Mobile Robotic Systems with Partially Centralized Control

Sergey Chuprov
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
Saint-Petersburg, Russia
drmyscull@gmail.com

Ilia Viksnin
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
Saint-Petersburg, Russia
wixnin@cit.ifmo.ru

Julia Kim
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
Saint-Petersburg, Russia
yulia1344@gmail.com

Danil Zakoldaev
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
Saint-Petersburg, Russia
d.zakoldaev@corp.ifmo.ru

Abstract—The paper discusses the work of mobile robotic systems. To ensure the information security of the system, a model for ensuring information security is proposed. One of the key aspects of ensuring information security is ensuring the confidentiality of information circulating in the system. As technical countermeasures, it is possible to use the organization of the system using police station models. Authors conduct a number of experiments using methods of trust and reputation for analyzing the effectiveness of such a system organization.

Keywords—multi-agent robotic system, information security, police office model, quantum encryption.

I. Introduction

Today the whole world stands in the way of automation and optimization of various processes. Active research is carried out on the development of the ideology of the Internet of Things [1], "smart" houses, cities designed to improve the quality of life, improve the efficiency of servicing and meeting the needs of residents of such cities or homes. With the development of global technological progress in various areas of our life, humanity is gradually introducing robotic systems capable of performing tasks faster, better and more accurately than a human being. Such systems include a set of technical devices, sensors, interconnected communication channels for the purpose of controlling the system using artificial intelligence. In scientific research, such systems, which are a combination of information and physical components, are called cyber-physical systems (CPS) [2]. Information components of such systems include elements that perform calculations, implement algorithms, and transfer data over a network. The physical components include analog elements and various physical devices that interact with the environment.

CPS also includes groups of mobile autonomous intelligent robotic devices communicating with each other in order to accomplish the task. The approach to the control of such systems due to the presence in them of a number of intelligent devices (so-called agents) has received the name of a “multi-agent”. Multi-agent robotic systems (MARS) are able to perform tasks through active inter-agent communications. Currently, such systems are being introduced in various spheres of human life, helping to optimize and automate processes. The range of tasks to be performed by the MARS includes search and rescue operations, liquidation of the consequences of natural or man-made disasters, control and protection of territory, movement of goods in warehouses, etc. Environmental conditions in performing such tasks can be hostile to robotic devices, their resistance to such conditions largely depends not only on engineering decisions, but also on correct behaviour and timely response in unforeseen circumstances, which is provided by the chosen control strategy.

An example of research in the field of coordinating the activities of a group of robots is the project [3-5], work on which was conducted with the support of the DARPA (Defense Advanced Research Projects Agency) of the US Department of Defense. The goal of the project was to develop a system that includes software and hardware for the control of a group of robots designed to monitor rooms. The structure of the system implies the centralized control of the group by the operator.

The authors of [6] used a multi-agent approach with centralized control to coordinate several unmanned aerial vehicles. In the described structure of the system there is an operator (human) who manages the "subordinate" group of unmanned aerial vehicles with the help of the man-machine interface. The authors conducted three experiments using a simulator and one in real conditions. The experiments showed the possibility of controlling a group of four unmanned aerial vehicles by a pilot who carried out control from an aircraft.

In the Japanese project "AMADEUS" [7] a group of scientists proposed the implementation of a group of robots for moving goods using decentralized control. In this project there is no centralized control node, so the planning of actions is carried out by several robotic devices that make up a multiplicity of loading robots. The system also has a variety of transport robots that receive tasks from loading robots and perform them.

In [8], the authors propose the use of hierarchical reinforcement learning, based on semi-autonomous control with the aim of training a group of robots to explore the terrain and find victims in urban search and rescue (USAR) environments. As a result of the conducted experiments, the authors come to the conclusion that this approach allows to effectively distribute tasks in a group of robots and contributes to their effective implementation, which in turn

increases the overall efficiency of the system. In this system, when the robot determines that it is unable to perform the task effectively, it asks for assistance from the operator. Thus, the members of the team of robots are able to make joint decisions on the distribution of tasks among team members and share their experience about the tasks accomplished.

Unlike the approach using a single robot to solve various problems, the use of MRS has several advantages. It is possible to distinguish such advantages as:

- autonomy - when applying an approach using a single robot, its effectiveness is limited by the charge of the battery, in the event of failure the robot needs time to recover, which reduces the effectiveness of tasks performing. In MARS, if one of the robots is lost or destroyed, its tasks are delegated to another robot capable of performing them;
- scalability - when changing the number of tasks or the size of the territory of operation, it is possible to change the number of agents without introducing cardinal changes in the principles of the functioning of the system;
- reliability - when applying an approach using a multifunctional robot to solve problems, its overall level of reliability will depend on the reliability of its various components (sensors, devices, etc.). The MARS mainly uses robots that which structure is simple, capable of replacing one another with the inability to perform tasks;
- low cost - since all robots in MARS are simple and capable of performing single simple tasks, they do not require large expenditures in production and maintenance;
- efficiency - there are tasks that a single robot cannot perform, but a group of robots can, for example, many tasks distributed on the terrain that require the constant movement of agents, or if environmental conditions do not allow the operation of large devices. In such tasks, the MARS are most effective;

The methods of centralized, decentralized and hybrid method of agent control can be used in the MARS. In [9], an analysis and a review of methods for distributing tasks among agents in multi-agent systems is presented. With centralized management, there is a central element in the system that has a powerful computing center, receives and transmits information through communication channels from a variety of agents, generates routes and distributes tasks among agents that are executors, and therefore may not have powerful computing centers.

