Developing Goals Directed Search Models Empowering Strategies Against Single Ownship Air Threats

Edward Pogossian	Dany Dionne	Arthur Grigoryan	Jean Couture	Elisa Shahbazian
Cognitive Algorithms &Models Lab., IPIA, Academy of Sciences, State Eng. University of Armenia epogossi@aua.am	R&D Department, Lockheed Martin Canada dany.dionne@gmail.com	Cognitive Algorithms &Models Lab., IPIA, Academy of Sciences of Armenia grigoryan.arthur@gmail.com	R&D Department, Lockheed Martin Canada jean.couture@lmco.com	OODA Technologies Inc .elisa.shahbazian@ooda.ca

ABSTRACT

This paper studies the construction of expert knowledge-based game models with the objective of increasing effectiveness of naval defense strategies against threats.

Game trees are generated for a simplified single ownship scenario that includes: uncertainty in the output of defense actions, varying time intervals for actions, and irregular undertaking of the actions. Experiments with deliberative planning with the game model demonstrated increased probabilities of survival of the ownship with respect to the worst-case situation.

1. INTRODUCTION

1.1. The objective of the paper is to develop effective decision-making systems for both defense and terrorism problems. The paper demonstrates increased effectiveness of strategies against threats elaborated from expert knowledge.

The work was realized in framework of the NATO Program of Security Through Science for Defense Against Terrorism, by IPIA, Academy of Sciences of Armenia and Centre for Research in Mathematics at the University of Montreal, Canada.

Pertaining to countermeasure against terrorism, the NATO Program identifies the following tasks:

a) Increasing timeliness and completeness of detection and identification of threat,

b) Providing an estimate of severity of threats,

c) Selecting strategies to act against the threats, and

d) Building a decision tree of all possible countermeasures against all threats and chose the most effective path in the three.

We study these tasks through the framework of games where hypotheses about solutions are known as *strategies*, where the *search space* is specified by *reproducible game trees* (SSRGT) and target solutions have to be discovered by methods able to systematic acquired knowledge about them.

For SSRGT problems it is typical to require acting according to optimal strategies, i.e. requiring that the solutions have to deliver recommendations on how to interpret the real world and how to act in it in the best way. For example, in the Intrusion Protection (IP) problem an agent - a decision-making system - stands against the intrusion by analyzing the possible strategies throughout a game tree and searching the best protection strategy.

Despite the fact, that the protection of networks has been becoming more effective, the detection of intrusions will remain the integral part of each serious secure system. There are two main categories of intrusion detection methods: the detection of anomalies [1] and the detection of abuses [3, 4].

1.2. In our approach to solve the IP problem [5] in addition to the known approaches of static identification, during the process of analyzing anomalies, the model of dynamic protection allows performing possible sceneries of intrusions and recommends the best way of protecting from them.

We define a class of *combating agents*, based on the following models and procedures:

- a game tree model for the target competition, including the sub-models of the states, actions and contractions, the rules to apply (contra)actions to the states and transform them to the new ones, descriptors of the goal states
- the optimal strategy search procedure, including the strategy planning unit, aimed to narrow the search area in the game tree, the plans quantification, their game tree based dynamic testing and the best actions selection units.

A Common Planning and Dynamic Testing methodology for combating agents is developed allowing constructing agents with the best, in the framework of corresponding game tree models, strategies. For example, for the IT problem it was outperforming system administrators and known standard protection systems in about 60% in experiments on fighting against 12 different types of known network attacks [5].

To increase the efficiency of the IGAF1 algorithm we developed its more advanced version able to acquire a range of expert knowledge in form of goals or rules and to increase the efficiency of strategy formation with increasing the amount of expert knowledge available to the algorithm. The new IGAF2 algorithm for a range of types of knowledge in form of goals and rules demonstrates strong tendency to increase the efficiency of strategy formation with increasing the amount of knowledge available to the system [6].

1.3. Defense strategies developed by Lockheed Martin Canada consist of a twofold approach:

1. Evaluating and ranking the threats based on their opportunity, capabilities and intent [7, 8].
2. Make the threat ineffective and/or remove the threats by producing reactive or deliberative engagement planning.

