

On the issue of building sea convoys from unmanned ships

Ilya Shipunov^{1,*}, *Anatoliy Nyrkov*¹, *Yuri Katorin*¹, *Vagiz Gaskarov*¹, and *Tatiana Knysh*¹

¹Admiral Makarov State University of Maritime and Inland Shipping, Dvinskaya Street 5/7, Saint-Petersburg, 198035, Russia

Abstract. This paper presents the concept of building full-fledged sea convoys, which include unmanned ships. Advantages of this approach to combining unmanned ships over those where the ship is considered as a separate unit are considered. The scheme of distribution (combining) of computing power inside the convoy is given. In this paper, a scheme is considered when the crew is present only on the lead ship. However, this does not mean that all other ships in the convoy should be only unmanned. It doesn't matter when considering this concept. The paper also proposes an algorithm for determining obstacles using optical sensors. The aspects of information security in such convoys are also considered. Particular attention is paid to the investigation of computer incidents on unmanned ships.

1 Introduction

The shipping industry is on the cusp of entering the era of unmanned shipping. An increasing number of maritime companies are starting to invest in this area of development of traditional shipping. Many developments are already helping the crews of traditional ships. Of course, to date, a sufficient number of engineering and theoretical options for the implementation of unmanned ships have been accumulated. However, in the course of development, new tasks arise that need to be solved already at early stages.

In the framework of the use of unmanned ships, a number of complex tasks arise due to the following factors:

- a ship is not a simple object for automated control;
- a huge number of external factors affecting the trajectory of movement;
- the complexity of navigation equipment and the variety of power facilities;
- a large array of information that must be processed by software in a short period of time to develop an optimal control action.

A possible simplification in solving these problems can be the transition from considering an unmanned ship as one unit to groups of such ships following a single route and united into one convoy.

* Corresponding author: mr-shis@yandex.ru

2 Methods and Materials

The key task is to guide the ship from the port of departure to the port of arrival in an autonomous mode. Let's consider some of the tasks that follow from it:

- ensuring control over the ship movement along the route;
- installation and maintenance (even on the route) of complex and expensive computing equipment;
- ensuring safe traffic.

Control over the ship movement can be carried out in a remote-visual mode (cameras of the ship itself, aerial photography from a drone), remotely-analytically (data from sensors and satellites in a text-graphic representation on the dispatcher's screen). Both methods assume a stable data link between the unmanned ship and the control center.

The computational power for steering a ship of this type can also be built according to the schemes shown in Figure 1.

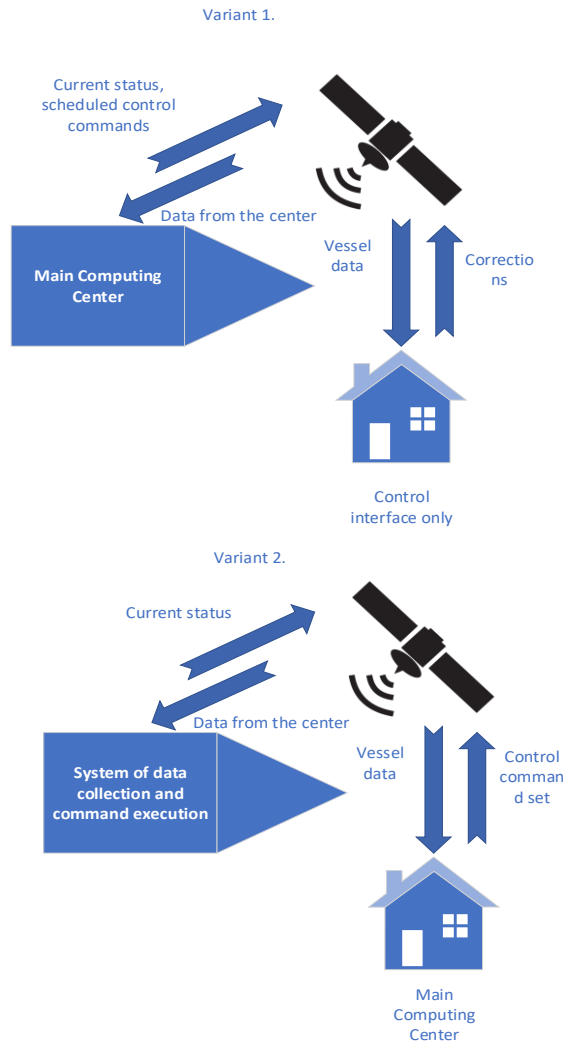


Fig. 1. Options for information interaction between the vessel and the shore center.