With a decentralized control each agent in the system has its own computing center to plan the route, communicate with many other agents, and make decisions about the distribution of tasks. During group positioning agents exchange knowledge acquired through communication channels, on the basis of which they make correction of the way and resolution of conflict situations.

In the case of a hybrid control method, there is one or more central control elements that, using the information received from the agents about the location, the resource balance, etc. distribute strategic tasks, the implementing agents within their group are already directly implementing tactical tasks using the decentralized control strategy.

II. Security problem in multi-agent robotic system

Any information system can be threatened with information security (IS) by intruders. CPS underlies the implementation of promising projects in the paradigm of the concept of "smart" cities, but they are not protected from attempts by intruders to violate the properties of IS. Information and physical elements of CPS can transmit various information about the important properties of the system. Having access to such information, an attacker can use it to implement an attack on the system, that in a scenario, if such systems manage smart cities, may have global consequences, for example, traffic collapse when attacking traffic control equipment, leakage of confidential information when attacking security objects infrastructure of medical institutions, etc.

For a long time, insufficient attention has been paid to the methods of securing MARS in the scientific community, but current trends in the introduction of such systems into various spheres of our life allow us to conclude that this aspect is an important component of the safe and continuous operation of the system. To ensure IS, it is necessary to provide important properties of IS, the definition of which is given in [10]:

- confidentiality - a guarantee that a subject who does not have the right to access information cannot read it;
- data integrity: ensuring that the information transmitted is not unauthorizedly altered by entities that do not have such rights;
- authentication of origin - ensuring that the source of information is genuine;
- availability - ensuring that information always reaches its recipient in a timely manner;
- non-repudiation: ensuring that the source of sent messages is responsible for these messages.

One of the approaches to securing the MARS IS was developed and described in [11] and was named "A Buddy Model of Security". In this paper, the authors consider the vulnerabilities that arise when communicating between agents in a multi-agent system, and also offer to deal with them using the proposed model. In this model, agents are responsible for the security of their neighbors, so the security function is evenly distributed to all system agents.

In [12], the authors propose a method of ensuring security, called the method of protected states. The essence of this method is to change the states of agents based on the type of activity: read only, only for execution, etc.

The ensuring of security with the help of cryptographic protocols is presented in [13]. The author offers secure protocols for mobile agents that can withstand static, semi-honest or malicious adversaries without the use of a special trusted subject in the system. The safety of the protocols was confirmed by the results of the experiments obtained on the real mobile-agent platform.

The authors of [14] presented a method for ensuring the IS of agents, called "Police Office Model" (POM). Within

the framework of the model it is proposed to divide the area of the system functioning into regions, and in each of the regions to introduce the agent responsible for the security of this region, while all the other agents in the region are "obey" to this agent. Each mobile agent has two components: master part and slave part. Master part is responsible for security operations, slave part is security free and responsible only for migrating. In [15], a modernized version of this model is presented in terms of IS. The authors described the mechanism of authorization between the agent and the "police office", introduced the concept of a certificate of validity and made the decomposition of the authorization process in time.

There is still some number of methods to ensure the availability and integrity of information in the multi-agent systems and the MARS. An analysis of existing research in this area allows us to conclude that there are no universal methods to ensure the confidentiality of information transmitted between agents. Thus, the relevance of this work is due to the inadequacy of the scientific and methodological apparatus of the region under investigation.

The authors of this paper propose to solve the problem of ensuring confidentiality in the system with the help of the POM [14] using quantum encryption of information transmitted between agents. Below is a description of the structure of the abstract MARS, a scheme of functioning and mechanisms for providing the IS, a model of IS in the MARS is presented.

