Intelligent Threat Assessment Processor (ITAP) using Genetic Algorithms and Fuzzy Logic

Paul Gonsalves                      Rachel Cunningham
Principal Scientist                        Scientist
Charles River Analytics, Inc.
Cambridge, MA, U.S.A.
pgonsalves@cra.com          rcunningham@cra.com

Nick Ton                     Dennis Okon
Software Engineer     Research Associate
nton@cra.com            dokon@cra.com

Abstract - The explosive growth in the area of information technology provides a tremendous opportunity for enhancing military warfighting capabilities. The management and processing of military intelligence information, the requisite assessment of enemy capabilities, intent, and objectives, and the generation of appropriate response recommendations form a critical element of battlespace operations. Here, we develop an Intelligent Threat Assessment Processor (ITAP) for enhancing tactical threat assessment. Our novel system integrates a genetic algorithm approach to predicting enemy courses of action (eCOAs), a fuzzy logic-based analysis of predicted eCOAs to infer enemy intent and objectives, and in conjunction with our ongoing development of an Intelligent Fusion and Asset Management Processor (IFAMP), provides the necessary functionality to support multi-level data fusion. We see considerable potential for this approach in enhancing existing tactical decision-aiding systems and addressing future information dominated battlespace requirements.

Keywords: Data fusion, threat assessment, genetic algorithms, fuzzy logic.

1 Introduction

Recent military operations and future battlefield requirements illustrate the importance of information superiority and the subsidiary need to provide enhanced battlespace awareness for the warfighter. However, with the promulgation of various inter-service information collection and dissemination mechanisms, a major challenge to achieve information dominance is how best to process and correlate data rapidly from many sources to generate a cohesive accurate picture of the battlespace and generate appropriate response recommendations, i.e., data fusion and visualization and decision-aiding remain critical processes.

The overall goal of data fusion is to combine data from multiple sources into information that has greater benefit than would have been derived from each of the contributing parts [1]. An obvious analogy exists between data fusion and human cognitive processing, in particular, the way humans process multi-sensory information (i.e., sight, sound, smell, ...etc.) to make inferences regarding the external environment. Current fusion methods for target location and track determination are based on parametric data association, and the use of either batch or sequential estimation techniques [2]. For target identification fusion, various methods have been applied, including parametric based, statistical, and clustering based algorithms, and model-based simulation and estimation. Efforts for higher-level fusion processing, including situation assessment and threat assessment, have relied on more cognitive and symbolic processing methods. However, these efforts have not been totally successful due to inflexibility to changing external environment conditions, non-repeatability of the target signatures, limited use of a priori information regarding sensor/asset capabilities/limitations, and inability to address the distributed nature of future battlespace systems.

To address these issues we have developed an Intelligent Threat Assessment Processor (ITAP) to provide prediction and interpretation of enemy courses of action (eCOAs). A course of action is defined in military terms as a possible plan related to the accomplishment of a mission. The ITAP architecture integrates two specific elements: a genetic algorithms (GAs) based module for determination of likely eCOAs, and a fuzzy logic-based module to analyze and interpret predicted eCOAs and to infer enemy intent and objectives and enemy capabilities and vulnerabilities, and a visualization and decision-aiding module for generating response recommendations and enhancing battlespace awareness. The course of action prediction module builds on our on-going work with a GA-based military planning tool dubbed FOX [3].

Additionally, ITAP makes extensive use as well as enhances our Intelligent Fusion and Asset Management Processor (IFAMP) project [4]. The goal of IFAMP is to develop an integrated software application that can fuse information from disparate sources and provide the capability to detect, track, classify, and engage targets and provide timely assessment of the situation. Additionally, IFAMP supports functionality for the control and management of sensor and information assets. IFAMP incorporates the following components: a fuzzy logic low level fusion manager, fuzzy logic event detection, belief networks for situation assessment, and a fuzzy-based asset management component. There is a
natural fit between IFAMP and ITAP. Specifically, the Bayesian belief network based situation assessment can provide the GA eCOA predictor with the necessary current disposition and composition of enemy forces. Conversely, outputs of the ITAP, such as eCOA and enemy intent and capabilities, can be fed back to the IFAMP belief network component to post as evidence. Additionally, this threat evidence can facilitate a speculative analysis mode for the belief network where the goal is to determine what information is critical to answer the high-level information requirements (e.g. where enemy’s main attack will be concentrated). Such information provides specific focus for the asset management module of IFAMP.

