

The Collective Behavior of Robots Based on the Internet-of-Things Paradigm

Vyacheslav Abrosimov^{1*}, Alexander Mazurov²

¹⁾ *Ministry of Defence of the Russian Federation, Moscow, Russia*

E-mail: avk787@yandex.ru

²⁾ *Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia*

E-mail: alexander.mazurov08@gmail.com

Abstract: This paper considers a group of autonomous robots performing collective tasks in an antagonistic environment. The environment can significantly hamper information exchange and decision-making in the group. Well-known methods are intended for performing collective tasks by a large group of relatively simple objects and have obvious advantages (high reliability, potential complexity increase, etc.). However, these methods neglect the specifics of collective behavior in an antagonistic environment. Moreover, they are inapplicable when a collective mission is fulfilled by a few objects expensive for production and maintenance. We propose a new approach to collective mission fulfillment based on the principle of collectivism and the Internet-of-Things paradigm. The novelty of the approach is that each robot in the group is valuable: with different resources and functionality, they assist each other. The robots execute different roles within the group, operating independently to fulfill a collective mission. The robots are equipped with observation sensors and motion detectors. The functions and resources of robots are represented as external services. A service-oriented mutual assistance architecture is designed for robots to resolve conflicts and problem situations caused by the environment: each robot can use the resources and functionality of other robots via online requests when needed. Such spontaneous relations provide a fundamental opportunity for the collective management of unpredicted situations and the possibility of changing behavioral scenarios when fulfilling a collective mission, leading to self-organization. The effectiveness of this approach is illustrated by an example: a group of robots attacks a complex target secured by a defense system.

Keywords: robot, antagonistic environment, Internet-of-Things, collective mission, mutual assistance, conflict resolution, cooperative strategy.

1. INTRODUCTION

In many applications, heterogeneous robots have to move cooperatively in time and space to fulfill a collective mission. Preset cooperative strategies are almost not implemented in practice due to different factors. Here, we mention objective natural factors (night-time, fog, rain, etc.) and subjective factors, e.g., an active counteraction of other robots pursuing opposite goals. This counteraction of an environment may have critical consequences for the efficiency of collective mission fulfillment.

Theoretically, there are two fundamental approaches to construct collective behavioral strategies of robots. Within the first approach, robots use some mechanism for adapting to a current situation. Note that such adaptation must be collective, and biological adaptation mechanisms [7] are efficient. Like biological specimen, robots in these mechanisms are comparatively independent and obey rather simple rules without cooperation. The development of biological algorithms requires much time, accumulated experience, and knowledge. The second approach is self-organization: under limited time to solve tasks and

* Corresponding author: avk787@yandex.ru

an active counteraction of an environment, the group control of robots should be designed in the class of self-organizing systems [20]. Self-organization implies a joint assessment of situational awareness but an autonomous motion of robots. In this case, each robot performs its task as part of the collective mission. However, under existing threats to the collective mission (e.g., failure, termination, or restricted functionality), cooperation and assistance can be reasonable or vital for robots.

This paper draws an analogy between the collective control principles for a group of autonomous robots and the Internet-of-Things (IoT) paradigm. Network design and communication of things are crucial for the IoT. Speaking simplistically, the sensors of systems communicate and control the sensors of the other systems. Such a statement seems intuitively clear for things (systems) controlled without intelligent means. If control systems of objects are intelligent, then sensor commands from objects to other objects may contradict their individual behavioral strategies. Collective control design for groups of such intelligent objects requires negotiations. As a rule, negotiations are organized using the principles of competition [16]. Considering earlier publications, we hypothesize (and try to validate) that in such conditions, an efficient approach is to train control systems of autonomous robots based on the principles of collectivism. Each robot should be ready to execute another (generally, subordinate) role, allocating its functions and resources to other robots whenever necessary, for fulfilling the collective mission in a current situation.

2. A SURVEY OF RELATED LITERATURE

The subject matter is at the junction of several fields, namely, machine-to-machine interaction (M2M), the Internet of Things (IoT), and the group motion of robots. However, all three fields together were addressed in a few publications.

According to the surveys on M2M methods [10, 13, 17, 18], a unified platform would hardly be developed. At the same time, numerous Open Source realizations are expected to yield good engineering solutions for interacting robots with collective tasks.

As emphasized in the paper [12], robots performing a common task must exchange information about the environment. In particular, Jha and Gupta proposed a communication architecture with an algorithm for searching the lost network members to route the information from a lost source robot to a destination robot. An appropriate robot for routing in the network is selected based on its load, estimated by different factors (ongoing processes, battery power, connectivity, or storage space). The idle robots have an effective role in the network to increase the efficiency of the communication system.

The authors [11] extended the computation and information-sharing capabilities of networked robotics by proposing a cloud robotic architecture. The cloud robotics architecture leverages the combination of a virtual ad-hoc cloud formed by machine-to-machine (M2M) communications among participating robots. Cloud robotics utilizes elastic computing models, in which resources are dynamically allocated from a shared resource pool in the cloud to support task offloading and information sharing in robotic applications.