III. Information Security Model of Multi-Agent Robotic System

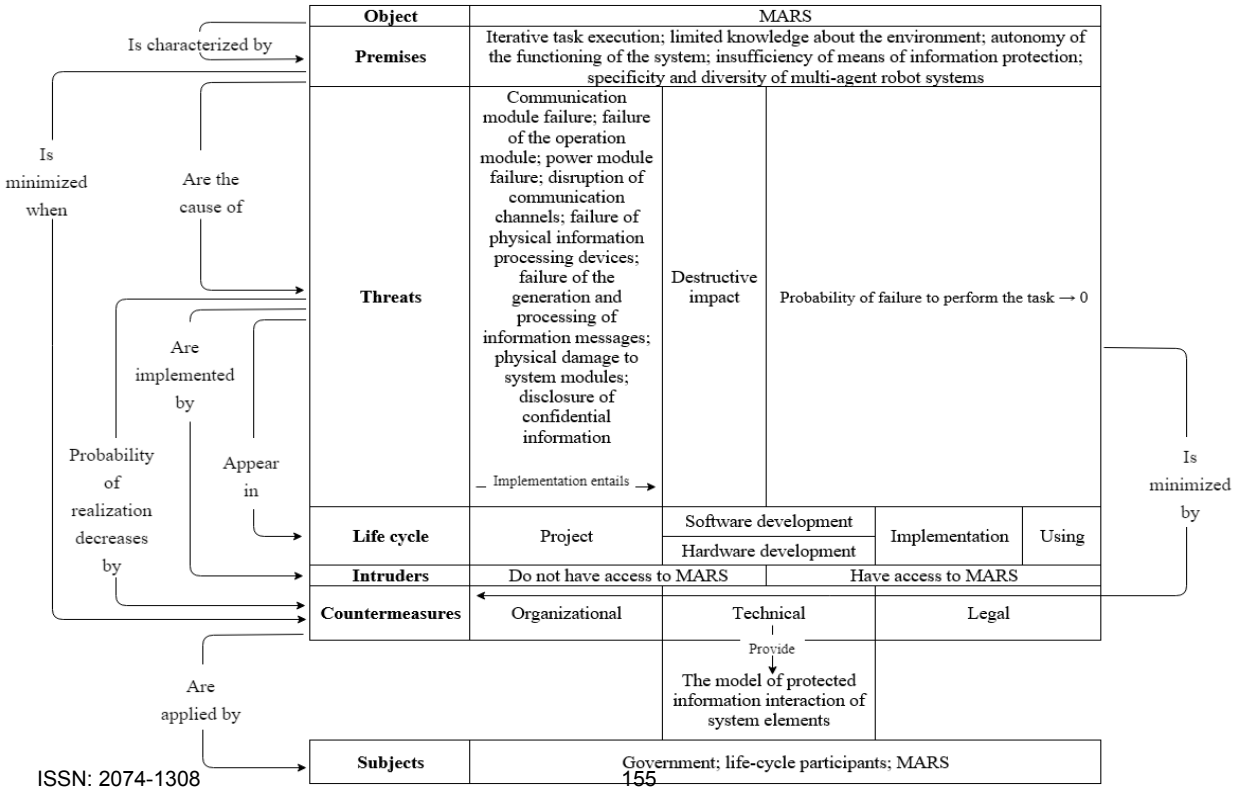
As it was said above, the ensuring of IS in MARS is one of the most important parts of the correct and secure functioning of the system. To ensure IS in MARS it is necessary to determine the significant threats typical for such systems. The presence of vulnerabilities in MARS is due to a number of features of the structure of the operation of MARS. Due to the existence of such features, we can distinguish the following prerequisites for the emergence of threats:

Fig. 1. Generalized model of MARS IS

- iterative task execution;
- limited knowledge about the environment,
- autonomy of the functioning of the system;
- insufficiency of means of information protection;
- specificity and diversity of multi-agent robot systems.

The main threats to IS typical for the MARS can be divided into hardware and software. The implementation of hardware threats is possible in the event of failures, malfunctions or failures of the hardware parts of the MARS. The implementation of software threats is possible if there are failures, violations or failures in the software parts of the MARS.

In order to determine the types of possible intruders of IS in the MARS, it is necessary to determine the main stages of the system life cycle. Based on these stages, it is possible to assess the influence of the life-cycle participant on the development and operation of the system. In the context of the MARS it is possible to distinguish such stages as: design the project, development, implementation, use. The life cycle of the system is schematically shown in the figure 2.



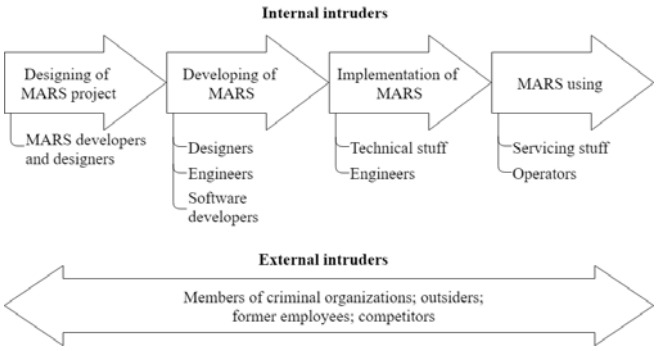


Fig. 2. Internal and external intruders classification on the MARS life cycle stages

The analysis of these stages allows us to divide the offenders into two groups:

1) *those who do not have access to work with MARS - persons of this group can be attributed to external intruders;*

2) *those who have access to work with MARS - these persons can carry out attacks using the rights to work with MARS.*

Thus, an analysis of the main threats and types of intruders makes it possible to develop a model of MARS IS, presented on figure 1. The subjects of providing IS are: the government, owner of MARS, participants of the life cycle. The object of ensuring IS is MARS. The government seeks to provide IS by developing legislative and legal acts aimed at monitoring the work of life cycle participants, regulating relationships with participants of the life cycle with the owner of the MARS and developing countermeasures to eliminate the vulnerabilities of the MARS. Participants in the life cycle take countermeasures to minimize risks and eliminate vulnerabilities by developing security solutions, the MARS owner develops organizational countermeasures.

