A method of counteracting Byzantine robots with a random behavior strategy during collective design-making in swarm robotic systems

Fariza Tebueva, Sergey Ryabtsev*, and Igor Struchkov

Institute of Mathematics and Information Technologies named after Professor N.I. Chervyakov, North Caucasus Federal University, Stavropol, Russian Federation

Abstract. The active introduction of robotics swarm systems into life brings the issues of their information security up to date. Known security approaches often do not take into account the peculiarities of the implementation of swarm systems, such as collective design-making, and only consider the presence of Byzantine robots with a strategy of behavior consisting in voting against a majority when a consensus is reached. The aim of this work is to increase the security of the collective design-making process in a swarm robotics system from the imposition of false and ineffective alternatives by Byzantine robots with a random behavior strategy. It is proposed to use an approach based on the use of a distributed ledger and analysis of deviations in the process of collective design-making, which will allow identifying and isolating harmful effects. The solution to the problem of detecting Byzantine robots is based on the application of the criterion of the degree of confidence of a robot in choosing an alternative when a consensus is reached by the swarm system and is based on the assumption that the distribution of the degree of confidence of a Byzantine robot due to ignoring the parameters of the external environment and voting for random alternatives is significantly different from the behavior an ordinary robot. The elements of novelty of the presented solution include the use of the degree of confidence criterion to ensure the safety of collective design-making and the ability to take into account various strategies of behavior of Byzantine robots. The use of the presented solution makes it possible to increase the efficiency of reaching consensus by a swarm robotics system in the presence of Byzantine robots. The simulation for a swarm of 20 robots, including 5 Byzantine ones with random behavior, showed an increase in the probability of correctly reaching a consensus by 12.5%. The practical significance of the presented solutions lies in the possibility of ensuring the stability of reaching consensus by a swarm robotics system in the presence of robots with harmful behavior.

1 Introduction

* Corresponding author: nalfartorn@yandex.ru

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).
The issues of ensuring the required safety of swarm robotics systems (swarm robotics systems) are one of the barriers to their widespread practical application [1]. The existing paradigm of information security (IS) is often not suitable for use in swarm robotics systems, because, firstly, swarm robotics systems have significant resource constraints, and secondly, they have a set of specific features. Signs and characteristics of swarm robotics systems are described in detail and investigated in a number of works [2–5] and differ significantly from the usual objects of IS, such as, for example, information systems of enterprises. One of the most important features of swarm robotics systems from the point of view of IS is collective design-making. With an increase in the number of Byzantine robots (BR), the efficiency of the swarm robotics systems [6] is significantly reduced due to the imposition of ineffective or random alternatives in the process of collective design-making. Thus, the issues of ensuring IS of the collective design-making process in swarm robotics systems are of particular relevance.

The analysis of publications allowed us to identify several large groups of studies in this area:

1. Research based on trust and reputation. The essence of such technologies lies in the use of systems of establishing, trusted relationships, based on determining the reputation of individual agents/nodes [7,8].
2. Research based on traffic and behavior analysis; involving the development of technologies and methods aimed at detecting and tracking anomalous values and methods for verifying individual robots [9,10].
3. Research based on special models of IS management, suitable for use in a swarm robotics systems [11].
4. Research based on distributed ledger and blockchain applications. The essence of the application of distributed ledger technologies in the tasks of ensuring information security of collective design-making and coordination is that a collective solution in a SWARM ROBOTICS SYSTEMS can be achieved in a completely decentralized way, and the goals of using consensus achievement algorithms in blockchain systems are similar to the goals of collective design-making in swarm robotics systems [12–15].

The approach proposed in this work can be attributed to the 2nd and 4th groups of studies since it is based on a method that uses a distributed registry and at the same time uses an analysis of the degree of confidence of the robot in choosing an alternative for detecting a BR.

The complexity of applying the methods of the second group should include: the absence of a global communication channel in swarm robotics systems and the fact that local interactions of SWARM ROBOTICS SYSTEMS limit the communication of the entire system. On the one hand, this is the key to the easy scalability of the swarm robotics systems and increases the reliability and flexibility of the swarm, and on the other hand, it makes it difficult to analyze for IS. The use of blockchain solves this issue, but the blockchain itself is labor intensive in terms of hardware costs. This fact and the fact that the swarm robotics systems has small computing resources limits the possibilities of using blockchain. The article [15] provides a successful example of using blockchain technology to provide IS for collective design-making. To avoid high hardware costs, this paper uses a distributed ledger approach without using a hash function [16].

