Double-loop GA for determining the Nash equilibrium solutions

Gregory Levitin
The Israel Electric Corporation Ltd., Haifa

Email: levitin@iec.co.il
web page: http://iew3.technion.ac.il/~levitin

Kjell Hausken
Faculty of Social Sciences, University of Stavanger, Norway
Email: kjell.hausken@uis.no
web page: http://www1.uis.no/vit/oks/hausken/

Abstract. The paper suggests a GA – based approach for optimizing the defense of complex multi-state series-parallel systems. It considers a generalized model of damage caused to a system by intentional attack assuming that the defender has multiple alternatives of defense strategy that presumes separation and protection of system elements. The attacker also has multiple alternatives of his attack strategy based on combination of different possible attack actions against different groups of system elements. Both the attacker and the defender try to maximize their utilities that depend on their strategies' cost and on the expected damage caused by the attack. The problem is defined as a non-cooperative game between the attacker and the defender. An optimization algorithm is presented that uses a universal generating function technique for evaluating the losses caused by system performance reduction, and a genetic algorithm for determining the Nash equilibrium solution.

Key words: game theory, survivability, optimization, defense, attack, protection, separation, genetic algorithms.

1 INTRODUCTION

This paper considers a situation where a defended system is composed from components consisting of elements with different performance and reliability. The defender can separate the elements and protect them using different protection actions. The attacker can use different combination of attack actions against separated and protected groups of elements. For each protected group of elements the attack success probability (probability of the group destruction) is determined for every combination of protection and attack actions. The damage caused by the attack is associated with partial system incapacitation (reduction of the overall system performance) and with the losses of inherent value of the destroyed system elements.

Both the defender and the attacker have perfect knowledge about the system and the strategies of each other. Both choose their optimal strategies. This means considering the situation as a non cooperative game between two agents. A two-loop genetic algorithm is used to find the Nash equilibrium solutions [1] of the game.

2 THE MODEL

2.1 Defender's and attackers strategies

The system consists of N statistically independent components composing a series-parallel configuration. Each component n consists of K_n elements of the same functionality connected in parallel. Each element k in component n is characterized by its inherent value assessed by the defender and the attacker (w_{nk} and W_{nk} respectively), nominal performance x_{nk}, and availability p_{nk}. The states of the elements are independent.

The elements within any component can be separated (to avoid the entire component destruction by a single attack). Parallel elements not separated from one another are considered to belong to the same protection group (PG). The PGs can be protected. All the elements belonging to the same PG are destroyed by the same successful attack. More than one PG cannot be destroyed by a single attack. Without separation, either all elements or no elements within the component are destroyed.

Because system elements with the same functionality can have different performance rates, and different availability, the way the elements are distributed among the PGs affects the system survivability. The element separation problem for each component n can be considered as a problem of partitioning a set Φ_n of K_n items into a collection of M_n mutually disjoint subsets Φ_{nm}, i.e. such that

$$\bigcup_{m=1}^{M_n} \Phi_{nm} = \Phi_n, \tag{1}$$

$$\Phi_{ni} \cap \Phi_{nj} = \varnothing,\ i \neq j. \tag{2}$$

Each set can contain from 0 to K_n elements. If $|\Phi_{nm}|=K_n$, and $|\Phi_{nk}|=0$ for any $k\neq m$, all of the elements of component n are gathered within a single PG; if $|\Phi_{nm}|\leq 1$ for any m, all of the elements are separated. The total number of PGs in a component must not be equal to or less than the number of elements in the component because some PGs can remain empty, being used as false targets for the attacker.

The partition of the set Φ_n can be represented by the vector $\{\gamma_{nk}, 1\leq k\leq K_n\}$, where γ_{nk} is the number of the subset to which element k belongs ($1\leq\gamma_{nk}\leq M_n$). The matrix $\boldsymbol{\gamma}$ of values γ_{nk} for $1\leq k\leq K_n$, and $1\leq n\leq N$ determines the elements' distribution among the protection groups for the entire system (separation strategy of the defender).

