JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

CONFIDENTIALITY ASSURANCE IN MULTI-AGENT ROBOTIC SYSTEM

Zakoldaev D. A.[1], Vorobeva A. A[2]

[1,2]PhD, associate Professor, Department Computer Systems Design and Security, St. Petersburg National Research University of Information Technologies, Mechanics and Optics, Russia, St. Petersburg

Email: d.zakoldaev@itmo.ru

Received: 14 March 2020 Revised and Accepted: 8 July 2020

ABSTRACT: In this paper, the authors consider the feasibility of using quantum encryption in a multi-agent robotic system. The authors consider examples of such systems, describe the functional structure of the system in question, describe the scheme for ensuring information security. Finally, the authors see the use of quantum cryptographic algorithms appropriate for resolving the issue of confidentiality in multi-agent robotic systems and believe that this method has the potential for further scientific developments in the field of security in multi-agent robotic systems.

KEYWORDS: multi-agent robotic system; quantum encryption; information security

I. INTRODUCTION

At the turn of the 20th and 21st centuries, interest was growing in the problem of constructing autonomous robotic systems in connection with the expansion of their field of application and the expansion of capabilities in the field of robotics. Multi-agent robotic systems (MARS), as organized groups of robots, have a great potential for development in the field of industry, transport, and different dangerous and complex tasks i.e. elimination of consequences of disasters, rescue and search operations, security tasks, etc. (1)

Work on the project "MARTHA" (2) was conducted in France with the aim of developing methods for organizing group interaction of robots for organizing the transportation of goods in the premises through the centralized management of the group. This method of organizing management was used in the DARPA project in the development of software and hardware for managing groups of robotic scouts for monitoring premises (3).

The existence of such MARS makes it possible to accomplish the tasks autonomously, making calculations of high accuracy, to improve the reliability of the systems used at a low cost of equipment. A single task can be assigned to a single robot. When the complexity of the task increases, it is necessary to increase the computing power and the quantity of available resources, which can be achieved by increasing the number of used robots.

In this paper, we consider the MARS, consisting of a set of agent-bases $B = \{b_1,b_2,...,b_m\}$, a set of agent-robots $R = \{r_1,r_2,...,r_n\}$ and of a set of information transmitted in the system $I = \{i_1,i_2,...,i_l\}$.

The bases are randomly distributed over the territory of MARS functioning, the “coverage zone” of the base b_j will be called the zone in which boundaries the agents are able to maintain communication with b_j base. The I is stand for the set of elementary messages that are transmitted in the system and contain data about the identification numbers of the agents, their coordinates, data on the tasks assigned, etc. The set $T = \{t_1,t_2,...,t_k\}$ contains tasks, which are distributed among agent-robots by the bases using task auction. The examples of task allocation auctions in MARS can be find in (4).

Necessary conditions for the selection of the agent r_i by the performer of the task t_j are:

- sufficient resources available for the task;
- the resource costs of the agent r_i for the task are minimal relative to the costs of other agents;
- the status of the agent is "free" (at the moment the agent does not perform any other task from the given set).

In this system, the agent’s task is to move from the starting point A to the end point B within the scope of any of the bases. The goal of the robot group is to perform all tasks with maximum efficiency.

Communication and control among agents occurs on a two-level communication channel. Centralized control is implemented at the robot-base level. The robot-agent sends the requested data to the base, in which coverage zone it is, and also receives a response from it in the form of a task or message. Decentralized (swarm) interaction is realized at the level of the set B. Agent-bases make decisions about the distribution of tasks between the agents of the set *R*, about checking these agents for violations, for blocking robots-intruders, etc.

II. CONFIDENTIALITY IN MARS

For correct functioning of MARS, it is necessary to ensure the information security (IS) of the system.

To achieve a high level of MARS security, a number of hardware, and software are used to ensure the confidentiality, integrity and availability of stored and transmitted information in the system.