The paper is organized as follows. Section 2 introduces the scope and overall architecture of ITAP. Section 3 details the major components of ITAP including the GA-based generation of enemy courses of action and a the fuzzy logic approach to eCOA decomposition and overall threat assessment. Section 4 presents ITAP sample results for a given military tactical battlefield scenario. Section 5 concludes the paper with relevant conclusions and a discussion of future work.

2 System Description

2.1 Levels of Data Fusion

The Joint Directors of Laboratories (JDL) Data Fusion Subpanel have identified five levels of fusion processing products [5]:

- Level 0 (Sub-Object Assessment): Fused estimates of object signals or features
- Level 1 (Object Assessment): Fused position and identity estimates
- Level 2 (Situation Assessment): Friendly or hostile military situation assessments
- Level 3 (Impact Assessment): Hostile force threat assessments
- Level 4 DF (Process Refinement): Control of assets via process refinement

Across these levels of information products, the generality of the results increases from the very specific (e.g., “wheeled vehicles detected at location X”) to the more general (e.g., “enemy’s main attack will at location X”). Level 0 processing includes signal detection and feature extraction. At level 1, also referred to as object assessment, numeric procedures such as estimation (e.g., Kalman filtering) or pattern recognition dominate the processing operations. Object assessment information products arise from single and multi-source processing (such as target tracking) by sampling the external environment with available sensors and other information sources. The products of this processing are position and identity estimates for targets or platforms in the composite field of view.

Symbolic reasoning processes involving higher levels of abstraction and inference dominate the level 2 (situation assessment) and 3 (impact assessment) fusion operations. Situation abstraction is the construction of a generalized situation representation from incomplete data sets to yield a contextual interpretation of level 1 products. This level of inference is concerned with deriving knowledge from some type of pattern analysis of level 1 data. Whereas levels 1 through 3 concern themselves with processing and refining information or what can be termed estimation functions, level 4, or process refinement, involves the integrated management and coordination of the available sensor and information assets, or what can be termed as control functions. Process refinement functions seek to enhance estimation performance including earlier target detection and recognition, improved tracking, increased situation assessment, and timely threat assessment.

ITAP deals specifically with level 3 impact or threat assessment. The distinction between levels 2 and 3 is that level 3 products attempt to quantify the threat’s capability and predict its intent by projecting into the future, whereas level 2 results seek to indicate current hostile behavior patterns. Elements of level 3 include determining enemy capabilities and vulnerabilities based on the current assessment and awareness of enemy and friendly composition and disposition. A major element threat refinement is the prediction and evaluation of enemy courses of actions (eCOAs). A COA is defined as a plan to accomplish a mission or related to the accomplishment of a mission. Five elements are inherent in COAS: 1) type of operation (WHAT), 2) timing of the operation (WHEN); 3) location (WHERE); 4) employment of assets (HOW); and overall objectives and goals (WHY). Any method that seeks to determine or predict possible enemy COAs (eCOAs) provides a valuable information source and planning tool for not only in the scope of data fusion (specifically for the collection management or process refinement), but more in the operational or command and control domain. Both of these areas are addressed in ITAP.

2.2 ITAP Scope

Figure 1 shows the overall scope of our ITAP system for threat assessment processing within the overall context of the different levels of data and information fusion. Figure 1 also illustrates how ITAP relates to our on-going IFAMP effort. As shown, we begin with a specification of the external environment. This includes the specification of all friendly, hostile, and neutral forces, as well as a description of the local terrain and current weather conditions. The collection assets sense information about the external environment. Figure 1 lists a common set of platforms including J-STARS, UAVs, AWACS, etc. Data from these sensors/assets are then fused (object assessment) within IFAMP level 1 processing to generate individual target tracks and to classify and characterize targets.

The situation assessment module of IFAMP uses this fused track data to generate a current situational state from detected events. The total situation assessment state is then forwarded to the ITAP module. The ITAP module is responsible for inferring enemy intent and objectives, as well as enemy/friendly capabilities and vulnerabilities. In particular, ITAP provides a means to predict enemy
courses of actions (eCOAs). These eCOAs are then analyzed to infer enemy high-level information, specifically, high-level evidence concerning enemy intent, enemy mission objectives, and enemy capabilities, and vulnerabilities. This high-level threat assessment evidence is then fed back to the IFAMP level 2 module. ITAP’s scope also goes beyond the four levels of data and information fusion, by addressing decision-aiding and battlefield visualization aspects. These two aspects were not addressed in the research presented here, but have been proposed for a follow-on effort to support the operations planning and execution phases.

