Police Office Model for Mobile Robotic Systems with Quantum Encryption

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

Egor Marinenkov
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
Saint-Petersburg, Russia
egormarinenkov@gmail.com

Nikita Shepin
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
Saint-Petersburg, Russia
shepkanturgorn@gmail.com

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

***Abstract*— This paper presents a study on assessment of the effectiveness of the multi-agent robotic system in various variations: without using encryption of messages, transmitted between agents, using "classical" cryptographic algorithms and using messages encryption via quantum cryptographic algorithms. One of the key aspects of the effective functioning of mobile robotics is the maintenance of information security. The analysis of methods and models of information security of multi-agent information systems was carried out. This analysis showed the existence of a large number of methods for ensuring information security of the group, however, many of these techniques related to confidentiality of information cannot guarantee an unambiguous maintenance of this feature. The authors consider the use quantum encryption as one of the most important methods, which guarantees the solution of this problem. Existing approaches to the generation of quantum encryption keys require considerable time. To compare the efficiency of the multi-agent robotic systems the authors developed a software simulator. The time spent by a group of robots to fulfill all the goals was used as a criterion work effectiveness of multi-agent robotic system. On the basis of the obtained modeling results, a conclusion is made about the advisability of using quantum encryption.**

***Keywords*— multi-agent robotic system, information security, quantum cryptography, agent, robot, police office model**

I. INTRODUCTION

Rapid development of the era of robotics has been starting since 60th years of the last century and continuing today. At the dawn of the new century intellectual robotic systems have been developed as a part of multi-agent systems, used for solving complex problems, required high reliability [1].

Generally, for solving the majority of problems single or groups of robots are being used, in which every robot is independent of others. This approach allows solving separate simple tasks, however it is notable for its limitations of resources and capabilities of the single robotic device. Groups of interacting robots became widely used for solving complex tasks more effectively, this groups begun to be called intellectual multi-agent robotic systems (MARS) [2]. Currently, MARS begun to be widely used in different spheres of human activity in order to automation and optimization to better address complex and/or dangerous work in in various fields of our life. [3-14]

There are two approaches to robotic systems development: [15]

- using single robot, constitutes complex multifunctional object;
- using group of robots, each of which is a simple object.

In the first case, with increasing of task complexity there is the issue of robots resources limitation. Robots functional is being expanded, cost and complexity increasing respectively. Under this approach reliability is due to least resilient component of the system, what makes system dependent on one of the robotic device component, failure of which may affect the functioning the whole system.

Under second approach subtasks is being separated among group of autonomous robots. These robots are relatively simple, what have positive impact on reliability and extensibility of the system in case of increasing tasks complexity. [15]

II. INFORMATION SECURITY OF MULTI-AGENT ROBOTIC SYSTEM

Information security (IS) is considered as significant component of correctly functioning MARS. Interaction in MARS is based on communication between agents and also on communication of information and physical components. During this interaction may arise vulnerabilities, which affecting the efficiency of the system functioning. Ensuring basic IS features of the system are necessary to reduce probability of threat realization. Such features are:

- confidentiality – guarantees protection from the disclosure of information, transferred between agents to third parties. To ensure this feature, it is necessary to implement secure data transfer between agents;
- integrity – guarantees that data has not been modified during transmission. To maintain the efficiency of the system, it is necessary to ensure the integrity of the entire stream of transmitted data;

- availability – guarantee of the possibility of receiving information by the agent in the presence of such a right. The deterioration in accessibility can be caused by different attacks on the system.

In [16] authors divided main attacks on multi-agent systems on 16 classes, analyzed different methods of information security and divided the methods into prevention and detection methods using DREAD methodic. The existing methods of MARS IS allows to achieve acceptable values of security under destructive information impacts committed by an intruder [17,18]. For example, methods of mobile cryptography allow to achieve acceptable values of availability and confidentiality of information in the system [19]. Also, acceptable values of the availability and confidentiality of information in the system can be attained with the help of protected conditions method [20].

