Original article
https://doi.org/10.21683/1729-2646-2020-20-2-35-42

Development of algorithms of self-organizing network for reliable data exchange between autonomous robots

Alexander V. Ermakov[1*], Larisa I. Suchkova[1]
[1]*Polzunov Altai State Technical University, Russian Federation, Altai Krai, Barnaul*
[*]*tour0@ya.ru*

Alexander V. Ermakov

Larisa I. Suchkova

Abstract. *Factors affecting the reliability of data transmission in networks with nodes with periodic availability were considered. The principles of data transfer between robots are described; the need for global connectivity of communications within an autonomous system is shown, since the non-availability of information on the intentions of other robots reduces the effectiveness of the robotics system as a whole and affects the fault tolerance of a team of independent actors performing distributed activities. It is shown that the existing solutions to the problem of data exchange based on general-purpose IP networks have drawbacks; therefore, as the basis for organizing autonomous robot networks, we used developments in the domain of topological models of communication systems allowing us to build self-organizing computer networks. The requirements for the designed network for reliable message transfer between autonomous robots are listed, the option of organizing reliable message delivery using overlay networks, which expand the functionality of underlying networks, is selected. An overview of existing popular controlled and non-controlled overlay networks is given; their applicability for communication within a team of autonomous robots is evaluated. The features and specifics of data transfer in a team of autonomous robots are listed. The algorithms and architecture of the overlay self-organizing network were described by means of generally accepted methods of constructing decentralized networks with zero configurations. As a result of the work, general principles of operation of the designed network were proposed, the message structure for the delivery algorithm was described; two independent data streams were created, i.e. service and payload; an algorithm for sending messages between network nodes and an algorithm for collecting and synchronizing the global network status were developed. In order to increase the dependability and fault tolerance of the network, it is proposed to store the global network status at each node. The principles of operation of a distributed storage are described. For the purpose of notification on changes in the global status of the network, it is proposed to use an additional data stream for intra-network service messages. A flood routing algorithm was developed to reduce delays and speed up the synchronization of the global status of a network and consistency maintenance. It is proposed to provide network connectivity using the HELLO protocol to establish and maintain adjacency relations between network nodes. The paper provides examples of adding and removing network nodes, examines possible scalability problems of the developed overlay network and methods for solving them. It confirms the criteria and indicators for achieving the effect of self-organization of nodes in the network. The designed network is compared with existing alternatives. For the developed algorithms, examples of latency estimates in message delivery are given. The theoretical limitations of the overlay network in the presence of intentional and unintentional defects are indicated; an example of restoring the network after a failure is set forth.*

Keywords: *dependability; message delivery; guaranteed data delivery; overlay network; autonomous robot; group interaction; multi-agent robotic system.*

For citation: *Ermakov A.V., Suchkova L.I. Development of algorithms of self-organizing network for reliable data exchange between autonomous robots. Dependability. 2020;2: 35-42. https://doi.org/10.21683/1729-2646-2020-20-2-35-42*

Received on: *21.11.2019* / **Upon revision:** *14.04.2020* / **For printing:** *17.06.2020.*

Introduction

Successful task execution by a team of robots depends on the reliability of communications between its members, namely guaranteed delivery of messages to the actor and receipt of feedback.

The problem associated with improving the reliability of data transmission in a network with flickering nodes was considered by Lavrov D.N. in [1–2]. A flickering node is understood as an intermediate device able to transmit messages and is characterized by unstable operation or varied presence in the network, e.g., as the result of spatial movement of the node.

The concept of alternate availability nodes is applicable to major mobile objects, such as ships, airplanes, trains, robotics systems [3]. Know-how in the area of topology models of communication systems exists and can be applied to self-organizing computer networks. The key specificity of such algorithms consists in the impossibility to guarantee information transfer via the specified route due to the dynamic nature of the network and varying topology.

The matters related to the interaction within a team of mobile robots emerged in the 1980s; before that, research was focused on individual robotics systems or distributed systems not associated with robotics [4].

Jun Ota's research [5] confirms the existence of a class of problems that are optimally resolved through the use of swarm robotics, one of the fundamental tenets of which consists in the ability of parallel and independent execution of subtasks that reduces the total time of task performance. Any system that uses a set of interchangeable agents allows improving fault tolerance by simply replacing a failed robot, however, the creation of multifunctional agents is associated with high costs as compared to the creation of single-purpose agents. The distributed approach allows designing specialized robots that perform tasks that other agents struggle with [6].

As we know from the paper by Michael Krieger, Jean-Bernard Billeter and Laurent Keller [7], when tasks are partitioned among robots, reduced system efficiency may be observed. For instance, even if the total cost of a multiagent system proves to be lower than that of an integral solution, managing such system may be difficult due to the decentralized nature or absence of a global data storage. The absence of information on the intentions of other agents can cause a situation when individual robots will interfere with each other in terms of task performance. In order to avoid that, global connectivity is required that would ensure reliable data exchange between autonomous robots for the purpose of local and global planning and subsequent performance of local tasks by each agent.