The first option involves the placement of the main computing power on board the ship. On the one hand, this allows the ship to be as autonomous as possible even in the absence of communication with the control center. With such an arrangement, the coastal center performs the functions of a spotter and either agrees with the proposed actions of the sea drone, or makes adjustments. On the other hand, all the capacities are serviced exclusively by one ship, and in conditions of movement without maneuvers, part of the computing power is idle. Also, in case of a failure of any node of the system, if the duplicate (backup) systems cannot ensure correct operation, there is a big problem with prompt repair.

The second option assumes that more modest computing devices are on board, which are sufficient for collecting and transmitting information about the current indicators of the vessel's sensors and launching control commands transmitted from the coastal center. This configuration reduces the number of elements that may need to be repaired on board. Also, with this option, the coastal computing center is able to navigate several unmanned ships at once, reducing the idle time of computing power.

To implement both options, a stable channel of information exchange between the ship and the coastal center is required. However, satellite communication cannot be stable enough on all parts of the route in order to pump such a volume of data through itself. Another factor affecting security is the speed of data transmission over an unstable channel. This can have a dramatic negative effect on the maneuvering of the ship in a non-standard situation.

Also, both configurations are not protected from attacks, in which the technology of spoofing signals from the attacked ship is used. In this case, the coastal center will see that the ship continues to follow the route correctly. And even if the signal is simply interrupted (a jammer will be used), the task force will have to spend a large amount of time before arriving at the crime scene.

Let's try to find a compromise by building a new configuration that includes all the positive characteristics proposed in the classical versions and minimizes the problem nodes of both configurations. To do this, we will draw up a minimum list of requirements for such a configuration.

List of requirements:

- mixed mode of operator observation of the controlled object;
- stable channel of information exchange between the control center and the controlled object;
- minimum delay in the transmission of information;
- minimum response time to a non-standard situation;
- minimum downtime of computing power (possibility of parallel computing for several ships);
- control over the relevance of data transmitted from the control object.

The most difficult are the requirements related to the communication channel. This is caused by the fact that there is a rather long distance between the ship on the high seas and the control center, and the ship is constantly changing its location and environmental conditions, which negatively affects the quality of communication. However, it is quite simple to organize a stable channel between objects located at a short distance, and it is not necessary to use satellite communication. Note that the solution to this issue will also help in solving the rest of those put forward earlier.

Let's consider a modern train. It consists of a locomotive, in which absolutely all the control potential is concentrated, and cars, which can be of different types, the main condition is that the coupling mechanisms are compatible. Thus, we can start talking not about separately existing autonomous ships, but about sea convoys. A possible scheme of such convoys is shown in Figure 2.

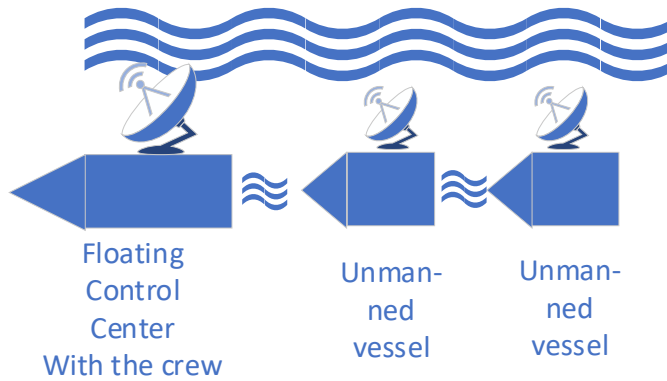


Fig. 2. Possible convoy interaction scheme.