Many MARS currently being created, for example, Google Driverless Car (5), are used to work with confidential data such as user data, location coordinates, etc. In this case, additional protection of information exchange channels and databases is necessary. Lack of proper attention to the problem of securing confidentiality of information in the MARS can lead to the interception and use of the data obtained, access to the system and destructive impact on it (6).

The notion of "confidentiality" in the MARS will be understood as the state of the system's security against unauthorized access to information inside the system. The consequences of breach of confidentiality entail damage, the size of which is determined by the degree of confidentiality of the disclosed data (7).

We introduce the following characteristics for each element of the set of elementary messages $I = \{i_1, i_{2,\dots,}i_l\}$:

- Coefficient of information cost $c = \{1,2,3\}$. This coefficient characterizes the amount of damage in case of information disclosure or its interception by an attacker;
- Coefficient of relevance of information $a = \{1,2,3\}$. This coefficient characterizes the degree of relevance of information for a given time iteration.

Based on these coefficients, we introduce the degree of confidentiality of the message:

$q = c * a$

In this case, the set of elementary messages has the following form of recording:

$I = \{i \mid q\}$, *where* $q = \{1,2,3,4,6,9\}$

The required level of security of information transmission and storage channels for different cost indicators and the relevance of messages are assessed to ensure the proper level of confidentiality and presented in table 1.

Table 1. Required level of security

		Cost of information		
		1	2	3
Relevance of information	1	medium	medium	high
	2	medium	high	very high
	3	high	very high	very high

III. INFORMATION INTERACTION BETWEEN AGENTS USING QUANTUM ENCRYPTION

We consider three possible models for the functioning of the MARS:

1. without the use of encryption of the communication channel between robots and bases;
2. using the algorithms of "classical" encryption (DES, AES, RSA, etc.);
3. using the algorithms of quantum encryption.

The algorithms of agent interaction in such systems differ from each other by the presence of a chain of actions associated with encryption of channels. In the first model, agents interact without using encryption algorithms. The second uses “classical” cryptographic algorithms for encryption, which means the time spent on encrypting and decrypting messages. Agents in the third model use algorithms for quantum encryption. In this scheme, the agent-bases have a module with a receiver and a transmitter for communicating with the bases, at the upper level, and also with a receiver and transmitter for communicating with the lower-level robot agents. The lower-level robots have a receiver and transmitter only for communicating with the bases and do not have the opportunity to communicate with other lower-level robots. Such a solution is difficult to implement, but this is an engineering task that will be solved in the future. Quantum key generation occurs according to the following algorithm:

1. Agent-transmitter A (Alice) sends a random sequence of photons to the agent-receiver B (Bob);
2. Bob analyzes the information received;
3. Alice and Bob form a "draft" version of the encryption key;
4. Clarify the encryption key. At this stage, Alice and Bob identify errors in the draft version of the key or form a new one, returning to paragraph 1 of this algorithm;
5. Enhance the secret of the key using the hash function passed by Alice.