Authors of [21] are considering problems that affect the integrity of the information circulating in the system. Such problems often caused by malfunctions in a particular element. Authors of [22] divide the IS instruments on three categories: proactive mechanisms, reactive mechanisms, principles of design and analysis. Buddy Security Model [23] and a Xudong's Police Office Model [18] serves as examples of MARS IS, however these models are not universal and have their drawbacks. It should be noted that the universal approaches of robotics systems IS are not exist yet [24]. This is due to a large variety of unique features of different kinds of MARS, dependence on aims and tasks of such MARS.

Analyzing existing mechanisms of IS in multi-agent systems (MAS (MARS)), it can be conditionally divided into two groups - based on principles of decentralized control of IS and centralized control of IS [2]. In the implementation of centralized approach IS tasks is solving by special structures, which called Police Offices in Xudong's model [18]. In this model MAS divided into several areas, each of which has a module responsible for interacting and tasks distribution among agents.

III. Information security among agents in Police Office model (POM)

Information interaction (II) in the system is realized using the POM, that described in [18]. Models of MARS functioning in current work can be described as follows:

1) *without using link encryption between robot-agents and agent-bases;*
2) *using "classic" encryption algorithms;*
3) *using quantum encryption algorithms.*

For all models, there are a number of common actions. The algorithm of functioning differs only absence or presence of an encryption algorithm and related actions to this algorithm. In the first model of functioning there is no link encryption, and agents do not spend time on encryption and decryption procedures. The second model implies the use "classical" cryptographic algorithms for messages encryption. Under the methods of "classical" encryption are understood such cryptographic algorithms as RSA, AES, DES and so on. [25-27] The third model uses quantum communication channel encryption. Modern research in the field of quantum cryptography allows the generation of quantum keys in such a way that any intruder attempted to introduce into the communication channel will certainly be detected. [28] There are some algorithms of quantum cryptography: BB82 [29], B92 [30], BB84(4+2) protocol [31], the Einstein-Podolsky-Rosen (EPR) scheme [32, 33], etc. Before sending and after receiving massages agents need time for encryption and decryption procedures. In the model with quantum encryption agents need to perform positioning procedure which means pointing sensors at each other to generate quantum key. Only after this actions agents begin to exchange encrypted messages.

The transfer of information between agents is organized as follows: each base has a module that consists of a receiver and a transmitter for communicating at the upper level, and the same module for transmitting messages at the lower level, between the base and the mobile robots. Robots, in turn, have a receiver and transmitter only for communicating with databases, without having the ability to communicate with each other. Before the message is sent, a cryptographic key is generated (in schemes using communication channel encryption). Such a scheme of functioning at the moment is difficult to implement from an engineering point of view, but this is a matter of time.

Diagram on the figure 1 demonstrates information flows among agents (b_i and b_j – bases, r_k – one of the robot-agents).

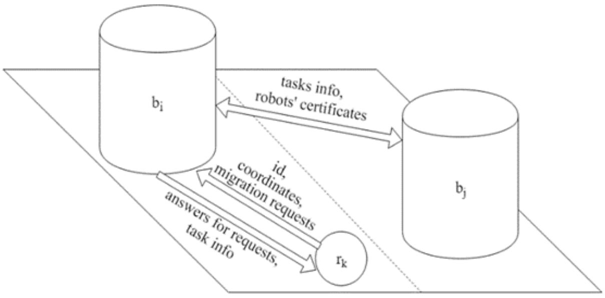


Fig. 1. Information flows among agents in the system

Functioning of the system with using various models differs only in functions and, respectively, in time, which agents require for performing this functions. On the figure 2 illustrated the diagram of system functioning without using link encryption. In this model agents of the system are not required to spend time on cypher-key generation and on encryption and decryption of transmitted information.

On the figure 3 illustrated function diagram of the system working using encryption of the information transmitted among agents via "classic" cryptographic algorithms. Before the communication session begins, robot-agent and base need to generate cypher-key between each other, after that agents can exchange encrypted messages.

On the figure 4 illustrated the function diagram of the model with quantum link encryption of the messages transmitted among agents. Before the communication session begins, robot-agent and base need to perform the positioning procedure, which is required for pointing quantum sensors at each other for the subsequent cypher-key generation. Only then agents able to exchange encrypted messages.