The convoy is headed by a ship with a crew on board. This vessel performs all maneuvers in manual mode. Electronic means record the ship's behavior and build a basic model of the maneuver. All ships of the convoy are connected by two communication channels: common channel - where access is open for each vessel, and the coupling channel. This channel is individual, and its members are designated as master and slave. Thus, a kind of information chain will be organized. This approach is needed in order to ensure information exchange even if the common channel does not work correctly for some reason. This channel will also allow neighboring ships to view each other's status and, if necessary, report a malfunction to the control center. A break in this chain will indicate an attempt to hijack a ship and the need for urgent action.

The ships in the convoy will be located at such a distance so as not to interfere with each other's maneuvering on the one hand, and on the other hand, so that it is possible to provide video surveillance of the ship's progress by means of the ships in front and behind. This will allow the control center to monitor the convoy participants both by telemetry data from the vessel and by means of a video stream from neighboring vessels.

Also, such an organization can solve the issues of minimizing the downtime of computing power, delays in the transfer of information and reaction time to an unusual situation.

An important aspect is also the possibility of organizing control over the actions of the control center when considering emergency situations. Storing the so-called logs directly on board the lead ship is not safe. Since there is a possibility of intentional data corruption. Within the framework of the concept of such a convoy, it is possible to organize the storage of data in a database distributed among the convoy participants. The block chain can receive blocks of two types: control commands (source control center) and information on the vessel's response (source of convoy participant). This approach will prevent the substitution of control commands and concealment of control violations.

Let us consider a possible principle of constructing control commands for a single autonomous ship. Let there are two vectors of parameters $V1$ - parameters that rarely change relative to the current route (vessel length, width, displacement, etc.) and $V2$ - parameters that change often (course, current speed, wind, etc.). The values of vector $V1$ are mostly set (updated) by the operator in preparation for the voyage, the $V2$ values are changed automatically in accordance with the data received from the sensors and corrective data from the control center. On the approach to the maneuver point, the mechanism for preparing an ordered set of control commands should start. This set should be generated as a result of the maneuver preparation function - $F(V1, V2, V3)$. Here $V3$ is a vector identical in structure to $V2$, but reflecting not the current state of the vessel, but those parameters that it should have at the end of the maneuver. The time of completion of the calculation,

checking for correctness and possible approval of the set by the control center should coincide with the position of the ship at the beginning of the maneuver zone, which also poses the task of forecasting at the stage of preparing the trip. When leaving the maneuver zone, the mechanism for checking compliance with V2, V3 should be launched and, if necessary, the corrective maneuver should be calculated.

The main problem of this approach is the great difficulty in compiling an algorithm for the function of preparation for the maneuver. This is caused by the large number of parameters that must be taken into account when preparing a solution. Within the framework of the convoy, a different approach may be used, since a manned ship will pass the maneuver point in front of the unmanned ships. This raises the problem of adapting the algorithm performed by the crew (AL) to the parameters of the unmanned ship. That is, the function of preparing a maneuver essentially becomes a corrective function having the form $F_k(V1, AL)$. In this case, V2 may not be involved, since there is already an algorithm for performing the maneuver. It should be noted that the algorithm of the correcting function must be updated after all the characteristics of V1 have been determined, i.e. after the end of loading and refueling.

Within the framework of the development of unmanned ships, the drafting of various regulatory documents and regulations plays an important role. It was said above that for the correct operation of the correcting function, it is necessary to update the algorithm. This is caused by the fact that the composition of the convoy, as well as other input data, may change. However, it is impossible to assign one person to each ship. Therefore, it is necessary to put into circulation some documents that help in organizing the customization process. Let's draw an analogy with traditional ships.

To obtain the proper level of controllability of the ship during its development and in order for the boatmaster to have the necessary level of information about the maneuvering characteristics of the ship, the following list of documents was adopted by the IMO:

Circular MSC/Circ.389 dated 10.01.1985 – “Interim guidance for the assessment of the maneuverability of ships during their design”;

Resolution A.601(15) of 19.11.1987 - “Ensuring the availability and submission of information on maneuvering elements on board ships”;

Resolution MSC.137 (76) of 05.12.2002 – “Standards for the maneuverability of ships”;

Circular MSC/Circ.1053 dated 05.12.2002 - “Explanations on the standards for the maneuverability of a ship”.

