Combined architecture of an intelligent agent using models

V L Tokarev and A A Sychugov

FSBEI HE «Tula State University», Tula, Russia

E-mail: xru2003@list.ru

Abstract. The article considers the problem of building a multi-agent system for solving information security problems of automated process control systems. The architecture of an intelligent agent is proposed and studied, the features of which are the presence of a set of models used both for assessing the security of a certain node of the security object – an automated system, and for making decisions aimed at increasing the level of security. The results obtained in the course of research improve both the scientific and methodological apparatus for integrating methods of multi-agent technologies, and expand the areas of its practical application.

1. Introduction

There are tasks, the solution of which cannot be a one-time act, but is a multi-stage process consisting in the selection and implementation of rational methods, methods of solving the problem at a specific time. Continuous development of rational solutions to such problems, in most cases, is almost impossible without computer support. One of the means of such support is decision support systems (DSS) for complex, difficult-to-formalize tasks [1].

The construction of such DSS, as a rule, includes the choice of the system architecture, the composition of its subsystems, the development of each subsystem and their training – setting the system up to solve problems of a certain class. That is, the creation of a decision support system for tasks of a certain class is deeply individual: one DSS can correspond to each class of tasks.

The article considers a method for constructing a decision support system for problems of various classes based on a single architecture – in the form of a multi-agent system (MAS) built on a set of interconnected intelligent agents [2]. Using the example of solving the problems of ensuring information security of automated process control systems, the problem of building an intelligent agent – the basis of the MAS - is studied.

The following can be attributed to the peculiarities of information security tasks [3]:

- The object of protection is information about the state of the technological process that circulates in the automated process control system and experiences various kinds of disturbing effects that affect the integrity, confidentiality and availability.
- Certain data is subject to protection, the loss or disclosure of which may cause damage to the organization.
- The main task of information security is to ensure the confidentiality, integrity and availability of data, taking into account the expediency of using security measures.
- Ensuring the security of information is a continuous process consisting in the implementation of rational methods, means and ways to improve the security system.
Information security can be ensured only with the integrated use of all available means of protection in all structural elements of an automated system and at all stages of the technological cycle of information processing.

Information protection is effective when the costs of its implementation do not exceed the possible losses from the implementation of information threats.

When working with protected information, the powers and rights of users should be clearly defined.

Strict accounting of cases and attempts of unauthorized access to confidential information is required.

The information security system should provide for monitoring the integrity of the security tools and responding to their failure.

The information security threat in the automated control system is understood as events or actions that can lead to distortion, unauthorized use or even destruction of information resources, as well as software and hardware. The implementation of a threat is called an attack.

Disturbing effects on the automated control system may be accidental and may be accidental or unintentional. Their source may be: hardware failure, incorrect user actions, software errors, etc., at the same time, the damage can be significant.

However, the greatest danger is posed by deliberate threats, which, unlike accidental ones, are aimed at causing maximum damage.

The problem of ensuring the information security of automated control systems is urgent and requires the development of fundamentally new approaches to solve it, based on the use of advanced information technologies and mathematical modeling.

2. Problem statement

The distribution and dynamism of the processes of implementing threats and preventing them motivates the use of decentralized architectures and appropriate technologies to solve the problem.

This was the reason for choosing multi-agent systems based on an intelligent agent that has an internal representation of the situation and reasoning capabilities that allows us to predict information security risks, anticipate possible reactions to its actions, draw conclusions and predict future changes in the situation.

To do this, agents must have a situation modeling apparatus. The development of such an intelligent agent is the main task.

By an intelligent agent, we will understand an intelligent system that has the ability to accept influences from the environment and from other agents of a multi-agent system (MAS), determine its reaction to each impact and carry out this reaction [4]. The main feature of such agents is their ability to independently perform any actions. Another feature is that the agent is not a material entity, but a virtual one – it is a process that implements a program that generates real actions and messages. The following requirements are usually imposed on such agents: autonomy; reactivity; pro-activity [2].