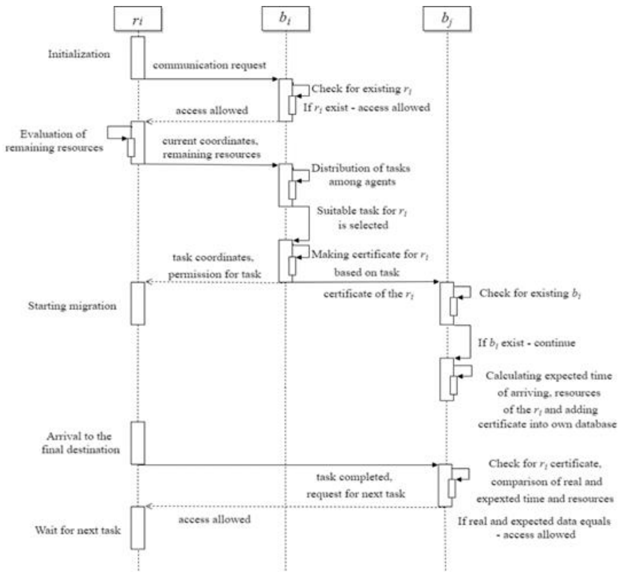

ri
bi
bj
Initialization
communication request
Check for existing ri
If ri exist - access allowed
access allowed
Evaluation of remaining resources
current coordinates, remaining resources
Distribution of tasks among agents
Suitable task for ri is selected
task coordinates, permission for task
Making certificate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

Fig. 2. Function diagram of system working using model without message encryption

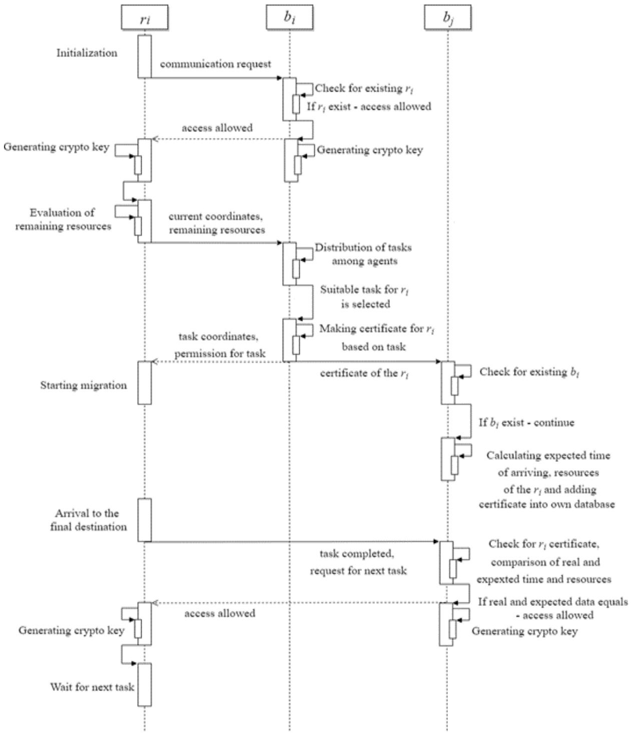

ri
bi
bj
Initialization
communication request
Check for existing ri
If ri exist - access allowed
access allowed
Generating crypto key
Generating crypto key
Evaluation of remaining resources
current coordinates, remaining resources
Distribution of tasks among agents
Suitable task for ri is selected
Making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

Fig. 3. Function diagram of system working using model with message encryption via “classical” cryptographic algorithms

