Trust and Reputation Mechanisms for Multi-agent Robotic Systems

Igor A. Zikratov[1], Ilya S. Lebedev[1], and Andrei V. Gurtov[2]

[1] ITMO University, Russia
[2] Helsinki Institute for Information Technology HIIT and
Department of Computer Science and Engineering, Aalto University, Finland

Abstract. In this paper we analyze the functioning of multi-agent robotic systems with decentralized control in conditions of destructive information influences from robots-saboteurs. We considered a type of hidden attacks using interception of messages, formation and transmission of misinformation to a group of robots, and also realizing other actions which have no visible signs of invasion into a group of robots. We analyze existing models of information security of the multi-agent information system based on a measure of trust, calculated in the course of interaction of agents. We suggest a mechanism of information security in which robots-agents produce levels of trust to each other on the basis of the situation analysis developing on a certain step of an iterative algorithm with the use of onboard sensor devices. For improving the metric of likeness of objects relating to one category ("saboteur" or "legitimate agent") we suggest an algorithm to calculate reputation of agents as a measure of the public opinion created in time about qualities of robots of the category "saboteur" in a group of legitimate robots-agents. It is shown that inter-cluster distance can serve as a metric of quality of trust models in multi-agent systems. We give an example showing the use of the developed mechanism for detection of saboteurs in different situations in using the basic algorithm of distribution of targets in a group of robots.

Keywords: Information security, groups of robots, multi-agent robotic systems, attack, vulnerability, modeling.

1 Introduction

Groups of robots implementing a complex system which consists of many simple devices is a new and actively developing direction of group robotic technology. We assume that desirable group behavior arises from interaction of robots-agents among themselves and their interaction with the environment. The interaction of agents happens in the environment out of a controlled territory that is in conditions where there is a possibility of physical access to robots by the attacker. In such system agents possess several important properties [1]:

S. Balandin et al. (Eds.): NEW2AN/ruSMART 2014, LNCS 8638, pp. 106–120, 2014.

- autonomy: agents are at least partially independent;
- limited view: none of agents have a view of whole system, or the system is so complicated that the knowledge of it has no practical application for the agent;
- decentralization: there are no agents who control all group.

Unique features of a multi-agent robotic system (MRS) complicate the use of existing mechanisms of information security (IS) and give opportunity to attackers to impact on group algorithms (adaptive behavior). The need for research in information security (IS), and also the qualitative description of main threats and features of their implementation in relation to MRS led to appearance of several publications [2, 3]. One of unique threats inherent for MRS as a multi-agent system is the use by attackers of robots-saboteurs who realize harmful actions. We understand robot-saboteur activities as a harmful information influence (attack) directed on implementation of a threat to information security concerning robots-agents R_{j} ($\mathrm{j} = \overline{1, \mathrm{N}}$) and realized with the use of information tools and technologies as a result of which the new action selected by agents won't promote an increase of system functionality in available conditions.

In this article we consider mechanisms of soft security directed on detection and neutralization of hidden attacks which do not have identified signs unlike attacks which are carried out by jamming of communication links, DDoS-attacks, cracking and compromising of ciphers, etc. In case of the hidden attacks, robots, their systems and communication links function in a standard mode. Realizing a hidden attack, robots-saboteurs of a warring party can provide false or misleading information, and traditional mechanisms of security can't protect users from this type of threats.

For protection against such hidden attacks we can use a method of the protected agent states, methods of mobile cryptography, a method of Ksyudong [6], Buddy Security Model [7, 8], which matches well with the principles of creation of decentralized systems. Besides, for providing of protection of the user from such threats, we use mechanisms of social monitoring, namely trust and reputation systems. These mechanisms are based on calculation of trust of agents to each other, realized in the course of monitoring of actions of an agent in the system [8, 9, 10, 11, 12]. Distinction in ways of computation of the trust level is caused by features of the domain where interaction of participants takes place. It can be the electronic markets, peer-to-peer networks, on-line social networks, etc. As a result, in existing models of trust there are different treatments of the concept of trust and reputation, different subjects and objects of trust are considered.

The goal of this paper is development of a method of protection of MRS from hidden attacks of robots-saboteurs, based on computation of a measure of trust and reputation to robots-agents in a group of robots in case of decentralized control.

