## **INTRODUCTION**

Today the number of researchers takes attention to the collective management of unmanned machines based on radio remote control. It is the task of executing the works with the risk to human life, the need to fulfill the tasks in constraints of time, a long period carries out routine work. Application tasks of collective control include search and monitoring operations, extinguishing fires in large areas of the earth's surface and other (Dang & Horn, 2015 & Nathan et al, 2005), combat and antiterrorist operations (Karpenko, 2010). More recently, theoretical studies other problems of application, challenges, and research problems related to the network use of UAV appeared in (Mozaffari et al, 2018). Despite the real advantages of temporary and quantitative solution of specific problems based on the network use of unmanned aerial vehicles (UAVs), there are a number of technical challenges associated with this application.

Considering the UAV group for information transfer, it is necessary to take into account the need to allocate an additional communication channel for controlling real-time actions and avoiding collision. Another problem of a network from a UAV is the mobility of flying machines that do not have centralized control, there is also the need to protect them from mutual and crosstalk, which is more difficult than for stationary or terrestrial execution. This leads to constraints of budget and the bandwidth of the communication channel, as well as the need to create and development of mechanisms for managing the reception and transmission of data (Zeng et al, 2016).

When managing the behavior of the group UAVs, it needs to transfer large amounts of information to the ground control station. To simplify the processing of information, the information is transmitted in small packets. The movement of aircraft, equipment failures, jamming of the radio signals, some data packets may be lost or, for example, there may be no confirmation of its receipt.

Some authors offer methods of the networks actions planning of UAVs, which based on discipline schedule, i.e. the order of processing of the transmitted packages (Kaur, 2011 & Niyato, 2005; Issariyakul, 2006; Bezruk et al, 2011; Gong et al, 2018). Nevertheless, an important task becomes developing algorithms compensate for lost packets or overloading. A natural approach to solving this problem is to resend lost packets to the point of reception and processing this information or overcoming this overloading. Then we have a network, and UAVs are the nodes of this network.

Network overload is one of the main problems that users of computer networks occasionally encounter. This problem causes a decrease in the bandwidth of the network, an increase in the passage time or loss of packets. It is this phenomenon that results in the termination of some network services, such as VoIP, interactive applications, chat, access to remote resources, and others. Lately, when there is an exponential growth of networks, this problem during their operation becomes the acuter.

One of the overload factors is excess buffering of the transmission channel (Gettys, 2011; Arefin & Amin, 2010). A buffer is required for data transmission over a communication line if the sender and the recipient have different processing pace. In this case, the buffer delays the transmission of packets at the time of acceptance and initial processing by the recipient. Filling the buffer leads to loss of packets transmitted. This phenomenon can be observed in routers, wireless access points, bridges, gateways, satellite devices.

Exclusion of overload is solved in several ways. You can achieve buffer overload by controlling queues and methods of prediction. Overload control methods control overload after it occurs, while prediction methods eliminate overload by controlling the transmission rate of the network on the network, enabling overloading and preventing it in typical "bottlenecks" of the network. The main tool of network operating systems for preventing overloads in Cisco is the use of algorithms of Weighted Random Early Detection (WRED) (Cisco, 2004).

In the duplex mode of switching ports control it is possible to implement a feedback mechanism that is introduced for Ethernet networks with IEEE 802.3x specification. The mechanism is implemented by introducing a sub-level of MAC level control, which introduces a time-stamping parameter for other nodes. The time is measured at 512-bit intervals of a specific Ethernet implementation, the range of possible stopping options is in the range 0 − 65535. After the stop time is completed, the transmission is restored.

Overloading can be eliminated if bandwidth reservation is introduced based on binary methods. In this case, the user Quality of Service (QoS) applications provided a portion of the throughput of the channel, the other part is reserved for other users, which is carried out through the use of the logical connection. But this happens at the hardware level, which introduces priorities to specific user applications, such as video conferencing. Therefore, the entire network of equipment in the transmission channel must support this technology, but this is not always the case.

In mobile networks, a typical solution to overload is the network reconfiguration. The paper analyzes the possibility of recovering throughput of a computer network, generating traffic in different conditions of network connections, determining the configuration with less load, establishing the relationship between the fall of traffic and its restoration due to the reservation.