The paper [14] considered the conceptual similarities and differences of M2M and IoT. As noted, M2M supplier competencies tend to focus on the “plumbing” aspects mentioned earlier, particularly embedded hardware and cellular telecommunications networks. Many are starting to add cloud capability through internal development, acquisition, or partnering, but this represents new terrain for most M2M suppliers. IoT solution suppliers, on the other hand, tend to emphasize software capabilities and particularly enterprise integration. These are important distinctions.

Duarte et al. [8] proposed swarm robotics systems to carry out marine environmental monitoring missions. In swarm robotics systems, each individual unit is relatively simple and inexpensive. The robots rely on decentralized control and local communication, allowing the swarm to scale to hundreds of units and cover large areas. The cited authors studied the

application of a swarm of aquatic robots to environmental monitoring tasks. The first part of the study synthesized swarm control for a temperature monitoring mission and validated the results with a real swarm robotics system. Then, the authors conducted a simulation-based evaluation of the robots' performance over large areas and with large swarm sizes and demonstrated the swarm's robustness to faults. According to the results obtained, swarm robotics systems are suited for environmental monitoring tasks by efficiently covering a target area, allowing redundancy in the data collection process, and tolerating individual robot faults.

The paper [6] presented a survey of related work in the area of self-organization and discussed future research opportunities and challenges for self-organization in the IoT. Athreya and Tague considered the process of discovering available peer devices to support and initiate communications during self-organization. They discussed how establishing peer connectivity could lead to end-to-end path establishment allowing for connectivity in the self-organized network. Service recovery management is the process of recovering from local failures of devices and avoiding network service disruptions in the self-organized network.

Yadav, McCann, and Pereira [19] introduced an extended and improved emergent broadcast slot (EBS) scheme, which facilitates collaboration for robust communication and is energy efficient. In the EBS, nodes communication units remain in sleeping mode and are awake to communicate. The EBS scheme is fully decentralized: nodes coordinate their wake-up window, partially overlapping within each duty-cycle, to avoid message collisions.

In the paper [15] closely relating to the subject matter, Ray introduced a new concept called the Internet of Robotic Things (IoRT). This concept tackles the issues for supporting control and monitoring activities at deployment sites and industrial automations, where intelligent things can monitor peripheral events, induce sensor data acquired from various sources, and use ad-hoc, local, and distributed "machine intelligence" to determine an appropriate course of actions. The ultimate goal is to control or disseminate static or dynamic position-aware robotic things in the physical world through a seamless manner by providing a means for utilizing them as the IoRT. Although progressive advancements can be seen in multi-robotic systems, and robots are constantly getting enriched by easier developmental functionalities, such vertical robotic service-centric silos are not enough for continuously and seamlessly supporting for which they are meant.

Thus, the collective management of unpredicted situations and the possibility of changing scenarios were not properly considered in the literature on the collective behavior of objects (particularly robots). If an object cannot perform an assigned task (due to exhausted resources, new conditions in the environment, etc.), it becomes unnecessary for the group. Well-known methods are intended for performing collective tasks by a large group of relatively simple objects. They have obvious advantages such as high reliability (loss of one object does not affect the entire group's performance), potential complexity increase (the complexity of tasks can be increased by adding new objects to the group), and others. However, these methods neglect the specifics of collective behavior in an antagonistic environment. Moreover, they are inapplicable when a collective mission is fulfilled by a few objects expensive for production and maintenance. Of particular interest are practical situations when an object enters the enemy's counteraction zone (is exposed to a threat), and other objects in the group have the resources and functionality to eliminate this threat.

Therefore, we propose a new approach to collective mission fulfillment based on the principle of collectivism and the Internet-of-Things paradigm. The novelty of the approach is that each robot in the group is valuable: with different resources and functionality, they assist each other. The robots execute different roles within the group, operating independently to fulfill a collective mission. The robots are equipped with observation sensors and motion detectors. The functions and resources of robots are represented as external services. A service-oriented mutual assistance architecture is designed for robots to resolve conflicts and

problem situations caused by the environment. Within the Internet-of-Things paradigm, each robot can use the resources and functionality of other robots via online requests when needed. Such spontaneous relations provide a fundamental opportunity for the collective management of unpredicted situations and the possibility of changing behavioral scenarios when fulfilling a collective mission, leading to self-organization. The effectiveness of the proposed approach is illustrated by an example: a group of robots attacks a complex target secured by a defense system.

3. ROBOT'S SITUATIONAL AWARENESS

Each robot has to implement an individual control strategy and coordinate its actions with other group robots. Therefore, each robot needs to know and predict its position and the situation in an environment (particularly the states of other robots). In other words, each robot must have situational awareness [9]. Situational awareness forms the basis of the individual behavioral rules of a robot designed to fulfill a collective mission within a group. Nowadays, researchers identify three main elements in the concept of situational awareness: information about the environmental situation in time and space, situation assessment and prediction (scenarios of further development) in the form of events, individual actions, and other participants' actions.

In practice, situational awareness is realized by specific models of data acquisition, accumulation, storage, and analysis, including access rules for robots.