The rest of the paper is organized as follows. In Section 2, we provide a brief survey on multi-agent robotic systems. In Section 3, we develop a model of multi-agent decision making using trust and reputation. In Section 4, we describe implementation of the model as well as its simulated functionality. Finally, Section 5 concludes the paper.

2 Functioning of Systems with Decentralized Planning of Actions

Robots-agents of MRS, unlike agents of MS, are equipped with the onboard sensor and measuring device from which the robot receives information about environment, and also a radio channel intended for information exchange in the course of execution of the target. We consider MRS actions when using the most widespread iterative procedure of optimization of a group decision, distribution of targets in a group of robots [13]. MRS functioning for this goal in a general form looks as follows.

Assume there are *M* targets and a group of robots which consists of *N* robots R_{j} ($\mathrm{j} = \overline{1,\mathrm{N}}$). A squad of forces (a number of robots for target execution) shall be selected for each target. The target is *provided* when it is selected by the necessary number of robots. The remained robots will form a reserve cluster. Each robot-agent knows coordinates of a target, its own coordinates, and a required squad of forces for each target. The robot "R" estimates efficiency of its actions for each target and tells an array of the estimates $D_j = [d_{j1},\ \ d_{j2},\ \ldots,\ \ d_{jM}]$ to remaining members of group. Matrix "D" with dimensionality (*N, M*), which elements are estimates of efficiency of the robot "*j*" for target "*l*", is created in a processor device (CPU) of each robot. Iterative procedures of formation of the group plan as a result of which for each target $T_l \in \mathbf{T}_c$ the equation maximum is provided, begins after matrix formation

$$\mathbf{Y}_c = \sum_{j,l=1}^{N} d_{jl} n_{jl} \to max, \tag{1}$$

in case of restrictions

$$\sum_{l=1}^{N} n_{jl} = 1,$$
$$\sum_{j=1}^{N} n_{jl} = n_l^{max},$$
$$d_{jl} \geq 0,$$

where

$$n_{jl} = \begin{cases} 1, & \text{if "}j\text{" robot selects "}l\text{" target,} \\ 0, & \text{otherwise.} \end{cases}$$

Here $j = \overline{1,N},\ l = \overline{1,N},$ a n_l^{max} is a necessary number of robots which must select "l" target.

The basis for iterative procedures is the analysis by every robot-agent of an array of estimates of efficiency and a selection of a target for which the value of an assessment of the efficiency is maximal. Then there is an information exchange about the selected decisions, the analysis and "discussion" of the decisions made by other robots. The agents with the value d_l, select the suitable target “*l*”, “eliminate” from a matrix **D** the provided targets and the robots which have selected the target according to an equation (1). As in the memory of all robots there are identical matrices **D**, and results of computation will match. The procedure repeats until all targets of a set *M* are provided. There is a modification of this algorithm which allows to consider not only estimates d_{jl}, but also a possibly of changes of a goal function if a robot R_j refuses the target selected from the current iterative loop and will select other target. A minor modification of the algorithm allows to resolve a situation when there are some agents with identical estimates of efficiency on one target.

Let’s review a trivial example. Assume a group of seven robots (*N*=7) needs to distribute two targets (*M*=2) A and B. It is known that each target should be provided with two agents. We will consider the distance from a robot to a target as a metric of efficiency of the target. That is, the closer the robot is located to the target, the higher is its efficiency. Assume the matrix **D** with estimates of efficiency looks as follows:

	A	B
D_1	3.2	1.0
D_2	1.9	2.5
D_3	0.7	5.4
D_4	3.6	3.5
D_5	5.8	3.4
D_6	4.2	5.6
D_7	5.8	1.4

Then as a result of algorithm operation, the target A will be provided with agents R_2 and R_3, and the target B will be provided with agents R_1 and R_7.

It is obvious that destructive information influences of robots-saboteurs can include transmission to members of a group of a vector of the estimates containing false information, violations of the rules, made in discussion of decisions (unreasonable announcements about a selection of the targets), etc. As a part of a squad of forces intended for the target, there could be saboteurs who would not execute actions required from the legitimate agents concerning the target. Carrying out such attacks can result to not reaching of the maximum by (1), and/or appearance of actually not provided targets. For example, if robot R_5 is the saboteur, it can realize “soft” influence to the target A:

$$D_5 = [\mathbf{0.8}, \quad 3.4].$$

As a result of their attack robots R_5 and R_3 will be assigned to the target A, and this target won’t be provided with a required number of legitimate agents.