The ultimate goal for establishing a careful evaluation of threats is to optimize the efficiency of engagement planning that will neutralize or remove the threats. Lockheed Martin Canada has studied over the years different schemes to build engagement plans. In general, a compromise between the times allowed computing the plan and the quality of the plan must be made. Tabu search and genetic algorithms have been examined and have provided some interesting planning results but required significant amount of time when the number of threats is large, i.e. typically larger than 5 or 6.

The SSRGT methodology presented in the current project offers a promising alternate way to investigate planning. At first glance, the current engagement situation can easily be mapped for example to a chess game: ships and planes for both threats and own force represent chess pieces, which move and attack according to specific rules (e.g. speed,

maneuverability, weaponry) and pursue the goal of destroying the other force's assets or main asset.

1.4. The objectives of the project are to develop new expert knowledge based models for increasing effectiveness of defense strategies against threats, including

1. models of defense problems where class of hypotheses about solutions are strategies and space of their search is specified by game trees
2. IGAF strategy search algorithms for defense problems
3. models of expert knowledge empowering IGAF strategies against threats.

The paper presents results of adequate modeling of the one ownship air threats defense problem by SSRGT games.

2. SCENARIO

The scenario involves two parties designated "defense" and "threats", respectively. Each party contains players. Each player responds to the actions taken by the opposite party.

The defense party has a single player, i.e., the ownship.

The threats party may have several players in the form of missiles and aircrafts. The types of threat players can be regrouped into categories, e.g., missile of type xxx, aircrafts of type yyy. An additional category can be defined for threat players whose type is uncertain.

In the simplified scenario, all the threat players belong to a single category of missiles. Several threat players may attack concurrently.

The threat players are generated as follows:

a) All threat players are created at the start of the scenario.

b) The maximum number of threat players is $N_{\text{threats}}^{\max} = 8$.

c) The initial position of each threat is uniformly and randomly selected in an area of space satisfying the conditions:
- Initial range of 5 to 80 km from ownship,
- Polar angle between 0^o and 90^o (i.e, angle in the vertical plane),
- Any azimuthal angle (i.e., angle in the horizontal plane).

Assumptions:

i. It is assumed that the threats are ranked by the defense player. In the simplified scenario, the ranking function is the range: the closer the threat, the higher the rank of the threat.

ii. It is assumed that the defense player may bundle up concurrent defense actions. The admissible bundles must satisfy the engagement rules.

iii. A bundle of defense actions must ensure that only one defense action per threat is undertaken at any given time.

Each action results into a transformation in the scenario. The sets of defense actions, defense bundles, threat actions, and their associated transformation rules are assumed finite and known.

3. DEFENSE AND THREAT STRATEGIES

The objective of a defense strategy, P_D, is to prescribe a unique defense bundles for every admissible threat actions. Since the defense strategy is in general not unique, one must be selected from the known set of admissible defense strategies, S_D. The selection process requires the formulation of a defense objective and of a corresponding utility function to be maximized. The selected defense strategy is denoted $P_D^* \in S_D$.

Similarly, a threat strategy, P_T, is composed of a set that prescribes a threat action bundle for every admissible defense action. The threat strategy belongs to a known set of admissible threat strategies, S_T. A threat objective and a threat utility function are required to select a unique threat strategy.

Example:

Let S_D ={D1, D2, D3} be the set of admissible defense bundles, and let S_T ={T1, T2, T3} be the set of admissible threat actions. One admissible defense strategy, P_D, could be

P_D = {T1->D1, T2->D2, T3->D1}

where T1->D1 means that if the threat action T1 is undertaken, the defense bundle D1 is prescribed by the defense strategy.

3.1 Objectives, utility functions, and formulation of the game

In the simplified scenario, the ownship has for primary defense objective to survive, while the primary objective of the threat party is to damage the opponent. The defense and threat objectives are described by utility functions denoted U_D and U_T, respectively.

Two utility functions are involved, one for the defense player and one for the threat players. The purpose of the defense utility function is to weight each defense strategy with respect to the defense objectives. Similarly, the threat utility function weights the threat strategies with respect to the threat objectives.