2.3 ITAP Architecture

Figure 2 shows the Intelligent Threat Assessment Processor (ITAP) architecture and how it interfaces with our on-going IFAMP effort. ITAP consists of two main modules: a GA based eCOA prediction module based on the FOX military planning tool and an eCOA decomposition inferencing module based on fuzzy logic expert systems. As shown in Figure 2, IFAMP level 2 belief networks supply the FOX tool with initial specification of enemy disposition and composition, so as to constrain the GA-based search. After decomposition of predicted eCOA into enemy intent/objectives and capabilities/vulnerabilities within ITAP’s fuzzy logic-based eCOA decomposition module, (dubbed the Fuzzy logic Post Processor (FLP2) the information is passed on to command and control (C2) decision-aiding systems and, in turn back to IFAMP level 2 belief networks. The high level enemy information is used within IFAMP in a speculative manner to determine critical information requirements – a vital element of the collection management process. Details relevant to GAs and the FOX tool for eCOA prediction are provided in section 3.1, and decomposition using fuzzy logic of FOX generated eCOA state vector is discussed in section 3.2.

3 ITAP Component Descriptions

3.1 Enemy Course of Action (eCOA) Generation

Systems design problems that require optimizing a function depending on a large number of parameters pose a significant challenge. Such problems (of which eCOA generation is an example) possess a large parametric space from which to choose, the possibility of large infeasible and non-uniform areas, and the presence of numerous local minima or maxima. To solve these problems, one generally resorts to either analytical gradients or numerical searches. Some of these techniques may be time consuming either in developing the optimization approach or in their execution, and may lead only to
locally optimal solutions. In some instances, the problem is simplified to satisfy the optimization technique, resulting in a solution that is optimal for only an approximate problem. Recently, genetic algorithms (GAs) have gained popularity in solving optimization problems while treating the function to be optimized as a black box [6]. Genetic algorithms are parameter search procedures based upon the mechanics of natural genetics. They combine a Darwinian survival-of-the-fittest philosophy with a random, yet structured information exchange among a population of artificial chromosomes. GAs have been shown to do well on problems that are difficult to solve using traditional techniques [7] [8].

FOX [3] is a genetic algorithms (GA)-based planning support tool for assisting military intelligence and maneuver battlestaff in rapidly generating and assessing battlefield courses of actions (COAs). FOX’s efficiency in generating large numbers of potential COAs stems from its high-level (abstract) representation of the battlespace and forces. Wargaming at a high representational level enables a rapid search through the COA-space for generally desirable solutions. In FOX’s current configuration, these high-level candidate COAs are then presented to human analysts for a more in-depth analysis and detailed planning effort needed to fully define the COAs. However, this COA planning and analysis process could be further accelerated by a decision support tool to help generate detailed operation plans. Whereas, our ongoing FOX work has concentrated on development of friendly COAs for planning purposes, for ITAP we have transitioned FOX to support the generation of enemy COAs to support threat assessment as shown in figure 3.

The three major components of FOX are: 1) the GA optimization software itself; 2) a Wargamer which plays out GA generated enemy COAs against a representative set of friendly COAs; and 3) a Performance Evaluator (or fitness function in GA parlance) that assigns a score or fitness of a given string or solution.

FOX employs a high-level representation of battlefield engagements. It assumes a generic maneuver box (or area of interest) having several parallel avenues of approach (AAs), which are orthogonal to several lines of defensible terrain (LDTs). An LDT is a string of roughly adjacent choke points cutting across all the AAs providing a naturally strong defensive position. The offensive forces are modeled as moving from tactical assembly areas (TAAs) behind the forward edge of the battle area (FEBA) toward an envisioned limit of advance (LOA) beyond the furthest LDT. Thus far, FOX has been developed as an offensive COA generation tool but can be generalized to generate optimized defensive COAs as well. FOX currently supports common ground forces including mechanized infantry and armored units. However, given the essential similarity of features used to describe functional elements across all echelons (e.g., firepower, speed of movement, size, etc.), adaptation to other scenarios is expected to be straightforward.