3 Model of Information Security for Multi-agent Robotic Systems on the Basis of Reputation and Trust Computation

Definition 1. *The trust in this case is a measure which characterizes readiness of the subject to interact with an object in this situation.* According to the trust relationships policy, an agent can be blocked when trust to this agent is below some preset value. Then the low level of trust won't allow the saboteur to make a destructive impact on decision-making by agents. It follows from this that actions of the saboteur on increase of trust are assumed by involvement of the robot in achievement of the target of MRS, and it contradicts the logic of its use from the point of view of the attacker.

Trust level computation process in a general form is the following [14]. After the start of an iterative loop the robot "*j*" (robot-object of the trust) ($j = \overline{1, N}$), receives in the active phase of the current iteration in the disposal communication link and access to processor devices (CPU) of robots-members of the group. Based on available information about states and the current actions of members of group, the object decides an action in case of which the value of the goal function is maximal, and provides access on writing information about the made decision in robots-subjects. Remaining robots-agents (subjects of trust), after having received this information, check:

a) the acquired information regarding compliance;

b) "usefulness" of the action selected by the robot-object from the point of view of an increment the goal function.

If the robot "*i*" (robot-subject) ($i \neq j$) as a result of a check received the positive decision, it gives the positive vote for the robot-object "*j*", and reports about it to remaining subjects. Each subject, having received data on results about the check of an object by other subjects, counts the number of the positive and negative votes given for it, calculating trust of object "*j*".

However in MRS there can be an implementation of groups of saboteurs which highly appreciate each other, and lowly appreciate other members of a group. Discrediting of legitimate agents can be a consequence of such actions [14]. For the solution of this problem it is necessary to introduce a concept of reputation in the mechanism of IS.

Definition 2. *Reputation is a public opinion created in time about qualities of this or that agent-subject.* Then in case of a count of positive and negative votes given for object, the reputation of voting subjects by summing of their estimates will be considered. In this case influence of agents with low reputation on trust computation process to an object will be smaller, than subjects with high reputation. We note that the reputation value depends on history of interaction of the agent in a group, and on time of stay in it.

Thus, the concepts of trust and reputation of multi-agent systems are actually used for recognition in a group of robots of robots-saboteurs implemented by an attacker. Then for the solution of the task of recognition of entered signs of trust and reputation should provide the greatest similarity of objects within a group (cluster) and the greatest distance between groups (clusters). In the simple case we will speak about two clusters: "legitimate agents" and "robots-saboteurs".

4 Implementation of Model of Information Security on the Basis of Trust Level Computation

We will show model implementation using the already considered example of distribution of targets in a group of robots.

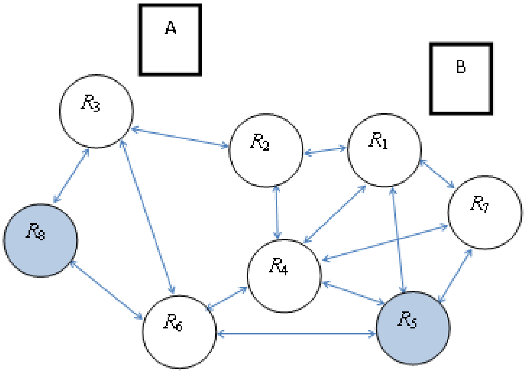

Fig. 1. Distribution of targets in the presence of saboteurs

Assume, that in a group of robots in Figure 1 there are two robots-saboteurs (robots 5 and 8), their task is prevention of selection of targets by a squad of forces.

In Figure 1 the relative positioning of robots and targets is shown, and also arrows between agents designate communications by means of onboard sensor and measuring devices, for example visual communication. We assume that all agents of the considered group have a radio communication channel for information exchange.

Step 1. Each robot-agent creates a vector of efficiency estimates, and tells the estimates to all members of a group. Assume robots-saboteurs carry out an attack which includes misinformation of agents concerning their distance to the target: $D_5 = [\mathbf{0.8},\ \ 3.4]$, $D_8 = [3.1,\ \ \mathbf{0.2}]$. As a result in the CPU of each robot the matrix **D** of efficiency estimates is created, which looks like follows

D_1	3.2	1.0
D_2	1.9	2.5
D_3	0.7	5.4
D_4	3.6	3.5
D_5	**0.8**	3.4
D_6	4.2	5.6
D_7	5.8	1.4
D_8	3.1	**0.2**

From the second step, the actions of information security directed on detection of destructive influences are executed.

