Police office model for multi-agent robotic systems

Police office model for multi-agent robotic systems

Ilya Viksnin[1*], Sergey Chuprov[1], Maria Usova[1], Danil Zakoldaev[1]

[1] Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, Kronverksky Pr., 49, St. Petersburg, 197101, Russia

* E-mail: wixnin@cit.ifmo.ru

Abstract. The paper discusses the methods of protecting information in mobile robotic systems. The problem of ensuring information security is formulated and the ways to solve it are considered. 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 office model. The authors have developed a software simulator and conducted a number of experiments using methods of trust and reputation for analyzing the effectiveness of such a system organization. Interpretation of experimental results allows us to conclude that the methods used are appropriate.

1. 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. In scientific research, such systems, which are a combination of information and physical components, are called cyber-physical systems (CPS) [2].

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.

Suitable examples of research in the field of coordinating the activities of a group of robots are the projects [3–8].

Unlike the approach using a single robot to solve various problems, the use of MARS 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 [9].

2. Security problem in Multi-agent robotic system

Intruders can threaten any information system with information security (IS). 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.

Some approaches that have gained popularity for ensuring IS in MARS have been described in the [11–13].

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.

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.

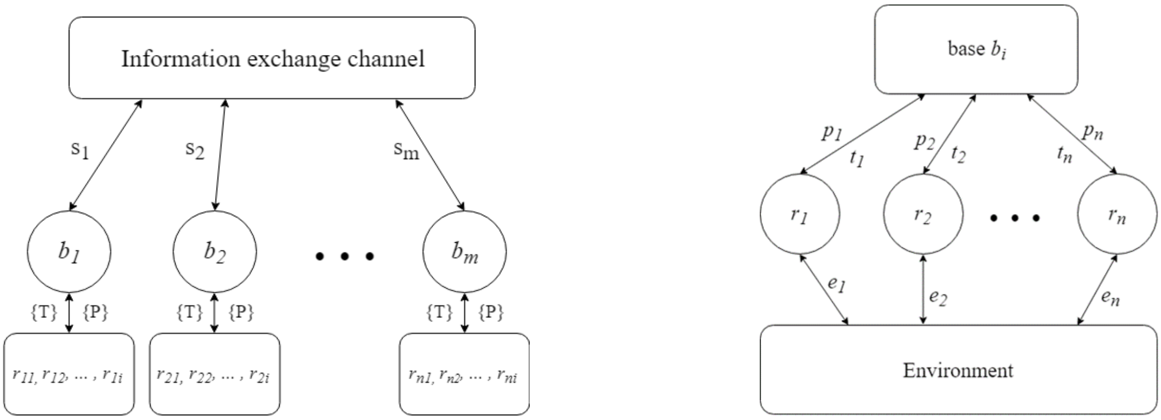
Methods of ensuring confidentiality of information are one of the key aspects of the successful operation of the MARS. The authors of the paper consider the application of quantum encryption methods as one of the ways to solve this problem. However, the use of quantum encryption requires a change in 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.

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. 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 [17–19].

3. Police office model for mobile robotic systems

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 $B=\{b_1,b_2,...,b_m\}$ 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 $R=\{r_1,r_2,...,r_n\}$ 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 (a), 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.



(a) (b)

Figure 1. (a) agent-bases top-level interaction diagram; (b) diagram of the low-level interaction between robots and bases.

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 1 (b), 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.

The tasks are the set $T=\{t_1,t_2,...t_p\}$ 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.

