

# Old papers: Uncertainty Handling for Military Intelligence Systems

Something I had laying around the office; thought it would be useful for the archives in a "what i thought when I was 10 years younger" sort of way.

## ABSTRACT

We describe sources of and techniques for handling uncertainty in military intelligence models. We discuss issues for extending and using these models to generate counterintelligence- recognise groups of uncertainly-labelled entities and recognise variations in behaviour patterns.

## INTRODUCTION

Intelligence is the information that a commander uses to make his decisions. It is an informed view of the current area of interest of a commander or policymaker, in a form that he can use to improve his position relative to another, usually opposing, commander.

Uses of intelligence include the basis for command decision making and the creation of uncertainty in opposing commanders' systems and minds. Commanders use intelligence to recognise situations (situation awareness), predict changes in situations, predict an enemy's behaviour (threat assessment) and decide which actions to take (planning) The quality and availability of intelligence (rather than information) determines whether a force is reactive (can only react to its environment or opponent's moves) or proactive (can make informed plans and manipulate its situation).

Two major problems for commanders in the Persian Gulf conflict were the volume and complexity of intelligence data. If these are to be alleviated, methods for producing efficient representations of input data and information must be found – this includes automating the processing of raw intelligence data into useful knowledge

## MILITARY INTELLIGENCE PROCESSING

Know the enemy and know yourself in a hundred battles you will never be in peril, When you are ignorant of the enemy but know yourself- your chances of winning or losing are equal, If ignorant of both your enemy and yourself- you are certain in every battle to be in peril' (Sun Tsu)

The role of intelligence processing is to make sense of the world by piecing together the uncertain, conflicting but usually copious evidence available

Intelligence is information that is pertinent to the current area of interest of a commander or policy maker, in a form that he can use to improve his position relative to another, usually opposing, commander. Although some intelligence work is the stuff of James Bond and Le Carre novels, intelligence analysis is painstaking sifting of information to gain insight into the actions and intents

of another party Intelligence processing creates a model, or informed belief, of the state of that part of the world which is relevant to a commander's decisions and actions. Intelligence is produced by fusing uncertain and often untrustworthy information (sensor outputs and text-based reports) with prior knowledge (e.g. enemy equipment and tactics). This is a natural process for humans, but when the input data size becomes too large to process within the time constraints given, or too complex to think clearly about (people do not reason rationally under uncertainty), then automation of some of the processing must be considered. The flow of analysis is usually based on the intelligence cycle : Direction - deciding what intelligence is needed; Collection - collecting information; Collation - sorting information; Evaluation - processing information into intelligence; and Dissemination - giving that intelligence to the commanders/ users (NB this is the UK definition of the intelligence cycle; different labels are used in the US definition)

Current intelligence is gathered on a limited number of topics or geographical areas, but currently irrelevant basic intelligence is also processed and stored ready for when the attention of a commander or situation shifts. The creation of intelligence models is cyclic; as a better picture of the world is generated, the gaps in the commander's knowledge are pointed out, and more intelligence gathering is needed (this is shown in the diagram below by a feedback loop from collection to evaluation).

Characteristics of intelligence systems are that they are driven by a set of goals (the commanders requests for information), have information sources that can be partially controlled, situations that change over time and a large body of input information that is uncertain and incomplete. There is normally at least one non cooperating red agent capable of actions against the blue commander using these systems. Enemy actions against blue's intelligence operations include counterintelligence and deception: attempts to distort blue's model of the world. Other agents that may need to be modelled include neutral forces and civilians. Intelligence processing concentrates on resolving the uncertainties caused by inaccurate, infrequent and incomplete inputs, cultural differences, counterintelligence and approximate reasoning.