6. The scheme of the system functioning using the mechanisms of quantum encryption is presented in fig. 1.

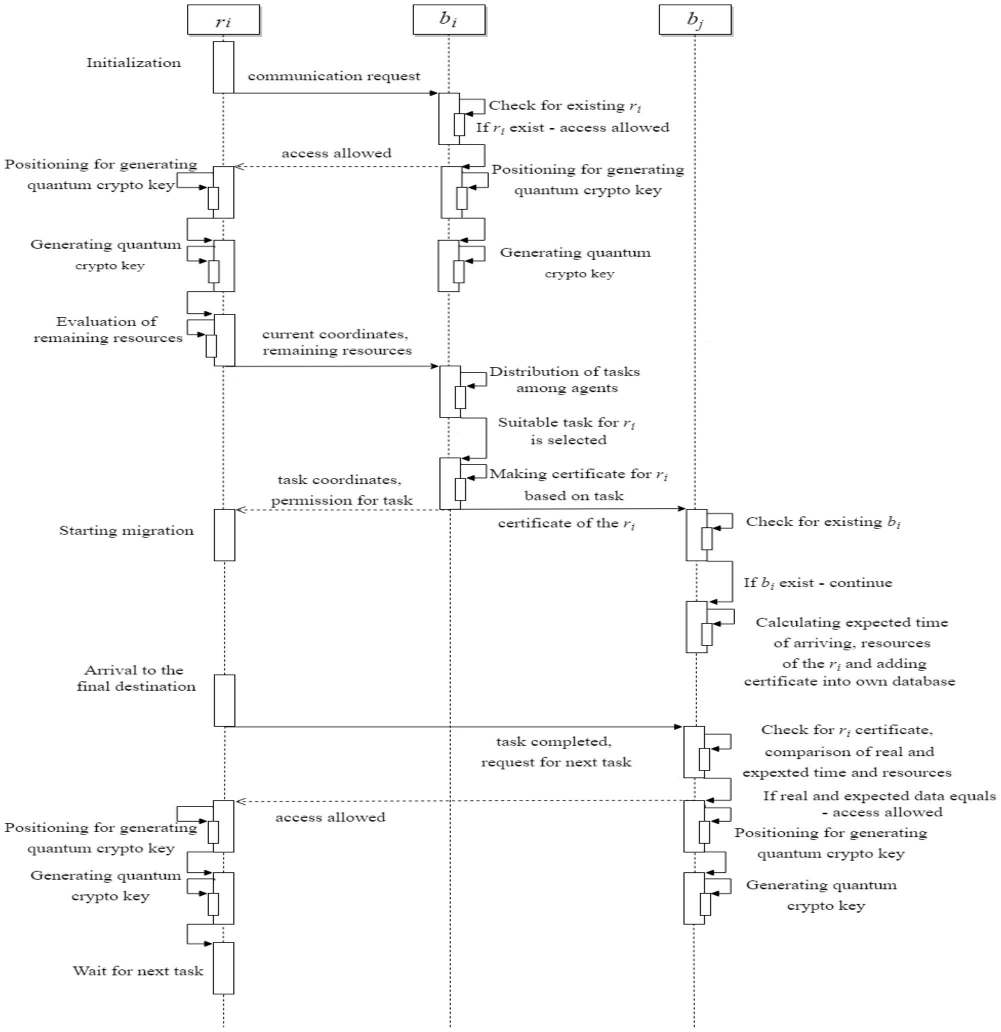
ri
b_i
b_j
Initialization
communication request
Check for existing r_i
If r_i exist - access allowed
access allowed
Positioning for generating quantum crypto key
Positioning for generating quantum crypto key
Generating quantum crypto key
Generating quantum crypto key
Evaluation of remaining resources
current coordinates, remaining resources
Distribution of tasks among agents
Suitable task for r_i is selected
Making certificate for r_i based on task
task coordinates, permission for task
Starting migration
certificate of the r_i
Check for existing b_i
If b_i exist - continue
Calculating expected time of arriving, resources of the r_i and adding certificate into own database
Arrival to the final destination
task completed, request for next task
Check for r_i certificate, comparison of real and expexted time and resources
If real and expected data equals - access allowed
access allowed
Positioning for generating quantum crypto key
Positioning for generating quantum crypto key
Generating quantum crypto key
Generating quantum crypto key
Wait for next task

Figure 1: Function diagram of system working using model with link encryption via quantum

Each key has its lifetime t_{key}, which needs to be replaced with a new one after this time iteration.

The algorithms of quantum cryptography are widely used in data storage and transmission systems, since their use allows to achieve a high level of system security: the probability of choosing a certificate randomly tends to zero.