In addition, to perform the tasks of providing information security, agents must meet additional requirements:

- The ability to communicate and interact with other agents or personnel of the automated control system.
- The ability to predict the development of the situation that develops during the operation of the automated control system, under the influence of external disturbances, to assess the risks of information security in the automated control system in real time;
- The ability to identify fixed assets and intangible assets, sources of threats, vulnerabilities, potential impact and manage risks.
As a methodological basis for solving such a problem, the methods of conceptual modeling [4], methods of artificial intelligence [5, 6] are used.

3. Solving the problem

The following approach is chosen to solve the problem.

Agents in the MAS are divided by type of activity and are united in teams. Each team is opposed to a specific threat and this is ensured by the appropriate configuration of the agent team. According to the type of activity, they are divided as follows:

- agents for collecting and pre-processing the collected information;
- agents for filtering information included in the automated process, control system-filter agents;
- agents - event detection detectors;
- agents for selecting the “decision tree”, etc.

Formally, the conceptual model of an intelligent agent can be represented as:

\[ A = \{g, w, V_N, d, c_g\}, \]

where:
- \( G \) is a set of agent goals,
- \( W \) is a set of procedures for collecting an array of data about the operation of the AU performed in the “sliding window” mode,
- \( V_N \) is an updated data array of volume \( N \),
- \( D \) is a set of procedures for processing an array of \( V_N \),
- \( C \) is a set of agent organizational structures, each of which is determined by the goal \( g \).

For example, if the goal is \( g = \) “intrusion detection in the automated control system”, then \( w = \) “procedure for collecting an array of information about the operation of the automated control system”, \( d = \) “procedure for detecting anomalies in the operation of the automated control system for a given time interval \( t \ (N) \)”, \( c_g \) is the organizational structure of the agent corresponding to the algorithm for detecting anomalies in the sample \( V_N \), obtained during the previous time interval \( t \).

The internal structure of the agent, describing its functional device, is determined by the purpose of making a decision \( g \in G \) and includes the subsystems of: models, knowledge base, a decision-making (response) module and working memory. To coordinate work with other agents from the MAS, the agent structure also includes the subsystems of: coordination and agent management. The agent communicates with the environment through the input and output modules.

A variant of the general model of agent activity can be represented in the form of a multi-layer semantic network

\[ Activity \to Situation \to Action \to Operation, \]

the components of which are the following relations:
- \( Activity = F \) (environment, needs, motivations, planning, knowledge);
- \( Situation = sit \) (activity, circumstances, desires, modeling, beliefs);
- \( Action = act \) (situation, objects, goals, strategies, skills);
- \( Operation = op \) (action, conditions, tasks, tactics, skills).

The capabilities of any intelligent agent are determined by its architecture. Existing agent architectures can be classified as follows:

- knowledge-based architectures, for example, presented in the form of production rules [7]. Examples of such architectures include the architectures described in [8, 9]. Their advantage is the presence of a developed knowledge base, and the disadvantage is the lack of flexibility of the reasoning mechanism.
reactive architectures based on the reaction to environmental influences [10]. Examples of such architectures include the architectures described in [11-13]. Their advantage is the ability of the agent to quickly respond to external events, and the disadvantage is the level of "intelligence", insufficient to support solutions to information security problems, the features of which were indicated in the introduction.

combined architectures based on a combination of a knowledge base (usually in the form of production rules) and a mechanism for responding to changes in current situations [14]. Examples of such architecture include the Touring Machine architecture, IDS architecture, and others described in [15]. This architecture combines all the advantages of rule-based and reactive architectures.

Considering that the main requirement for the agent architecture in the context of the problem being solved is the ability to assess the values of information security risks at some point in time, and obtaining such estimates is impossible without modeling the observed processes [16], an architecture based on models of both the environment of the security object node, the security object node itself, with which the agent is directly connected, the behavior of other MAS agents, and a model for assessing the security risk value of this node is proposed.

4. Intelligent agent architecture

The proposed architecture is based on a well-known combined architecture, in which it is proposed to integrate a complex of dynamic models, with the help of which the agent becomes able to solve the tasks set.

It is proposed to use models of the environment; the node of the security object (automated control system); the behavior of other MAS agents, as well as to use the module for assessing the current situation.

