International Journal of 3D Printing Technologies and Dijital Industry
Uluslararası 3B Yazıcı Teknolojileri ve Dijital Endüstri Dergisi

SIMULATION OF A DISTRIBUTED DECISION-MAKING SYSTEM IN CYBER SECURITY

Oleksandr Milov[a]*, Stanislav Milevskyi[a], Volodymyr Aleksiyev[a]

Simon Kuznets Kharkiv National University of Economics, Economic InformaticsFaculty, Cyber Security and Information Technology Department, UKRAINE

* *Correponding Author: Oleksandr.Milov@hneu.net*

(Received: 20.04.2019**; Revised:** 21.06.2019**; Accepted:** 26.06.2019**)**

ABSTRACT

The challenges of improving the effectiveness of countering cyber-terrorism clearly demonstrated that the success of this activity is largely determined by the behavior of those who involved in this conflict.The proposed in this article approach is based on the assumption that none of the decision makers has a complete and accessible model of confrontation in a cyber-conflict. More precisely, each agent knows about the actions of a separate part of the system for which he is an "expert". Therefore multiagent distributed decision-making models were proposed to face that challenges.

Keywords: Decision making.Agent. Cybersecurity. Distributed structure.

1. INTRODUCTION

The need to address the challenges of improving the effectiveness of countering cyber-terrorism clearly demonstrated that the success of this activity is largely determined by the behavior of those who involved in this conflict. Therefore, one of the most promising areas is the study of both the forms of conflict between the parties, and the methods of joint activity of each of the opposing parties of the conflict. The most promising tools of such a study are the methods of simulation, among which the last time should be noted the methods of agent-oriented modeling.

When designing agent-oriented models, it is important to answer the question of how to model decision-making processes by agents of the parties to the conflict, because, as practice shows, it is the behavioral aspects of the parties to the conflict that are decisive in achieving the goals of each party.

2. LITERATURE REVIEW

A large number of models of decision making by the agent can be found in the literature, each of which is inspired by different goals and research questions. In [1], a review of 14 architectures of decision-making agents that attracted the interest of researchers was presented. They range from rule-based production systems to psychological-neurological approaches. For each of the architectures, an overview of its structure is given, research questions are highlighted, which were answered with its help, and the reasons for choosing the decision-making model provided by the creators are presented. The purpose of this fundamental review was to provide recommendations to choose decision-making models of the agent, their level of simplicity or complexity, that can be used for different research question.

The behavioral aspects of attack results are presented in [2-4] and the relationship between cyber-attacks and the decision-making process is modeled. The methods of real modeling are presented to stimulate the expected behavior, in particular the effects of cyber-attacks on decision-making. The authors present a set of cyber-attack and protection parameters that can be used to assess the impact of cyber-attacks on

human behavior and vice versa.

In [5], researchers describe the motivation and "profile" of various types of hackers in order to better understand their behavior and improve the defense position of enterprises. A prognostic model was also developed to categorize people as hackers or potential hackers in order to predict a person's susceptibility to illegal hacker behavior. The considered independent variables include age, gender, level of education, professional status and personal moral philosophy, and the dependent variable is behavior (measured by the desire to hack into a computer system).

The mentioned works relate to the analysis and modeling of behavioral aspects of opposition in the conditions of cyber conflict. It should be noted that, first of all, the structural features of the systems are decisive in the formation of the behavior of one or another type. Therefore, it is of interest article [6]. It proposes new strategies for supporting distributed solutions that affect the most basic structures of decision support systems. For distributed decision support systems that are focused on the parties to the conflict, there are models of agent cooperation that take advantage of the opportunities offered by the latest distributed technologies. This model allows to develop dynamic, self-organizing, self-managing and self-recovering distributed decision-making and support systems.
Even a brief review of publications shows that the main focus when considering behavioral aspects is placed on the individual behavior of participants in a cyber-conflict. Therefore, it is necessary to recognize the actuality of work on the study of decision-making structures in a cyber-conflict.