The defense utility function $U_D : P_D \times P_T \to \mathrm{R}^1$ is selected to be the probability of survival of the ownship in the worst-case scenario. The worst-case scenario is the one in which the threats and the ownship always survive to the defense and threat actions.

In the simplified scenario with a single threat action, the probability of survival is calculated as:

$$U_D(P_D, P_T) = f(P_D) \prod_{i=1}^{N_{\text{engaged}}^{\text{threats}}} \left(1 - P_{\text{kill}}^i(P_D) P_{\text{kill}}^{\text{threat}}\right)$$

where

$$P_{\text{kill}}^i(P_D) = \prod_{j=1}^{N_{\text{actions}}^i} \left(1 - P_{\text{kill}}^{\text{actions}}(i,j)\right)$$

$$f(P_D) = \begin{cases} 1, & \text{if } P_D \text{ engages the } N_{\text{engaged}}^{\text{threats}} \text{ closest threats} \\ 0, & \text{otherwise} \end{cases}$$

$$N_{\text{engaged}}^{\text{threats}} = \begin{cases} N^{\text{threats}}, & \text{if } N^{\text{threats}} \le 3 \\ 3, & \text{otherwise} \end{cases}$$

with $N_{engaged}^{threats}$ is the number of threat that can be engaged, the function $f(P_D)$ ensures that only defense strategies that engage the closest threats first are considered, $P_{\text{kill}}^i(P_D)$ is the probability that threat i is destroyed by the defense strategy P_D, and $P_{\text{kill}}^{\text{threat}}$ is the probability that the threat action destroy the ownship. The value of $P_{\text{kill}}^{\text{threat}}$ is provided later in section 5.2. The value of $P_{\text{kill}}^{\text{actions}}(i,j)$ is the probability that the threat i is destroyed by the defense action j; this value is provided later in section 5.1 for each type of action.

The threat utility function is selected to be the opposite functions $U_T = -U_D$ due to the choice of defense and threat. The utility functions being opposite functions, a zero-sum game is generated. The solution of the zero-sum game

guarantees that the utility of the defense player has at least the value U_D^*

$$U_D^* = \max_{P_D \in S_D} \min_{P_T \in S_T} U(P_D, P_T), \quad U(P_D, P_T) \square U_D(P_D, P_T),$$

provided that the defense player adopts the game optimal defense strategy P_D^*

$$P_D^* = \arg\max_{P_D \in S_D} \left\{ \min_{P_T \in S_T} U(P_D, P_T) \right\}$$

4. GAME TREE GENERATION

The naval game tree (NGT) describes all the admissible sequence of threat responses and defense responses. The branching in the NGT is generated by the capabilities of the players and the uncertainties in the game, i.e., branches are created for:

a) each category of threat players and each category of defense players,
b) each admissible defense and threat bundle of actions, and
c) each possible outcomes of the transformation rules (when the outcome of a response is uncertain).

The set of admissible defense actions depends on the current situation and how this situation is transformed by the actions. For example, some defense actions are available only when a threat is between threshold ranges. The value of these threshold ranges may vary dynamically, differ for each type of defense action, and depend on the weather conditions, the weapon setup and status, the ownship course, etc.

4.1. List of actions and their characteristics

The set of actions of NGT is defined below. The ownship can apply several defense actions concurrently in presence of several threats. These concurrent defense actions are called "bundles". The set of admissible bundle of actions will be defined in section 8 with respect to specific nominal situations.

4.2. Defense actions of ownship and Time period for completion of the defense actions

It is assumed that all the defense actions of the ownship involve a sequence of three steps:

a) search and lock on target,
b) fire and target intercept, and
c) kill assessment.

It is also assumed that fixed time periods are required for completion of the search and lock step, and of the kill assessment step.

Three types of defense action are available:

i) launch a long range surface-air missile (SAM),
ii) shoot the medium range gun,
iii) shoot the short range gun.