Data exchange in constantly changing external conditions is a factor that directly affects the operational stability and efficiency of a team of robots. In this context, the development and research of reliable communication algorithms are relevant and serve to improve the functional dependability of a robotics system as a whole. In [8], experimental research of fault tolerance is cited that shows the importance of assuring reliable communication in respect to a team of robot.

Of special interest is the research of the algorithms of communication between autonomous robots, as the dependability and stability of their operation affect the decision-making time and coordinated activities of the team as a whole.

Currently, short-range communication is based on mesh networks that are distributed self-organizing networks with meshed topology deployed using Wi-Fi networks [9].

Higher-level protocols, such as TCP, guarantee reliable delivery of messages over such networks. However, due to the growing scope of communications on the Internet and requirement of fault-free operation of the network, adding new basic protocols and modifying their structure in order to provide new services became difficult [10]. Overlay networks allow extending a network's functionality without interfering with lower-level basic protocols [11] and can provide the following services: establishment of disruption-tolerant networks [12], rendezvous points [13], search [14–15]. It is difficult to provide such services at the IP level.

The commonly used overlay networks ensure reliable delivery of messages to a network node in various ways. Some networks specialize on anonymity (tor [16], I2P [17]) guaranteeing safe delivery, others rely on fast Wi-Fi network deployment (MANET [18], netsukuku [19]).

Overlay networks separate themselves from lower-level protocols. Thus, for instance, a network may use a different communication media in different segments of a heterogeneous network. The only requirement for the networks an overlay network operates with is the availability of an inter-subnet route. Figure 1 shows an example of overlay network constructed on top of an IP network.

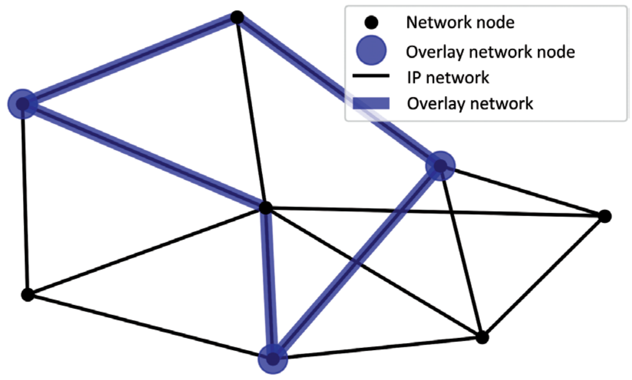

Fig. 1. An example of overlay network constructed on top of an IP network

The authors of [10] classify overlay networks into two major groups:

- controlled networks, where each node is aware of all nodes of the network and their capabilities;

- non-controlled networks, where none of the nodes is aware of the whole network topology.

Non-controlled networks are normally constructed using local area networks. Controlled overlay networks, on the contrary, are centralized or have one of the mechanisms of distributed storage of global network status, e.g. distributed hash tables (DHT) [20–22].

The tor network uses TCP flows for communication between network nodes and onion routing for passing messages within the network. It is not fully decentralized, as catalog servers exist that store information on the network status [16]. The tor network requires the availability of the Internet.

Other peer-to-peer or BPE-based networks do not have the function of passing messages to other nodes, and they require Internet in order to operate.

Thus, currently there are no network solutions for reliable communication within a team of autonomous robots.

In the context of the development of algorithms of reliable communication between autonomous robots, a self-organizing network must meet the following requirements:

- no need for manual node setting;
- a network client must be simple and easy to install (among other things, not require kernel patches or a specific version of the operating system);
- the network must operate at user level with no specific privileges;
- the network must operate on top of standard TCP and/or UDP protocols.

The existing overlay networks that were considered above do not meet the requirements, which urged the decision to develop an algorithm for reliable data exchange using an overlay network.

Structure of a self-organizing network

It is proposed to use an overlay network for the purpose of data exchange between autonomous robots. In such network, information is exchanged at the application layer based on the OSI model on top of the standard TCP and UDP protocols.

In order to connect to an overlay network, a client computing unit, e.g. the onboard computer of an autonomous robot, runs software that established connection with other network nodes and performs data transfer between intermediate nodes. Each node of a network at each moment in time maintains several connections while ensuring channel redundancy.