Intelligence models are :

- \* incomplete (we can never model the entire world),
- \* disruptible (models will always be vulnerable to external influences and counterintelligence),
- \* limited (models will always be limited by sensor capabilities),
- \* uncertain (input information and processing are usually uncertain) and
- \* continuously changing (models must deal with stale data and changes over time)

Military intelligence can go one step further than just modelling an uncertain

World; in using counterintelligence and deception about his plans, situation and actions, a commander is creating uncertainty in an opposing commander's models

The use of counterintelligence is one of the main differences between military intelligence and other uncertainty handling models (although there are similarities in handling counterintelligence, fraud, input errors and cultural differences).

## AUTOMATING INTELLIGENCE PROCESSING

Although intelligence is currently processed by analysts, its automation is being driven by

increasingly smaller time-frames, greater volume and complexity of available information Intelligence processing is increasingly similar to high-level data fusion (intelligence level fusion); making sense of the world from as much input data and information as possible.

Military conflict is essentially chaotic It is a sequence of well-defined moves that interact locally, yet produce long-range effects At the local level it is still possible to model these effects if they are bounded by physical laws, resources and the trained behaviour or rules of the parties involved During the cold war, the West faced known enemies on known territory with well modelled outcomes (a winter war across Germany) Post cold-war intelligence analysis deals with more uncertain (less is known about the enemy) and complex (conflict is more likely to be in a setting which contains neutral populations) environments and forces Although small-scale, terrorist and guerilla conflict may seem random, they are still constrained (by environment and logistics), their players still trained (often in tactics well known to the west) and their sequences of actions still partially predictable.

Automated intelligence analysis systems are limited by time constraints and are unlikely to produce perfect summaries of the world It should be stressed that their prime function should be to improve current intelligence analysis The aim of this work is not to produce exact solutions and assessments of uncertain inputs and situations, but to give a commander as honest an assessment of a battlefield as possible within the constraints of the inputs, uncertainties and processing time available This paper focuses on the sources of and methods for handling uncertainty in military intelligence systems: [5] discusses other aspects of automating intelligence processing in greater depth.

War is the realm of uncertainty three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty, the commander must work in a medium which his eyes cannot see which his best deductive powers cannot always fathom and with which- because of constant changes- he can rarely become familiar [4]

Uncertainty is not an important issue most of the time, as a commander will recognise the situation and react to it. Issues to be addressed include sources of uncertainty, whether we can improve our sensor allocations to reduce uncertainty, and how much uncertainty matters (how much uncertainty we can tolerate before a system is ignored or useless).

An intelligence processing system should use all (or as much as possible) of the information available to it This information is more than just input reports and sensor data; the context of an operation, open source, analysts' knowledge and the needs, preferences of users are also available. The systems should not take every input fact as certain; fortunately, most of this information is tagged with source and information credibility, sensor accuracy or a range of possible values.

The reasoning framework used cannot be divorced from decisions about how to handle uncertainty The aim of an intelligence processing system is to use prior experience and knowledge to pull out the information implicit in input data, whilst losing as little of that information as possible One of the main differences between reasoning frameworks is the point at which they discard information This ranges from rule-based expert systems, which force a user to decide on the truth or falsity of input statements, to systems which manage uncertainty about inputs, conclusions and reasoning to produce an assessment of a situation which takes account of all of these This latter system is most

desirable.

## COUNTERINTELLIGENCE AND ERRONEOUS INPUTS

Counterintelligence is the main difference between uncertainty handling in military and other systems. Modelling a military domain is compounded by an enemy attempting to deceive sensors and subtly change our models of the situation. Counterintelligence manifests itself as conflicts between conclusions and unexpected lack of accumulation of supporting evidence. Conflicts can be traced back to sources and information and counterintelligence hypotheses included and evaluated. This can be incorporated from the outset by regarding inputs as observations of hidden information (either intelligence or counterintelligence).