Step 2. Agents by means of their OSMD execute verification of data in an array **D**. The robot "*j*" writes results of verification into an array of estimates $V_j = [v_{j1},\ \ v_{j2},\ \ldots,\ \ v_{jM}]$, and tells it to members of the group. Here: $v_{ji} = -1$, if the information transferred by the robot "*i*", is not confirmed by data of OSMD of robot "*j*": $v_{ji} = 1$ otherwise. If the robot "*i*" doesn't watch robot "*j*" by means of its OSMD then v_{ji}= 0. For example, for the situation in Figure 1, the robot R_1 will make the following array $V_1 = [1{,}1{,}0{,}1{,}-1{,}0{,}1{,}0]$. As the robot-saboteur R_5 is in an area of coverage of the onboard sensor and measuring unit, the robot R_1 found out that robot R_5 is from the target A at the distance exceeding the value specified in an array D$_5$. Agents R_3, R_6 and R_8 are out of coverage of the OSMD of the robot R_1, that caused appearance of zeros on the appropriate positions of an array. It is necessary to note that saboteurs R_5 and R_8 can act in coordination. In this case they can realize the following actions:

1. To give each other marks “1” confirming reliability of transferred data even in a case when they are not in the area of coverage of their OSMD.
2. To give marks “-1” to remaining members of the group for their discrediting in case of detecting by their OSMD.

Thus, as a result of execution of step 2 in the CPU of each robot the array **V** is created. This array for a reviewed example looks like follows:

Table 1. Array of action estimates of members of a group

	1	2	3	4	5	6	7	8
1	1	1	0	1	-1	0	1	0
2	1	1	1	1	0	0	0	0
3	0	1	1	0	0	1	0	-1
4	1	1	0	1	-1	1	1	0
5	-1	0	0	-1	1	-1	-1	**1**
6	0	0	1	1	-1	1	0	-1
7	1	0	0	1	-1	0	1	0
8	0	0	-1	0	**1**	-1	0	1

Apparently from the table, a column represents a set of estimates from all members of a group of the certain agent. Value of trust of this agent in a simple case can be equal to division of quantity of the positive voices γ^+ on total quantity of voices $\gamma = \gamma^+ + \gamma^-$ [9]:

$$w_i = \frac{\gamma^+}{\gamma^+ + \gamma^-} \,. \tag{2}$$

For a reviewed example (Table 1) the trust levels of agents the group are calculated with formula (2), will have values: **T** = [0.8, 1.0, 0.75, 0.83, 0.33, 0.6, 0.75, 0.33].

*Step 3.*Computation of agents’ reputation.

If on step 2 agents estimated actions of those objects which were in the area of coverage of their OSMD (that is direct interactions of agents), the actions on step 3 can be regarded as the analysis of interaction of agents with the remaining members of the group who have expressed opinions about observed objects.

We will consider an array of estimates **V** in Table 1. The analysis of this array shows that there are objects of an assessment which are watched by the OSMD of several robots; for example, robots 1 and 2 watched actions of robot 4 and expressed the estimates. Then if the robot's "*i*" assessment concerning action of object "*k*", matches the mark which has been stated by robot "*j*" concerning the same action of object "*k*", it will be the base of an increase of the reputation level. Otherwise there is a reduction. In the reviewed example, the analysis of the table shows that interaction of robots 1 and 2 can be considered as follows:

1. The reputation increases by 1, if robots 1 and 2 are in the area of coverage of their OSMD, and gave to each other the positive marks.
2. The reputation increases by 1, if robots 1 and 2 watched robot 4 actions by means of their OSMD, and their estimates of its actions matched.
3. The total reputation of the robot 2 received in case of interaction with robot 1, and total reputation of the robot 1 received in case of interaction with robot 2 is equal 2.

The reputation is calculated in the analysis of interaction of robots 3 and 1, will be equal 1, as without watching each other, these agents watched actions of robot 2 and their estimates of its actions matched. Having carried out the similar analysis of the array **V** each robot creates an array **S** of reputation level estimates.