Let's consider the behavior of agent-violators, with a different level of access to the system.

If the intruder has access to the MARS, he can introduce agents-saboteurs, sabotaging tasks in one of the following ways:

1) *to come to the goal himself and not to perform the required actions;*
2) *lead to the goal of another saboteur who also does not perform the necessary actions;*
3) *reduce the total number of agents reaching the target, to a number less than those requested by the agents.*

There are a large number of methods for countering these types of attacks [11-15]. At the same time, there remains the issue of countering violators who introduce saboteur agents into the group, whom the system falsely identifies as allies.

Thus, the question arises of countering intruders who do not have access to the MARS, but are capable of introducing a saboteur agent. A similar agent-saboteur will impersonate existing agents. To do this, the intruder should be able to intercept messages within the framework of the MARS, or to give this opportunity to the saboteur.

Thus, methods of ensuring confidentiality of information are one of the key aspects of the successful operation of the MARS. The authors of the paper consider the application of quantum encryption methods as one of the ways to solve this problem. However, the use of quantum encryption requires a change in the algorithm for the functioning of the system. At the same time, we can say that at the current time the use of quantum encryption is sufficient to ensure the confidentiality of information in the system.

IV. Police Office Model for Mobile Robotic System

The fundamental laws of quantum physics state that when you try to measure one parameter of a photon, it is impossible not to distort the other. This statement underlies the methods of quantum encryption. Modern research in the field of quantum cryptography argues that it is possible to create a cryptographic system in which in any case eavesdropping of transmitted information will be detected. Attempting to measure the parameters of transmitted information introduces infringements that legitimate users can detect and conclude that the interceptor is present. [16] This feature allows the use of quantum encryption methods to solve the problem of confidentiality of information transmitted in the system. There are a number of protocols for the distribution of quantum encryption keys, for example, such as BB82 (Bennett and Brassard 1984) [17], B92 (Bennett 1992) [18], BB84 (4 + 2) protocol (Huttner et al., 1995) 19], etc.

In the context of this study, it is proposed to use the following scheme of information interaction (II) between MARS agents.

The zone of the system functioning is divided into equal areas, in the center of which are fixed agents - autonomous robots making up the set $B = \{b_1, b_2, \ldots, b_m\}$ and performing the role of "police stations" (bases). The bases have their own "coverage zone", the diameter of which depends on the technical capabilities of the communication facilities installed on the base for communication with other agents. These robots have a powerful computing center and are responsible for controlling the movement and distribution of tasks for simple mobile autonomous unmanned robots that make up the set $R = \{r_1, r_2, \ldots, r_n\}$ that perform the tasks of moving from point A to point B. There are two levels of II: upper and lower. At the upper level, the interaction takes place between the databases, the module with the receiver and the information transmitter for communication with other bases, and another one for communicating with the agents of the lower level. Such communication is shown schematically in figure 1, where $\{T\}$ - set of tasks, which base entrust to robots, $\{P\}$ - set of robot's characteristics, s - connection from the base to the information exchange channel.

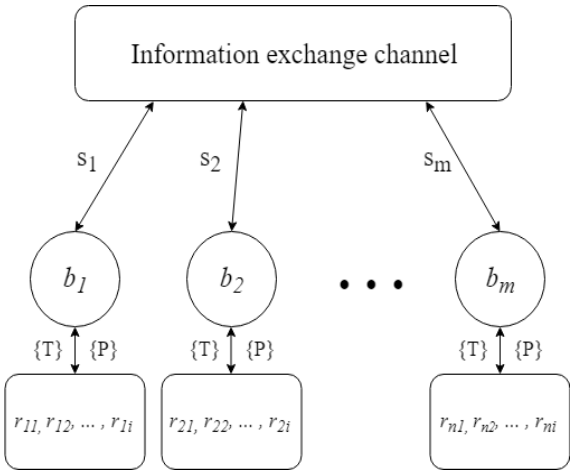


Fig. 3. Agent-bases top-level interaction diagram

At the lower level, the II occurs between the bases and mobile robots. Robots-performers have a module with a receiver and transmitter for communication with the bases and do not have the opportunity to communicate with other robots-performers. Such an interaction is shown schematically in figure 2, where t - one of the tasks, which base entrust to robot, p - one of the characteristics, which robot transmit to the base, e - information, which robot gather via sensors from the environment.