Structure of the message for delivery logic

A message is the minimal data unit transmitted within an overlay network. UDP packets are used for announcing changes within a network and low-priority notifications; they are received and parsed completely, which reduces the processing time. TCP requires a more complex processing algorithm. However, the fixed-size message header and

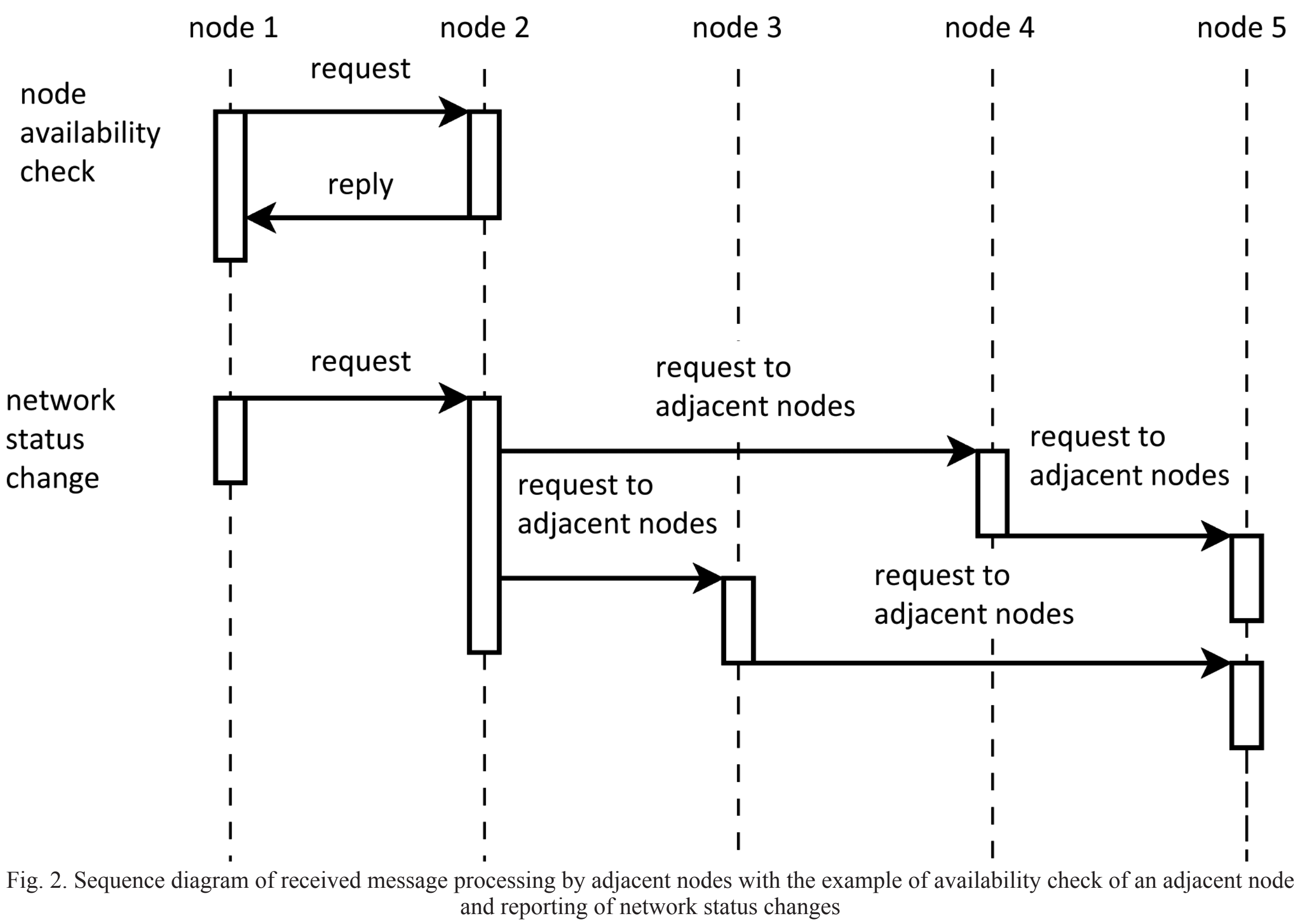

Fig. 2. Sequence diagram of received message processing by adjacent nodes with the example of availability check of an adjacent node and reporting of network status changes

presence of the data length field enable parsing the incoming TCP flow into individual messages.

A message is described with a formal structure: {IDsrc; IDdest; CMD; LEN; P}, where:

IDsrc is the source node identifier (8 bytes);

IDdest is the destination node identifier (8 bytes);

CMD is the type of the message (1 byte);

LEN is the length of the data field (unsigned integer, 2 byteы);

P is the protobuf2-coded data field of the length of LEN bytes [23].

Thus, a message consists of a header of the length of 19 bytes and variable-length data field.

A cell header {IDsrc; IDdest; CMD; LEN} contains a sender identifier and a recipient identifier. Node identifiers are 64-bit numbers comprised of a pair of IP addresses: {IPiface; IPext}, where:

IPiface is the network interface IP;

IPextis is the external IP address.

We believe such identification to be sufficient for our purposes. It allows nodes to generate unique identifiers for themselves, thus reducing the probability of collision to zero.