The structure of chapter as follows: the next section contains some relative research in this problem and problem statement, Section 3 − 6 presented some results respect to lost packages in different schemes of transmission and their simulation, Section 7 – 9 present reconfigurations of a system based on graph approach if it is in overloading condition, main results of chapter present Section 10.

## **BACKGROUND AND PROBLEM STATEMENT**

The computer network usually operates with different data rates. In this case, we can meet the overloading problem. The problem of overloading takes place not only in Ethernet networks but also in mobile networks. The presence of many agents of the mobile network results in its overload, which to a large extent is solved by routing task under the condition of changing the topology of the network. Since there is no single effective routing algorithm for computer networks, therefore, dynamic traffic distribution is proposed to solve based on routing problems in the existing agent system to determining related agents (Kucherov, 2016).

Using UAV equipped with the appropriate kit is one of the solutions of the problem of mobile networks congestion (Rohde & Wietfeld, 2012). The question of overloading a mobile network in conditions of interference of intentional and unintentional origin is solved by the authors of work (Kucherov & Kozub, 2015). An efficient mobile communication network is created by reconfiguring the directional diagrams of the base station antennas. The requirements for a topology with the best noise immunity of cellular communication are put forward.

One of the recent works in this direction (Lastovchenko et al, 2009) proposes a method for constructing optimization models of a computer network, which are designed to perform tasks by placing nodes of the network structure using the spreadsheet environment. The nodes of the network are divided into servers and clients linked to them. The configuration of the graph of such a network is created by solving the maximizing problem based on nonlinear optimization.

For optimizing the data flow when tracking multiple objects requires an iterative approach and therefore time costs (Zhang et al, 2008). A method of tracking the window in controlling the flow of data in the local network formed by mobile agents is proposed by the authors (Issariyakul, 2006). An analysis of the above approach shows the effectiveness of using an adaptive observation window based on a flow control mechanism known as Automatic Repetition Query (ARQ). The established properties of the control mechanism allow determining the optimal size of the window of observation and packets for data transmission over the network.

A comparative analysis of the wireless network topologies for the UAV group showed the existence of a number of problems that must be solved for stable and reliable network operation (Gupta, 2015). The method of coordination in case of loss of communication for the reconfiguration of the network topology can be used in the management of autonomous UAVs (Grancharova, 2013). The methodology for evaluating the quality of the reconfigurable topology of Wi-Fi Asynchronous Transfer Mode (WATM) networks based on the reliability of their functioning is given in (Lastovchenko et al 2009). An approach developed by the author of the paper (Gorbunov, 2006) is based on step-by-step monitoring of the thresholds of non-repudiation and restoration of the computer network. The next step is determined by the ratio of the growth rate of readiness to increase the cost of its support. In (Fortz & Throup, 2002) the bandwidth of the multisensory system, which is based on the network principle of action, is considered.

The adequacy of network reconfiguration in the conditions of natural and artificial obstacles is analyzed according to the scheme "destruction-reproduction" in (Ventcel, 1988). It should be noted that in most studies, for example (Frenkel et al, 2013), network elements are assumed to be non-recoverable, which, of course, simplifies the task, but does not always correspond to practice.

The purpose of the paper is to evaluate the reliability of traffic of a computer network, which operates in conditions of overload due to artificial and natural constraints, which leads to a change in the configuration of the system.

We will consider a computer network, the nodes of which are able to process information and exchange data, and in addition to changing the configuration of the system. The network management method corresponds to the «client-server» architecture.

The network has a definite topology, which is described by a weighted graph *G* = (*V*, *E*), in which *V* is a set of the nodes, the number of nodes *V* (*G*) = *N*, and *E* are weighted edges, the number of edges *G* (*E*) = *M*. Each edge (*i*, *j*) corresponds to the number *wij*>0, which is called the weight of the edge (*i*, *j*), *i* = 1..*N*, *j* = 1..*M*. In the case when (*i*, *j*) ∉ *G*, *wij* = ∞.