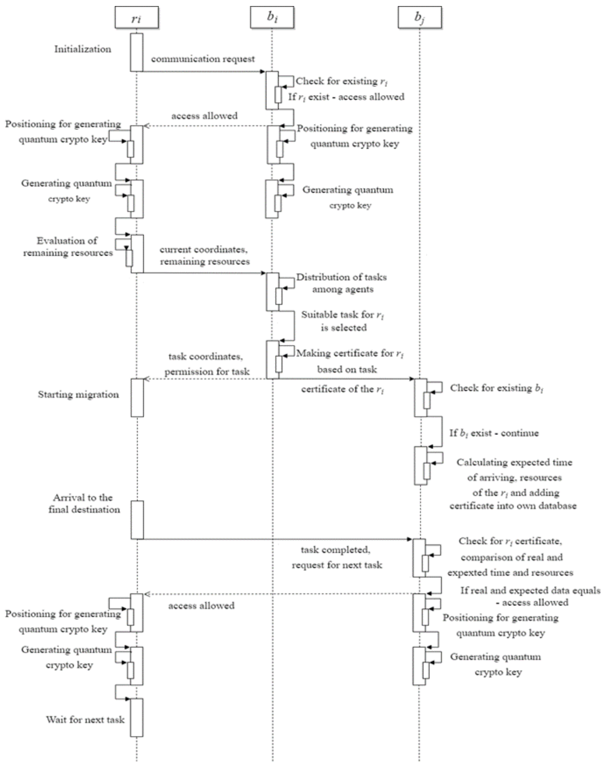

ri
bi
bj
Initialization
communication request
Check for existing ri
If ri exist - access allowed
access allowed
Positioning for generating quantum crypto key
Positioning for generating quantum crypto key
Generating quantum crypto key
Generating quantum crypto key
Evaluation of remaining resources
current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

Fig. 4. Function diagram of system working using model with message encryption via quantum cryptographic algorithms

IV. Experiments Design

Main characteristics:

- The polygon is a square area 25 on 25 cells, over which agents move;
- 9 fixed agents-bases *b*, 20 mobile robot agents *r*;
- each base *b* occupies one cell and has its own coverage area, which is 11%-15% (it is necessary that the base zones are "overlapping", so that they can communicate with each other) from the size of the polygon in the center of which it is located and acts as a police station;
- each robot agent *r* occupies one cell;
- agents must perform *N* tasks;
- *T* (time to reach the goal) → min;
- tasks → max.

A group of agents begins to perform the tasks on the polygon territory. The goal is to perform all tasks with maximum efficiency (spending less time). The task is to move the robots from a certain cell of A to a certain cell B. The goal is achieved if all tasks are completed. The tasks are known to all agents from the beginning of operation, they are distributed by agent-bases between robot-agents using an auction which determines the robot to perform the task as efficiently as possible (spending less resources). If a robot that performs the task fails, it is delegated to another robot using an auction. At the beginning of the experiment, a number of tasks are distributed among the robots, the following tasks are distributed as previous tasks are completed.

Each agent has a unique identifier (id), each base has its own database of bases, a database of robotic agents and a database of tasks.

The robot exchanges the following types of information with the bases – id, information about the remaining resources, current coordinates, requests for movement, status (busy/free).

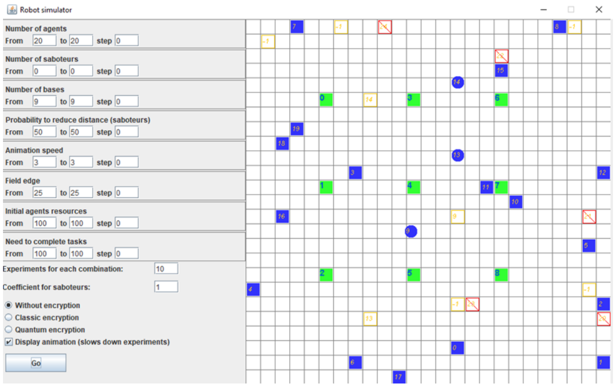
The experiment is performed without using encryption of communication channels between agents, using "classical" encryption and using quantum encryption of communication channels. At the end of the experiment, the time of the group's operation should be recorded.

Steps of the experiment may be presented as follow:

- base b_i, located in the group start area, distributes tasks between robots r by an auction;
- the robot r_i, chosen for the task, sends the request to the database to move to the endpoint of the task (authorization takes place only once, at the beginning of the experiment);
- the database checks the presence of this robot r_i in the database, after which it gives the robot a unique certificate and robot starts to perform the task;
- after the robot has gone to perform the task, the b_i base sends the certificate to the base b_j, in which action zone the end point of the robot r_i route is located;
- base b_j receives a certificate from the b_i database, checks the existence of the b_i base in the database, calculates the remainder of resources and the arrival time of the robot r_i, then enters the certificate into its own database;
- upon arrival of the robot r_i to the end point of the route, in the zone of the base b_j, the robot presents its certificate to the base b_j, the base b_j compares it with the available certificate and, in the absence of conflicting information, gives the robot r_i access to the b_j base;

V. Results

A software simulator was developed by authors for system behavior modeling and evaluating the effectiveness of the system models. The simulator is written in Java and has simple user interface. The results are written to a .csv file. On the figure 5 interface is presented.