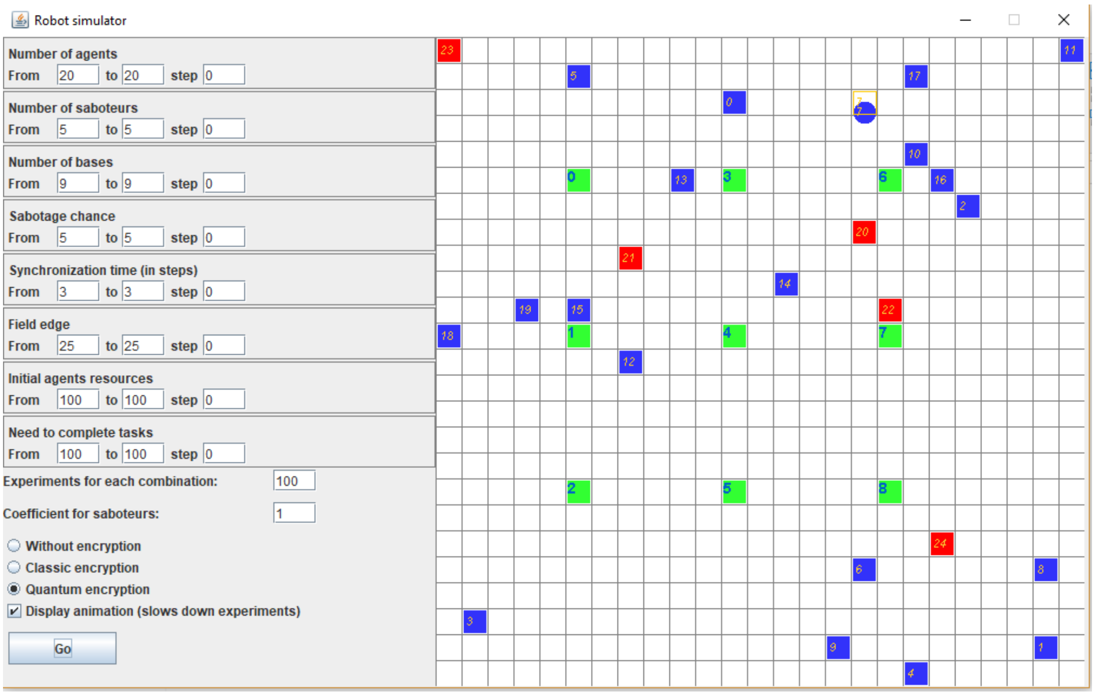
4. Experimental part

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.

The following conditions were set within the framework of experiment:

- 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 2.



Number of agents
From 20 to 20 step 0

Number of saboteurs
From 5 to 5 step 0

Number of bases
From 9 to 9 step 0

Sabotage chance
From 5 to 5 step 0

Synchronization time (in steps)
From 3 to 3 step 0

Field edge
From 25 to 25 step 0

Initial agents resources
From 100 to 100 step 0

Need to complete tasks
From 100 to 100 step 0

Experiments for each combination: 100

Coefficient for saboteurs: 1

○ Without encryption
○ Classic encryption
● Quantum encryption
☑ Display animation (slows down experiments)

Figure 2. 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.

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].

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.

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.

Table 1. 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 2. 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

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.

5. Conclusion

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 the 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* (Boston: Springer)

[2] Wolf W 2009 *Computer* **42** (3) 88–89

[3] Rybski P E, Paul E et al. 2002 *IEEE transactions on Robotics and Automation* **18** (5) 713–727

[4] Stoeter S A, Burt I T and Papanikolopoulos N 2003 *Proc. of the IEEE Intern. Conf. on Robotics and Automation* 4264–4269

[5] Drenner A et al. 2002 *Proc. of the 2002 IEEE Intern. Conf. on Robotics and Automation* 1069–1074

[6] Baxter J W, Horn G S and Leivers D P 2008 *Knowledge-Based Systems* **21** (3) 232–237

[7] Kamada T and Oikawa K 1998 *IEEE Intern. Conf. on Robotics and Automation* 2229–2236

[8] Liu Y and Nejat G 2016 *Journal of Field Robotics* **33** (4) 512–536

[9] Yan Z, Jouandeau N and Cherif A A 2013 *International Journal of Advanced Robotic Systems* **10** (12) 399

[10] Borselius N 2002 *Electronics & Communication Engineering Journal* **14** (5) 211–218

[11] Page J, Zaslavsky A, Indrawan M 2004 *Proc. of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation* 17–25

[12] Sander T and Tschudin C F 1998 *Protecting mobile agents against malicious hosts. In Mobile agents and security* (Berlin: Springer)

[13] Tate S R 2004 *Mobile agent security through multi-agent cryptographic protocols* (Denton: University of North Texas)

[14] Guan X, Yang Y and You J 2000 *Proc. of Fourth Int. Conf./Exhibition on High Performance Computing in the Asia-Pacific Region* 1165

[15] Zikratov I A, Lebedev I S, Gurtov A V and Kuzmich E V 2014 *Proc. Of IEEE 8th International Conference* 1–5

[16] Scarani V et al. 2009 *Rev. Mod. Phys.* **81** 1301–1350

[17] Bennett C H and Brassard G 1984 *Proc. of the IEEE International Conference on Computers, Systems and Signal Processing* 175–179

[18] Bennett C H 1992 *Physical review letters* **68** (21) 3121

[19] Huttner B, Imoto N, Gisin N and Mor T 1995 *Physical Review A* **51** (3) 1863

[20] Dias M B, Zlot R, Kalra N and Stentz A 2006 *Proc. of the IEEE* **94** (7) 1257–1270

[21] Viksnin I I, Iureva R A, Komarov I I and Drannik A L 2016 *Proc. of 18th Conference FRUCT-ISPIT* 364–369