3. MAIN RESULTS

Any goal-oriented activity is associated with decision-making, therefore, intuitive ideas about the content and structure of the problem of decision-making are quite obvious. This work is limited to the class of those tasks in which decisions are made by a variety of decision makers (DM), between which information necessary for decision-making is distributed, and which function in parallel, interacting with each other in the decision-making process.

Below we consider the problem of designing the structure of interaction between a group of decision makers for effective real-time management of a complex, large-scale cyber-security system. An attempt was made to combine classical concepts of decision making with approaches in the field of distributed (network) systems management. The proposed approach defines three characteristics:
1) Multidisciplinary and conceptual approach,
2) the level of detail that determines the applicability to solve any practical problem,
3) openness, which means that the proposed approach is only one of many that could be offered to solve this problem.

Thus, the work reflects the process of designing a structure in which the problems of decision-making in decentralized systems can be successfully presented. The proposed approach is based on the assumption that none of the decision makers has a complete and accessible model of confrontation in a cyber-conflict. More precisely, each agent knows about the actions of a separate part of the system for which he is an "expert". He does not know anything about the structure of the system outside his subject area; and an assessment of the impact of hiss decisions on the rest of the system and the influence of external decisions on his particular subsystem should be obtained as a result of interaction with other agents like him. Thus, the decision-making process is distributed among the decision makers, and the coordination of planned actions largely depends on the available interaction resources. The proposed structure can be used to design teams in which a person acts as one of the decision-making resources.

In order to achieve many interesting results of the centralized decision making theory, four main concepts will be used together:
1) concept of state according to Markov;
2) Bayesian probability theory law;
3) the use of a scalar index of global performance;
4) dynamic programming.

When these concepts are used for group decision makers (multiple decision makers), the following problems arise. Each agent can calculate its own conditional probabilities of process states, but dynamic programming requires knowledge of at least conditional probabilities for input signals provided by other agents. This, in turn, leads to the need for any agent to obtain models of other agents (which have memory, at least in the form of conditional probabilities, and, therefore, the state space) so that those other agents would have models of the previous ones (and their models), etc. Moreover, the problem of forming an optimal decentralized decision-making strategy usually becomes difficult in this structure.

One way to eliminate these limitations concerning the completeness of knowledge affecting the state is to provide each agent with only a model of a part of the state space and the associated dynamics. However, the models used by all agents should in some way describe the system as a whole, and each agent should know that there are other parts of the system and they affect the part of the system that is assigned to him. Based on this, we can formulate the first principle of the proposed approach: “Each decision-making agent has a limited model of the controlled system”.

Now consider two agents interacting with each other so that the actions of one (“A”) directly affect the dynamics of the other (“B”). It is clear that there is a need for communication between them. “B” should advise on the actions he has taken so that their consequences could be explained; “A” is obligated to inform “B” about his goals, since “B” can plan actions to help “A” to achieve them. However, care should be taken to prevent strategies where an infinite-capacity channel is used to transmit all messages to a single node, which in this case implements the usual centralized strategy; therefore, constraints on certain types of connections should be imposed. Experience has shown that the inclusion of analytical communication costs or restrictions on their volume is extremely difficult.

If two agents have models that are almost completely nonintersecting in their variables, then the set of attributes that they could exchange is naturally limited. All that two interacting agents could share is the set of interaction variables produced by the agent that influences the other. This would be the only general context that they would have as a basis for communication; thus, the second principle is formulated: “the relationship between agents takes place only in terms of indicators directly related to the main interaction variables”.

The usual approach to the distribution of the processing load among the decision making agents is to use iterative exchanges between them. Such an approach, although often effective, usually requires a significant bandwidth of the feedback means, since several iterations must be performed at each step to determine the set of current control inputs. For this reason, strategies should work as described below. The following principle is formulated as follows: "it is necessary to avoid iterative methods that involve communication between agents at each step."