The network has two specific vertices designated *S* (source) and *T* (terminal). It is assumed that for any vertex *V* ≠ *S* there exists a path leading from *S* to *T* and passing through *V*. Vertexes are considered to be absolutely trustworthy and cannot be denied, but edges can refuse. The weight of the edge *wij* characterizes the performance of the channel. If it fails, the performance drops and the weight *wij* decreases. Restoration begins at the time of edge failure. The functions of fail-free operation *FE*(*t*) and restoration *WE*(*t*) (distribution functions) of the edge *Eij* are given. The functions *FE*(*t*) are assumed to be absolutely continuous, i.e. there are density *fE*(*t*).

If a simultaneous failure of the edges *E*1, ..., *EM* entails a complete network failure (the path from *S* to *T* is violated), this set is called a cut. A cut is called minimal if no edge can be removed from it so that the network goes into a failure state. The network can be considered as a series-parallel connection of arcs. In parallel connection of arcs, they belong to one cut.

If *S*1, ..., *ST* is a cut set, then the network productivity at the moment *t* is determined by

$P\left(V'(t)\right)=\min\_{1\leq j\leq T}\sum\_{E\in S\_{j}}^{}c\_{j}\left[1-V\_{E}(t)\right],$ (1)

where $V^{'}\left(t\right)=(V\_{E}\left(t\right),E\in G)$, *VE*(*t*)=0, if the edge *E* is in working order at the moment *t*, and *VE*(*t*), if the edge is on recovery. In accordance with formula (1), the performance is determined by the minimum amount throughput of vertices in working state across all cuts. At each point in time, the system requires a certain level of performance. If at some point the performance becomes less than the availability of level, then a functional failure occurs.

We introduce a Markovian process ξ having a finite set of states *I* = {1, …, *n*} and given by the probabilities *Pij* of the transition of the embedded Markovian chain and the conditional functions *Bij*(*t*) of the time distribution between the transitions.

The function *Bij*(*t*) is assumed to be absolutely continuous; there are densities *bij*(*t*). It is also assumed that all states form one class of essential states, and ξ(0) = 1 with probability 1. If ξ(*t*) = *j*, then the level of required capacity is equal ς(*j*), i.e. a random process ς(ξ(*t*)) specifies the performance required from the system at the time *t*. It is assumed that ς(*j*) is a monotonically increasing function, ς(*j*)>0. The system operates in normal mode, if *P*(*V*′(*t*)) > ς(ξ(*t*)). The moment *t* of its refusal is defined as *tr* = inf {*t*: *P*(*V*′(*t*)) > ς(ξ(*t*))}.

Our aim of the study is to estimate the probability *Q*(*t*) of a functional failure from a degree of network congestion on a long interval, i.e. *t*→∞.

## **PACKETS TRANSMISSION**

Let have a group from *n* UAVs, which gives information to the operator's remote control by radio link. Figure 1 shows the typical use of UAVs in the monitoring task. Because of the obstacles on the ground, the presence of monitoring noise the transferring information to control point may come by the chain, in which the intermediate UAVs are repeaters.



*Figure 1. A typical application of the group of UAVs.*

Operator and UAV exchange this information as usually by packages. The package is some amount of binary information, organized in a certain way that named protocol.

All UAVs transmit information to the ground control station in asynchronous mode; therefore, the input stream in the processing system has the form

, (2)

where  is the data flow from *i* of the source and . Here the problems of auto identification, authentication don’t solve. The packages from all UAVs are considered as whole one stream.

The main problem in this transferring data is motion UAVs, mismatch processing speeds in reception and transmission points, buffer overload is due to data retrieval on a low speed, re-transmission data to another address, and errors during transmission data. Consequently, it becomes necessary to control the flow of data.

There are some methods to control the flow of data. Among them stop and wait, return to the *M* steps, selective rejection. The last two approaches are known as a mechanism automatic repetition query (ARQ) [8]. The first scheme works as follows: if the sender sent the package, the receiver sends the confirmation it readies to get the next package. In this case, we have errors of two types. One type of error can turn out because of transmission package and another − in time receiving confirmation. In accordance to the second scheme is entering a “sliding window” for transmission *M* packages. Error in package leads to the need to repeat their and all the subsequent packets transmitted in this window. In the case, selective rejection is repeated only the packages that have been damaged and the packages which have the waiting time are expired.