For unmanned ships, either similar documents should be created, taking into account their specifics and other regulatory documents in this area, or corrections should be made to these documents.

For the purpose of setting the corrective function, an analogue of resolution A.601(15) is required.

In accordance with this document, the ship must have information on the topic of handling. This should include a pilot card, a poster of maneuvering characteristics. These forms contain sufficient information about the state of the system that propels the vessel, as well as about the loading. In addition, thanks to the maneuvering characteristics poster, the adjuster will always know the basic parameters of the ship's handling. In general, the information in the listed documents is sufficient for fine adjustment.

Of course, it is not necessary to keep all this on paper and in the form of posters. All this can be recorded in the database of the ship itself and can be provided to an authorized person in electronic form at any time.

As it was discussed above, with this concept, it is not necessary to equip all vessels with a complete set of sensors. With this approach, the analysis of the surrounding static obstacles is sufficient to be carried out by the lead vessel using its equipment. After that, it is possible to transfer this data along the chain to the next ships. This does not mean that all

other ships in the convoy should be blind. However, simpler sensing systems can be installed on them, which will lead to cost savings when building a ship.

Following steps can be used as an object recognition algorithm.

1. Determination of boundaries. The Canny edge detector is perfect for this. It uses a multi-stage algorithm to detect a wide variety of edges in images.
2. Definition of lines. The data obtained from the previous step can be used for the Hough transform.
3. Further, already knowing the results of the second step and the parameters of the ship, it is necessary to build a rectangle in which the ship is inscribed, the rectangles of the surrounding objects, and position it all on the plane. Then plot or correct the route.

It makes no sense to take all the steps for every ship. It is enough to transfer the geo-position and all the data for calculating the last step along the chain.

As already mentioned at the very beginning, when operating unmanned ships in the event of cyber-attacks, it is very difficult to counteract the intruder due to the distance from the protected object, but it is quite possible to ensure the operation of the computer incident recognition system. Analyze attacks and take all possible actions to counter them.

The computer incident investigation system can be implemented based on The Volatility Framework - an open source project written in the Python programming language, which is the most widely used platform for memory forensics. This framework allows examination of RAM dumps from various operating systems. It has extensive analysis capabilities:

- analysis of processes;
- detection of API hooks in processes and kernel memory;
- unloading processes for reverse engineering;
- creation of timelines from artefacts in memory;
- search for hidden and embedded code;
- YARA support.

Here is a basic list of the features of this framework. With a deeper study, it opens up ample opportunities for analyzing random access memory. The system will use algorithms from Volatility and automatically analyze reports. In this case, it will take less time to process a separate core memory dump. In addition, automatic analysis will help to minimize the human factor when viewing reports. In situations where a person has not noticed the embedded code or dangerous process, the automatic analysis system will draw the attention of specialists to them.

In addition, this framework is distinguished by the speed of the algorithms compared to competitors, as well as the extensible API with script support.

YARA is a system designed to facilitate the work of researchers and is included in the Volatility framework. It allows specialists to write their own rules for identifying malware images in the system (or any other patterns that can be described in text or binary format). YARA is used in such products as Kaspersky Lab, ESET, Radare2, McAfee, and so on. The above is the relevance of using this system in the analysis of computer incidents. The rule base should be regularly updated in a manner similar to the ever-evolving area of malware.

Using Volatility and the YARA rule base, it is possible to thoroughly scan for viruses in the RAM of the attacked system (host), as well as track the paths along which the virus entered the system.

The advantages of Volatility also include a wide range of supported operating systems and memory formats. The Volatility Framework is maintained and regularly updated. In addition, this framework has the ability to expand its functionality by writing custom plugins that can be easily integrated into the system. Plugins for Volatility and rules for

YARA provide endless opportunities to improve the incident investigation system and allow it to develop modularly, which does not require serious costs for software development and updates. It is enough to develop a plugin for a specific task and place it next to the incident investigation system.