Robot simulator

Number of agents
From 20 to 20 step 0

Number of saboteurs
From 0 to 0 step 0

Number of bases
From 9 to 9 step 0

Probability to reduce distance (saboteurs)
From 50 to 50 step 0

Animation speed
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: 10

Coefficient for saboteurs: 1

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

Fig. 5. Interface of the developed simulator.

An experiment was conducted to assess the behavior of the system and compare the time spent on performing all tasks. 10 experiments were performed for each model of the system functioning, the results for each model are shown in the table 1.

During each experiment, the target of the robots was to perform 100 tasks. At the beginning of each experiment, the robots are located at random positions of the polygon, which explains the time difference between the experiments. Analyzing the obtained results, it can be seen that the model using quantum encryption spends a little longer time, within the limits of the tasks assigned, to perform tasks than the other two models. At the same time, with the use of quantum encryption, the confidentiality of the information transmitted between agents is constantly ensured. This fact makes the model using quantum encryption a solution to the problem of maintaining confidentiality of information in the submitted MARS.

This fact makes the model using quantum encryption a solution to the problem of maintaining confidentiality of information in the submitted MARS.

TABLE I. Time, required for performing 100 tasks by the system without intruders

Type	***Unprotected***	***Classic***	***Quantum***
Time	105	212	290
	103	200	363
	120	196	342
	186	178	303
	105	215	278
	119	174	252
	135	167	447
	127	201	351
	119	201	285
	135	224	261
Average	125,4	196,8	317,2

CONCLUSION

In this work, the authors reviewed the existing means of ensuring the information security of the multi-agent robotic system. The basic principles of using POM with the use of quantum link encryption between agents of the system are considered. This study showed that existing mechanisms to ensure the information security of multi-agent robotic systems can not completely eliminate the problem of maintaining confidentiality of information. The authors considered a variant of using quantum key generation in the transmission of messages between agents. This option requires more time, but can guarantee the solution of the problem of maintaining confidentiality of information. To assess the effectiveness of the system, a software simulator was developed, data was obtained and analyzed, and a conclusion was made about the advisability of using quantum encryption in multi-agent robotic systems.

Further research in this area is planned by the authors to be linked to a model for assessing the risks of violations of information security. Thus, it is planned to assess the protection of multi-agent robotic system from various destructive information impacts. In addition, it seems important to determine the optimal parameters used for quantum key generation.

REFERENCES

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

[2] Anurag Ganguli, Sara Susca, Sonia Mart´ınez, Francesco Bullo, Jorge Cortes. On collective motion in sensor networks: sample problems and distributed algorithms // 44th IEEE Conference on Decision and Control, and the European Control Conference 2005.

[3] Stoeter, S. A., Rybski, P. E., Erickson, M. D., Gini, M., Hougen, D. F., Krantz, D. G., ... & Wyman, M. (2000, July). A robot team for exploration and surveillance: Design and architecture. In Proc. of the Int'l Conf. on Intelligent Autonomous Systems (pp. 767-774).

[4] Luo R.C., Chou Y.T., Liao C.T., Lai C.C., Tsai A.C. NCCU security warrior: An intelligent security robot system. IECON Proceedings (Industrial Electronics Conference). Taipei, Taiwan, 2007, art. no. 4460380, pp. 2960–2965. doi: 10.1109/IECON.2007.4460380

[5] Flann N.S., Moore K.L., Ma L. A small mobile robot for security and inspection operations. Control Engineering Practice, 2002, vol. 10, no. 11, pp. 1265–1270.