Assume that the system consists of a source, which transmits packages of fixed length *Tpac*, and the receiver, which confirm its decision sent to the request. Time data transmission in one direction is *Tdir*. Considered that the time duration of packages processing and transmission confirmation is very small, so they can be neglected, and then the time required transferring one packet

. (3)

If necessary, *N*-time to repeat transmission one package until successful reception that this time increases to a value

. (4)

Also is given the probability of damage to the package *p*. Let consider different schemes of the packets’ transmission.

## **The Scheme of Stop and Wait**

As known, throughput is a metric characteristic that showing the relation limiting the number of passing units (information items, the volume) per unit of time through a channel. In our case throughput is value *C*, which calculated such as

. (5)

If we set  that (5) we can write in the form

. (6)

The throughput *C* in (6) is normalized and takes values in the interval [0; 1]. If  then *C*→1, that corresponds to a high productivity channel, and if  then *C*→0, that corresponds to low productivity channel.

If a transmission error occurs and the information is the necessary repetition of data being sent, the throughput channel deteriorates in *N*-time

. (7)

In the general case *N* in (7) is a random value, which for a long transmission interval determined by the probability

, (8)

where *k* – the number of repetitions transmission and *p*<1. In accordance with [17, formula (21.2-39)] record (8) transformed to

, (9)

then (7) write in the form

. (10)

Formula (10) is setting loading ability radio channel in the scheme with stop and wait.

## **ARQ Scheme**

Let’s begin to consider its effect when errors transmission is absent. For the *M*-packages defining the size of the sliding window, there are two variants for transferring information.

*Case* 1. The size sliding window *M* more than the time allowed for transmission of information, i.e. *M* ≥ 1 + 2. In this case, the channel is not overloaded and has the best performance. This statement allows to set the numerator (6) limit the transmission time value, then the throughput is equal to *C* = 1.

*Case* 2. The transmission tme of the channel is limited to the size of the window, i.e. *M* < 1 + 2. Here the numeratorequals *M* and (6) can be written as

. (11)

Transmission errors are deteriorated throughput that in the case with selective rejection when returning on *N* steps for single package occurs in virtue of (9), (10), takes the form

. (12)

In the scheme of return on *N* steps retransmit *L* packages. Here, the number of return *N* steps is a function of the number of transmitted packages

. (13)

In (13) *f* (*k*) is the total number of retransmitted packages and a lost packet transmitted *k* times. *f* (*k*) can be represented as (Stallings, 2002)

. (14)

After the substitution of (14) to (8) is obtained by the number of the repeated packages

. (15)

For the derivation of (15) essentially used the results of (21.2-38) and (21.2-39) in (Korn and Korn, 1968).

Substituting (15) into (7) and considering the cases 1 and 2 relatives to the size *M = L* of the sliding window, we obtained throughput for ARQ-mechanism that based of return on *N* steps

 (16)

Expressions (12) and (16) correspond to throughput data flow control mechanism with ARQ. It is noteworthy that for *M* = 1, both expressions degenerates to scheme stop and wait (9).

Expression (6), (11), (12), (16) prove the following

THEOREM. If the size *M* of the window satisfies the condition , then the channel is effectively used and .

Corollary. The number of bits *l* of the sliding window is determined by the expression

. (17)

Formula (17) follows from the theorem and the value  and

. (18)

## **Simulation Packet Transmission**

We validate the analytical results obtained and analyze them. In all study estimates throughput, we assume that the probability of errors in the transmission of the data packages is *p* = 10-3.

The value *M* is selected from the condition (18), where *l* is the number of bits of the transmitted package. Selected the numbers of 1, 7, 127, wherein the number M1 = 1 corresponds to a scheme stop and wait, M2 = 7 applies to packets of small size (3 bits) and M3 = 127 (7 bits) is typically used in high-speed wide-area networks.

The value of the number *a*= is determined by the time of the transmission and time spread packages to the point of control. Considering different data rates and different transfer size package the values  are in interval 0 to 1000.