Depending on the type of CMD message, the message handler is selected. Cells are classified into two groups, i.e. the control and the transmit cells. Control cells are processed by destination nodes. That may include, for instance, cell availability check commands, network status change requests and responses (see Fig. 2). Transmit cells contain data that need to be processed if the recipient identifier matches the current node or transmit farther along the network.

The message processing procedure proposed by the authors has been implemented as software [24].

Algorithm of collection and synchronization of network status

A network intended for exchanging data between autonomous robots is controlled, i.e. it has a globally updateable status that contains information on all network nodes. The entire information on the network status is stored in each node. Thus, data redundancy increases the dependability and overall reliability of the network.

When a new node is added to the network, other LAN nodes are detected by means of a broadcast. In case of successful detection, communication is established with adjacent nodes and network status is synchronized. At this stage, message exchange occurs in all channels simultaneously (flooding) [1].

Flood routing is used for notification of changes in network status, for instance, when a new node is added. A network node sends the received packets to all of its direct neighbours, except the one, from which it was received. That approach improves the reliability of service information delivery and increases the probability of message reception by all the nodes of the network. The problem of message duplication is resolved through cashing of the received messages and inhibition of repeated message sending.

Figure 3 shows the block diagram of the system operation. A node receives a message from the network; depending on the value of CMD message type, flood routing algorithm is launched. The received packet is checked in the packet cache buffer in the random-access memory. If the packet is found in the cache, i.e. it was received earlier, the algorithm stops, discarding the packet and not processing it. Otherwise, the packet is added to the cache, replacing the oldest entries in the cache. Then, data field P from the packet is decoded and applied to the acquired global network status. Upon committing changes, the network status is rehashed. With that, local changes are complete; after that, adjacent nodes are notified by bulk messaging of the received message. An updated list of adjacent nodes is made, while the packet is immediately sent over UDP to nodes, from which a HELLO packet was recently received; for other network nodes, the generated packet is queued for subsequent asynchronous sending.

Besides flood routing, network status data consistency is maintained in all nodes through scheduled sending to adjacent nodes the hash of the list of known network node identifiers. In case of matching hash, adjacent nodes are synchronized. The capability to receive network status data from an adjacent node allows reducing the time of new node inclusion and not overwhelm the network with many complex messages [25].

Each node sends HELLO packets to the adjacent nodes, notifying them of its availability. Before network client shutdown it sends the respective notification over the network. In case of disconnection of or upon HELLO packet timeout a node makes several attempts to reconnect to the lost node. If the node proves to be unavailable, a message on the removal of the identifier from the network status is generated. Thus, network malfunctions are detected and prompt reaction is enabled [26].

Dependability is a complex physical property, therefore there is no single generalized criterion and indicator that would characterize dependability of technology in a sufficiently complete manner. Only a family of criteria allows evaluating the dependability of a complex technical system. The choice of criteria depends on the type of the technical item, its function and required completeness of dependability estimation [27].

One of the criteria of dependability of an overlay network is the latencies. It is assumed that an overlay network is to ensure reliable message delivery in cases of temporary unavailability of communication between adjacent nodes, including due to intentional or unintentional defects. Additionally, the specificity of application of the proposed network with autonomous robotics systems must be taken into consideration. In this context, priority is given to immediate message delivery, and a brief fault of delivery is preferable to a long delay (500 ms or more for some tasks). Another characteristic feature is the mutual independence of messages. In the proposed network the order of delivery is not important, which allows us optimizing the delivery algorithms and protocol subject to this criterion.