The general view of the proposed intelligent agent architecture is shown in figure 1. The main components of which include the knowledge base, the model subsystem, the decision-making module, working memory, input and output modules, the agent coordination and management subsystems.

The agent's knowledge base is based on a production model of knowledge representation, for the implementation of which three modules are used (database; production system; interpreter) and has a three-level structure:

- knowledge of the subject area;
- knowledge of interaction, usually in the form of general declarative rules of conduct, as well as rules of a procedural nature;
- management knowledge.

The knowledge base, including the knowledge management module, is developed in Java, since it is necessary to ensure the agent's ability to migrate over the network [17].

The working memory is intended for storing temporary data received from the coordination subsystem, the user and the decision-making module. The working memory also contains information about goals, current and completed tasks, incoming and outgoing messages, and parameters of the current situation.

The subsystem of models that provides an assessment of the situation at the current time is a set of linguistic models [18]:

- the environment in which the agent functions, which is recurrently called during the modeling process;
- the object of protection (the AC node);
- the behavior of other MAs agents;
- the assessment of information security risks of the corresponding AC node.
The obtained estimates become the basis not only for assessing the information security risk of the entire automated control system as a whole, but also for making decisions to reduce the risk both in the analyzed node of the automated control system and the entire system.

![Diagram of the proposed intelligent agent architecture](image)

**Figure 1.** The general view of the proposed intelligent agent architecture.

*The decision-making subsystem* includes a decision-making module (*D*) and a *response module* (*R*). *Module D* implements the resolution of a conflicting set of rules, i.e. the choice of one rule from the set of applicable ones, using a trial-type strategy with a return [19] - storing the results of applying rule chains is used with further search on the Tg solution tree corresponding to the current *Sit eSit* situation, determined by the situation assessment module of the MS model subsystem.

*The response module* (*R*) uses the agent’s knowledge of a procedural nature, which is based on the concept of a “behavior fragment” - a template for the agent's reaction to some typical situations. This allows the agent in typical situations not to refer to the procedure for developing (planning) solutions, but to directly use a “ready-made” solution corresponding to the current situation.

The *R* module is implemented using standard languages for describing the behavior of agents – the algebra of actions and the algebra of behaviors.
The coordination subsystem, which includes modules for interaction and conflict management, participates in the design of plans for the joint behavior of agents to achieve a common goal and/or to fulfill their obligations to other agents.

The interaction module implements the general principles and conditions for the exchange of messages during the joint actions of agents.

The conflict management module allows an agent to make decisions when receiving conflicting information from other agents.

The agent management subsystem generates, executes and reconstructs agent action plans, and also contains a planning mechanism that allows you to build individual plans.

The input module contains sensors responsible for the agent's perception of information received from the outside world and from other agents. For example, for the task of detecting intrusions, it can contain immune detectors – special agents that recognize signs of intrusions into the protected AC [20].

The developed solutions are implemented by the output module through effectors that affect the outside world and other agents, sending them messages of different content.

5. Research of an intelligent agent

In this paper, the following approach was used to evaluate the effectiveness of agent architectures with a set of models in MAS.

The efficiency (accuracy and speed) of agents with different architectures were compared: one agent with a basic architecture, the other with a subsystem for assessing the situation using appropriate models, i.e. with the architecture shown in figure 1.

The goal of detecting intrusions into the local network was chosen as the goal of the agents. The global network was used as an external environment in the form of traffic taken from the KDD Cup 1999 database.

The experiments made it possible to draw the following conclusions:

• the prospects of using intelligent agents with an architecture that uses a set of models to develop solutions to problems of ensuring information security of automated systems;
• a multi-agent system built on agents with the architecture shown in figure 1 can become the basis for building an effective information security system for most automated systems;
• an important issue that requires detailed study is the development of a procedure for the agent to automatically build a decision tree for threats of an unknown type.

6. Conclusion

The scientific and methodological foundations of the integration of multi-agent technologies and methods of building intelligent agents for the tasks of ensuring information security of automated process control systems are proposed.

A combined architecture of an intelligent agent with a set of models has been developed. An approach to creating a multi-agent system on agents with such an architecture is proposed.