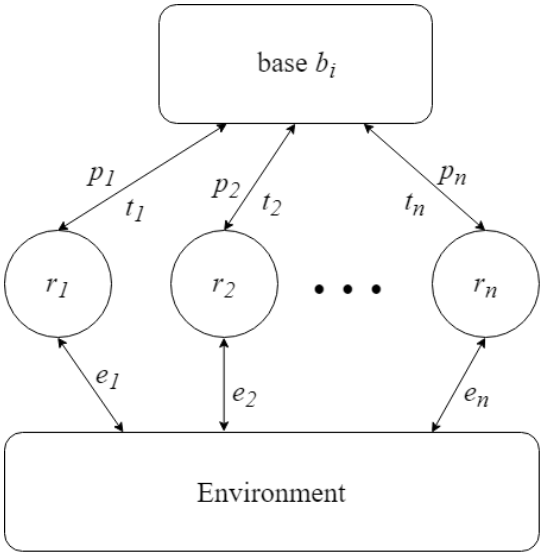


Fig. 4. Diagram of the low-level interaction between robots and bases

Such a scheme of functioning in the context of quantum encryption is complicated in practical implementation, but this is an engineering task that will be solved in the future.

The tasks are the set $T = \{t_1, t_2, \dots, t_p\}$ and represent the movement of the robot-performer from point A to point B. From the beginning of the functioning of the system, the coordinates of all tasks are known to all agents. The distribution of tasks by the bases of the robots-executors is carried out according to the scheme of the auction: for executing the task, a performer is chosen who will spend the optimal amount of resources and is at the distance closest to the target. An overview of methods for distributing problems and examples can be found in [20]. In the event of failure of the robot that received the task, its task is delegated to another serviceable robot by the algorithm of the auction.

The functional scheme of obtaining and executing the task by an agent using POM with quantum encryption of transmitted messages is shown in figure 5.

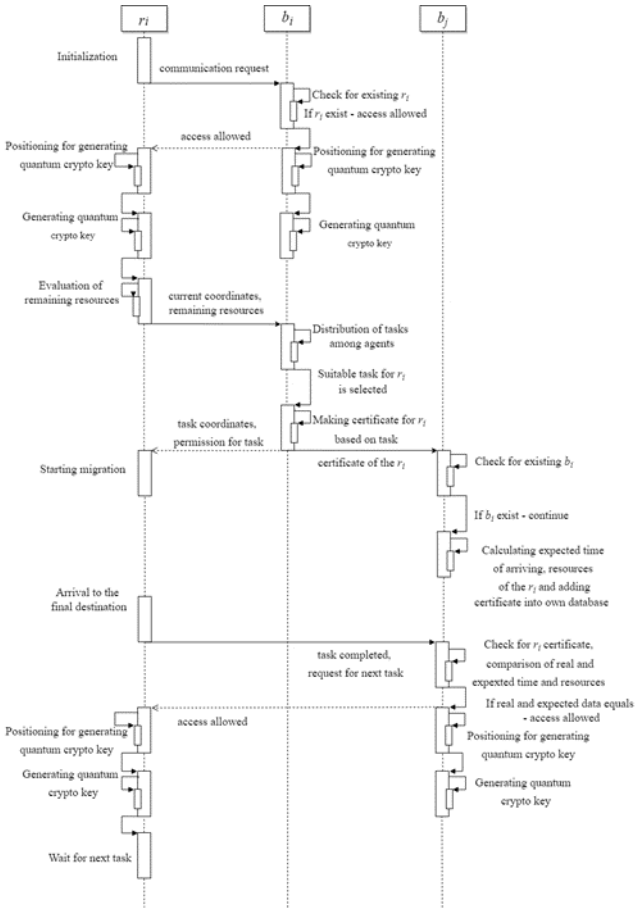


Fig. 5. Function diagram of system working using quantum message encryption

Below is a more detailed description of the iterative actions presented in figure 3:

1) after initialization (the start of the system operation), the r_i agent sends a request for communication to the b_i base, in which "coverage zone" r_i is located;

2) the b_i checks whether the r_i is valid by checking its identification number with the database of agents functioning in the system. Such database is available for each base in the system;

3) upon successful verification, the agents b_i and r_i begin to generate a quantum cryptographic key. Before this, it is necessary to perform a positioning procedure, it is the pointing of technical devices designed to generate a key on each other, which is necessary for generating a quantum key;

4) after successful generation of the key, the agent r_i provides b_i with the remaining amount of resources, based on this information, b_i selects the appropriate task, generates a certificate based on the information about the transferred task, and sends such certificate to the base b_i in the "coverage zone" of which the end point of the task. After these actions r_i starts moving to the target;

5) b_i receives a certificate from b_i, produces in its database a b_i existence verification, in case of a successful verification, saves the certificate at home;

6) arriving at the target r_i informs b_i of the fulfillment of the task, b_i also, as in paragraphs 2-3, checks the existence of the agent and generates the quantum cryptographic key;

7) after these procedures, b_i checks the information in the certificate with the information about the remaining resources provided by r_i. On successful verification, b_i distributes to r_i the next task and r_i is sent to execute it;

V. Experimental Part

The authors of the study consider the issue of the correct performing of the tasks facing the MARS, in the presence of agents-saboteurs. It is understood that the agent-saboteur is able to impersonate a normal agent and take on the tasks facing him. When the task is received, the agent-saboteur does not fulfill it, but simply remains in place. Thus, an agent-saboteur, similar to other agents of the group only on the properties of II, can be introduced into the II of MARS, but differing in other features.