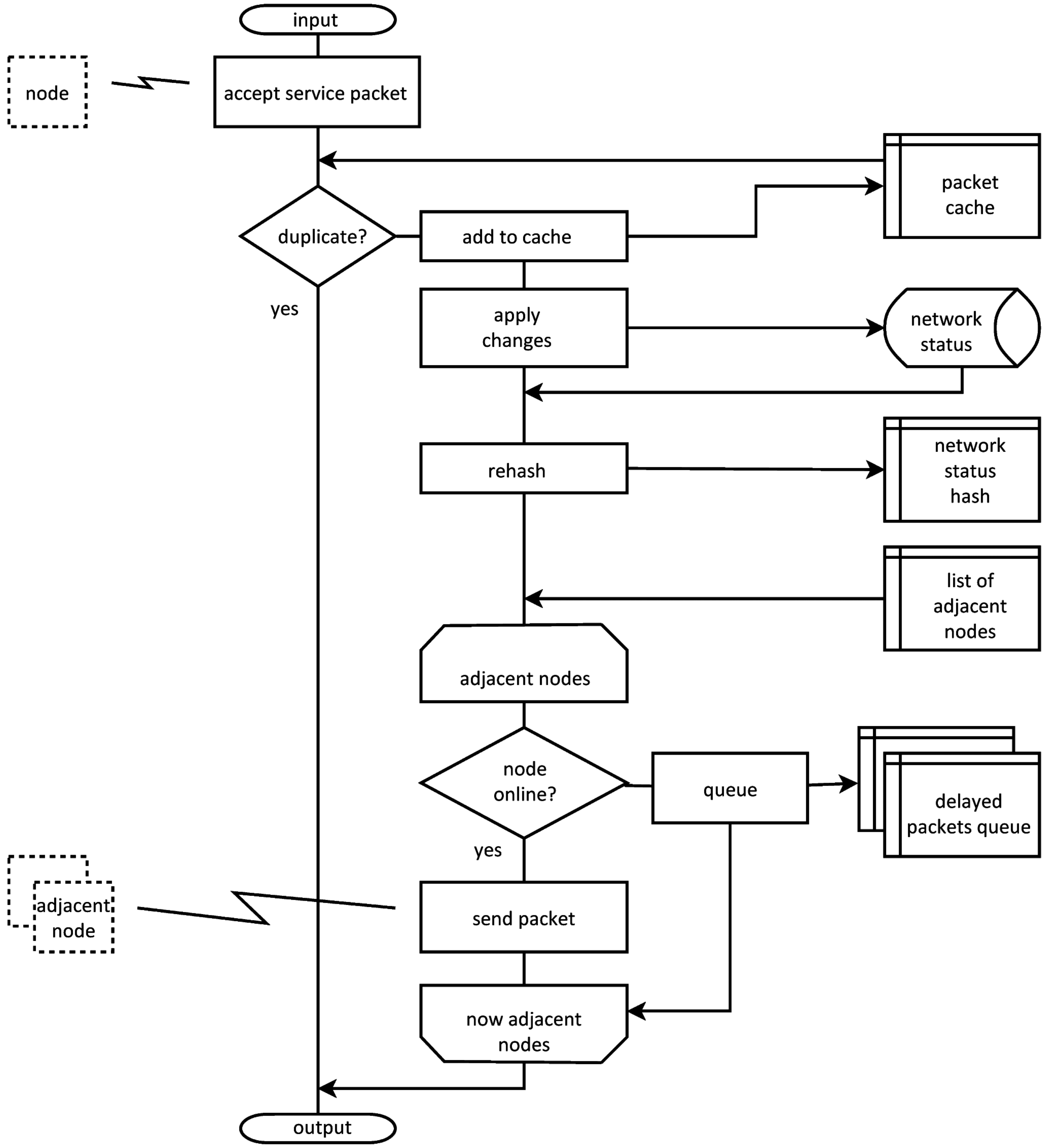

Fig. 3. System operation diagram for the flooding routing algorithm

Experimental testing of the developed data exchange algorithms

For the purpose of the experiment, a test network was created that consisted of a Cisco Catalyst 2960 router and six computers running under Ubuntu 18.04. In order to emulate several networks, five VLAN were configured on the PCs, with two computers in VLAN 0 and one in the others. The routing rules prohibited direct exchange of IP packets between all subnetworks except VLAN 0. As the result of the experiment network self-organization was confirmed; the operability of the developed algorithms was studied.

The existing TCP and UDP network protocols were experimentally tested using an active test network. For that purpose, data was sent between two routed nodes. Packet losses were emulated using the network interface of a node with an iptables rule and the statistic module that allows rule-based selection of a part of packets. For TCP, one connection was opened, within which overlay network cells were sent. UDP lacks a mechanism of delivery confirmation,