Table 2. Array **S** of reputation level estimates of agents

	1	2	3	4	5	6	7	8
1		2	1	4	-3	2	3	-1
2	2		1	2	-2	2	2	-2
3	1	1		2	-1	2	0	-2
4	4	2	2		-4	2	3	-1
5	-3	-2	-1	-4		-2	-3	1
6	2	2	2	2	-2		2	-2
7	3	2	0	3	-3	2		0
8	-1	-2	-2	-1	2	-2	0	

From here it is possible to calculate the level of reputation of each agent q_j, as a result of the relations to it of all members of a group in the course of their direct interaction, and interaction with neighbors. Using formula (2), we obtain the following values of a vector $\mathbf{Q} = [0.75,\ 0.69,\ 0.66,\ 0.72,\ 0.12,\ 0.77,\ 0.11]$.

Step 4. Accounting of change of reputation level.

We note that values of vector **Q** do not match the reputation from Definition 2, because components of a vector consider "opinion" of a group about objects, created based on analysis results of only one situation. For the accounting of a factor of time in operations [15, 16] it is suggested to use strictly increasing functions. It is known that function and frequency curve of the random value which characterize duration of functioning of a complex system, an enterprise or a living being, etc. can be described by Veybulla-Gnedenko's function as follows:

$$F(t) = 1 - e^{-at^k}, \tag{3}$$

where “a” determines the scale, and “k” the type of a frequency curve. In case of constant intensity of iterative procedures in the algorithm of distribution of the targets it is possible to assume k=1. If assumed iteration number as the parameter of time, the type of function of time will looks like as in Figure 2.

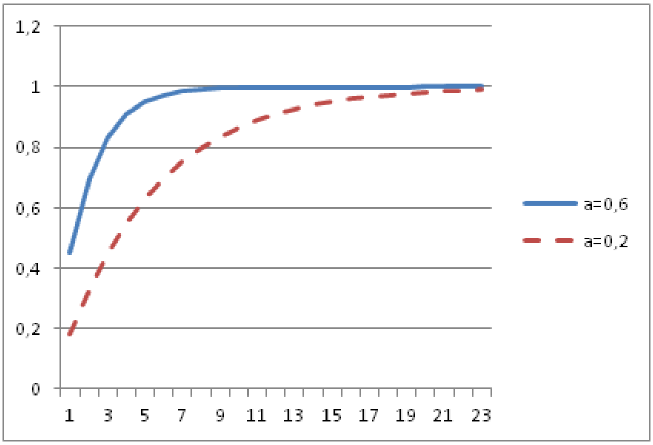

Fig. 2. Influence of parameter “a” on the reputation level with an increase in the number of iterations “*l*”

From Figure 2 it is visible that setting the parameter according to the trust relationships policy accepted in system, it’s possible to control the growth of speed of object reputation.

Thus, a scalar multiplication of vector **Q** on value F(*l*), where *l* is the number of the current iteration of target distribution algorithm, will allow to control influence of beginners with a small level of reputation on the process of estimation of agents’ trust level in the current situation.

Step 5. Taking into account aforesaid the formula for calculation of trust level (2) will looks as follows:

$$w_i = \frac{p_i}{p_i + n_i}, \tag{4}$$

where

$$p_i = \sum_{j=0}^{N} h_{ij} \cdot q_j \cdot F(l),$$

$$n_i = \sum_{j=0}^{N} g_{ij} \cdot q_j \cdot F(l).$$

Values h_{ij} and g_{ij} are defined by the analysis of estimates v_{ij} of array **V**:

$$h_{ij} = \begin{cases} 1, & \text{if robot "}j\text{" positively estimated actions of robot "}i\text{"}, \\ 0, & \text{otherwise} \end{cases}$$

$$g_{ij} = \begin{cases} 1, & \text{if robot "}j\text{" negatively estimated actions of robot "}i\text{"}, \\ 0, & \text{otherwise.} \end{cases}$$

Then for a reviewed example we will finally receive component values of a vector of the trust level, calculated with **W** = [0.96, 1.0, 0.94, 0.97, 0.071, 0.9, 0.95, 0.08] (Fig.3).