## THE USER'S UNCERTAINTY

The information output includes physical data (geography and positions; movements of forces), tactics and expected behaviour patterns, and social factors. Although most of these should have uncertainties associated with them, they currently do not, and one of the first questions in building an intelligence processing system should be whether this matters and if so, how much. The final point at which information is discarded (uncertainty occurs) is in the user's mind. Knowing what the user is interested in (user profiling) can focus the output. Even if an honest summary of the situation has been produced, complete with uncertainties; probabilities of different scenarios and actions, if this model is not transferred to the user's model of the world, then the processing will have been useless. Users also suffer from hypothesis lock in which alternative explanations are rejected regardless of accumulating evidence. Managing this phenomena requires good explanation of reasoning, uncertainty and evidence.

## ARCHITECTURE

The choice of reasoning framework is central to this work, both in its flexibility and its handling of uncertainty. Although intelligence is currently processed by human analysts, attempts to model it have included fuzzy logic, belief networks, assumption-based truth maintenance systems and rule-bases with exceptions. A Belief Network is a network (nodes connected by links) of variables that probabilistically represents a model - ie the beliefs that a user has about a world. Its main use is as a reasoning framework for manipulating and combining uncertain knowledge about both symbolic and numeric information. Belief networks can be extended to make decisions based on a users' stated preferences. Such networks are known as Influence Diagrams. There is a large body of research into many aspects of their use which includes learning networks from data, temporal (dynamic) networks and efficient evidence propagation. We consider Belief Networks to be an appropriate framework because they handle uncertainty in a mathematically rigorous way, and they can be manipulated to provide more than just a model of a world. Our experience in using belief networks for such a complex and uncertain application has, however, highlighted shortcomings in current belief network theory. Key problems identified include the lack of high-level structure,

treatment of time-varying information (including hysteresis effects), correlation between the real world and the model, slow speed (we may need to accept tradeoffs between uncertainty and execution times), handling of ignorance, and their single model (viewpoint) of the world.

## GROUPS AND OBJECT HIERARCHIES

Analysis of typical intelligence problems has shown information to be hierarchical (and sometimes fractal), grouped and layered. An example is air picture compilation where an aircraft can carry several different weapons (which are each applicable to different types of target), and aircraft of different types are grouped into packages which then perform single missions. We propose the use of an object-oriented framework, where each object (i.e. aircraft) contains a network that can inherit nodes, sub-nets and conditional probability tables from a class hierarchy. Each object network contains hooks - nodes that correspond to similar nodes in other objects' networks. Links between these nodes are often simple one-to-one conditional probability tables, but can be more complex; for instance, a package will have a one-to-many relationship with several aircraft. This allows the dynamic creation of large networks from components. It also allows the use of default propagations across objects (which are often single nodes in higher-level networks), default sub-networks (prototypes) and extra functionality (for instance the modification of input data). Using these robust architectures should improve network design times, but some consideration needs to be made of how much representation accuracy is lost in using them (for example whether adding an extra child link to a node will change the importance of its other children proportionally). Much of the theory has already been covered in discussions of semantic networks, plates, meta-nodes and representing conditional probabilities as networks. We propose the use of self-organisation to create the boundaries between sub-nets, and the use of constraint satisfaction techniques to decide which hooks should be joined.

## REAL-TIME PROCESSING

Intelligence processing is real-time and computationally expensive. Ideas for overcoming the time-constraints and bottlenecks caused when processing large amounts of data include distributed processing, using hierarchical architectures to limit the spread of information, and modifying analog radial basis function chip designs to belief network representations. We propose limiting propagation by collection of information at the boundaries of meta-nodes, approximate propagation across these boundaries, then propagation of batches of information properly when time allows. Propagation can thus occur at the node or metanode level. When propagation is allowed to proceed at both levels simultaneously (this is equivalent to using two layers of networks- one deterministic/approximate, the other detailed/probabilistic) the output will reflect the most detailed model for the time and attention constraints.

## USING REAL-WORLD INPUTS

How a network corresponds to the real world, particularly the pragmatic and semantic subtleties of

representing evidence uncertainty and ignorance, is also interesting. The problem of unreliable witnesses is so rife in intelligence processing that all information and human sources have reliability estimates attached to them. Current attempts to model this partial ignorance include using techniques from possibility theory to handle vague inputs, and using evidence nodes to spread the probabilities at input nodes.