To carry out work on the study and collection of digital evidence, it is necessary to adhere to the principles of immutability, integrity, completeness of information and its reliability. Accordingly, one of the main stages in the investigation of computer incidents is to determine the list of stolen, modified and deleted information. Captured memory dumps will certainly help to determine the sequence of actions of the attacker and hard disk dumps - to recover lost data. To protect the analysis system, it is necessary to provide backup power to the equipment, and configure the backup system to avoid unintentional loss of data.

3 Discussion

In the summer of 2020, DARPA came up with the concept of sea trains, but aimed at military purposes. For example, to evacuate other ships from a war zone. However, DARPA suggests leaving the lead ship unmanned as well. This can be bad for the formation of a caravan of ships of various types.

In Russia, more and more people are talking about the use of unmanned ships in the harsh climate of the northern sea route. Note that in the concept discussed in the article, there are no restrictions on the class of the lead ship. It can also be an icebreaker. However, to extend this concept to ice traffic, additional parameters will need to be introduced into the control function. And it is also necessary to adjust the composition of the convoy, ensuring the passage of ships.

4 Conclusion

Unfortunately, unmanned shipping today still has very few practical trips. Whether such a concept will be more profitable than single trips will be possible to reliably say only with the accumulation of a sufficient amount of information about the economic side of the issue.

References

1. A.P. Nyrkov, A.A. Zhilenkov, S.S. Sokolov, et al., Autom Remote Control **79**, 195 (2018) <https://doi.org/10.1134/S0005117918010174>
2. A.P. Nyrkov, N.B. Glebov, R.O. Novoselov, O.M. Alimov, S.G. Chernyi, *IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS*, 132-135 (2018) <https://doi.org/10.1109/ITMQIS.2018.8525058>
3. I.S. Shipunov, A.P. Nyrkov, M.V. Kardakova, Y.F. Katorin, V.V. Vychuzhanin, *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 497 - 500 (2020) <https://doi.org/10.1109/EIConRus49466.2020.9039181>
4. I. Shipunov, A. Nyrkov, V. Korotkov, O. Alimov, T. Knysch, E3S Web of Conferences **203**, 05005 (2020) <https://doi.org/10.1051/e3sconf/202020305005>
5. S. Sokolov, A. Zhilenkov, S. Chernyi, A. Nyrkov, N. Glebov, *Bulletin of Electrical Engineering and Informatics* **9(3)**, 1268 - 1275 (2020) <https://doi.org/10.11591/eei.v9i3.1293>

6. V. Veselkov, N. Vikhrov, A. Nyrkov, S. Chernyi, I. Titov, *IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW) St. Petersburg*, 598-601 (2017) <https://doi.org/10.1109/EIConRus.2017.7910625>
7. M. Kardakova, I. Shipunov, A. Nyrkov, T. Knysh, *Advances in Intelligent Systems and Computing* **982**, 481 – 490 (2020) https://doi.org/10.1007/978-3-030-19756-8_46
8. I.S. Shipunov, K.S. Voevodskiy, A.P. Nyrkov, Y.F. Katorin, Y.A. Gatchin, *IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW) St. Petersburg*, 339-343 (2019) <https://doi.org/10.1109/EIConRus.2019.8657219>
9. I.S. Shipunov, K.S. Voevodskiy, A.P. Nyrkov, Y.F. Katorin, Y.A. Gatchin, *IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW) St. Petersburg*, 344-347 (2019) <https://doi.org/10.1109/EIConRus.2019.8657215>
10. A.P. Nyrkov, Y.F. Katorin, V.D. Gaskarov, Y.V. Kosyak, A.V. Sauchev, *IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW) St. Petersburg*, 98-101 (2018) <https://doi.org/10.1109/EIConRus.2018.8317039>
11. A.A. Zhilenkov, S.S. Sokolov, S.G. Chernyi, A.P. Nyrkov, *Journal of Intelligent and Fuzzy Systems* **38(5)**, 6619 – 6625 (2020) <https://doi.org/10.3233/JIFS-179741>
12. A. Nyrkov, K. Goloskokov, E. Koroleva, S. Sokolov, A. Zhilenkov, S. Chernyi, *Advances in Systems, Control and Automation. Lecture Notes in Electrical Engineering* **442**, 387-394 (2018) https://doi.org/10.1007/978-981-10-4762-6_37