3.1. Information about the environment

There exist two main sources of information about the environment. The first source is the observation systems of a robot. This group includes various technical means, e.g., optical, ultrasonic, infrared sensors, etc. However, the technical capabilities of such sensors to observe and measure environmental parameters are limited in principle. The second source is external monitoring systems, e.g., aerospace monitoring systems, remote information support systems deployed at a considerable distance to the operational space of robots, and others. As a rule, such monitoring systems enable robots to perform collective tasks.

The sources mentioned can be used to design a full-scale geo-informational system to describe situational awareness. This paper considers the following simple case. We divide the operational space of a group of robots into a finite number of domains (segments). Each segment can be characterized by different parameters: coordinates, size, the probability of problem occurrence, and others. (A problem is an event in the environment that affects the operation of a robot in a segment.)

Let us adopt an elementary description of a segment:

$$seg = \{x_r, y_r, z_r, H, \Delta seg, e, p_k^e, \beta_k^e\}, \quad (3.1)$$

with the following notations:

x_r, y_r, z_r are the coordinates of the center of the segment seg in a given coordinate system;

H is the shape of the segment seg ;

Δseg are the dimensions of the segment seg ;

e is an event observed or predicted in the segment seg ;

p_k^e is the probability (or possibility) of the event e for the k -robot in the segment seg ;

β_k^e is the probability (or possibility) of threat to the k -robot's task under the event e in the segment seg .

Assume that an event is detected by the robot's sensors or external monitoring systems. The range of possible events and threats (including their characteristics p_k^e and β_k^e) should be defined by simulating group motion and learning in advance.

3.2. Robot's status

Now we introduce the concept of the robot's status, *Stat*. The intelligent robots under consideration act autonomously to fulfill a collective mission. Each robot has an individual functionality (capabilities) and individual characteristics to realize the functionality. A robot may execute several roles. With a role assigned, a robot acts and observes the environment in its narrow sphere of responsibility due to the limited capabilities of its observation systems. For moving in the operational space, a robot uses a system of actuators with different sensors (position, tilt, displacement, etc.) implementing the corresponding functions (movement, maneuver, stop, and others).

Let each k -robot be represented by an ordered set

$$Stat(t) = \{k, Role_k, M_k, \gamma_k, seg(t), seg(t + \delta t), r_k(t), Func_k, \Psi_k, \alpha_k, \mu_k, G_k\} \forall k \in K, \quad (3.2)$$

where:

k is the robot's number in the group;

$Role_k$ is the robot's role;

M_k is the robot's route in the environment;

γ_k is the robot's value (significance) for the group;

$seg(t)$ is the robot's location (segment) at a time instant t ;

$seg(t + \delta t)$ is the predicted robot's location (segment) at a time instant $(t + \delta t)$;

$r_k(t)$ is the robot's residual resources at a time instant t ;

$Func_k$ is the robot's functionality (set of functions);

Ψ_k is a coefficient reflecting the robot's skills and experience;

α_k is the robot's attribute of activity (operability);

μ_k is the robot's willingness to assist other robots (the behavioral paradigm formed by learning);

finally, G_k is the robot's capabilities to reduce the environment's degree of counteraction.

All robots transmit their statuses online to an information resource on the Internet. Any robot has online access to this information resource.

3.3. Influence factors

The environment is antagonistic and has different influence factors F . The first source of such factors, denoted by F^A , is uncontrolled objective conditions of the environment that hamper collective mission fulfillment (e.g., night-time, fog, or rain). The second source F^B relates to a specially organized counteraction (e.g., the defense systems of a potential target under attack). The factors can be formally described by a set of attributes. In many cases, they are not deterministic. For example, reconnaissance means detect the opponent's antagonistic systems and capabilities only approximately; the probability of a sustainable malicious interference for communication means is high. On the other hand, robots and their sensors may fail due to different reasons. The unpredictability of possible situations complicates the definition and fulfillment of tasks by robots. Therefore, it is necessary to use probabilistic or fuzzy variables to describe the attributes of influence factors.

3.4. Events in the environment

An event occurs if a set of influence factors shows itself in specific conditions. An event $e \in E$ is the consequence of the influence factors $F^A(t)$ and $F^B(t)$ affecting the robot's status integrally at a given time instant t . An event e occurs due to realizing a set of factors with definite characteristics:

$$\sum_A F^A \cap \sum_B F^B \rightarrow e \rightarrow Stat(t). \quad (3.3)$$

An event e is characterized by its probability p^e , a segment seg^e of the operational space where it occurs, and its threat β_k^e to the task of the k -robot. In principle, the events can be divided into groups. According to practical evidence, such groups are finite for a given environment and a given class of collective missions. However, influence factors as the sources of an event are often unknown, while an event itself may critically affect robots.