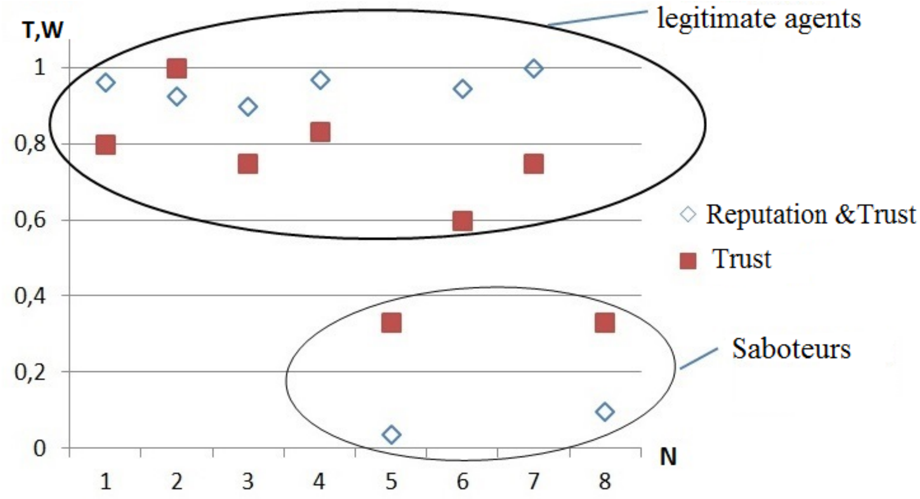

Fig. 3. Characteristics of agents on the trust level **T** and reputation & trust level **W**

From Figure 3 and calculations it is visible that when using measures of trust and reputation (formulas 3 and 4) cluster X_{la} “legitimate agents”, to which robots 1-4, 6 and 7 belong, is at bigger distance from cluster X_d “saboteurs” (robots 5 and 8), than when using only the trust measure.

$$\left|X^{1}_{\text{ų}la} - X^{1}_{\text{ų}d}\right| = 0{,}45 < \left|X^{2}_{\text{ų}la} - X^{2}_{\text{ų}d}\right| = 0.88,$$

where $X^{i}_{\text{ų}la}$ and $X^{i}_{\text{ų}d}$ are the centers of clusters, which calculated as $X_{\text{ų}} = {}^{\sum w_i}/_{n}$ with use of a formula (2) or formulas (3) and (4). As a result of execution of step 5 there is detection of saboteurs by the criterion of recognition accepted in the system, and further steps which directed on execution of the basic algorithm of the targets distribution without the information transferred by robots-saboteurs.

It is possible to show that further actions of saboteurs as a part of a group lead to an increase of intercluster distance between objects of cluster X_{la} “legitimate agents” and objects of cluster X_d “saboteurs”. So for a situation in Figure 4, when robots changed their positions in space, and the following iteration of a target distribution is carried out, we obtain the following results:

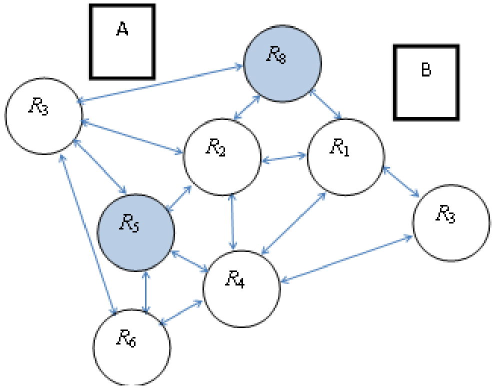

Fig. 4. Situation development on the second step of iterative process of target distribution

Table 3. Array **V** of action estimates of members of a group in the second step of iteration

	1	2	3	4	5	6	7	8
1	1	1	0	1	0	0	1	-1
2	1	1	1	1	-1	0	0	-1
3	0	1	1	0	-1	1	0	-1
4	1	1	0	1	-1	1	1	0
5	0	-1	-1	-1		-1	0	1
6	0	0	1	1	-1	1	0	0
7	1	0	0	1	0	0	1	0
8	-1	-1	-1	0	1	0	0	1

Table 4. Array **S** of reputation estimates of agents in the second step of iteration

	1	2	3	4	5	6	7	8
1		3	2	3	-2	1	2	-2
2	3		3	3	-3	3	2	-3
3	2	3		3	-3	2	0	-2
4	3	3	3		-3	2	2	-2
5	-2	-3	-3	-3		-3	-1	2
6	1	3	2	2	-3		1	-1
7	2	2	0	2	-1	1		-1
8	-2	-3	-2	-2	1	-1	-1	

Then the vector of the trust level will be equal $\mathbf{W} = [0.95, 0.93, 0.904, 0.98, 0.052, 0.97, 1.00, 0.093]$, and intercluster distance, calculated on formulas (3) and (4), increases.

$$\left|X_{\text{ц}la}^{3}-X_{\text{ц}d}^{3}\right| = 1.075 > \left|X_{\text{ц}la}^{2}-X_{\text{ц}d}^{2}\right| = 0.88.$$

We will consider an algorithm for operation in case of appearance of new objects.