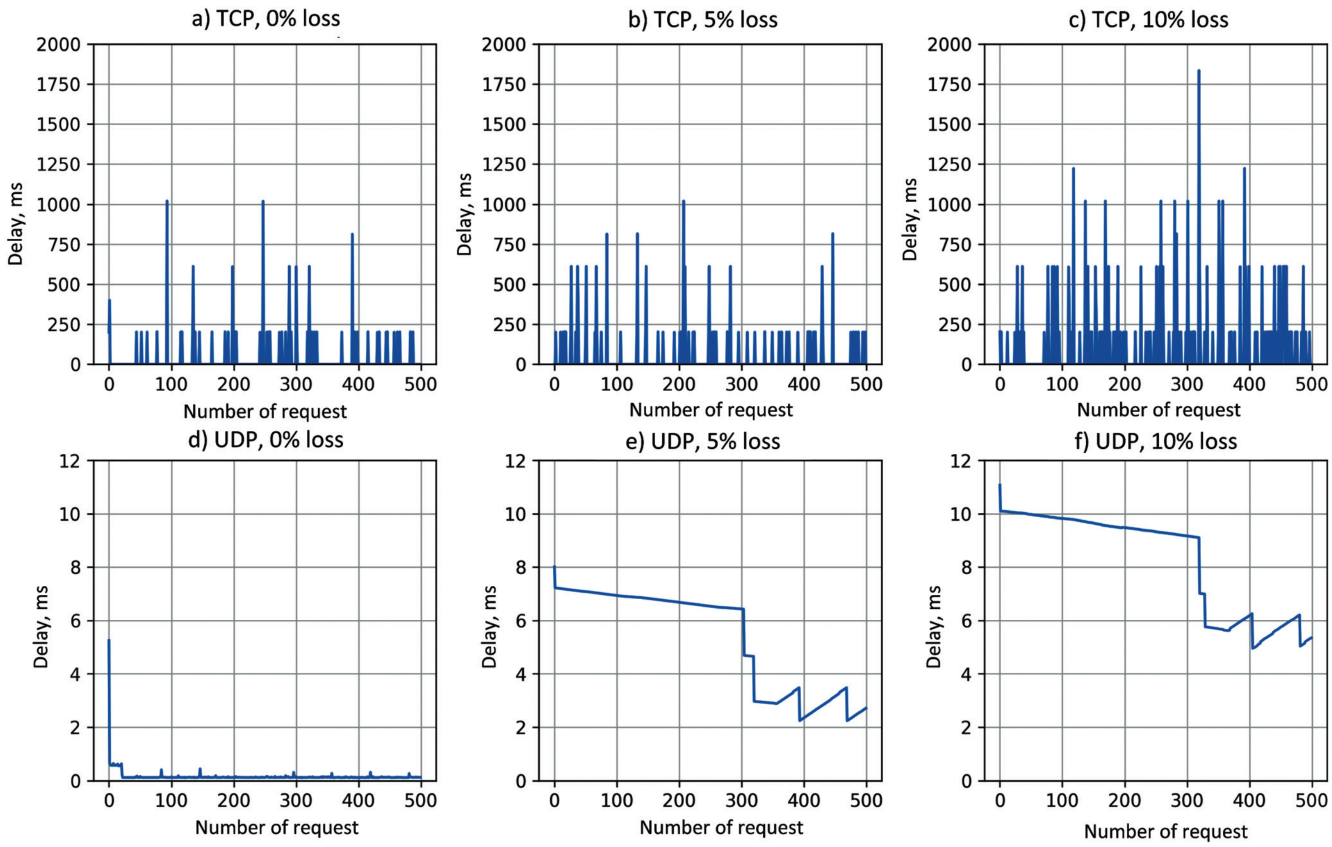

Fig. 4. Comparison of the delays of packet delivery by standard protocols subject to packet loss in the network: a) TCP, 0% loss; b) TCP, 5% loss; c) TCP, 10% loss; d) UDP, 0% loss; e) UDP, 5% loss; f) UDP, 10% loss