3.5. Situation in the environment

A set of events occurring in the environment forms a certain situation $s \in S$ for each robot. The current situation affects the fulfillment of a collective mission by robots. In an antagonistic environment, a realized situation causes a loss for the group of robots. For the i -robot ($i \in I \supseteq K$), the loss consists in its missed contribution δw_i^- to a collective objective function W :

$$s \in S: \sum_E e \rightarrow Stat(t) \rightarrow \delta w_k^-. \quad (3.4)$$

The total loss for the group is the sum of the missed contributions of all robots from the set $I \supseteq K$ for which this situation becomes critical:

$$\delta W = \sum_I \delta w_i^-. \quad (3.5)$$

Any situation requires collective decision-making by the group of robots. In the set of all admissible decisions D for the s -situation, an optimal decision d_{opt}^s minimizes the total loss:

$$d_{opt}^s = \min_D \delta W. \quad (3.6)$$

3.6. Precedents

There is nothing new under the sun despite an intrinsic uncertainty of collective mission fulfillment in antagonistic environments. Humankind has accumulated a rich experience of actions in different situations. This experience is yielded by mathematical, physical, and simulation modeling of different situations, carried out a priori. The correctness of model-based solutions is verified a posteriori in practice. Robots are trained to choose proper actions in different situations using learning procedures and the results of modeling. The robot's behavioral paradigm forms its intelligence. Therefore, we can specify a set of precedents (similar situations in the past) for any collective mission. What is important, we know the decisions made in such precedents, including their efficiency and consequences. Hence, a robot can analyze its status and the statuses of other robots, detect current situations, and seek appropriate decisions in a neighborhood of well-known (validated) decisions to establish self-organization rules.

3.7. State of the environment

The set of factors F , related events E , and situations S generated by these events represents the environment's current state $Env(t)$ at a given time instant t . Therefore, the state $Env(t)$ is formed according to the following scheme: realization of influence factors in the environment \Rightarrow occurrence of events affecting robots \Rightarrow formation of a situation in a given segment of the operational space and losses for robots \Rightarrow the environment with fixed factors, events, situations, and precedents.

Consider an illustrative example. A group of fire-suppression robots is eliminating the consequences of an earthquake. The earthquake is described by factors (the time and duration of earth shocks). A set of these factors, realized within 24 hours, generates events (destruction of buildings). A sequence of such events forms a situation (fire). There exist numerous precedents of fire suppression depending on the intensity and rate of propagation. Robots make decisions considering the current situation and the experience of similar operations.

The scheme described above (factors \Rightarrow events \Rightarrow situations \Rightarrow environment's state \Rightarrow precedents) has no crisp mathematical relations. Physical and other regularities or patterns are also absent. The underlying processes can be described by variations (increase or decrease) in the activity of the environment and robots. It is possible to identify several types of such variations. For example, the probability of destruction increases when a robot approaches a dangerous zone. If a robot can affect the environment, the latter's negative impact can be reduced. When external observation systems monitor a territory, events occur in discrete time: an event can be detected at a time instant ($t^* + 0$) although it was not the case at a previous time instant ($t^* - 0$). Discontinuities of activity are also possible, e.g., when robots lose communication. In contrast, the phenomenon of "hyperactivity" can be observed: as robots restore communication, they have to act in another (essentially complicated) situation.

What are possible ways to model situational awareness without crisp mathematical and physical relationships among the observed phenomena? The theory of neural networks provides one solution; see the paper [1]. Hopefully, the neural model described therein can be implemented in practice.

4. ROBOT AS A THING IN THE IOT PARADIGM

We accept a conventional proposition of the Internet of Things: each thing provides a state-function interface for interaction, making it accessible to external users and other things. Nowadays, researchers are oriented towards IoT-based technologies with a high market priority (Intelligent house, Intelligent public transport, and others). There exists scarce information on using the IoT in complex, intelligent controlled objects (and their interaction), mostly for marketing purposes.

Let us endow a robot with the following properties intrinsic to the IoT paradigm.

4.1. *Collectivism as the main principle of interaction*

Each robot operates autonomously but can interact with other robots simultaneously and independently. Unlike the existing approaches, we incorporate the principles of collectivism in the interaction of robots, as described in the book [3]. Each robot in a group is learned to one of the three paradigms of collective behavior: altruistic behavior (a higher priority for group's tasks), egoistic behavior (a higher priority for individual tasks), and pragmatic behavior (decision-making with a complex priority choice algorithm). The details were described in the paper [2]. In this statement, while performing individual tasks according to its behavioral paradigm, each robot possesses information about the existing problems of other robots in their tasks and expresses its willingness to solve these problems using its functionality and residual resources (if necessary). This collectivism of the autonomous behavior of robots within the group is a prerequisite to creating an innovative service-oriented interaction architecture of robots, which guarantees a proper operation of the entire group regardless of the states of individual robots through the role and functional interchangeability of robots and their mutual assistance (cooperation).

4.2. *Functionality as service*

Robot's roles are defined by its functionality, behavioral paradigm, and the scale of learning for different actions in complex situations. Modern autonomous robots have a multifunctional design. While fulfilling a collective mission, in addition to its main functional role, each robot may have (reveal) another potentially admissible role depending on its status, role, functionality, and residual resources. Some examples of roles include Leader (a robot initiating control commands), Cooperator (a robot collaborating with other robots in collective mission fulfillment), Communicator (a robot responsible for interaction and communication), Executor (a robot implementing actions), Resource (a partially or

completely informed robot placed in reserve; participates in collective mission fulfillment by request only), and other roles. Under the principle of collectivism, any robot accepting another role offers its functionality and resources to other robots as an external service available to solve their tasks. On the other hand, any robot may request required functionality and resources from other robots and use them if necessary. With interaction processes organized in this way, each robot disposes of additional functionality, which appreciably enlarges its capabilities. Moreover, the entire group considerably increases the adaptability to the negative impact of the antagonistic environment.