In the current version of FOX for eCOA generation, eCOAs are characterized in terms of the specific allocation of subordinate units (resolved down to the level of companies) to avenues of approach and the assigned missions of those units, the allocation of general (brigade-level) resources to subordinate units, and the specifics of doctrinal rules of combat (e.g., criteria for use of reserve forces etc.). FOX takes as input a configuration of enemy units (companies) along a particular LDT and then searches through the space of possible eCOAs to find one maximizing a fitness measure reflecting remaining endgame enemy strength and amount of terrain captured. The optimization is accomplished using the framework of genetic algorithms (GAs) via the following process: 1) an initial population of offensive or defensive (enemy) eCOAs is created; 2) each of these eCOAs is wargamed against a range of offensive (friendly) COAs; 3) each eCOA’s fitness function is evaluated; 4) the least fit eCOAs are removed from the population; 5) the genetic variation operator (e.g., mutation, cross-over) is applied.

Figure 3: FOX Genetic Algorithms-based eCOA Generation
resulting in a new population. This cycle is repeated until the fitness functions show no further improvement in outcome. Initial results using the generic scenario described above indicate that FOX can produce a variety of good eCOAs, as assessed by military intelligence analysts [3].

3.2 Fuzzy Logic for eCOA Decomposition and Threat Assessment

Fuzzy logic as proposed by Lofti Zadeh [9] provides a mathematical concept to deal with uncertainty in human decision-making. Zadeh was concerned with how humans can process imprecise non-numerical, or linguistic, information (i.e., big, small, very fast, heavy, etc.) to perform a given task. He argued that if a human can perform complex tasks with this imprecise knowledge, then a machine would also benefit from such an approach. Fuzzy logic has been successfully applied in such areas as statistical analysis, pattern recognition, image analysis, robotics, decision theory, and control theory.

Within the ITAP system, fuzzy logic is employed within the Fuzzy Logic Post-Processor (FLP2) module to perform decomposition of the FOX eCOA state vector and overall threat assessment. Specifically, the FLP2 parses and analyzes the FOX eCOA state vector to infer threat assessment information including: most likely location of enemy’s main effort; which avenue of approach is more likely; does either faction have especially favorable conditions (i.e., does one finish the battle in a strong position, when the other is especially weak); and comparative advantage of opposing forces at the end of the engagement. Based on these results, the FLP2 then updates the relative situation assessment states as specied in the IFAMP belief networks [4].

4 Performance Demonstration

Performance demonstration of the ITAP system involved addressing threat assessment for a specific tactical scenario. The scenario is a ground force-on-force friendly offensive/enemy defensive tactical scenario in which a regimental size enemy force will be defending in region somewhere between demarcated by four phase lines (PL). The friendly brigade task force’s mission is to seize a key piece of terrain dubbed OBJ JODI. Demonstration results are presented in turn for the FOX eCOA generation and for the FLP2 eCOA decomposition and threat assessment.

4.1 FOX Performance Demonstration

FOX was run with varying inputs, specifically related to likely friendly COAs, initial strength level for enemy forces, and whether enemy forces were dug in for defensive purposes or were mobile for attack purposes. Friendly COA variation is related to which avenue of approach (or route) the friendly forces choice to attack, i.e., either attacking from the north or south. Initial strength level for enemy forces was based on an assumption of the effectiveness of prior friendly force infiltration attack as specified by the scenario.

Figure 4 shows the final frame from a FOX generated eCOA. The eCOA here is assuming that friendly forces (denoted by the darker colored unit icons) take a southerly approach and enemy (denoted by the lighter colored unit icons) forces are in an attack mode. In the course of this eCOA, enemy forces take the northern avenue of approach to engage a friendly supporting attack, whilst leaving the key terrain area (OBJ JODI) undefended. What results in the final frame of this eCOA, as shown in figure 4, is that the friendly forces are able to take the objective area (labeled OBJ JODI), albeit with some losses. The end strengths of the individual units is denoted by the bar level on the right side of the individual unit icons. A level the same height as the icon denotes full unit strength, while no level denotes that unit has been destroyed (e.g. the three enemy units located near the objective area).