Thereby, an agent-saboteur, similar to other agents of the group only on the properties of IW, can be introduced into the information interaction, but differing in other features. The base in which "coverage zone" the task is located, knows the time interval that the agent needs to perform the task. If the task has not been completed after this time, the request for execution is sent to other agents.

Within the framework of experiment the following conditions were set:

- the number of executing agents in the system is 20;
- the number of bases in the system is 9;
- the number of tasks is 100;
- the size of experimental polygon: 25x25 cells.

The general view of the simulator is shown in figure 6.

As additional methods for ensuring the IS of the approach, we consider the coefficients of trust / reputation [21], calculated locally for each group of agents. In order to completely lose efficiency, it is necessary that the total number of saboteurs exceed 50% of the total swarm size [21], Thus, we can talk about the stability of this approach to the emergence of intruders of IS. The calculated indicators of trust and reputation levels for each of the robots are transferred to other police stations, if necessary. Thus, we can say that trust and reputation cease to be calculated locally and become a global indicator.

The course of the experiment can be represented as follows.

At the time of the experiment's initialization, two swarms of robots are created in such a way that the zones of their connection do not intersect, hence, we can speak of two isolated swarms. Each swarm is aware of the existence of two goals to be achieved.

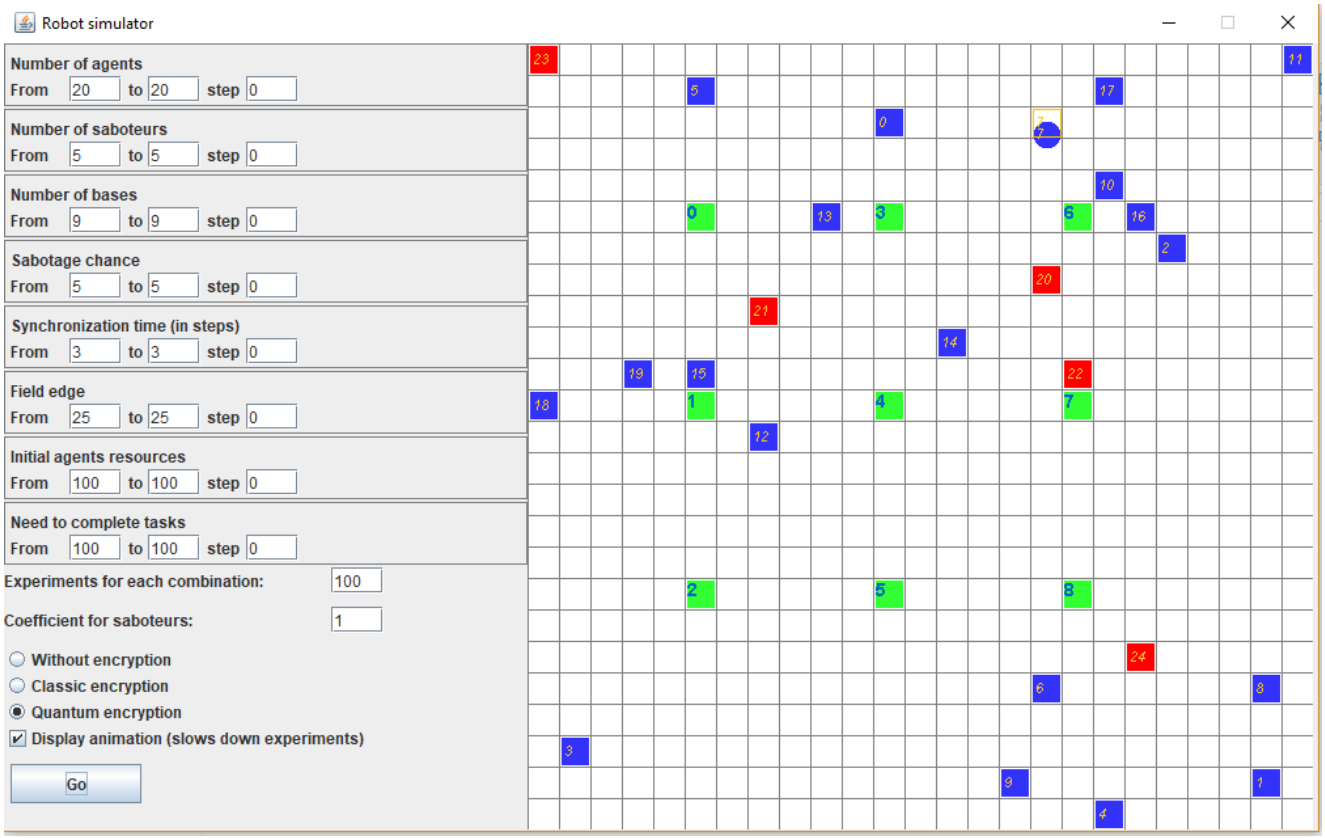


Fig. 6. Graphical interface of the MARS functioning software simulator. Blue color indicates allied agents, red - saboteurs, green – bases. The parameters of the experiment are set on the left side of the interface.