Each defense action requires a period of time to elapse before completion. This time period, Δt_c, is calculated as

$$\Delta t_c = \Delta t_{\text{search}} + \Delta t_{\text{fire}} + \Delta t_{\text{kill}}$$

The characteristics of the defense actions and time periods are provided by the experts.

4.3. Threat actions

It is assumed that there is a single category of threats: an anti-ship missile (ASM). This ASM has a single available threat action: directly incoming toward the ownship. The characteristics of this threat action are:

- speed : $v_{\text{ASM}} = 850$ m/s
- trajectory : straight line
- probability of kill : $P_{\text{ASM}}^{\text{kill}} = 0.50$

4.4. Rules of engagement

The rules of engagement are employed to define the set of admissible bundles of defense actions. These bundles are function of the current situation.

Several of the engagement rules stem from the fact that the SAM and the medium range gun share the same STIR. There are only two STIR available to the SAM and gun. Each STIR can track only one target at a time.

The CIWS has its own independent STIR.

4.5. List of the bundles of defense actions

The set of admissible defense action bundles, B_D, is to be constructed online in three steps:

a) select the set of possible defense action bundles, B_D^{possible}, based on the number of threats ,
b) by pruning the selected set, get a reduced set of defense action bundles admissible with respect to the position of the threats, $B_D^{\text{position}} \subset B_D^{\text{possible}}$, and
c) get the set if admissible defense action bundles by pruning again with respect to the current status of the weapons and STIR, $B_D \subset B_D^{\text{position}}$.

Admissible bundles of ***defense actions*** are provided by the tables 1, 2 and 3 provided by ***experts*** (EDA):

1. List of possible defense action bundles with respect to the number of threats. Notice that there are six types of actions associated with the medium range gun, i.e., one for each type of salvo
2. List of possible defense actions with respect to the position of a single threat. There are a total of eight possible actions: SAM, CIWS, and six types of gun's salvo. The set of possible defense actions depends on the range of the threat and on its azimuthal ($\theta = 0$ looking forward) and polar angles ($\phi = 90$ looking upward)
3. Possible defense actions with respect to the weapons and STIR status.

4.6. Transformation rules

The transformation rules describe the outcome of the defense and threat actions.

In this scenario, the outcome of all the defense and threat actions is uncertain. The outcome can be one of two possibilities: (i) the opponent is destroyed, or (ii) the opponent survived. Hence,

a. Transformation rules of defense actions
   i) the threat is destroyed with probability P_{kill}, or
   ii) the threat survived with probability $1 - P_{\text{kill}}$

b. Transformation rules of the threats' action
   i) the ownship is destroyed with probability P_{kill}, or
   ii) the ownship survived with probability $1 - P_{\text{kill}}$

4.7. Time discretization of the scenario

The simplified scenario requires decisions about actions at discrete point in time. The time interval between decisions varies with respect to the situation.
A decision is required in the following situations:

a) at the moment a threat crosses one of the threshold ranges, and
b) at the instant a currently engaged defense action gets completed, see section 0.

5. GENERATION of ALL POSSIBLE STRATEGIES

5.1. Algorithm of generation of NGT strategies

strategies (GNGTS) works in the following 8 steps:

1. Create lists L1, L2 of subtrees of NGT
2. Add root node of NGT to L1
3. For any tree Ti from L1 find the most left node K with the depth not exceeding given max H and allowing to add new nodes from NGT. If K exist go to the step 4 otherwise to 8
4. Generate list DK = {DK1,...,DKn} of all nodes incidental to K by the **Procedure of Relevant Actions** for situations of NGT. If DK is not empty go to 5 otherwise to 3
5. For any DKj, j=1,n , Ti and K create a new tree NTj by adding DKj to the node K in Ti and add NTj to the list L2
6. Copy L2 to L1
7. Clean L2
8. End the work.

The Procedure of Relevant Actions for situations of NGT is based on the EDA tables 1-3 which filter the actions in the following 3 steps:

1. table 1 filters the set BS1 of all bundles {SAM_F, GUN_4S_F, SAM_B} having more than one weapon and common illuminator
2. table 2 filters the set BS2 of all bundles for single threats satisfied to conditions of their actual applications
3. table 3 filters the set BS3 of all bundles in accordance with the state of motion and STIR status.