4.3. Mutual Assistance as a basis of behavioral strategies

A robot may implement different levels of access to its functionality. This property allows creating networks of robots differing by structure and complexity: common networks, networks with complex structure and subordination, networks with hidden elements, and others. (A hidden element shows itself if necessary, e.g., a sacrifice.) A robot can be identified in a network as a part of another robot. It can be hidden or identified through another robot, forming new networks. Such networks can implement different behavioral strategies for a group of robots in the antagonistic environment, depending on the events and current situation. Here, major aspects are allocating tasks and goals before collective mission fulfillment, routing, and coordinating the individual behavioral strategies of robots during mission fulfillment.

Thus, we interpret a robot as a thing in the IoT paradigm. Each robot informs other robots about its status and acts as an external service for them, and the robot's attributes describe its admissible roles, functionality, and residual resources to solve tasks within a collective mission. The robot's functions and resources can be requested and used by other robots. On the other hand, the capabilities of a given robot can be enlarged (if necessary) using the functionality, roles, and resources of other robots.

4.4. Provision of robot's functionality to other robots

In the operational space with an antagonistic environment, robots need different functionality (e.g., reconnaissance, the capability to reduce or even neutralize counteraction, concealed motion, etc.). In standard solutions, the robot's functionality decreases over time due to consumed resources. However, the approach with assistance from other robots allows increasing and extending the robot's functionality.

Each k -robot (3.2) can be assigned a set of functions (its functionality):

$$Func_k = \{f_{1k}, f_{2k}, \dots, f_{jk}, \dots, f_{jk}\} \forall k \in K. \quad (4.1)$$

A characteristic f_{jk} in the set $Func_k$ can be another set containing several numerical, probabilistic, and fuzzy parameters. For example, the characteristic f_{3k} can be the robot's effective distance (in terms of its impact on the environment), the angular range and efficiency of this impact depending on the environment's counteraction (a probabilistic or fuzzy variable), the admissible number of such impacts, etc. Combining the functional characteristics of robots in rows and their parameters in columns, we construct matrices completely describing the robot's functionality. Different matrices of this type can be formed depending on the robot's design, functionality, and learning paradigms.

The paper [4] considered a group of controlled objects (agents) and developed a role allocation algorithm with a ranking procedure based on the closeness to role requirements in terms of functionality and characteristics. Applying this algorithm, we find an appropriate robot for assistance. Assume that due to an event $e \in E$, an m -robot ($m \in K$) was impacted by an antagonistic environment when performing its individual tasks. As a consequence, some functional capabilities f_{jm} of the robot were decreased to an inadmissible level, $f_{jm} < f_{jm}^*$. Requesting or rendering assistance can be formally described by activating a special variable

a_m of the robot's status. In response to the alarm signal ($a_m = 1$), negotiations are organized among the other k -robots ($k \in K$). In a technical sense, it is necessary to find a g -robot, $g \in K$, with maximum functional capabilities for assistance and enough resources to implement this functionality:

$$g : f_{jg}^* = \max_{K - \{m\}} f_{jk} \quad \forall k \in K, \forall j \in J. \quad (4.2)$$

The g -robot with the value f_{jg}^* will be assigned the highest priority during negotiations. According to practical evidence, the following parameters should be introduced for choosing an appropriate robot for assistance:

- the weights ξ_f that describe the significance of each function f_j for collective mission fulfillment;
- the significance γ_k of each k -robot for the entire group (e.g., Leader must be eliminated from the list of potential assistants);
- the practical experience Ψ_k of each k -robot in the same (or similar) role in precedents;
- the skill of each k -agent in a required function acquired by learning (e.g., the "sacrifice" function $\mu_k \in [0,1]$; see the paper [2] for details).

5. AN APPROACH TO DESIGN LOCAL SELF-ORGANIZATION RULES OF ROBOTS

5.1. Specific features of collective strategy formation

Consider a group of robots, and let their collective mission be the passage through the counteraction zones of an antagonistic environment with a minimum loss of a collective objective function. The counteraction means seek to hamper collective mission fulfillment as much as possible through a negative impact on the robots for disrupting their normal operation and even neutralizing them.

The collective objective function is given by the sum of the contributions δw_k of all k -robots, $k \in K$:

$$W = \sum_K \delta w_k. \quad (5.1)$$

We will interpret the environment's impact on a robot as an event $e \in E$. Due to this impact, the contribution of each k -robot is reduced by a value δw_k^e , which describes the corresponding loss. While fulfilling the collective mission, the group of robots seeks to achieve $\max_E W$ over all possible events E , whereas the environment's goal is to generate events $e \in E$ to achieve $\max_E \delta w_k^{e-} \quad \forall e \in E, \forall k \in K$.