In addition, the analyzed studies in this area, as a rule, are considered as BR with the behavior of voting against the majority, while the behavior of a BR can have a variety of strategies. An integrated approach to IS requires consideration of all possible strategies for the behavior of a BR. In the article [17] the authors consider 3 possible types of strategies for the behavior of a BR, among them the contrarians are malicious robots that always opposes the majority of the group, the wishy-washy are malicious robots that keep changing their opinion every control loop and the sectis an organised group of zealots which are malicious robots that ignore any information from the environment and the neighbours and keep
communicating a constant opinion for a (possibly) inferior option, the above experiments consider groups and robots-opponents. The present study focuses on the random type of behavior of a BR and is based on assessing the degree of the robot's confidence in choosing an alternative. The aim of the work is to increase the security of collective design-making in swarm robotics systems from a BR with random behavior. The hypothesis is that, based on the degree of confidence, it is possible to identify a BR with random behavior strategy and exclude it from the collective design-making process due to the fact that a BR with random behavior will change its mind more often and its degree of confidence will turn out to be excellent.

2 Materials and methods

2.1 Experimental setup and simulation environment

The questions of collective design-making in the SWARM ROBOTICS SYSTEMS will be considered in the problem of reaching consensus using the classical problem setting [18]. For all experiments and simulations carried out in the framework of this work, the collective design-making problem of the most probable sign of the environment was used.

In this task, the purpose of the swarm robotics systems was to make a collective decision and choose one of two actions in the presence of several BR with a random behavior strategy: $A_1 = \text{vote for white}$ and $A_2 = \text{vote for black}$.

The choice of action is based on knowledge about the environment - the scene that robots form in the process of its research.

Consider the parameters of the experiments carried out in this work:

- The robots are limited to a $2 \times 2$ m square stage with four walls around perimeter.
- The grid consists of areas $S_j$, $S_1$ – white areas, $S_2$ – black areas.
- The ratio $S_2/S_1$ is $45/55$, i.e. the scene is 55% white and 45% black.
- In the process of exploring the scene, 20 e-puck robots are involved, moving along the surface and able to perceive the color of the surface below them. The robots have the following characteristics: a diameter of 7 cm, a maximum speed of 16 cm / s, RGB LED illumination, 8 proximity sensors, a surface color detection sensor, and a module for local information exchange, consisting of 12 infrared (IR) transceivers.
- Robots can communicate with each other only if there is no other robot interfering with communication, and if the distance between robots is less than $d_n = 22$ sm.
- At the end of the successful launch of the experiment, the SWARM ROBOTICS SYSTEMS will have an opinion about the choice of the action $A_i$, corresponding to the most frequently occurring color.

By random BR we mean robots that constantly change their minds in each collective design-making cycle. These robots ignore any information from the environment and neighbors. Random robots lead to denial of service, which corresponds to a decision deadlock in which a swarm cannot reach consensus [17].

The strategy of random BR behavior, by analogy with the strategies described in chapter 6.1 [3] can be described as:

$$N_{ij} = \text{rand} \ N_{ij},$$

where $N_{ij}$, utility for each action $A_i$ and state $S_j$, which is determined by the areas on the stage counted by the robots at the moment based on the ratio of white and black, $i$ is the selected action.
For the research, the ARGoS software was used with the ARGoS-Epuck add-on [19]. Before the start of the experiment, the robots generate a random scene of difficulty 0.8. Robots are randomly placed inside the scene.

The influence of BR with random behavior on the efficiency ($T_N^{\text{correct}}$ and $E_N$) of reaching a consensus of classical methods [20] and the method based on a distributed ledger, depending on the presence of BR with random behavior (b), is shown in Figure 1, where each column, as well as on all subsequent figures represent the results of 50 experimental runs.

---

**Fig. 1.** Influence of random BR on the efficiency of reaching consensus in collective design-making in classical methods and the distributed ledger method.
To assess the impact of BR, 2 indicators of the effectiveness of the swarm robotics systems are used [15]:

– exit probability \( E_N \), this is “the probability to make the best decision, computed as the proportion of runs that converge to consensus on opinion a.” [23]. In our experiments: \( a=w \) (‘white’).