Between robots an auction is held, during which a list of robots going to the targets is determined. Based on the postulate of the isolation of agents, it can be argued that the number of robots that have achieved the goals will be more than required.

Suppose that each saboteur falsifies information about himself and poses as an existing normal agent. The remaining members of the swarm can detect the disturbance by means of sensory devices, i. e. discover the implementation of a new agent.

The authors of the work carried out two series of experiments. In each series, the following experimental conditions are considered:

- the size of each group of robots - from 10 to 100 robots (the exact value is determined randomly for each experiment);
- number of goals - 2;
- total number of intruders - 10% of the group size;
- the required number of robots to accomplish the task is 10% of the number of robots in a single swarm.

To compare the adequacy of the application of global and local indicators of trust/reputation, we introduce additional conditions for conducting the experiment. Suppose that after achieving the first tasks, two new tasks (tasks of the second level) are placed before the groups of robots located in the target locations.

In the first series of experiments, consider the situation in which a robot-intruder provides incorrect information regarding the cost of achieving his goal. Thus, the intruder can get the opportunity to go to the task without having objective prerequisites for this. Also, suppose that the robot-intruder moves to the target even without assigning it to this goal. Based on this assumption and the fact of defining two new tasks after reaching the initial ones, we can talk about the potential success of the attack on the tasks of the second level. The location of the intruder robot in the target area is not taken into account when determining the fulfillment of the task based on the number of robots.

Based on the conducted experiments, the results presented in Table 1 were obtained.

As can be seen from Table 1, the goals of the second level remain unfulfilled in most cases. reaching the goals of the first level robots do not allow to conduct an adequate assessment of their actions using indicators of trust and reputation. A misconception about the levels of trust and reputation leads to the fact that about 70% of robots-intruders remain unidentified.

To solve this problem, we use the notion of police stations. In the proposed experiments, police officers are used as elements that determine the values of trust and reputation for each robot located in their area of responsibility. After determining the plan for the fulfillment of the goal and the detection of intruders, the robots begin movements, during which they change their belonging to a particular police station. A policeman whose area of responsibility the robot entered is requesting information about his trust and reputation from the policeman who carried out the calculation of these data at the first stage. Even if the robot-intruder provides the right information at the second stage of the experiment, the policeman will not take it into account when determining plans for the fulfillment of goals. The results of the second series of experiments are presented in Table 2.

According to the results of the second series of experiments, it can be said that the threat of participation in the plans to fulfill the targets of robots-intruders is neutralized. Therefore, all targets will be met, when using police stations.

Based on the conducted experiments, we can talk about the success of the approach based on police stations for the implementation of the inter-zone information security policy. When using it, you can not only minimize the damage from the implementation of the threat, but also completely neutralize the possible threat. In addition, it is possible to use police officers not only as elements that provide information security, but also as elements that coordinate plans for the fulfillment of goals, which will lead to a reduction in the total costs of robots to fulfill their tasks.

TABLE I. THE RESULTS OF THE FIRST SERIES OF EXPERIMENTS

Index	Tasks of the first level	Tasks of the second level
	Value (%)	Value (%)
The average required number of robots to perform the task (of the total number of robots involved at this level)	5	5
The number of detected intruders (of the total number of intruders functioning at this stage)	100	30,4
Number of experiments with unfulfilled tasks (at least one task is not fulfilled)	0	75,3
The average number of robots that are not enough to perform tasks (from the general need)	0	69,3

TABLE II. THE RESULTS OF THE SECOND SERIES OF EXPERIMENTS

Index	Tasks of the first level	Tasks of the second level
	Value (%)	Value (%)
The average required number of robots to perform the task (of the total number of robots involved at this level)	5	5
The number of detected intruders (of the total number of intruders functioning at this stage)	100	100
Number of experiments with unfulfilled tasks (at least one task is not fulfilled)	0	0
The average number of robots that are not enough to perform tasks (from the general need)	0	0

REFERENCES

A model for ensuring the information security of mobile robotic systems is proposed. Within the framework of the model, possible intruders were analyzed, their types were listed. The need to ensure the confidentiality of information was determined, which directly affects the functioning of the system.

A theoretical security model for multi-agent robotic systems is proposed, which is based on the zonal security model and the model of police stations for distributed computing systems. This model, unlike the known models of access delimitation, allows the physical location of agents and describes the rules for differentiating access of physically remote entities to objects that are implemented by intrazonal and interzonal security monitors. This organization of access distribution allowed to solve the task of implementing a mechanism for tracking the current location of each subject and the object of the system, as well as to divide the multiple accesses of entities to objects into many legal (safe) accesses and accesses that violate the integrity of the system. An additional block of information security is the use of quantum encryption mechanisms, which at the moment guarantees the confidentiality of information.