A collective strategy of the group realizes the following.

a) The collective mission is decomposed into tasks with certain roles for each robot; for details, see the algorithm presented in the paper [4].

b) Information about the antagonistic environment and robots' statuses is registered. Considering the allocated roles, each robot forms algorithms for its individual tasks. (An example of a routing algorithm in the Earth surface monitoring problem by a group of heterogeneous robots was given in the book [3].)

c) While performing its tasks, each robot updates the situational awareness model by the following elements with a given period δt : (a) the robot's current status and (b) the current environment's state observed by the robot's sensors.

d) In response to occurring events (failures of robots or their sensors, exhaustion of robot's non-replenishable resources, detection of new counteraction means, etc.), the group organizes negotiations. The new roles and control strategies of robots are negotiated

depending on their statuses and learning paradigms to fulfill the collective mission in new situations. Note that the existing precedents are used for this purpose.

An important problem is to hide the actual roles of robots operating in the antagonistic environment. One interesting solution involves irrational behavioral strategies of robots; see the recent paper [5].

5.2. Specific features of individual strategy formation

As demonstrated by several researchers, the emergent collective behavior of objects can be constructed using their elementary interactions. For the class of problems under consideration, such elementary interactions include the following: updating the situational awareness model with the robot’s current status; requesting the current situation at a given location (point on a path); requesting assistance; rendering assistance; and so on.

Due to the negative impact of the antagonistic environment, some robots may fail to perform their tasks. Therefore, we design the robot’s individual strategy by realizing two principles as follows. First, each robot performs the individual tasks within its role defined when decomposing the collective mission. Second, to the extent possible, each robot considers the problems of other robots fulfilling the collective mission as unpredictable situations occur.

A typical strategy of each k -robot consists of two mutually complementing components, general and special. The general component includes:

1. permanently monitoring the environment by robot’s sensors and quantitatively assessing the influence factors (events and situations) and their attributes;
2. predicting the path for a time instant $(t + \delta t)$, where δt is a given period;
3. estimating the probability p_k^e of a critical event $e_k^*(t + \delta t)$ in the predicted motion zone and assessing the threats β_k^e created by the environment;
4. updating of the situational awareness model by the observed information;
5. analyzing an occurred situation $s \in S$ and incurred losses δw_k^- and assessing the individual functional capabilities to solve the problem;
6. acting to solve the problem;
7. when necessary (no individual solution), requesting assistance from the group ($a_k = 1$);
8. participating in negotiations (see the scheme (4.1), (4.2)) to provide the functionality $Func_k$ to other robots for performing their tasks.

The special component of the robot’s behavioral strategy reflects its particular features and depends on the roles.

5.3. Behavioral Rules for a Robot-Thing Assisting Other Robot-Things: An Example of Design

Consider an illustrative example to design robot’s behavioral rules within the IoT paradigm. Robots A and B have the same functionality (see Table 5.1) and perform individual tasks, moving towards targets to attack them. The targets are secured by the technical means of a defense system C .

Table 5.1 Functionality of robots ($k, m = A, B$)

Identifier	Function	Values
f_{1k} (Role)	Robot’s role in group	1—Leader; 2—Attacker; 3—Supporter; 4—Communicator
f_{2k}	Robot’s motion	v —forward motion with velocity v ; 0—stop; $(-v)$ —backward motion with velocity v


f_{3k}	Detection of threat to k -robot from defense system C	p_z^k —the probability of threat from z -defensive means C_z : $p_z^k = 0$ (no threat), $0 < p_z^k < 1$, $p_z^k = 1$ (annihilation of k -robot A by the defensive means C_z)
f_{4k}	Response or preventive impact of k -robot on defense system C	0—no preventive impacts; q_k^z —the number of preventive impacts on C_z ; p_{kq}^z —the reduced probability of threat from C_z due to q_k^z impacts of k -robot; 1—eliminated threat from C_z
f_{5km}	Assistance from k -robot to m -robot	0—no assistance required; 1—assistance required from any robot with appropriate functionality and sufficient resources; $k \rightarrow m$: k -robot assists m -robot
f_{6km}	Activation of the motion system of m -robot by k -robot	$v_{k \rightarrow m} = 0$ —the motion system of m -robot not activated by k -robot; $v_{k \rightarrow m} = 1$ —the motion system of m -robot activated by k -robot
f_{7km}	Activation of the combat system of m -robot by k -robot to impact defensive means	$h_{k \rightarrow m} = 0$ —the combat system of m -robot not activated by k -robot; $h_{k \rightarrow m} = 1$ —the combat system of m -robot activated by k -robot
f_{8k}	Activation of the observation system of m -robot by k -robot to acquire information on its route	$b_{k \rightarrow m} = 0$ —the observation system of m -robot not activated by k -robot; $b_{k \rightarrow m} = 1$ —the observation system of m -robot activated by k -robot
f_{9k}	The “sacrifice” paradigm of k -robot	1—“altruist”; 0—“egoist”; μ_k —“pragmatist” with the willingness for sacrifice μ_k

Consider two common events: the predicted path of a k -robot intersects the responsibility zone of the defense system C (the event e_1), and the operation of a k -robot is violated by the defense system C with a threat β_k^e under an admissible threat β_k^{e*} (the event e_2).