In Figure 2-6 shows the results of numerical modeling throughput for these initial data. Thus, in Figure 2, 3 is shown throughput selective rejection scheme and based on return on window sizes M1, M2, M3. Figure 4 and 5 are graphs of the bandwidth for different schemes of the window size M2 in comparison with the scheme stop and wait. So, Figure 4 correspondence for window size M2, and Figure 5 windows for size M3. Summarizes the results is shown in Figure 6 that allows us to understand the correspondence between the various schemes of flow control schemes that are considered.



*Figure 2. Function C (a) for stop and wait and selective rejection with sizes M1, M2, M3 sliding window.*



*Figure 3. Function C (a) for stop and wait and scheme ARQ based on return on M1, M2, M3 steps.*



*Figure 4. Function C (a) for stop and wait and scheme ARQ based on return on M2 steps.*



*Figure 5. Function C (a) for stop and wait and scheme ARQ based on return on M3 steps.*



*Figure 6. Function C (a) for stop and wait and schemes ARQ based on return and selective rejection of M1, M2, M3 steps*.

These figures show that if the effective load channel for scheme stop and wait for correspondence level is *a* = 1, then return and selective rejection schemes this is approximately equal to the number of *M*.

This analysis leads to the conclusion that the greatest throughput schemes are based on the approach of creating a sliding window. There is a direct relationship between the window size and bandwidth. The larger the window size, the higher the throughput is. By comparison two schemes creating a "sliding window" the best characteristics has the selective rejection scheme.

## **THE SYSTEM GRAPH APPROACH**

Data transmission on the network takes place according to the rules that are governed by the applicable protocols, according to which the address, size, and structure of the packet being transmitted are determined by the speed of data transmission.

The address can be individualized when the message is sent to only one agent, group when the message is sent to each agent in the group, or to a certain subgroup of agents. This method of addressing is basic to addressing in computer networks. The data transmission takes place from the source address to the receiver's address.

If the number of nodes is significant, then there is a need to pass information through transit nodes. However, it becomes necessary to lay a route to ensure a minimum of time for the delivery of information achieved by a minimum of transit nodes or the presence of channels with high bandwidth and reliability of communication lines. It goes without saying that a small increase in the number of transit nodes with high bandwidth is overwhelming over the minimum number of nodes with low bandwidth in terms of the time of transmission. Reliable communication channels are characterized by minimal loss of transmitted information.

Several sub-streams can pass through a node; they are distinguished by the address of the destination. It is clear that in order to determine the route that would provide equal time flows of different volumes of data, it is necessary to take into account the transmission speed of the individual lines and to enable the distributed of sub-streams and their assembly. The switching of nodes for the transmission of sub-streams is carried out by multiplexing of free channels. This task consists in determining the route of information passing to the endpoint. Distinguish between static and dynamic routes. A static route is given once or at a certain schedule and does not change within a certain time. Dynamic routes are calculated by appropriate algorithms depending on the topology and status of the information network. These include algorithms for finding the shortest distance in width, Dijkstra, Bellman-Ford (Stallings, 2002).

## **THE Dijkstra’s Algorithm**

The most common algorithm is the Dijkstra’s algorithm; it is considered to be the procedure for finding the shortest path on a weighted oriented graph. The algorithm is used by OSPF and IS-IS routing protocols in IP networks (Fortz and Throup, 2002). The edges of the graph have a weight *wij* such that

 (19)

The path length at each step *k* from the vertex s is determined by the rule

, (20)

where *L*(*k*) is path length after *k* step. Rule (20) does not allow passage along the arcs of graph *G* with a high weight. Thus, the set of vertices in the graph *G* is an ordered sequence of connected nodes that contains the shortest path from the vertex *s* to *k*. This path is shown in Figure 7 by the arrows



*Figure 7. The structure of the weighted graph.*

At each scheduled time point *i* on the router comes the total flow of information intended to be transmitted to each router *j*. This general stream defines a routing table that can be calculated by the matrix *P* (*t*) of the dimension *N*×*M* with the zero main diagonal

. (21)

In formula (21) the information streams associated with the corresponding IP addresses in the routing table, and *cij* is bandwidth. Cisco routers define weights according to the formula [20]