For each PG belonging to component $n,$ there are e_n+1 available protection actions. For example, the same group of elements can be located outdoor (cheapest, but most vulnerable protection), within a shed, or in an underground bunker (most expensive, but most effective protection). Each protection of type β_{nm} ($0\leq\beta_{nm}\leq e_n$) is characterized by its cost. The protection cost of any PG m in component n can also depend on the number of elements it comprises: $c_n(\beta_{nm},|\Phi_{nm}|)$. Protection action $\beta_{nm}=0$ corresponds to the absence of any protection. The cost of protection action 0 can be greater than zero because it represents the cost of the common infrastructure of the PG (the separation usually requires additional areas, constructions, communications, etc.)

The matrix $\boldsymbol{\beta}$ of the values of β_{nm} chosen for any PG $m,$ and component $n,$ represents the entire protection strategy of the defender.

The entire defender's defense strategy is defined as $\boldsymbol{\chi}=\{\boldsymbol{\gamma},\boldsymbol{\beta}\}$. Accounting for the overhead cost $o(\boldsymbol{\chi})$ (personnel, equipment, training, maintenance, facilities, transport, fuel, electricity, etc.) of defending the system, the total cost of the system defense strategy (separation and protection) $\boldsymbol{\chi}$ can be determined as

$$c(\boldsymbol{\chi})=o(\boldsymbol{\chi})+\sum_{n=1}^{N}\sum_{m=1}^{M_n} c_n(\beta_{nm},|\Phi_{nm}|). \tag{3}$$

It is assumed that only a single attack is possible against each PG since the attack leads to the attacker being detected and disabled [1,2]. The attacker has a set of E_n+1 available attack actions against any component n. For example, the same target (PG) can be attacked by a suicide bomber, by missiles with different types of warhead etc.

The strategy of the attacker can be represented by matrix $\boldsymbol{\alpha}=\{\alpha_{nm} \mid 1\le n\le N, 1\le m\le M_n\}$. Each attack action α_{nm} ($0\le\alpha_{nm}\le E_n$) is characterized by its cost $C_n(\alpha_{nm})$. If $\alpha_{nm}=0$ the PG m of component n is not attacked. The cost of attack action 0 is $C_n(0)=0$.

Accounting for the overhead cost $O(\boldsymbol{\alpha})$ of attacking, the total attack cost is

$$C(\boldsymbol{\alpha})=O(\boldsymbol{\alpha})+\sum_{n=1}^{N}\sum_{m=1}^{M_n}C_n(\alpha_{nm}). \tag{4}$$

Having the protection strategy $\boldsymbol{\beta}$ and the attacker's strategy $\boldsymbol{\alpha}$, one can obtain the probability of destruction for any PG m in component n as $v_n(\beta_{nm},\alpha_{nm})$. This function can be elicited from previous experience or from the expert opinion and can be represented in a table form for each component. It is obvious that $v_n(\beta_{nm},0)=0$.

For any given defender's strategy $\boldsymbol{\chi}$, and attacker's strategy $\boldsymbol{\alpha}$, one can determine the probabilistic distribution of the entire system performance (pmf of random value G) in the form g_s, $q_s(\boldsymbol{\alpha},\boldsymbol{\chi})=\Pr(G=g_s)$ ($1\le s\le S$) using the algorithm presented in [4]).

If the system totally fails when its performance becomes lower than the demand (and the entire demand F is not supplied), the expected cost of the damage is accessed by the defender and attacker as

$$\begin{aligned}\delta(\boldsymbol{\alpha},\boldsymbol{\chi},F) &= hF\sum_{s=1}^{S}q_s(\boldsymbol{\alpha},\boldsymbol{\chi})\cdot 1(g_s<F),\\ \Delta(\boldsymbol{\alpha},\boldsymbol{\chi},F) &= HF\sum_{s=1}^{S}q_s(\boldsymbol{\alpha},\boldsymbol{\chi})\cdot 1(g_s<F).\end{aligned} \tag{5}$$

If the damage associated with the system performance reduction below the demand F is proportional to the unsupplied demand, the expected cost of the damage is accessed by the defender and attacker as

$$\begin{aligned}\delta(\boldsymbol{\alpha},\boldsymbol{\chi},F) &= h\sum_{s=1}^{S}q_s(\boldsymbol{\alpha},\boldsymbol{\chi})\max(F-g_s,0),\\ \Delta(\boldsymbol{\alpha},\boldsymbol{\chi},F) &= H\sum_{s=1}^{S}q_s(\boldsymbol{\alpha},\boldsymbol{\chi})\max(F-g_s,0).\end{aligned} \tag{6}$$