– consensus time of correct outcomes \( T_N^{corr} \): this is the number of seconds needed until all non-Byzantine robots in the swarm have opinion ‘white.’ The metric is computed over all experimental runs that converged to ‘white’; runs that converged to ‘black’ are not considered.

Analyzing the results obtained, it can be observed that the DC method is the most stable from the point of view of the probability of completion \( E_N \) to random BR, other methods suffer a significant decrease in efficiency. Regarding the time of completion of the results \( T_N^{corr} \) we can conclude that the presence of malicious robots with random behavior obscures the time to reach a consensus in all cases. Thus, the problem of detecting and isolating BR with random behavior in the collective design-making process is urgent. This work focuses on a modification of the method [16] for detecting BR with random behavior.

### 2.2 A method for detecting BR with a random behavior strategy

The hypothesis is that a random robot, having a random strategy of behavior, does not take into account the signs of the external environment and information from other robots, which means that such a robot will often change its mind and its degree of confidence will be lower than that of an ordinary robot when voting on the most common feature of the environment. It is proposed to use confidence in the choice of color to detect BR with random behavior, which is calculated as:

\[
Y = \begin{cases} 
\frac{Q(b)}{Q(w)}, & \text{если } Q(b) < Q(w) \\
\frac{Q(w)}{Q(b)}, & \text{если } Q(b) > Q(w) 
\end{cases}
\]

where \( b, w \) – number of measurements of black and white, respectively, \( Q(b), Q(w) \) – the robot's assessment of the prevalence of a trait in the environment [18]. Thus, the \( Y \) value expresses a measure of the robot's confidence in choosing a color in the range from 0 to 1. The higher the value, the less confident the robot is in the selected color.

For the possibility of using such an approach, confidence was added to the method [16] in the exchanged data, although in this method it is not involved in the process of reaching a consensus in collective design-making, but is used in classical methods.

A study was carried out and the graphs of the ratio of the degree of confidence \( Y \) to time \( t \) for the entire swarm robotics systems for all robots were sharpened. However, since information about the entire system can only be taught to an observer who knows in advance which robots are random, graphs were also built for one individual robot who does not know which robots are BR, Figure 2.

The experiment carried out demonstrates the difference in the degree of confidence \( Y \) for ordinary and casual robots. Thus, the proposed approach makes it possible to determine BR with random behavior, however, in complex problems, that is, such that the ratio of the external environment signs will tend to 50 to 50, this approach may turn out to be ineffective due to the similarity in this case of the distribution of the degree of confidence of BR and ordinary robots.
This can cause deviations in the votes of ordinary robots, in connection with which it is necessary to approach the choice of the threshold for the deviation of votes from the conditions of a specific problem; in the experiments conducted as part of this work, the deviation threshold of 10% showed the best results.

3 Results

The results of applying a modification of the distributed ledger approach, which makes it possible to detect and exclude a BR with a random behavior strategy, are shown in Figure 3.

![Figure 3](image)

**Fig. 3.** Comparison of the method with a distributed ledger with its own modification for detecting a BR with random behavior strategy.
It can be observed that the efficiency of reaching consensus in the presence of a BR with random behavior using the proposed approach has increased. The simulation for a swarm of 20 robots, including 5 malicious ones with random behavior, showed an increase in the probability of correctly reaching consensus on average by 12.5%. Thus, the goal of this study to improve the security of collective design-making in swarm robotics systems by detecting and isolating a BR with random behavior has been achieved.

4 Discussion and conclusion

This paper discusses the problems of detecting a negative impact from malicious robots with a random strategy of behavior to achieve consensus in collective design-making in swarm robotics systems. The paper presents an approach to detecting a BR with random behavior strategy, based on the application of the parameter «degree of confidence» of the robot in choosing an alternative when reaching a consensus in SWARM ROBOTICS SYSTEMS. The use of the presented solution makes it possible to increase the efficiency of reaching consensus by a swarm robotic system in the presence of malicious robots. The simulation for a swarm of 20 robots, including 5 malicious ones with random behavior, showed an increase in the probability of correctly reaching a consensus by 12.5%.

