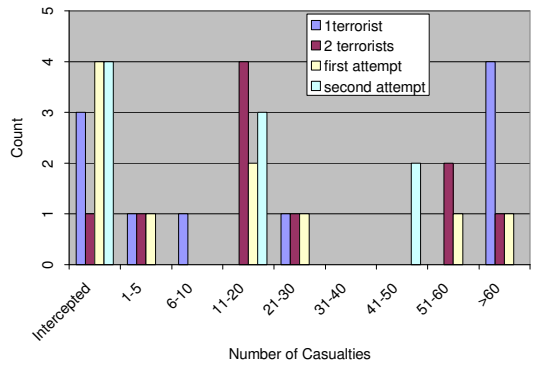

Figure 2. Frequency of casualties for one and two terrorist in a community of 940 people. The first and second attempts refer to the two terrorist scenario.

Figure 2 illustrates the following scenario - the target for the terrorists is the 'club' at 9:23 pm on a Friday night. The program is run ten times with ten police trying to intercept either one or two terrorists respectively within this community. The terrorists have a camouflage factor of 0.8 and a 50% chance that they will commit suicide if discovered early. The police have a perception factor of 0.8. The simulation starts on the previous Monday at 6:00 am. Figure 2 shows the numbers of deaths as a function of the frequency within each range.

In the ten runs with the single terrorist, the results were:

- Police intercept and arrest on 3 occasions.

- On four occasions there were casualties in excess of 60 people, of which only one was at the target time; the other three occasions, (two at the club and one at the cinema) the terrorist pre-emptively committed suicide on being intercepted.

- On the remaining three occasions the terrorist also took pre-emptive action resulting in less than 60 casualties. These occurred in shops and a restaurant respectively.

With two terrorists in the community, one complete interdiction occurred (arrest of both in the same run), even though the first and second terrorists were arrested four times each. Neither terrorist made it to the designated target time and chose pre-emptive suicide on the other occasions of discovery rather than arrest. The highest casualty rate occurred with two events occurring four days apart at the club. This demonstrates the ability to model coordinated attacks.

While these results are very preliminary, they demonstrate the ability to model both terrorist tactics and to study alternative interdiction strategies and relate those to the environment under study. An advantage of this discrete behaviour modelling is that multi agency resources as well as antagonistic behaviours of targets can easily be programmed into a simulation. Repeated simulation with the same parameters builds up a statistical pattern of domain behaviour as well as information on the outcome of changing the behaviour. If surveillance and intelligence data is available, then individual outcomes can be matched against real time data to give best prediction of the eventual outcome as well as the range of future strategies based on closest approach to reality. This uses a back correction forward predictor approach to modelling the outcome.

If you take customs maritime interception as an example against smuggling then you might have finite resources in planes, ships and shore people available. And these might be dispersed over several different agencies. Each resource has its own attributes including availability, location, speed etc. that dictate the range of surveillance and interception capabilities at any one time. Similarly targets can be given random attributes such as movement, size, speed, destination, degree of deception being used in behaviour that allows optimisation of deployment against them. This can be used as a planning tool for resourcing requirements. Superimposing targets from known information but still building in random attributes about what is not known allows forward prediction with back correction over time. As long as concurrent information is deployed to

all resources then tasking becomes a relatively simple matter to achieve a desired rate of success.

A question that arises in this approach is at what point do intervention strategies depend on resourcing availability before the system starts to fail? And, is there, an optimum amount of information required for a given success rate? These can also be tested in this type of modelling approach as well as alternative interdiction strategies. Standard interdiction models deal poorly with dispersed areas of surveillance and the time taken to achieve interdiction unless targets can be corralled. Even this involves a seven stage process of which one or more elements might fail. Furthermore what happens when intelligence gathered is part of a deception operation? A discrete behaviour model on the other hand can assess these types of changes because the statistics can be built up rather than assumed, such as failure rates, and other assumptions can also be gradually relaxed. This allows for continuous assessment of assumptions as real data becomes available. A critical process though is simultaneous display of exactly the same data across disparate control centres and resources so everybody is using exactly the same data in real time and where real time feedback on decisions can be used to enhance interpretation of the data and make forward predictions.