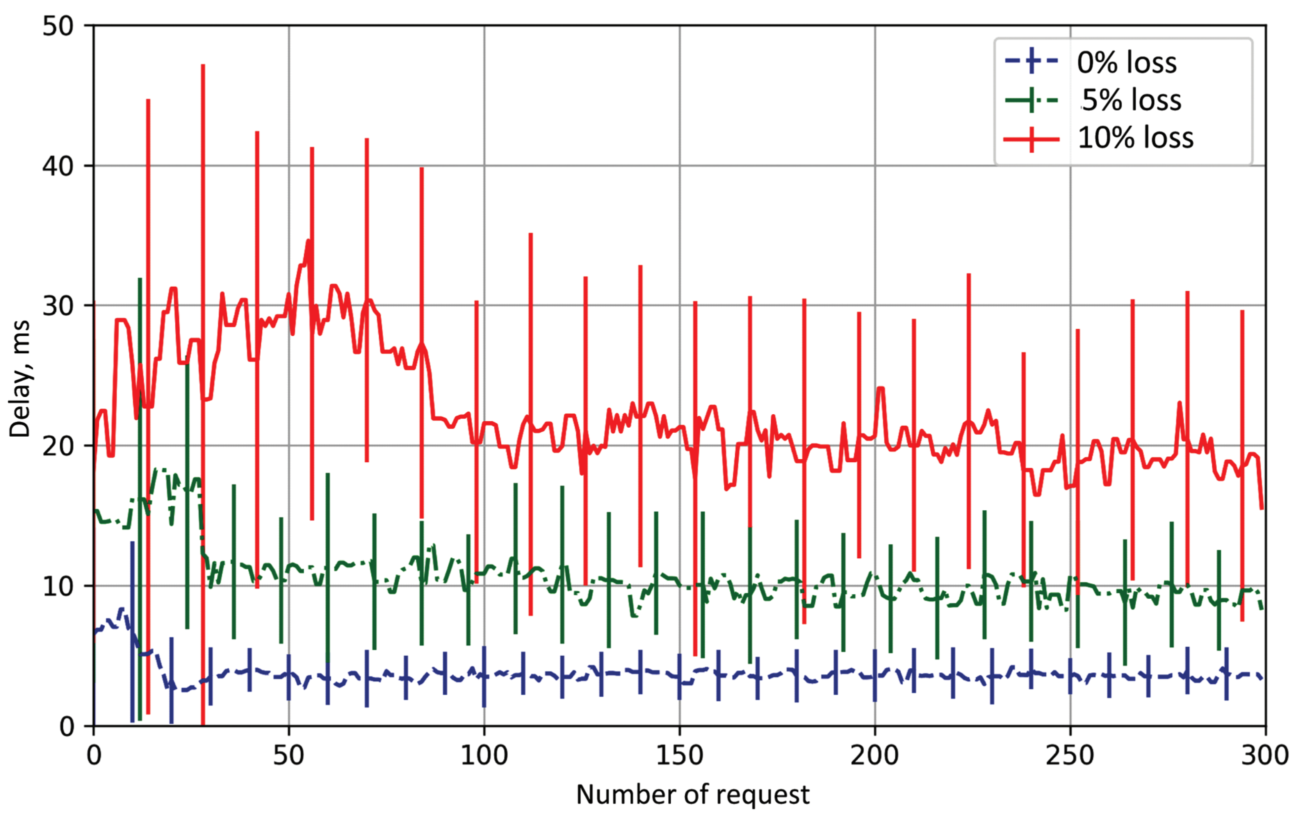

Fig. 5. Comparison of the delays of packet delivery within an overlay network subject to network defects

therefore the reception of each packet was confirmed by the receiving entity. If, upon time-out, no confirmation arrived, the packet was sent again.

Figure 4 shows the delays of delivery of each packet using standard TCP and UDP protocols under planned losses of 0%, 5% and 10% packets obtained during the experimental research.

Under no losses, UDP demonstrated minimal delays in data transfer, however, even under minimal losses the delay and amount of repeatedly sent data increase. Upon 300 to 400 sent packets, the delay settles (Figure 4, e and 4, f).

When TCP was used, establishing connection took long (up to a second in some cases) and reconnection was observed after disconnections. Such long single delays are unacceptable in networks used with autonomous robotics systems.

Knowing the results of research of delays associated with the use of existing data exchange protocols, we can estimate the dependability of the developed algorithms. Overlay networks were tested under the same conditions.

The proposed data exchange algorithm is characterized by shorter delays in normal operation and demonstrates higher dependability by enabling immediate delivery and minimization of failures that would occur because of untimely delivery of messages. The use of 0-RTT handshake (zero delay connection establishments) ensured the required performance of the overlay network.

The solutions' stability was verified over a month of operation with daily use of the network. No performance degradation or increasing delays were observed. The final results of the experiment are shown in Figure 5.

Conclusion

The authors developed operation algorithms of an overlay network subject to the particular conditions of its use by autonomous robots. The proposed approach will enable reliable data exchange within an autonomous system, thus ensuring the effect of collective mission performance with distribution of roles and subtasks, which would be impossible with no inter-agent communication and continuous data exchange.

Such algorithms are the foundation of a test software system intended for the research of the data exchange process within a team of autonomous robots.

References

1. Lavrov D.N. Principles of building a protocol for guaranteed message delivery. *Mathematical structures and modeling*. 2018;4(48):139-146. DOI: 10.25513/2222-8772.2018.4.139-146. (in Russ.)

2. Guss S.V., Lavrov D.N. Approaches to implementing a secure delivery network protocol for multipath data transfer. *Mathematical structures and modeling*. 2018;2(46):95-101. DOI: 10.25513/2222-8772.2018.2.95-101. (in Russ.)

3. Sorokin A.A., Dmitriev V.N. Description of communication systems with dynamic network topology by means of model "flickering" graph. *Vestnik of Astrakhan State Technical University. Series: management, computer science and informatics*. 2009;2:134-139. (in Russ.)

4. Parker L.E. Distributed Intelligence: Overview of the Field and its Application in Multi-Robot Systems. *AAAI Fall Symposium: Technical Report, FS-07-06*. 2008:5–14. DOI: 10.14198/JoPha.2008.2.1.02.

5. Ota J. Multi-agent robot systems as distributed autonomous systems. *Advanced engineering informatics*. 2006;20(1):59-70. DOI: 10.1016/j.aei.2005.06.002.

6. Arai T. et al. Advances in multi-robot systems. *IEEE Transactions on robotics and automation*. 2002;18(5):655–661.

7. Krieger M.J.B., Billeter J.B., Keller L. Ant-like task allocation and recruitment in cooperative robots. *Nature*. 2000;406(6799):992–995. DOI: 10.1038/35023164.