The total expected damage caused by the attack should include the cost of losses associated with system performance reduction, and losses of inherent values of the destroyed elements and the infrastructure. The costs of the total expected damage are

$$\begin{aligned}d(\boldsymbol{\alpha},\boldsymbol{\chi},F) &= \sum_{n=1}^{N}\sum_{m=1}^{M_n}v_n(\alpha_{nm},\beta_{nm})(y_{nm}+\sum_{k\in\Phi_{nm}}w_{nk})+\delta(\boldsymbol{\alpha},\boldsymbol{\chi},F),\\ D(\boldsymbol{\alpha},\boldsymbol{\chi},F) &= \sum_{n=1}^{N}\sum_{m=1}^{M_n}v_n(\alpha_{nm},\beta_{nm})(Y_{nm}+\sum_{k\in\Phi_{nm}}W_{nk})+\Delta(\boldsymbol{\alpha},\boldsymbol{\chi},F).\end{aligned} \tag{7}$$

The utilities of the defender and the attacker are

$$\begin{aligned}u(\boldsymbol{\alpha},\boldsymbol{\chi},F) &= -d(\boldsymbol{\alpha},\boldsymbol{\chi},F)-c(\boldsymbol{\chi}),\\ U(\boldsymbol{\alpha},\boldsymbol{\chi},F) &= D(\boldsymbol{\alpha},\boldsymbol{\chi},F)-C(\boldsymbol{\alpha})\end{aligned} \tag{8}$$

Both the defender and attacker seek to maximize their utilities.

2.2 The Nash equilibria

We assume that both the defender and the attacker have perfect knowledge about each other’s strategies and that no binding agreements are allowed. A Nash equilibrium [1] arises when neither the defender nor the attacker prefers to deviate unilaterally to another strategy. The definition of this equilibrium is

$$u(\boldsymbol{\alpha}^*,\boldsymbol{\chi}^*,F)\geq u(\boldsymbol{\alpha}^*,\boldsymbol{\chi},F) \text{ for all } \boldsymbol{\chi}\in\boldsymbol{X},\ c(\boldsymbol{\chi})\leq b,$$
$$U(\boldsymbol{\alpha}^*,\boldsymbol{\chi}^*,F)\geq u(\boldsymbol{\alpha},\boldsymbol{\chi}^*,F) \text{ for all } \boldsymbol{\alpha}\in\boldsymbol{A},\ C(\boldsymbol{\alpha})\leq B, \quad (9)$$

where $\boldsymbol{X}$ and $\boldsymbol{A}$ are sets of possible defender's and attacker's strategies respectively, b and B are defender's and attacker's budgets. This means that the Nash equilibrium is a profile of strategies ($\boldsymbol{\alpha}^*,\boldsymbol{\chi}^*$) such that each agent's strategy is an optimal response to the other agent's strategy.

When the damage is evaluated the same by the defender and the attacker ($h=H$, $w_{nk}=W_{nk}$, $y_{nm}=Y_{nm}$ for any n and m), and the defender and attacker have budgets that are much less than the expected damage, the definition of the equilibrium can be as follows:

$$D(\boldsymbol{\alpha}^*,\boldsymbol{\chi}^*,F)\leq D(\boldsymbol{\alpha}^*,\boldsymbol{\chi},F) \text{ for all } \boldsymbol{\chi}\in\boldsymbol{X},\ c(\boldsymbol{\chi})\leq b,$$
$$D(\boldsymbol{\alpha}^*,\boldsymbol{\chi}^*,F)\geq D(\boldsymbol{\alpha},\boldsymbol{\chi}^*,F) \text{ for all } \boldsymbol{\alpha}\in\boldsymbol{A},\ C(\boldsymbol{\alpha})\leq B, \quad (10)$$

Nash equilibria are determined by running through the $|\boldsymbol{X}|\times|\boldsymbol{A}|$ available strategy combinations and systematically excluding dominated strategy combinations as specified by (9). Those strategy combinations ($\boldsymbol{\alpha}^*,\boldsymbol{\chi}^*$) that remain, of which there is at least one but may be several, are Nash equilibria.