Figure 5 shows the corresponding final frame when the enemy forces stay in a purely defensive posture. The assumption here is that the friendly main attack effort is proceeding from the southerly route with a support attack in the northerly route. As shown, the enemy forces inflict heavy damage on the friendly forces and are able to defend the key terrain area. Similar results are also noted.
when the friendly main and support attacks switch approaches. Using the FOX GA-based optimizations of enemy COAs provides an automated method for the generation of viable and distinctive eCOAs. These eCOAs are optimized for the given situation (e.g. initial unit strengths, current avenue of approach taken, etc.) and order of battle. With the GA mechanism, the capability exists to wargame thousands of eCOAs, thus providing a valuable tool for threat assessment. Additionally, capability exists to use this mechanism to enhance perception management functionally. That is, use the tool in a what-if mode by iteratively determining the input friendly COA that will generate a desired (form the friendly perspective) eCOA. The issue then becomes how can the friendly forces make the enemy forces perceive that the determined friendly COA is the one currently being executed, i.e. a perception management problem.

4.2 FLP2 Performance Demonstration

Figure 6 shows FLP2 sample performance demonstration results for decomposing FOX eCOA information into threat assessment information. The output compares two generated eCOAs and determines how best to update a belief network for situation assessment. The rulebase implemented for this demonstration had approximately thirty rules for eCOA decomposition. Specific elements addressed within the rulebase included avenue of approaches taken by enemy forces, comparison of initial versus end strengths for both opposing forces, types of units employed in the eCOA, determination of main effort, possible location of obstacles (e.g. tank barriers), and vulnerability analysis. All this information was weighted and a determination of which eCOA to pick was based on the favorability from the enemy forces' perspective.

From our preliminary research, we conclude that the human-like reasoning provided by fuzzy rule-based processing provides a strong method for post-processing enemy courses of action and identifying their weaknesses.

Figure 5: Example FOX Generated eCOA from Tactical Scenario – Enemy Defending

---

**Processing enemy's course of action...**

**First eCOA:**
- Blue has 4 units in conflict with 4 red units.
- The blue force retains some to most of its initial strength.
- Final strength comparison: blue and red forces are of similar strength.

**General information:**
- South AA is left undefended in this scenario.
- Conditions appear equally favorable for both forces.
- Main resistance is likely to be in the north AA.

**Processing enemy's course of action...**

**Second eCOA:**
- Blue has 4 units in conflict with 4 red units.
- The blue force retains some to most of its initial strength.
- Final strength comparison: blue forces are somewhat weaker than red forces.

**General information:**
- North AA is left undefended in this scenario.
- Conditions appear equally favorable for both forces.
- Main resistance is likely to be in the south AA.

**Comparison of eCOAs:**
- Updated the main effort and obstacle location nodes of the belief net based on the second COA, which had a higher enemy end strength.
- The main effort node was updated with a 2.25 to 1.0 ratio of AA livelihoods, and the obstacle node was updated with a 1.1 to 1.0 ratio.

Figure 6: FLP2 Sample Results for eCOA Decomposition
and strengths. The rulebase proved itself consistently able to judge whether one or another side had a distinct advantage in battle, and where an avenue of attack was left unguarded. Future expansions of the rulebase will include more extensive pattern-matching algorithms to more accurately characterize enemy attack patterns.

5 Conclusions

The performance demonstration results demonstrate the feasibility of the genetic algorithm paradigm for predicting the most likely course of battle in a tactical scenario. FOX's capacity to wargame thousands of eCOA instances greatly enhances the overall threat assessment capability of IFAMP/ITAP, and has significant potential as a perception management tool. The genetic algorithm allows for the generation of viable, optimized COAs in a short span of time, and functions as a valuable aid to the human cognition process.

The preliminary GA-based methodology for eCOA prediction described in this paper can be enhanced in many ways. The two most promising enhancement paths are extension of the wargamer to allow for different types of units that are not currently supported (e.g. air assets) while incorporating additional features such as terrain detail, and expanding FOX to address non-standard scenarios such as asymmetric warfare.

From this preliminary research, one can also conclude that the human-like reasoning provided by fuzzy rule-based processing provides a strong method for post-processing enemy courses of action and identifying their weaknesses and strengths. The rulebase proved itself consistently able to judge whether one or another side had a distinct advantage in battle, and where an avenue of attack was left unguarded. Future expansions of the rulebase will include more extensive pattern-matching algorithms to more accurately characterize enemy attack patterns.

Acknowledgements

The work detailed in this paper was performed under USAF Contract C30602-99-C-0101. The authors thank the Technical Monitor, Mr. Michael Hinman, of the Air Force Research Laboratory Information Directorate (Rome, NY) for his guidance and support.

References