 (22)

Since the algorithm (20) is iterative, the number of iterations is determined by the number of vertices of the graph, so the time complexity of the algorithm *O*(*N*). Within each iteration, a new passage takes place taking into account the new (*j* + 1) vertex. In this case, the peaks with the greatest weight are released, and the length of the path with new vertices is renewed, the best result is remembered. This is the same as the number of vertices. The overall performance of the algorithm is estimated to be *O* (*N*2). Thus, the Dijkstra’s algorithm is resource-intensive, but due to the knowledge of the network topology and the path to the desired node, the router always finds an alternative path to the desired network node in the event of problems in any node of the specified path.

Resetting capacity should take into account the network load. To control the router is supplemented by means of load measurement, which will create a similar (2) matrix of loads *С* = | *сij* |. Then the backup reservation algorithm can be written as

 (23)

where Δ is the fraction that compensates for the overload.

## **Estimated System Reconfiguration**

By reconfiguration of the information system, we will understand the change in the structure of the system, which refers to the size or its topology. The feature of reconfiguration is the restructuring of the structure and topology of the system to eliminate overloads and failures in the system. It is believed that the network carries out its functions, while exchanges between nodes are carried out. The examples of a reconfigurable system are shown in Figure 8, 9.



*Figure 8. The structure of the information system in graph form.*



*Figure 9. Changing the structure of the information system as a result of a loss of communication.*

Thus, due to overloads or crashes, the topology of a local full network is changed to the "bus".

In accordance with the general idea of a computer network (1), it is a system with a limited number of possible states. Therefore, its behavior can be modeled using a mathematical apparatus for analyzing Markov chains.

We will assume that in the process of operation, a computer network consisting of a finite set of elements *N*, exchanges information between all the elements in the OSPF or RIP protocols, which corresponds to the conditions for the normal functioning of the system. The initial state of the network is denoted by *S*1. If for some accidental reason the elements of the network are starting to fail, or information exchange may be lost, the system is moving to another state. We will assume that the elements of the system are not overloaded simultaneously, but one by one, therefore successive transitions from state *S*1 to states *S*2, *S*3, ..., *Si* are performed at certain intervals of time Δ*t*, *i* stands for state number. A sequential set of states of the computer network and transitions between them forms the Markov chain. Since the chain is consistent, the operation of the system can be filed in the form of a scheme "death-propagation" (Ventcel, 1988).

Let the computer network consist of *n* nodes, therefore, according to the approach to the "death-multiplication" scheme, we introduce the states *Si*, *i* = 1..(*n* + 1), where *S*1 is the state of the network, which corresponds to the functioning of all nodes without overload. Under the influence of external and internal factors, the throughput of channels in the network with fixed intensity deteriorates λ, which is associated with weighting factors *wij* in (6). In this case, the transition to the state occurs, when the nodes gradually lose the packets, successively one after the other. Thus, the transition to the state *S*2 occurs when no works the node number 1, and so on, and therefore *Sn + q* − the computer network has ceased to perform tasks in connection with the failure (*n* − *q*) nodes. The system can also take measures to increase the throughput, which occurs with the intensity of μ> λ. At the same time, the successive transitions from the states of *Si* to the *Si*-1 state occur with intensity μ. We find the probabilities *qi* of finding a computer network in each of the finite states *Si* and analyze them. The probabilities of finding a system in the final states are based on the formulas [20]

 (24)

Example. Let us consider this problem for the case network as in Figure 8 where *n* = 5, λ = 0.5, and μ1 = 0.8, μ2 = 1.6, μ3 = 2.4. The results of the calculation by the formulas (7) are shown in Figure 10. The analysis of the figure shows that the less the μ, the better the system is handling the packets, the more likely it is to be in a state with minimal delay and less probability of being in the state with the greatest delays.

**

*Figure 10. Degradation of the computer network in conditions of intense loads.*

As can be seen from the figure, if μ> (2..5) λ, the system becomes more sensitive to loads of different types. The failure of two or more nodes becomes critical for a network of this type.