As an example, let us consider the 2007 attempted bombings in the London Haymarket, where an attempt was made to triangulate and sequentially detonate two car bombs. Analysis of this type of problem before the fact requires an analysis of the space and its use over time. This analysis is twofold, the analysis of the connectivity between spaces which can be used to determine where people can go and analysis of typical movement of people throughout the day. Both of these are then used to set up population movement in the domain of interest. Overlaying alternative behaviours such as interdiction agencies responses and the cues on which they act as well as alternative aggressor strategies allows analysis of the space for terrorist opportunities and the likely interdiction. Many different weapon systems can be assessed because each has its own constraints related to the space and geography, which dictate how these can be deployed. It also allows for testing of interdictions strategies and response to an event based on different degrees of intelligence or surveillance as well as determining the most effective use of data coming from that space.

5. CONCLUSION

The aim of this paper is to combine basic 3D tactical analysis concept with multiagent modelling and interdiction tactics theory, thus developing a more dynamic analysis. We believe, this approach leads us on the way to developing more advanced 3D GIS –based tool as a planning device when developing counter terrorist plans for complex spaces. The object of such a tool is to demonstrate where in complex environments the critical path of multiagent threats can be interdicted.

REFERENCES

[1] Connor, R.J. Boer, R. Prorok, P.C. Weed, D.L. (2000) Investigation of Design and Bias Issues in Case-Control Studies of Cancer Screening Using Microsimulation, American Journal of Epidemiol; 151:991-8.

[2] Flaherty, C. (September 2008) 3D Tactics and Information Deception, *Journal of Information Warfare*. Vol. 7, issue 2. pp. 49-58.

[3] Flaherty, C. Green, A.R. (17/18 July, 2008) 3D Tactics, Interdiction and Multiagent Modelling. *International Crime Science Conference* (University College London, Centre for Security and Crime Science).

[4] Flaherty, C. (16/17 July, 2007) 'Mass Space Vulnerabilities Analysis in 3-D Tactics, International Crime Science Conference', *University College London, Centre for Security and Crime Science*.

[5] Hazen, M.G. Burton, R. Klingbeil, R. Sullivan, K. Fewell, M.P. Grivell, I. Philp, C. Marland, P. (January 2003) 'The Analysis of Network-Centric Maritime Interdiction Operations (MIO) Using Queuing Theory'. *Eighth International Command and Control Research and Technology Symposium*.

[6] Krieger, CR. (Spring 1989) 'Air Interdiction'. *Airpower Journal*.

[7] Lawes, I. (2006), 'Land Force Air and Missile Defence: Dealing with the Complexities of Future Warfighting', *Australian Army Journal*, 4 Volume III, Number 2, 2006, p. 110.

[8] Merz, J. (May 1991) Microsimulation – a survey of principles, developments and applications, International Journal of Forecasting, vol. 7, no. 1, pp. 77-104, , available online at http://ideas.repec.org/a/eee/intfor/v7y1991i1p77-104.html.

[9] Orcutt, G. (1957) A New Type of Socio-Economic System, The Review of Economics and Statistics, vol. 39, no. 2, pp. 116-123.

[10] Pita, J. Jain, M. Marecki, J. Ordóñez, F. Portway, C. Tambe, M. Western, C. Paruchuri, P. Kraus, S. (May, 12-16., 2008) Deployed ARMOR Protection: The Application of a Game Theoretic Model for Security at the Los Angeles International Airport. *Proceedings of 7th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2008) - Industry and Applications Track, Berger, Burg, Nishiyama (eds.), Estoril, Portugal*.

[11] Weinstein MC. Recent Developments in Decision – Analytic Modelling for Economic Evaluation, Pharmacoeconomics. 2006; 24(11): 1043- 1053.