Let us formulate the behavioral rules of robots A and B with functionalities $Func_A$ and $Func_B$, respectively; see Table 5.2.

Table 5.2 Strategies of robots A and B in the responsibility zone of defense system C

Step	Events in environment	Data in the situational awareness model	Local rules for robots A and B										
			Robot	Func	1	2	3	4	5	6	7	8	9
					Role	v	p_z^k	q_k^z	H	$v_{A \rightarrow B}$	$h_{A \rightarrow B}$	$b_{A \rightarrow B}$	μ_k
1	$e_1 = 0$	$\beta_A^e \leq \beta_A^{e*}$ $\beta_B^e \leq \beta_B^{e*}$	A	$Func_A$	2	v_A	0	0	0	0	0	0	0
			B	$Func_B$	2	v_B	0	0	0	0	0	0	1
2	$e_1 = 1$	$\beta_A^e \leq \beta_A^{e*}$	A	$Func_A$	2	v_A	0	0	0	0	0	0	0

		$\beta_B^e \leq \beta_B^{e*}$	B	Func _B	2	v_B	0	0	0	0	0	0	1
3	$e_1 = 1$ \wedge $e_2 = 1$	$\beta_A^e \geq \beta_A^{e*}$	A	Func _A	2	0	p_z^A	p_{Aq}^z	0	0	0	0	0
		$\beta_B^e \leq \beta_B^{e*}$	B	Func _B	2	v_B	0	0	0	0	0	0	1
4	$e_1 = 1$ \wedge $e_2 = 1$	$\beta_A^e \geq \beta_A^{e*}$	A	Func _A	2	0	1	0	1	-	-	-	0
		$\beta_B^e \leq \beta_B^{e*}$	B	Func _B	3	0	0	p_{Bq}^z	0	v_{B1}	1	1	1
5	$e_1 = 1$ \wedge $e_2 = 0$	$\beta_A^e \leq \beta_A^{e*}$	A	Func _A	2	v_A	1		$B \rightarrow A$	-	-	-	0
		$\beta_B^e \leq \beta_B^{e*}$	B	Func _B	3	-	0	1	$B \rightarrow A$	v_{B1}	0	1	1

Now, we analyze the actions performed by robots as things whose control systems can communicate and control each other.

At step 1 of the process, robots *A* and *B* are outside the potential threat zone. Both robots move to the given targets.

At step 2, the following event occurs: the predicted path of robot *A* intersects the responsibility zone of the defensive means C_z . However, the probability of annihilation does not exceed the given thresholds for robots *A* and *B*. There is no impact from C_z on robots *A* and *B*. The current situation on the predicted paths of the robots is not dangerous. Robots *A* and *B* continue their motion to the targets.

At step 3, a new event occurs in the environment: the defensive means C_z apply impact on robot *A* with the probability p_z^A . The current situation on the predicted path of robot *A* becomes dangerous. Learned in the egoistic paradigm, robot *A* stops applying q_A^z impacts on the defensive means C_z with the total success probability p_{Aq}^z . In turn, robot *B* executes the same role and continues to perform its individual tasks since robot *A* requests no assistance.

At step 4, the defensive means C_z apply impact on robot *A* without complete success: the latter's functionality is partially reduced (e.g., the observation system is damaged). Robot *A* requests assistance from robot *B*. Learned in the sacrifice paradigm, robot *B* assesses its functionality and available resources and suspends its individual tasks for executing the Supporter role: robot *B* authorizes using its observation and motion systems to robot *A*. Responding to the control system of robot *A*, robot *B* changes its velocity v_{B1} and direction. The combat system of robot *B* applies impact on the defensive means C_z with the probability of annihilation p_{Bq}^z .

At step 5, due to $p_{Bq}^z \geq p_z^B$, both robots win the duel, and robot *A* continues its motion to the target without threat (using the observation system of robot *B* for situational awareness). Robot *B* assesses the residual resources to optimize its route to the targets.

5. CONCLUSION

Therefore, applying the Internet-of-Things paradigm is a fundamentally new solution to design collective behavioral strategies of robots performing collective missions in antagonistic environments.

Implementing a group control strategy based on the principles of collectivism, we create and refine a networked service-oriented infrastructure. In a group of autonomous mobile robots, various relations arise and disappear among the observation and actuation systems of robots, depending on the events and situations in the environment. The generation processes of new relations are spontaneous, a priori unknown, and are dictated by the current situation and events occurring in the environment. The control systems of upper-level robots in the role hierarchy activate the control systems of the lower-level ones, reallocating their roles. If

the robots have no hierarchy, control issues are settled during negotiations using the principle of collectivism.

Thus, the IoT paradigm-based solution leads to self-organization. This aspect is particularly important due to the current engineering trend of constructing multifunctional robotic complexes using a group of simple robots with a small set of functions (instead of single complex platforms). Another determinant factor to use the IoT paradigm is the activation of control systems of robots by other robots according to the roles and structural hierarchy of the group.