### OTHER INTELLIGENCE MODELLING ISSUES

Other issues that have been identified which impact on the automation of intelligence processing are:

- \* representation of time-varying information feedback (for instance using recurrent belief networks and methods based on Markov chains)
- \* incremental build-up of errors from evidence removal (rebuilding networks using only currently available data),
- \* multiple space and timescales (no current solutions, but some signal processing theory may help),
- \* multiple utilities (multiple attribute utility theory)
- \* when to refer problems to human operators (sensitivity analysis to data and data flows)
- \* multiple viewpoints to give a spread of possible outcomes rather than a point view of the environment (layered networks to avoid repeating entire networks  
- see the section on real-time processing)
- \* reasoning about limited resources (colored network theory)
- \* discovering high-level patterns and trends in information, including behaviour patterns (adapting numeric pattern processing techniques to use symbolic inputs)
- \* generating behaviour novel plans (destabilising the networks - cf chaotic net theory)

### CREATING UNCERTAINTY

Since any view of an environment is subjective, limited by the knowledge and information available, that view is open to manipulation by an intelligent adversary. This is the basic premise of information warfare; the planning of counterintelligence and deception moves (i e mock-up tank emplacements) to manipulate or attack a red commander's mental model of the situation. Information warfare is a powerful technique which complements existing command and control warfare (the disruption of communications between the red commander, his forces and intelligence). We already have models of blue's view of a situation. Some theory already exists for the adjustment of network-based models to their input/outputs, and for multiple views of the same situation. It is therefore useful to adjust a blue model of a situation to create a blue estimate of the red commander's viewpoint, using red's known doctrine, sensors and reactions. Sensitivity analysis of blue's red commander model can then be used to determine which of several possible deception moves by blue would be most likely to alter the red commander's view of a situation to that desired by blue.

## EXAMPLE DOMAIN

The analysis of conflict, like game theory, embraces any interaction between parties with differing and usually contradictory aims. Intelligence analysis provides a viewpoint from which an agent or human can decide and act in the real world. Applications of intelligence processing techniques range from battlefield awareness to security systems and intelligent data mining; our example/test applications include classifying combat aircraft missions from sensor data and recognising criminal behaviour patterns.

## CONCLUSIONS

Intelligence processing is an interesting area for the application of uncertain reasoning techniques. The main difference between this and other applications is the deliberate creation of uncertainty (counterintelligence) both by own and opposing agents. This gives a new perspective on uncertainty - that of a useful thing to create.

## REFERENCES

1. NATO Intelligence Doctrine NATO report AINTP-1 1996
2. AN Shulsky Silent Warfare Brassey's US 1993
3. Sun Tsu The Art of War Oxford University Press
4. C von Clausewitz On War Princeton University Press
5. S,J Farmer Making Informed Decisions Intelligence Analysis for New Forms of Conflict IMA Conference on Modelling International Conflict- Oxford ),) April
6. W Feller An Introduction to Probability Theory and its Applications Wiley-
7. DA Norman and DG Bobrow On the data,limited and resources, limited processes Cognitive Psychology
8. R Szafranski A Theory of Information Warfare Preparing for, Airpower Journal- Spring
9. A Tversky and D Kahneman Judgement under uncertainty heuristics and biases, SIAM Journal on Computing
10. G Shafer Savage Revisited SIAM Journal on Computing
11. C Elkan The Paradoxical Success of Fuzzy Logic IEEE Expert- August
12. SG Hutchins and JG Morrison and RT Kelly Principles for Aiding Complex Military Decision Making Command and Control Research and Technology Symposium-Naval Postgraduate School- Monterey- California- June
13. J Pearl Probabilistic Reasoning in Intelligent Systems Morgan Kaufmann
14. RE Neapolitan Probabilistic Reasoning in Expert Systems Wiley
15. E Horvitz and F Jensen Uncertainty in Artificial Intelligence Morgan Kaufmann