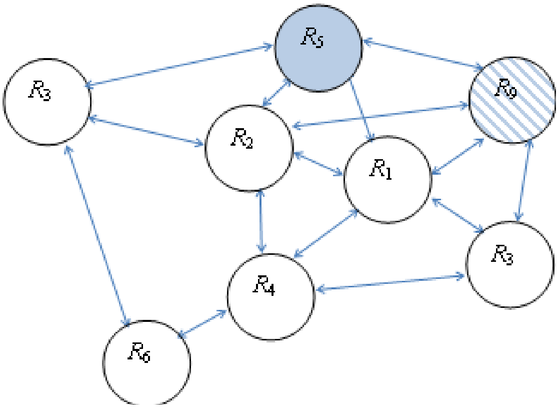

Fig. 5. Operation in case of appearance of a new agent

We assume that as a result of development of a situation there was a situation which is shown in Figure 5. Here R_9 is a new object. As for subjects of a group the interaction history with R_9 absent, its reputation at the moment from the point of view of a group is equal to zero.

We will assume that as a result of execution of steps 1-3 we receive the following arrays **V** and **S** of estimates:

Table 5. Array **V** of action estimates of members of a group on the third step of iteration

	1	2	3	4	5	6	7	9
1	1	1	0	1	-1	0	1	1
2	1	1	1	1	-1	0	0	1
3	0	1	1	0	-1	1	0	0
4	1	1	0	1	0	1	1	0
5	-1	-1	-1	0	1	0	0	-1
6	0	0	1	1	0	1	0	0
7	1	0	0	1	0	0	1	1
9	1	1	0	0	-1	0	1	1

In Table 6 we have a vector **Q** = $[0.83, 0.80, 0.82, 0.87, 0.067, 0.85, 0.83, 0.80]$. Considering that for objects $R_1 - R_7$ current iteration is the first, and for R_9 the first, the coefficients calculated on formula 3, when k=1 and a=0.6 will be equal $F(3) = 0.835$ and $F(1) = 0.451$. Then the reputation of agents will be equal:

$$\mathbf{Q} = [0.695,\ 0.667,\ 0.682,\ 0.73,\ 0.056,\ 0.71,\ 0.69,\ 0.36].$$

Apparently, robots with the smallest reputation are: robot-saboteur R_5 ($q_5 = 0.056$) and agent R_9 ($q_9 = 0.36$). If in the first case the low level of reputation is caused by the fact of detection by members of group of destructive actions from the robot R_5, in the second case the reason is the factor of time which is entered by function 3. It is obvious that changing a function parameter "a" makes possible to settle influence of a time factor.

Table 6. Array S of reputation estimates of agents on the third step of iteration

	1	2	3	4	5	6	7	9
1		3	2	3	-3	1	3	3
2	3		2	4	-4	2	2	3
3	2	2		2	-2	1	0	2
4	3	4	2		-2	1	2	2
5	-3	-4	-2	-2		-1	-2	-3
6	1	2	1	1	-1		1	0
7	3	2	0	2	-2	1		2
8	3	3	2	2	1	0	2	

Using a formula (4) we will receive component values of a vector of the trust level $\mathbf{W} = [0.98,\ 0.983,\ 0.97,\ 0.1,\ 0.03,\ 1.0,\ 1.0,\ 0.98]$. From here it is visible that the trust to agent-beginner is high, and the measure of closeness of this subject to object of a cluster "legitimate agents" is less than to an object of a cluster "saboteurs".

$$|X_{ųla} - X_9| = 0.013 < |X_{ųd} - X_9| = 0.95.$$

It is obvious that higher quality of recognition of the agents which make destructive information influences, with use of measures of trust and reputation is accompanied by the increasing volume of computing resources. So, in case of operation of the standard algorithm in the CPU of the agent it is necessary to create a matrix **D** of efficiency estimates with dimensionality (*N*, *M*). When using algorithm "1" it is necessary to create an array **V** of actions estimates of members of group with dimensionality (*N*, *N*), and when using algorithm "2" it is necessary to create an array **S** of reputation level estimates with same dimensionality. However from the point of view of the recognition quality, when categories of object closeness of one cluster can serve as a measure of this recognition quality, and remoteness between clusters, the scoring in use of such character space is obvious.