3 NASH GA TECHNIQUES

Proceeding systematically through all the $|\boldsymbol{X}|\times|\boldsymbol{A}|$ available strategy combinations to determine all the Nash equilibria for complex systems is an arduous task even for today's supercomputers. When facing complexity, heuristic search procedures are often called for. One way around this challenge is to apply genetic algorithms (GAs) which have proven successful in many areas including reliability optimization [5,6] and game theory [7]. The genetic algorithm developed in this section uses the damage function (10), assumed equal for the defender and the attacker. The budget constraints are binding for both agents.

3.1 Solution encoding

The GA requires solution representation in the form of strings. Any defense strategy $\boldsymbol{\chi}=\{\boldsymbol{\gamma},\boldsymbol{\beta}\}$ can be represented by concatenation of n integer strings $\{\gamma_{nk},\ 1\leq k\leq K_n\}$, and n integer strings $\{\beta_{nm},\ 1\leq m\leq M_n\}$ for $1\leq n\leq N$. The total length of the solution representation string is $2\sum_{n=1}^{N}K_n$. The substring $\boldsymbol{\gamma}$ determines the distribution of elements among protection groups, and the substring $\boldsymbol{\beta}$ determines types of protections chosen for the PG. Because the maximal possible number of protections is equal to the total number of elements in the system (in the case of total element separation), the length of substring $\boldsymbol{\beta}$ should be equal to the total number of the elements. If the number of PG defined by substring $\boldsymbol{\gamma}$ is less than the total number of system elements, the redundant elements of substring $\boldsymbol{\beta}$ are ignored.

Any attack strategy $\boldsymbol{\alpha}$ can be represented by concatenation of n integer strings $\{\alpha_{nm},\ 1\leq m\leq M_n\}$ for $1\leq n\leq N$.

3.2 Double-GA approaches for finding the Nash equilibria

First the GA was applied for finding the Nash equilibrium in a non-cooperative game with 2 players in [8,9]. In terms of the problem considered in this paper the approach works as follows. Let $\boldsymbol{\chi}$, $\boldsymbol{\alpha}$ be the concatenation of strings representing the potential solution (defender's and attackers strategy) for a dual objective optimization function (game), where u corresponds to the first criterion and U to the second one. The optimization task $u\rightarrow$max is assigned to GA1 and the optimization task $U\rightarrow$max to

GA2. Thus, GA1 optimizes χ with respect to the u criterion, while α is fixed. Symmetrically, GA2 optimizes α with respect to the U criterion, while χ is fixed. GA1 and GA2 are multistage procedures. Let χ_{k-1} be the best value found by GA1 at stage k -1, and α_{k-1} be the best value found by GA2 at stage k -1. At stage k, GA1 optimizes χ for fixed α_{k-1} and GA2 optimizes α for fixed χ_{k-1} . After the optimization process, GA1 sends the best value of χ (χ_k) to GA2 which will use it at stage k+1. Similarly, GA2 sends the best value of α (α_k) to GA1 which will use it at stage k +1. Nash equilibrium is reached when neither GA1 nor GA2 can further improve their criteria.

This alternating GA approach is effective in finding solutions of continuous problems with a single Nash equilibrium point. Being tested on the combinatorial problems (like one presented in this paper) it demonstrated no convergence to the Nash equilibria.

The following simple examples illustrate the fact that the alternating GA cannot guarantee finding equilibrium solutions of combinatorial problems. Let $|\boldsymbol{X}|=|\boldsymbol{A}|=3$. Table 1 illustrates applying the formulation in (9) with utilities (u,U) to the defender and attacker, and Table 2 illustrates applying the formulation in (10) with damage D for the defender and attacker.