[6] Song, M., Tarn, T. J., & Xi, N. (2000). Integration of task scheduling, action planning, and control in robotic manufacturing systems. Proceedings of the IEEE, 88(7), 1097-1107.

[7] Bock, T., & Linner, T. (2016). Construction robots: elementary technologies and single-task construction robots (Vol. 3). Cambridge University Press.

[8] Alami R. et al. Multi-robot cooperation in the MARTHA project //IEEE Robotics & Automation Magazine. – 1998. – Т. 5. – №. 1. – С. 36-47.

[9] Nourbakhsh, I. R., Sycara, K., Koes, M., Yong, M., Lewis, M., & Burion, S. (2005). Human-robot teaming for search and rescue. IEEE Pervasive Computing, (1), 72-78.

[10] Markusson, O., Andersson, G., Adolfsson, J., Pettersson, P., Öster, J., & Jägenstedt, P. (2015). U.S. Patent No. 8,942,862. Washington, DC: U.S. Patent and Trademark Office.

[11] Moosavian, S. A. A., & Papadopoulos, E. (2007). Free-flying robots in space: an overview of dynamics modeling, planning and control. Robotica, 25(5), 537-547.

[12] Preising, B., Hsia, T. C., & Mittelstadt, B. (1991). A literature review: robots in medicine. IEEE Engineering in Medicine and Biology Magazine, 10(2), 13-22.

[13] Shibata, T. (2004). An overview of human interactive robots for psychological enrichment. Proceedings of the IEEE, 92(11), 1749-1758.

[14] Kamada T., Oikawa K. AMADEUS: a mobile, autonomous decentralized utility system for indoor transportation //Robotics and Automation, 1998. Proceedings. 1998 IEEE International Conference on. – IEEE, 1998. – Т. 3. – С. 2229-2236.

[15] Şahin E. Swarm robotics: From sources of inspiration to domains of application //International workshop on swarm robotics. – Springer, Berlin, Heidelberg, 2004. – С. 10-20.

[16] Bijani S., Robertson D. A review of attacks and security approaches in open multi-agent systems //Artificial Intelligence Review. – 2014. – P. 1-30.

[17] Huynh T. D., Jennings N. R., Shadbolt N. Developing an integrated trust and reputation model for open multi-agent systems. – 2004.

[18] Guan X., Yang Y., You J. POM-a mobile agent security model against malicious hosts //hpc. – IEEE, 2000. – С. 1165.

[19] Neeran K. M., Tripathi A. R. Security in the Ajanta MobileAgent system //Technical Report. Department of Computer Science, University of Minnesota. – 1999.

[20] Sander T., Tschudin C. F. Protecting mobile agents against malicious hosts //Mobile agents and security. – Springer, Berlin, Heidelberg, 1998. – С. 44-60.

[21] Komali R. S., MacKenzie A. B., Gilles R. P. Effect of selfish node behavior on efficient topology design //IEEE Transactions on mobile computing. – 2008. – Т. 7. – №. 9. – С. 1057-1070.)

[22] Zissis D., Lekkas D. Addressing cloud computing security issues //Future Generation computer systems. – 2012. – Т. 28. – №. 3. – С. 583-592.

[23] 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. – С. 17-25.

[24] Huynh T. D., Jennings N. R., Shadbolt N. R. An integrated trust and reputation model for open multi-agent systems //Autonomous Agents and Multi-Agent Systems. – 2006. – Т. 13. – №. 2. – С. 119-154.

[25] Rivest, Ronald L., Adi Shamir, and Leonard M. Adleman. "Cryptographic communications system and method." U.S. Patent No. 4,405,829. 20 Sep. 1983.

[26] NIST, AES. "Advanced encryption standard." FIPS Publication 197 (2001)

[27] DES Standard, D. E. (1977). Federal information processing standards publication 46. National Bureau of Standards, US Department of Commerce, 23.

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

[29] 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.

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

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

[32] Ekert, A. K. (1991). AK Ekert, Phys. Rev. Lett. 67, 661 (1991). Phys. Rev. Lett., 67, 661.

[33] Bennett, C. H., Brassard, G., & Mermin, N. D. (1992). Quantum cryptography without Bell's theorem. Physical Review Letters, 68(5), 557.