Finally, the very definition of the structure being modeled ensures that agents will often be unaware of the many events taking place that may ultimately influence them. The probabilistic approach to such uncertainty is not well defined; it seems preferable to resolve uncertainty, assuming the worst case. This gives the attractive advantage of granting local autonomy to decision makers: communication acts as a means to reach agreements between two agents, limiting the actions of each of them. However, everyone can be free to choose one of several alternatives within the agreed limits, knowing that the other will consider his choice as the worst possible case. This leads to the formulation of the following principle: “uncertainty about the future actions of the agent will be resolved either by exchanging messages, or the worst case may be assumed”.

We define a distributed decision making system as a tuple

$$MAS = \langle A, E, R, ORG, ACT, COM, EV \rangle,$$

according to which it is understood as a set of *agents* A, able to function in some *environments* E, which are in certain *relations* R and interact with each other, forming some *organization* ORG with a set of individual and joint *actions* ACT (behavioral strategies and actions), including possible *communicative*

actions COM, and is characterized (as, by the way, individual agents) by *evolution possibilities* EV.
The topology of the decision-making system can be expressed by the graph **G**, consisting of a finite set of nodes N and a set of arcs L

$$\mathbf{G} = (\mathbf{N}, \mathbf{L}). \quad (1)$$

For convenience, suppose the nodes are numbered 1,2, ..., |N| = N in some unique way. Arcs connect one node to another unidirectionally

$$\mathbf{L} \subseteq \mathbf{N} \times \mathbf{N} \quad (2)$$

where $(i,j) \subseteq \mathbf{L}$ indicates a link connecting node i with node j. **G** will display the main dynamic influence of the subsystem of the decision maker i on the subsystem of the decision maker j. (Note that i always affects i, which is the implicit owner of its own model i.)

Each arc will represent not only the dynamic interaction, but also the corresponding interface in the decision-making structure. Since the graph is not necessarily bidirectional, no assumptions about the symmetry of **G** need be made.

Arcs represent the relationships to each other of the subsystems modeled at each node, but their relationship to inputs, outputs, and system goals should also be considered.
Inputs:Each input into the system must be determined by one and only one agent (one that models his direct influence).

Outputs: Each output of the system in a similar way can be associated with exactly one agent that models their origin, based on the model variables of this agent.

Goals: Some agents tie specific targets to their individual models. Other agents will not have any individual goals – their function is to organize (coordinate) the actions of other agents so that the goals of the latter are achieved.

This maintains the distinction between the decision agent in the node *i*, A_i, and the model of the subsystem that he possesses M_i. The model may contain formalized ideas about how to interact with other agents, the behavior strategies and actions of the agent itself, as well as the possibility of the agent evolution.

Now we can say that the problem of making a distributed decision is presented in the form of a structure if local models M_i and interaction relationships **G** are defined.
Each local model M_i complete in the sense that it has a kind of Markov properties: There are many "states" X_i, but the local state transition function depends on interaction variables that reflect the effects of parts of the system modeled by other agents. Such a formulation leads to the necessity of implementing reflexive models. Interaction variables are selected from the sets Z_{ij}, that reflect the influence of the subsystem managed by agent *i* on the subsystem managed by the agent *j*. They are defined as the values of the interaction functions as follows

$$g_{ij}: X_i \rightarrow Z_{ij} \quad (3)$$

Determining interaction values z_{ij} for each state x_i, of function g_{ij} will usually be irreversible; there will be some pair x_i^1 and x_i^2 such that

$$g_{ij}(x_i^1) = g_{ij}(x_i^2) \text{ at } x_i^1 \neq x_i^2 \quad (4)$$

for any *i* and *j*. That is, it can be a formula by which it is impossible to unambiguously restore the state.
Management and observation spaces are defined as follows:
U_i – multiple controls from which an agent *i* can choose;
Y_i – measurements that can be obtained by the agent *j*.
Now the model *M*, which the agent possesses, can be defined. This is “the eight” consisting of the following components:
X_i – set of the local states;
$\{Z_{ij}\}$ – aggregate state sets;