BS3 comprise the set of permit table defense actions.
Let's prove that the above algorithm GNGTS provides all possible strategies of NGT

5.2. Proposition. Given situation S and max depth H of analysis of strategies of NGT algorithm GNGTS guarantees generation of all strategies rooted in S.

Preposition. *Given situation S and max depth H of analysis of the strategies of NGT the above algorithm GNGTS guarantees the generation of all NGT strategies rooted in S.*

Proof.
Let's prove by contradiction.
Assume there is a strategy Ti not generated by the algorithm and Ck= S, S1, …, Sk is a chain in Ti from S to Sk.
In accord with the step 4 of the algorithm all incidental to S nodes including S2 will be generated due the edge (S, S1) couldn't exist in the game tree NGT if (S, S1) is not legally generated action from the node S in the NGT.
Thus, the algorithm will generate an intermediate tree T1 with the chain C1=S, S1.
Analogically, for the node S1 the tree T2 will be generated with the chain C2=S,S1,S2.
Eventually, this reasoning brings to generating by the algorithm of the tree Tk with the chain Ck.
Therefore, there is no chains of any strategy not generated by the algorithm what proves the preposition.

6. EXPERIMENTS

The results of experiments with searching the best strategy in the NGT for a single ownship are provided in the table below.
It appears that for the case when waiting conditions are ignored search time in the NGT for the best strategies is significantly less compared with ones for TABU system [10].

Initial data for the threats	Utility of the optimal defense strategy/ Probability of survival of the ownship)	Maximal deepness of the game tree search
$r(0) = 60$ km $\theta = 90^o$ $\phi = 45^o$	U = 0.4844	H = 4
$r_1(0) = 60$ km $r_2(0) = 70$ $\theta_1 = 30^o$ $\theta_2 = 20$ $\phi_1 = 45^o$ $\phi_2 = 45$	U = 0.4793	H = 6
$r_1(0) = 65$ km $r_2(0) = 70$ $\theta_1 = 90^o$ $\theta_2 = 30$ $\phi_1 = 40^o$ $\phi_2 = 150$	U = 0.4691	H = 6

Here is the listing of calculations for the second example of the table:

```
Navy system builds 1.0.1
Enter Treats count 2
Enter Treat1 distance in meters 60000
Enter Treat1 Fi angle degrees 45
Enter Treat1 Teta angle degrees 30
Enter Treat2 distance in meters 70000
Enter Treat2 Fi angle degrees 45
Enter Treat2 Teta angle degrees 20

Best Strategy Mark = 0.480043

    Current Knot Util = 1
    Start at time = 0
    isa destroyed Treat1 = 0;
    isa destroyed Treat2 = 0;
    {SAM_F , NO_WEAPON }
        Current Knot Util = 0.1875
        Start at time = 55.1972
        isa destroyed Treat1 = 0;
        isa destroyed Treat2 = 0;
        {SAM_F , NO_WEAPON }
            Current Knot Util = 0.
            Start at time = 69.808
            isa destroyed Treat1 =
            isa destroyed Treat2 =
            {NO_WEAPON , GUN_4S_F
                Current BRANCH
            isa destroyed Treat1 =
            isa destroyed Treat2 =
            Current Knot Util = 0.
            Start at time = 69.808
            isa destroyed Treat1 =
```

isa destroyed Treat2 =
{NO_WEAPON , GUN_4S_F
Current BRANCH
isa destroyed Treat1 =
isa destroyed Treat2 =
Current Knot Util = 0.1875
Start at time = 55.1972
isa destroyed Treat1 = 0;
isa destroyed Treat2 = 0;
{SAM_F , NO_WEAPON }
Current Knot Util = 0.
Start at time = 69.808
isa destroyed Treat1 =
isa destroyed Treat2 =
{NO_WEAPON , GUN_4S_F
Current BRANCH
isa destroyed Treat1 =
lic, 20-22 October 2003

7. CONCLUSION

Definition of a simplified naval defense scenario with multiple threats is considered.