The efficiency of the model is demonstrated through its use in developing a mechanism for protecting the classical iterative task of distributing robots for several purposes. The proposed model made it possible to implement a mechanism for protecting multi-agent robotic systems from so-called "soft" attacks, which are the main threat to the system because of the absence of their clearly identifiable features and the possibility of implementing it during the regular operation of the system without the risk of their rapid detection.

REFERENCES

[1] Kopetz, H. (2011). Internet of things. In Real-time systems (pp. 307-323). Springer, Boston, MA.

[2] Wolf, W. Cyber-physical systems / W. Wolf // Computer. – 2009. – T. 42. – №. 3. – P. 88–89.

[3] Rybski P. E., Burt I., Dahlin T., Gini M., Hougen D. F., Krantz D. G., Nageotte F., Papanikolopoulos N., Stoeter S.A. System Architecture for Versatile Autonomous and Teleoperated Control of Multiple Miniature Robots // Proc. of the 2001 IEEE Intern. Conf. on Robotics and Automation, Seoul, Korea, May 2001.

[4] Stoeter S.A., Burt I. T, Papanikolopoulos N. Scout Robot Motion Model // Proc. of the IEEE Intern. Conf. on Robotics and Automation, Taipei, Taiwan, May 2003.

[5] Drenner A., Burt I., Dahlin T., Kratochvil B., McMillen C. P., Nelson B., Papanikolopoulos N., Rybski P. E., Stubbs K., Waletzko D., Yesin K. B. Mobility Enhancements to the Scout Robot Platform // Proc. of the 2002 IEEE Intern. Conf. on Robotics and Automation, Washington, DC, May 2002. — P. 1069–1074.

[6] Baxter J. W., Horn G. S., Leivers D. P. Fly-by-agent: Controlling a pool of UAVs via a multi-agent system //Knowledge-Based Systems. – 2008. – T. 21. – №. 3. – C. 232-237.

[7] Kamada T., Oikawa K. AMADEUS: A Mobile, Autonomous Decentralized Utility System for Indoor Transportation // IEEE Intern. Conf. on Robotics and Automation, Leuven, Belgium, May 16–20, 1998. — V. 4. — P. 2229–2236.

[8] Liu, Y., & Nejat, G. (2016). Multirobot cooperative learning for semiautonomous control in urban search and rescue applications. Journal of Field Robotics, 33(4), 512-536.

[9] Yan, Z., Jouandeau, N., & Cherif, A. A. (2013). A survey and analysis of multi-robot coordination. International Journal of Advanced Robotic Systems, 10(12), 399.

[10] Borselius, N. (2002). Mobile agent security. Electronics & Communication Engineering Journal, 14(5), 211-218.

[11] Page J., Zaslavsky A., Indrawan M. A buddy model of security for mobile agent communities operating in pervasive scenarios //Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation-Volume 32. – Australian Computer Society, Inc., 2004. – C. 17-25.

[12] Sander, T., & Tschudin, C. F. (1998). Protecting mobile agents against malicious hosts. In Mobile agents and security (pp. 44-60). Springer, Berlin, Heidelberg.

[13] Tate, S. R. (2004). Mobile agent security through multi-agent cryptographic protocols (Doctoral dissertation, UNIVERSITY OF NORTH TEXAS).

[14] Guan, X., Yang, Y., & You, J. (2000, May). POM-a mobile agent security model against malicious hosts. In hpc (p. 1165). IEEE.

[15] Zikratov, I. A., Lebedev, I. S., Gurtov, A. V., & Kuzmich, E. V. (2014, October). Securing swarm intellect robots with a police office model. In Application of Information and Communication Technologies (AICT), 2014 IEEE 8th International Conference on (pp. 1-5). IEEE.

[16] Scarani V, Bechmann-Pasquinucci H, Cerf N J et al. 2009 Rev. Mod. Phys. 81 1301–1350

[17] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India ~IEEE, New York, 1984), pp. 175–179.

[18] Bennett, Charles H. "Quantum cryptography using any two nonorthogonal states." Physical review letters 68.21 (1992): 3121

[19] Huttner, B., Imoto, N., Gisin, N., & Mor, T. (1995). Quantum cryptography with coherent states. Physical Review A, 51(3), 1863.

[20] M. B. Dias, R. Zlot, N. Kalra and A. Stentz, "Market-Based Multirobot Coordination: A Survey and Analysis," in Proceedings of the IEEE, vol. 94, no. 7, pp. 1257-1270, July 2006. doi: 10.1109/JPROC.2006.876939

[21] Viksnin I.I., Iureva R.A., Komarov I.I., Drannik A.L. Assessment of stability of algorithms based on trust and reputation model // Proc. 18th Conference FRUCT-ISPIT. St. Petersburg, Russia, 2016. P. 364–369.