The advantages of the approach are lower hardware costs compared to blockchain because it does not use hash functions, as well as some universality, which lies in the fact that the method is based on collective design-making mechanisms, which are fairly similar on different hardware platforms of swarm robotics systems. The proposed approach can serve as a basis for the development of more complex mechanisms for providing IS in swarm robotics systems, however, it has a number of disadvantages, the elimination of which determines the future directions of work in this area:

1. For complex tasks with an equal ratio of $S_2/S_1$ features close to $50/50$, i.e. if the scene has 50% white and 50% black cells, the approach is ineffective, since the distribution of ordinary robots will be very similar to the distribution of malicious random robots. This fact can cause false positives and rejection of the voices of ordinary robots.

2. For simple tasks that will be completed quickly, a situation may arise with an insufficient amount of data to make a decision to isolate a robot, since obvious differences between BR and ordinary robots begin to be observed after 2000 steps. Thus, if the task completes quickly, then it is difficult to detect a BR with random behavior strategy without false positives.

The presented approach can be applied not only in swarm robotics systems, but also in other similar technologies, tasks in which may require a decentralized approach to management and consensus building. The practical significance of the presented solutions lies in the possibility of ensuring the stability of the achievement of consensus by a swarm robotic system in the presence of robots with faulty or harmful behavior.

The reported study was funded by Russian Ministry of Science (information security), project №10/2020.

References

1. F. Higgins, A. Tomlinson, and K. M. Martin, Int. J. Adv. Secur. F., Tomlinson, A., Martin, K. M., Int. J. Adv. Secur. 2(2), 288 (2009)

2. A. Zakiev, T. Tsoy, and E. Magid, Lect. Notes Comput. Sci., 291 (2018)

3. H. Hamann, Swarm Robotics: A Formal Approach (2018)
4. I. Navarro and F. Matía, ISRN Robot. **2013**, 1 (2013)
5. L. Bayindir, Neurocomputing **172**, 292 (2016)
6. I. Sargeant and A. Tomlinson, IntelliSys 2016 Proc. SAI Intell. Syst. Conf. 628 (2018)
7. I. A. Zikratov, I. S. Lebedev, and A. V. Gurto, Int. Conf. Next Gener. Wired/Wireless Netw (2014)
8. E. Basan, A. Basan, and A. Nekrasov, Sensors **19**, 4007 (2019)
9. E. Basan, A. Basan, and O. Makarevich, EEE, 516 (2018)
10. I. Sargeant and A. Tomlinson, *Intrusion Detection in Robotic Swarms* (2020)
11. I. A. Zikratov, I. S. Lebedev, A. V. Gurto, and E. V. Kuzmich, IEEE, 1 (2014)
12. T. T. Nguyen, A. Hatua, and A. H. Sung, Adv. Intell. Syst. Comput., 118 (2020)
13. J. Luo, B. Ding, and J. Xu, IEEE, 577 (2019)
14. Y. Nishida, K. Kaneko, S. Sharma, and K. Sakurai, IEEE, 524 (2018)
15. M. Strobel, V., Ferrer, E.C., Dorigo, Proc. Int. Jt. Conf. Auton. Agents Multiagent Syst. AAMAS 1, 541 (2018)
16. V. I. Petrenko, F. B. Tebueva, S. S. Ryabtsev, M. M. Gurchinsky, and I. V. Struchkov, IOP Conf. Ser. Mater. Sci. Eng. (2020)
17. F. Canciani, M. S. Talamali, J. A. R. Marshall, and A. Reina, *Keep Calm and Vote on: Swarm Resiliency in Collective Decision Making* (2019)
18. M. Dorigo, M. Birattari, and M. Brambilla, Scholarpedia **9**, 1463 (2014)
19. C. Pinciroli, V. Trianni, R. O’Grady, G. Pini, A. Brutschy, M. Brambilla, N. Mathews, E. Ferrante, G. Di Caro, F. Ducatelle, M. Birattari, L. M. Gambardella, and M. Dorigo, Swarm Intell. **6**, 271 (2012)
20. G. Valentini, D. Brambilla, H. Hamann, and M. Dorigo, Lect. Notes Comput. Sci. (Including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics, 65 (2016)