Generation of the game three for the simplified single ownship scenario is provided overcoming the following main difficulties:

- The output of the defense actions is uncertain. There are two possible outputs with known realization probabilities,
- The time interval for completion of a defense action is different from one defense action to another,
- Several defense actions can be undertaken simultaneously, and
- A defense action can be undertaken while other defense actions are still ongoing.

The reactive planning solution is implemented to serve as a comparison baseline (to assess the benefits of deliberative planning).

It is shown that solution of the game tree for deliberative planning maximizes the probability of survival of the ownship with respect to the worst-case situation.

Scenarios with up to 8 threats are considered. Monte Carlo simulations are employed to statistically assess the benefits of the proposed deliberative planning.

REFERENCES

[1] Chi, S.-D., Park, J.S., Jung, K.-C., Lee, J.-S.: Network "Security Modeling and Cyber Attack Simulation Methodology", *Lecture Notes in Computer Science*, Vol.2119 2001.

[2] V. Gorodetski, I. Kotenko, "Attacks against Computer Network: Formal Grammar Based Framework and Simulation" *Tool. Proc. of the 5 Intern. Conf. "Recent Advances in Intrusion Detection", Lecture Notes in Computer Science*, vol. 2516, Springer Verlag, pp.219-238, 2002.

[3] K. Ilgun, R.A. Kemmerer, P.A. Porras, "State Transition Analysis: A Rule-Based Intrusion Detection System", *IEEE Trans. Software Eng.* vol. 21, no. 3, Mar. 1995

[4] V. Paxson, Bro, "A System for Detecting Network Intruders in Real-Time, Proc", *Seventh Usenix Security Symp., Usenix Assoc., Berkeley*, 1998

[5] E. Pogossian, A. Javadyan, "A Game Model For Effective Counteraction Against Computer Attacks In Intrusion Detection Systems", *NATO ASI 2003, Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Management*, Tsahkadzor, Armenia, August 19-30, 2003, pp.30.

[6] E. Pogossian, A. Javadyan, E. Ivanyan, "Effective Discovery of Intrusion Protection Strategies" *The International Workshop on Agents and Data Mining, St. Petersburg, Russia, 2005, Lecture Notes in Computer Science*, Vol. 3505, pp. 263-274

[7] J. Couture, E. Menard, "Issues with Developing Situation and Threat Assessment Capabilities", *Data Fusion Technologies for Harbour Protection, NATO Advanced Research Workshop, Tallinn, Estonia*, June 27-July 1, 2005.

[8] E. Menard, J. Couture, "Application of Improved Threat Evaluation for Threat Assessment, Multisensor Data and Information Processing for Rapid and Robust Situation and Threat Assessment", *NATO Advanced Study Institute, Albena, Bulgaria*, 16-27 May, 2005.

[9] D.Boily, "Agent Based Resource Management Simulation", *NATO Advanced Study Institute on "Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Management", Tsakhkadzor, Armenia*, 18-29 August 2003 (to be published by Kluwer Academic Publishers).

[10] D. Blodgett, M. Gendreau, F. Guertin, J.-Y. Potvin, Y. Seguin, "A Tabu Search Heuristic for Resource Management in Naval Warfare", *Centre for Research on Transportation, internal publication* No.98-63.

[11] P. Bergeron, J. Couture, J.-R. Duquet, M. Macieszczak, M. Mayrand, "A New Knowledge-Based System for the Study of Situation and Threat Assessment in the Context of Naval Warfare" *FUSION 98, Las Vegas*, Vol II, pp.926-933, 6-9 July 1998.

[12] E. Shahbazian, B. Chalmers, P. Bergeron, J.-R. Duquet, "Situational Awareness in the Tactical, Air Environment", *Paul Hall Center, Piney Point, Maryland*, pp. 57-77, June 8 & 9, 1999,

[13] E. Shahbazian, L. Baril, E. Menard, G. Michaud, D. Turgeon, "Analysis of Adaptive Data Fusion Approaches within LM Canada's Technology Demonstrator", *NATO RTO Symposium in Prague, Czech Repub*