		Attacker		
		α_1	α_2	α_3
Defender	χ_1	3,**9**	**4**,8	6,7
	χ_2	**8**,5	2,**16**	4,9
	χ_3	5,5	3,10	**7,12**

Table 1: 3 x 3 game with one Nash equilibrium (7,12) and utilities (u, U)

		Attacker		
		α_1	α_2	α_3
Defender	χ_1	D=14	D=4	D=10
	χ_2	D=5	D=12	D=11
	χ_3	D=7	D=6	D=8

Table 2: 3 x 3 game with one Nash equilibrium D=8 specifying the damage D

In Table 1 the bold numbers before the comma specify the defender's preferred action for each of the three attacker actions. Analogously, the bold numbers after the comma specify the attacker's preferred action for each of the three defender actions. This gives one Nash equilibrium (7,12). In Tables 1 and 2, any alternating procedure starting with χ_1, α_1 enters the infinite loop $(\chi_1, \alpha_1) \rightarrow (\chi_2, \alpha_1) \rightarrow (\chi_2, \alpha_2) \rightarrow (\chi_1, \alpha_2) \rightarrow (\chi_1, \alpha_1)$ and never reaches the equilibrium solution (χ_3, α_3).

In the case when the attacker tries to maximize and the defender tries to minimize the same expected damage subject to budget constraints (10) and the budgets are much less than the expected damage the approach that guarantees obtaining near equilibrium solution can be as follows. Apply GA1 that seeks for χ minimizing the expected damage D. For each χ generated by GA1 during the genetic search apply GA2 that seeks α maximizing D while χ is fixed. Use the obtained α with the given χ to calculate D that is used as the value of the objective function in GA1.

Consider using the suggested approach for finding equilibrium in the example presented in Table 2. For χ_1 GA2 provides solution $D(\chi_1, \alpha_1)$=14, for χ_2 GA2 provides solution $D(\chi_2, \alpha_2)$=12, for χ_3 GA2 provides solution $D(\chi_3, \alpha_3)$=8. GA1 chooses χ_3 that minimizes the damage. It can be seen that for the problem presented in Table 1 this approach also provides the equilibrium solution (7,12).

To apply the suggested double-GA a special algorithm for evaluating the expected damage *D* has been developed that minimizes computations associated with altering the attacker strategies $\boldsymbol{\alpha}$. This allowed reducing the computational burden of running GA2 for each solution of GA1. The results obtained by the suggested algorithm considerably outperform the results of the altering GA. However, for large scale problems the computation time of the suggested algorithm becomes prohibitive. Therefore developing an effective GA for obtaining Nash equilibria solutions in complex combinatorial games remains challenging task.

4 REFERENCES

[1] J. Nash, "Non-Cooperative Games", *Annals of Mathematics* **54**, 2, 286-295 (1951).

[2] V. M. Bier, A. Nagaraj, V. Abhichandani, "Protection of simple series and parallel systems with components of different values", *Reliability Engineering and System Safety* **87**, 313-323 (2005).

[3] N. Azaiez, V.M. Bier, "Optimal Resource Allocation for Security in Reliability Systems". *European Journal of Operational Research*, **181**, 2, 773-786 (2007).

[4] G. Levitin, "Optimal Defense Strategy against Intentional Attacks", *IEEE Transactions on Reliability*, **56**,1, 148-157 (2007).

[5] *Computational Intelligence in Reliability Engineering. Evolutionary Techniques in Reliability Analysis and Optimization,* G. Levitin (Ed.), Series: Studies in Computational Intelligence, Vol. 39, Springer-Verlag, 2006.

[6] G. Levitin, "Genetic Algorithms in Reliability Engineering. Guest editorial", *Reliability Engineering and System Safety*, **91**(9), pp. 975-976 (2006).

[7] R.E. Marks, "Playing games with Genetic Algorithms", In S.-H. Chen (editor), *Evolutionary Computation in Economics and Finance,* Physica Verlag, 2002.

[8] J. Periaux, H.Q. Chen, B. Mantel, M. Sefrioui, H.T. Sui, "Combining game theory and genetic algorithms with application to DDM-nozzle optimization problems", *Finite elements in analysis and design*, **27**, 417-429 (2001).

[9] M. Sefrioui, J. Periaux, "Nash Genetic Algorithms: Examples and applications", *Proceedings of the IEEE Conference on Evolutionary Computation, ICEC* 1, 509-516 (2000).