## **CONCLUSIONS**

Exchange information with the group UAV is done by radio channel "UAV- point control". The movement of UAV and equipment imperfections causes errors in reception information or overloading. Troubleshooting the received information is achieved by repetition of data packages or reconfiguration network is called flow control.

In this chapter analyzes the known methods of flow control that are focused on re-processing of the lost information. These are methods to stop and wait, to repeat the last *N* packages and selective rejection. The absence of errors in the received information is estimated by ARQ based on a sliding window. In the investigation, the indicator of bandwidth is essentially used.

Also, based on the analysis of protocols and routing algorithms, it has been established that the efficiency of a computer network is determined by the possibility of its operation in conditions of overloads and failures, which is the result of excessive buffering of the system. One of the effective ways to reduce the impact of overloads on the network is to reserve the bandwidth of the channels and to compensate for its share in the channels that are most exposed. According to the analysis of the network under the scheme of "death-propagation", it is established that the action of the system functions if the ratio of the intensity of overload to the intensity of the increase in throughput does not exceed the value of 0,2 ... 0,5.

## Further research on the functioning of the computer network is planned to focus on analyzing its dynamic properties.

## **REFERENCES**

Dang A. D., and Horn J., (2015). Formation Control of Leader-Following UAVs to Track a Moving Target in a Dynamic Environment, *Journal of Automation and Control Engineering*, 1, 1−8.

Nathan S., Janusz M., Milind T., Paul S., Lewis J.P., and Kasinadhuni N., (2005). The Future of Disaster Response: Humans Working with Multiagent Teams Using DEFACTO. Published Articles & Papers. Paper 41. <http://research.create.usc.edu/published_papers/41>.

Karpenko A.V., (2010). Complex «LEER» with Unmanned Aerial Vehicle «ORLAN-10»,  http://bastion-opk.ru/orlan-10/ .

Mozaffari M., Saad W., Bennis M., Nam Y.-H., and Debbah M., (2018). A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems, https://arxiv.org/abs/1803.00680.

Zeng Y., Zhang R., Lim T.J., (2016). Wireless communications with unmanned aerial vehicles: opportunities and challenges. *IEEE Communications Magazine*, 54 (5), 38-42.

Kaur P., Singh D., Singh G., and Singh N., (2011). Analysis, comparison and performance evaluation of BNP scheduling algorithms in parallel processing, *International Journal of Information Technology and Knowledge Management*, 1 (4), 279−284.

Niyato D., (2005). Analysis of fair scheduling and connection admission control in differentiated services wireless networks, *Proceedings of the IEEE International Conference on Communications* (ICC’05), Seoul, Korea, 16–20 May 2005, Seoul, 3137–3141.

Zhang L., Li Y. and Nevatia R., (2008). Global Data Association for Multi-Object Tracking Using Network Flows. *Proceedings IEEE Conference on Computer Vision and Pattern Recognition,* 23-28 June 2008,Anchorage, AK, USA, 1 – 8.

Issariyakul T., (2006). Channel-quality-based opportunistic scheduling with ARQ in multi-rate wireless networks: modeling and analysis, *IEEE Transactions on Wireless Communications*, 4 (5), 796–806.

Bezruk V., Chebotareva D., and Ivanenko M., Jo S., (2014). Multicriteria Optimization in Planning of Mobile Communication Networks, *Proceeding of the 20th International Conference on Microwaves, Radar and Wireless Communications*. MIKON 2014, 16-18 June, Gdansk, Poland, 2014, 633–639.

Rohde S. and Wietfeld C., (2012). Interference Aware Positioning of Aerial Relays for Cell Overload and Outage Compensation, *Proceedings IEEE Vehicular Technology Conference (VTC Fall)*, 3 – 6 September 2012, Quebec City, QC, Canada, 1 – 5.

Kucherov D.P., and Kozub A. N., (2015). Control System Objects with Multiple Stream of Information. *Proceedings IEEE 3rd International Conference “Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)”*, 13−15 October 2015, Kyiv, Ukraine, 290−293.

Gupta L., Jain R., and Vaszkun G., (2015). Survey of Important Issues in UAV Communication Networks, *IEEE Communications Surveys and Tutorials*, PP (99), 1 − 32.