U_i – set of the inputs;
Y_i – set of the outputs;
f_i – function, that determines the next state;
h_i – function, that determines the next output;
$\{g_{ij}\}$ – aggregation functions;
c_i – local cost function;
where:

$$f_i: X_i \times Z_{1i} \times ... Z_{Ni} \times U_i \rightarrow X_i \quad (5)$$

$$g_{ij}: X_i \rightarrow Z_{ij} \quad (6)$$

$$h_i: X_i \times Z_{1i} \times ... \times Z_{Ni} \rightarrow Y_i \quad (7)$$

$$c_i: X_i \times X_i \times Z_{1i} \times ... \times Z_{Ni} \times U_i \rightarrow \boldsymbol{R} \quad (8)$$

Equation (5) expresses a constraint that reflects the fact that transitions depend only on the local state and interaction with immediate neighbors, as well as on control variables; equation (6) does the same for the outputs. Equation (8) defines a local objective function: $c_i(x_i, x_i^+, z_{1i}, z_{2i}, ..., z_{Ni}, u_i)$ - transition cost from state x_i at some point in time t in state x_i^+ at point in time t+1, when interaction variables are present $z_{1i}, z_{2i}, ..., z_{Ni}$, and applied u_i.

An important feature of the introduced formulation is that the concept of a centralized state has been replaced by the concept of a set of local states. To determine the future local response A_i for local inputs local state x_i knowledge is not enough; knowledge of future interactions from other modules is also required. Optimal decision strategies usually require the greatest possible amount of knowledge about the outcomes of possible decisions, and it should be expected that local decision making will be based on information collected regarding the local state and future interactions, in as much quantity as possible.

Observation functions h_i realize the relationship “one to one”: every agent at any given time t knows the state and interaction variables with complete certainty. This avoids the complications of the assessment problem and allows to focus on the problem of coordination. No assumption about the relationship of local goals with the goal of the organization as a whole has been made, since this involves considering a wider class of organizational structures.

Examples of problem areas in which the considered approach and the described models could be used are presented in [7-8]. The practical application and implementation for multi-agent decision making system the suggested models is future research of the authors.

4. CONCLUSION

The key concept of the proposed approach is the individual element of the system, an agent who is an expert in the unique subsystem of which he and he alone has the most complete knowledge, and for which he is responsible. For the considered systems, methods that support decision making can be developed.

REFERENCES

1. Balke T., Gilbert N. “How Do Agents Make Decisions? A Survey”, Journal of Artificial Societies and Social Simulation, # Vol. 17, No. 4, 2014.

2. Cayirci E., GhergherehchiR. “Modeling cyber attacks and their effects on decision process”Proceedings of the 2011 Winter Simulation Conference, 2011.

3. Bezerra, S., Y. Cherruault, Y. Fourcade, and G. Verron. “A Mathematical Model for the Human Decision-Making Process.” Elsevier Mathematical and Computer Modelling Vol. 24, No. 10, Pages 21-26, 1996.

4. Benjamin Dean and Rose McDermott, A Research Agenda to Improve Decision Making in Cyber Security Policy, 5 Penn. St. J.L. & Int'l Aff. 29 (). Available at: http://elibrary.law.psu.edu/jlia/vol5/iss1/4

5. Nicole Lang B., GuynesJ. "A Model for Predicting Hacker Behavior" AMCIS 2006 Proceedings. 409,http://aisel.aisnet.org/amcis2006/409, 2006.

6. Gachet A.,Haettenschwiler P. "Distributed Decision Support Systems - A Federalist Model of Cooperation", in Bisdorff R. (editor) Human Centered Processes - Distributed Decision Making and Man-Machine Cooperation, proceedings of the 14th MINI EURO Conference, Luxembourg: pp. 211-216, 2003.

7. Gachet, A. and Haettenschwiler P. "A Decentralized Approach to Distributed Decision Support Systems", Journal of Decision Systems Vol. 12, No. 2, Pages 141-158, 2003.

8. Erik Ydstie B. “Distributed decision making in complex organizations: the adaptive enterprise”, Computers and Chemical Engineering Vol. 9, Pages 11-27, 2004.