5 Conclusion

The developed model represents an approach to information security of MRS in which access control of a robot-agent to a group of robots is carried out on the basis of a measure of the trust level. It is produced by members of a group by the analysis of the situation which has developed on the certain step of an iterative process, taking into account the previous history of their interaction. Thus, the members of a group who for the first time appear in the coverage zone of the onboard sensor device of a robot-agent possess the minimum reputation. For increasing the trust level, an agent needs not only to execute functions for serving a target but also to give a correct feedback on the actions of other robots.

References

1. Wooldridge, M.: An Introduction to MultiAgent Systems, 366 p. John Wiley & Sons Ltd., paperback (2002) ISBN 0-471-49691-X
2. Higgins, F., Tomlinson, A., Martin, K.M.: Threats to the Swarm: Security Considerations for Swarm Robotics. International Journal on Advances in Security 2(2&3), 288–297 (2009)
3. Zikratov, I.A., Kozlova, E.V., Zikratova, T.V.: Analysis of vulnerability of robotic complexes with swarm intellect. Scientific and Technical Journal of Information Technologies, Mechanics and Optics 5(87), 149–154 (2013)
4. Neeran, K.M., Tripathi, A.R.: Security in the Ajanta MobileAgent system. Technical Report. Department of Computer Science, University of Minnesota (May 1999)
5. Sander, T., Tschudin, C.F.: Protecting Mobile Agents against malicious hosts. In: Vigna, G. (ed.) Mobile Agents and Security. LNCS, vol. 1419, pp. 44–60. Springer, Heidelberg (1998)
6. Xudong, G., Yiling, Y., Yinyuan, Y.: POM-a mobile agent security model against malicious hosts. In: Proceedings of High Performance Computing in the Asia-Pacific Region, vol. 2, pp. 1165–1166 (2000)
7. Page, J., Zaslavsky, A., Indrawan, M.: A Buddy model of security for mobile agent communities operating in pervasive scenarios. In: Proceeding of the 2nd ACM Intl. Workshop on Australian Information Security & Data Mining, vol. 54 (2004)
8. Page, Zaslavsky, A., Indrawan, M.: Ountering security vulnerabilities using a shared security buddy model schema in mobile agent communities. In: Proc. of the First International Workshop on Safety and Security in Multi-Agent Systems (SASEMAS 2004), pp. 85–101 (2004)
9. Schillo, M., Funk, P., Rovatsos, M.: Using trust for detecting deceitful agents in artificial societies. Applied Artificial Intelligence 14, 825–848 (2000)
10. Golbeck, J., Parsia, B., Hendler, J.: Trust Networks on the Semantic Web. In: Klusch, M., Omicini, A., Ossowski, S., Laamanen, H. (eds.) CIA 2003. LNCS (LNAI), vol. 2782, pp. 238–249. Springer, Heidelberg (2003)
11. Garcia-Morchon, O., Kuptsov, D., Gurtov, A., Wehrle, K.: Cooperative security in distributed networks. Computer Communications (COMCOM) 36(12), 1284–1297 (2013)
12. Ramchurn, S.D., Huynh, D., Jennings, N.R.: Trust in multi-agent systems. The Knowledge Engineering Review 19(1), 1–25 (2004)

13. Kalyaev, I.A., Gayduk, A.R., Kapustyan, S.G.: Models and algorithms of collective control in groups of robots, 280 p. Physmathlit, Moscow (2009)
14. Zikratov, I.A., Zikratova, T.V., Lebedev, I.S.: Confidential model of information security of multi-agent robotic systems with decentralized control. Scientific and Technical Journal of Information Technologies, Mechanics and Optics 2(90), 47–52 (2014)
15. Carter, J.: Reputation Formalization for an Information-Sharing Multi-Agent System. Computational Intelligence 18(2), 515–534
16. Beshta, A., Kipto, M.: Creation of model of trust to objects of an automated information system for preventing of destructive impact on system. News of Tomsk Polytechnic University 322(5), 104–108 (2013)