When an intruder tries to eavesdrop the channel, he inevitably makes mistakes in the information transmitted through the channel, so that it can be detected. (8)

On the other hand, the use of quantum encryption has a number of drawbacks (9):

- entails time costs for the formation of a certificate (key), encryption and decryption of messages;
- the key has a limited lifetime and needs to be replaced;

In order to assess the level of information security, the authors propose a model of threats and the model of the intruder. In the future, it is appropriate to conduct a risk assessment, based on these models.

The function diagram on the figure 2 describes agents' interaction using quantum encryption which includes the following stages:

1. on the first stage robot-agent r_i sends communication request to a base-agent b_i, which control this area, b_i checks if the agent exists;
2. agents r_i and b_i generate crypto key for encrypted channel;
3. after estimating of agents' resources the base b_i starts the tasks distribution between robot-agents. By the end of this stage, the robot r_i gets suitable task;

4. r_i moves from the area of the base b_i to the area of the base b_j which controls robot's movement;
5. on the final stage r_i sends communication request to the new controlling base-agent b_j. They generate new crypto-key and r_i waits for the new task.

IV. CONCLUSION

A model of functioning of a multi-agent robotic system is proposed. The model uses an approach to the organization of functioning on the basis of the Police Office Model - the area of the model is divided into equal areas where the "police offices" are located, which are responsible for the development of optimal plans of agents' actions. Between the "police offices" is carried out information interaction, which allows to guarantee the development of a joint optimal plan. Low-level agents (elements of the mobile robotic system) carry out the action plans provided to them. The connection between agents and "police offices", as well as between "police offices" is carried out using quantum encryption keys.

Based on the proposed model of functioning, a threat model has been developed that includes a classification of threats, as well as an assessment of the likelihood of their implementation. The use of this model will allow us to assess the main threats, which facilitates the adoption of optimal solutions for the implementation of the countermeasures by the owner of the mobile robotic system.

In addition to the threat model in, the intruder model is presented, including an assessment of the possibility of the intruder appearing at various stages of the system life cycle. The main ways to intruder's influence on the system are given.

The results obtained in this work can become the basis for further studies of the robustness of multi-agent robotic systems. Based on the proposed models of threats and the offender, it is planned to determine the methodology for assessing the risks of implementing threats to the information security of the multi-agent robotic system, and to develop a method for assessing the security of the system from various attacks.

ACKNOWLEDGEMENT

This article was prepared with the Financial support of the Ministry of Science and Higher Education of the Russian Federation under the agreement No. 075-15-2019-1707 from 22.11.2019 (identifier RFMEFI60519X0189, internal number 05.605.21.0189).

V. REFERENCES

[1] Liu, J., Wu, J., Jain, L. (2001). Multiagent Robotic Systems. Boca Raton: CRC Press.

[2] Alami R. et al., "Multi-robot cooperation in the MARTHA project", *IEEE Robotics & Automation Magazine*, vol.5.1, 1998, pp. 36-47.

[3] Rybski P. E. et al. "System architecture for versatile autonomous and teleoperated control of multiple miniature robots", *Robotics and Automation*, vol. 3, 2001, pp. 2917-2922.

[4] 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, July 2006, pp. 1257-1270

[5] Dethe S. N., Shevatkar V. S., Bijwe R. P., "Google Driverless Car", *IJSRSET*, vol. 2, April 2016, pp. 133-137.

[6] Poslad S., Charlton P., Calisti M. "Specifying standard security mechanisms in multi-agent systems", *Workshop on Deception, Fraud and Trust in Agent Societies*, 2002, pp. 163-176.

[7] Rabai L. B. A. et al., "A cybersecurity model in cloud computing environments", *Journal of King Saud University-Computer and Information Sciences*, 2013, vol. 25.1, pp. 63-75.

[8] C. Kollmitzer., M. Pivk, *Applied quantum cryptography*. Springer, 2010.

[9] D. Bouwmeester., A.K. Ekert and A. Zeilinger, *The physics of quantum information: quantum cryptography, quantum teleportation, quantum computation*. Springer Science & Business Media, 2013.