The implementation of the proposed approach provides the possibility of creating complexes of spatially distributed and effective information protection systems of automated process control systems.

Acknowledgments

The research was carried out with the financial support of the Russian Foundation for Basic Research within the framework of the scientific project No. 19-07-0110719.

References

[1] Tokarev V L 2007 Computer Support for Decision-Making (Moscow: SSU) 162 ISBN 978-5-8323-0451-9

[2] Gorodetsky V I 1998 Multi-agent systems: basic properties and models of behavior coordination Information Technologies and Computer systems I 22-34
[3] Tokarev V L and Sychugov A A 2019 Method of security audit of automated systems *Modeling optimization and information technologies* 7(1) retrieved from: http://moit.vivt.ru

[4] Russell C and Norving P 2006 *Artificial Intelligence: a Modern Approach* (Moscow: Williams) 1410

[5] Masloboev A V, Putilov V A and Shishaev M G 2007 Conceptual model of an Agent-Oriented Virtual Business Environment for Innovation Development *Collection of Scientific Works IMM of the KSC RAS: Information Technologies in Regional Development, Apatity, KSC RAS* 15-27

[6] Serugendo Giovanna Di Marzol 2005 Self-organization in multi-agent systems *Knowledge Engineering Review* 20(2) 65-89

[7] Nilsson N 2007 *The Physical Symbol System Hypothesis: Status and Prospects (50 years of artificial intelligence)* 1st ed Lasagna M, Iida F, Bongard J, et al (New York: Springer) 9-17

[8] Bugaychenko D Yu and Soloviev I P 2012 Abstract architecture of an intelligent agent and methods of its implementation *System programming (Collection of articles)* ed A N Terekhov, D Y Bulychev *Publishing House of St. Petersburg State University* 7(1) 218

[9] Stamatis P N, I Zaharakis D and Kameas A 2006 Exploiting ambient information into reactive agent architectures *Conference: Intelligent Environments IE* 06 (2nd IET International Conference 2)

[10] Caching G R and Deshendran M A 2018 *Hybrid POMDP-BDI Agent Architecture with Online Stochastic Planning and Plan Centre for Artificial Intelligence Research* (South Africa: University of KwaZulu-Natal, and CSIR Meraka)

[11] Wooldridge M J 2001 *Intelligent Agents Multiagent Systems* 27-79

[12] Burlina M A and Akhmadeev B A 2016 Analysis of the variety of architectures and methods of modeling decentralized systems based on an agent-oriented approach *Creative Economy* 7 150-69 retrieved from: https://rucont.ru/efd/412695, last accessed: 2021/19/07

[13] Marcus Gary F 2001 *The Algebraic Mind: Combining Connectionism and Cognitive Science (Learning, Development, and Conceptual Change)* (Cambridge, MA: MIT Press) ISBN978-0262632683

[14] Osipov G S 2011 *Methods of Artificial Intelligence* (Moscow: Fizmatlit)

[15] Gorodetsky V I, Grushinsky M S and Khabalov A V “Multi-Agent Systems” (Review). Retrieved from: http://doi.gendocs.ru/docs/index-234450.html

[16] Evaluation Criteria for IT Security, part 1: Introduction and General Models ISO/IEC 15408-1: 2009

[17] Tokarev V L and Sychugov A A 2018 Multi-agent system for network attack detection *International Journal of Civil Engineering and Technology (IJCIET)* 9(6)

[18] Tokarev V L and Gorbunova T I 2011 Building a multi-level model aimed at supporting decision-making of diagnostic problems *News of TSU: Technical Sciences. TSU Publishing House* 6(2) 104-10

[19] Polichka A E and Vostrikova AV 2016 “Algorithms for the Functioning of Production Knowledge Bases and a Description of the Mathematical Modeling Apparatus” Retrieved from: http://pnu.edu.ru/media/ ejournal/articles-2016/TGU_7_250.pdf

[20] Tokarev V L and Sychugov A A 2017 Detection of malicious software using immune detectors *Izvestiya Tula State University. Technical sciences. Issue. TSU Publishing House* 10 216-30

[21] Biryukov A A *Information Security. Defense and Attack* (Moscow: DMK-Press)