Many issues are beyond the scope of this paper. What are the consequences of communication failures? How will a robot “agree” to execute an auxiliary role in addition to its individual tasks? What is the efficiency of the suggested approach under different scales and counteraction of an environment? How can we design a service-oriented architecture of interaction for multifunctional controlled objects? How many levels should the resulting network be composed of? What is their structure? What are the required geo-informational models of situational awareness? These issues will be considered in future work.

REFERENCES

1. Abrosimov, V. (2015). Swarm intelligent control object’s movement simulation in net-centric environment using neural networks. In *IAENG Transactions on Engineering Sciences, Special Issue for the International Association of Engineers Conferences 2014* (pp. 301–314), World Scientific Publisher, https://doi.org/10.1142/9789814667364_0023
2. Abrosimov, V. (2016). The property of agent’s sacrifice: Definition, measure, effect and applications, *International Journal of Reasoning-based Intelligent Systems*, **8**(1/2), 76–83, <https://doi.org/10.1504/IJRIS.2016.080069>.
3. Abrosimov, V. (2017). *Kollektivy intellektual’nykh letatel’nykh apparatov* [Collectives of Intelligent Aircrafts]. Moscow, Russia: Nauka, [in Russian].
4. Abrosimov, V. (2017). Role allocation in a group of control objects. In *Recent Developments in Intelligent Nature-Inspired Computing* (pp. 206–224). IGI Global. <https://doi.org/10.4018/978-1-5225-2322-2.ch010>.
5. Abrosimov, V. & Mazurov, A. (2021). Irrational behavioral strategies for a swarm of mini-robots, *Vestn. St. Petersburg State Univ. Appl. Math. Comp. Sci. Contr. Proc.*, **17**(4), in press.
6. Athreya, A.P. & Tague, P. (2013). Network self-organization in the Internet of Things. *Proc. 2013 IEEE Int. Conf. on Sensing, Communications and Networking (SECON)*, 25–33. <https://doi.org/10.1109/SAHCN.2013.6644956>.
7. Bonabeau, E., Dorigo, M., & Theraulaz, G. (1999). *Swarm Intelligence: From Natural to Artificial Systems*. Oxford, UK: Oxford University Press.
8. Duarte, M., Carvalho, J., Costa, V., Christensen, A.L., et al. (2016). Application of swarm robotics systems to marine environmental monitoring. *Proc. IEEE/MTS OCEANS Conference*, Shanghai, China. <https://doi.org/10.1109/OCEANSAP.2016.7485429>.
9. Endsley, M.R. & Jones, D.G. (2012). *Designing for Situation Awareness: An Approach to Human-Centered Design*. CRC Press.
10. Galetić, V., Bojić, I., Kušek, M., Ježić, G., Dešić, S., & Huljenić, D. (2011). Basic principles of Machine-to-Machine communication and its impact on telecommunications industry. *Proc. of the 34th Int. Convention MIPRO*, 380–385.
11. Hu, G., Tay, W.P., & Wen, Y. (2012). Cloud robotics: architecture, challenges and applications, *IEEE Network*, **26**(3), 21–28. <https://doi.org/10.1109/MNET.2012.6201212>.
12. Jha, A., Gupta, K., & Sen, M. (2014). M2M communication system for networked robots with low memory footprint. *Proc. of Int. Conference on Information*

- Technology Systems and Innovation (ICITSI)*, 310–316. <https://doi.org/10.1109/ICITSI.2014.7048284a>.
13. Namiot, D. & Sneps-Snepe, M. (2014). On M2M software, *International Journal of Open Information Technologies*, **2**(6), 29–36.
 14. Polsonetti, C. (2014). *Know the difference between IoT and M2M*. [Online]. Available <https://www.automationworld.com/article/topics/cloud-computing/know-difference-between-iot-and-m2m>
 15. Ray, P.P. (2017). Internet of Robotic Things: concept, technologies, and challenges, *IEEE Access*, **4**(16), 9489–9499. <https://doi.org/10.1109/ACCESS.2017.2647747>
 16. Ren, F. (2010). Autonomous agent negotiations strategies in complex environment. *Ph.D. Thesis*, School of Computer Science and Software Engineering, Faculty of Engineering, University of Wollongong.
 17. Starsinic, M. (2010). System architecture challenges in the home M2M network. *Proc. IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 1–7.
 18. Tan, S.K., Sooriyabandara, M., & Fan., Z. (2011). M2M communications in the smart grid: applications, standards, enabling technologies, and research challenges. *International Journal of Digital Multimedia Broadcasting*, <https://doi.org/10.1155/2011/289015>.
 19. Yadav, P., McCann, J.A., & Pereira, T. (2017), Self-synchronization in duty-cycled Internet of Things (IoT) applications, *IEEE Internet of Things Journal*, **4**, 2058–2069. <https://doi.org/10.1109/JIOT.2017.2757138>
 20. Ye, D., Zhang, M., & Vasilakos, A.V. (2016). A survey of self-organization mechanisms in multiagent systems. *IEEE Transactions on Systems*, **47**(3), 441–461.