Grancharova A., Grøtli E.I., and Johansen T.A., (2013). Rotary-Wing UAVs Trajectory Planning by Distributed Linear MPC with Reconfigurable Communication Network Topologies. *IFAC Proceedings Volumes*, 46 (27), 198 – 205.

Lastovchenko М.М., Zubareva E.E., and Sachenko V.O., (2009). Method for analyzing the efficiency of the reconfiguration of the topology of wireless multi-server networks with increased noise immunity. *USM*, 6, 79 – 86.

Kuzmichov A.I., and Dodonov E.О., (2017). Optimization models of network structure. *Registration, storage, and processing of data*, 2, 24 – 35.

Gorbunov I. E., (2006). Methodology of analysis and synthesis of reconfigurable topologies of mobile communication networks. *Mathematical Machines and Systems,* 2, 48 – 59.

Fortz B., and Throup M. (2002). Optimizing OSPF / IS-IS weights in a changing world. *IEEE Journal on selected areas in communications*, 6, 1 – 31

Kucherov D.P., (2016). Reconfiguration multisensory system in conditions of impact of destabilizing factors. *Sensor Electronics and Мicrosystem Technologies*, 2 (13), 101 – 112.

Frenkel I.B., Karagrigoriou A., Lisnianski A., and Kleyner A.V., (2013). *Applied reliability engineering and risk analysis: probabilistic models and statistical inference*. New York, Wiley, USA.

Arefin Md.T., and Amin Md. R. (2010). Congestion Control and Buffering Technique for Video Streaming over IP. *International Journal of Latest Trends in Computing*. 1 (2), 133 – 137.

Gettys J., (2011). Bufferbloat: Dark Buffers in the Internet. Internet Computing. *IEEE Computer Society*, 3 (15), 96 − 95.

Cisco (2004). *Internetworking technologies*. Handbook. 4th edn. Cisco Press, USA

Ventcel E.S., (1988). *Issledovanie operacii: zadachi, principi, metodologia*. Moscow, Nauka, USSR.

Stallings W., (2002). *High-Speed Networks and Internets. Performance and Quality of Service*. N.-J.: Prentice Hall PTR.

Korn G.A., and Korn T.M., (1968). *Mathematical handbook*. NY: McGraw-Hill Book Company.

**ADDITIONAL READING**

Cormen T.H., Leiserson C.E., Rivest R.L., and Stein C., (2002). *Introduction to Algorithms*. NY: McGraw-Hill Book Company.

Dijkstra E.W., (1959). A Note on Two Problems in Connexion with Graph. *Numerische Mathematik*, 1, 269 − 271.

Jensen P.A., and Barnes J.W., (1980). *Network Flow Programming*. NY, John Wiley & Sons.

Cooper R.B., (1981). *Introduction to Queueing Theory*. NY Elsevier North Holland.

Taha A.H., (2003). *Operations Research: An Introduction*. Pearson Education Inc.

**KEY TERMS AND DEFINITIONS**

**Packets Transmission:** A network packet that formatted unit of data carried by a packet-switched network. A packet consists of control information and user data, which is also known as the payload.

**ARQ:** Automatic repeat request, also known as automatic repeat query, is an error-control method for data transmission that uses acknowledgements (messages sent by the receiver indicating that it has correctly received a packet) and timeouts (specified periods of time allowed to elapse before an acknowledgment is to be received) to achieve reliable data transmission over an unreliable service.

**Stop and wait**: A scheme [telecommunications](https://en.wikipedia.org/wiki/Telecommunications) to send information between two connected devices. It ensures that information is not lost due to dropped packets and that packets are received in the correct order.

**Weighted Random Early Detection:** The active queue management algorithm for managing router overflows, with the ability to prevent overload

**MAC**: This is the abbreviation of Media Access Control, it is the open systems interconnection basic reference model layer.

**Wi-Fi Asynchronous Transfer Mode**: These are the standards for carriage of a complete range of user traffic, including voice, data, and video signals".

**OSPF**: This is the abbreviation of the open shortest path first, it is a routing protocol for Internet Protocol (IP) networks.

**IS-IS**: This is a routing protocol designed to move information efficiently within a computer network, a group of physically connected computers or similar devices.