8. Winfield A.F.T., Nembrini J. Safety in numbers: Fault tolerance in robot swarms. *International Journal on Modelling Identification and Control*. 2006;1:30–37. DOI: 10.1504/IJMIC.2006.008645.

9. Bicket J. et al. Architecture and evaluation of an unplanned 802.11 b mesh network. Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM. ACM; 2005:31–42. DOI: 10.1145/1080829.1080833.

10. Srinivasan S. Design and use of managed overlay networks. Georgia Institute of Technology; 2007.

11. Clark D. et al. Overlay Networks and the Future of the Internet. *Communications and Strategies*. 2006;63:109.

12. Benson K.E. et al. Resilient overlays for IoT-based community infrastructure communications. 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI). 2016:152–163. DOI: 10.1109/IoTDI.2015.40.

13. Stoica I. et al. Internet indirection infrastructure. ACM SIGCOMM Computer Communication Review. ACM. 2002;3(4):73–86.

14. Ripeanu M. Peer-to-peer architecture case study: Gnutella network. Proceedings first international conference on peer-to-peer computing. IEEE. 2001:99–100. DOI: 10.1109/P2P.2001.990433.

15. Leibowitz N., Ripeanu M., Wierzbicki A. Deconstructing the kazaa network. Proceedings the Third IEEE Workshop on Internet Applications. WIAPP. 2003:112–120. DOI: 10.1109/WIAPP.2003.1210295.

16. Dingledine R., Mathewson N., Syverson P. Tor: The second-generation onion router. Naval Research Lab Washington DC; 2004.

17. Herrmann M., Grothoff C. Privacy-implications of performance-based peer selection by onion-routers: a real-world case study using I2P. International Symposium on Privacy Enhancing Technologies Symposium. Berlin, Heidelberg: Springer. 2011:155–174. DOI: 10.1007/978-3-642-22263-4_9.

18. Tandon N., Patel N. K. An Efficient Implementation of Multichannel Transceiver for Manet Multinet Environment. 10th International Conference on Computing, Communication and Networking Technolo-

gies (ICCCNT). IEEE. 2019:1–6. DOI: 10.1109/ICCCNT45670.2019.8944505.

19. Kudriashova E.E., Vovchenko A.V., Oleynikov R.O. [A study of the NETSUKUKU fractal set-based network]. *Vestnik Mezhdunarodnoy akademii sistemnykh issledovaniy. Informatika, ekologiya, ekonomika*. 2008. 11(1):55-57. (in Russ.)

20. Kumar A. et al. Ulysses: a robust, low-diameter, low-latency peer-to-peer network. *European transactions on telecommunications*. 2004. 15(6):571–587. DOI: 10.1002/ett.1013.

21. Rowstron A., Druschel P. Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems. IFIP/ACM International Conference on Distributed Systems Platforms and Open Distributed Processing. Berlin, Heidelberg: Springer; 2001.

22. Stoica I. et al. Chord: A scalable peer-to-peer lookup service for internet applications. *ACM SIGCOMM Computer Communication Review*. 2001. 31(4):149–160.

23. Feng J., Li J. Google protocol buffers research and application in online game. IEEE conference anthology. 2013:1–4. DOI: 10.1109/ANTHOLOGY.2013.6784954.

24. Ermakova A.V., Suchkova L.I. [Implementation of the data communication protocol between smart autonomous robots]. Certificate of official registration of computer software no. 2019666759 of December 13, 2019.

25. Ermakov A.V., Suchkova L.I. Designing a network communication environment for the implementation of the management system in the autonomous robots team. *South-Siberian Scientific Bulletin*. 2019;2(4):28–31. DOI: 10.25699/SSSB.2019.28.48969.

26. Ermakov A., Suchkova L. Development of Data Exchange Technology for Autonomous Robots Using a Self-Organizing Overlay Network. 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). IEEE. 2019:1–5. DOI: 10.1109/FarEastCon.2019.8934727.

27. Polovko A.M., Gurov S.V. [Introduction into the dependability theory: study guide: second edition, updated and revised]. Saint Petersburg: BHV-Peterburg; 2006. ISBN 5-94157-541-6. (in Russ.)

About the authors

Alexander V. Ermakov, post-graduate student, IT and Information Security Department, Altai State Technical University, 656038, Altai Krai, Barnaul, 46 Lenina Ave., Administration of Information and Telecommunication Support, Information Systems Development Unit, k.a. of Ermakov A.V., e-mail: tour0@ya.ru.

Larisa I. Suchkova, Doctor of Engineering, Prorector for Learning and Teaching, Altai State Technical University, 656038, Altai Krai, Barnaul, 46 Lenina Ave., k.a. of Suchkova L.I., Prorector for Learning and Teaching, e-mail: li.suchkova@yandex.ru

Authors' contribution

Ermakov A.V., overview of literature, development of algorithms.

Suchkova L.I., formalization of requirements and problem definition.