Integrity of information data flow in meteor communication networks

N M Bozhuk¹, I L Skripnik², Yu G Ksenofontov³⁴, V P Malyshev³ and M O Avdeeva³

¹Admiral Makarov State University of Maritime and Inland Shipping, 5/7 Dvinskaya St., Saint-Petersburg, 198035, Russia
²Saint-Petersburg University of State Fire Service of EMERCOM of Russia, 149 Moskovskiy Ave., Saint-Petersburg, 196105, Russia
³Peter the Great St.Petersburg Polytechnic University (SPbPU), 29 Polytechnicheskaya St., St.Petersburg, 195251, Russia
⁴E-mail: ksenofontov.ura@mail.ru

Abstract. The paper considers the issues of ensuring the integrity of the flow of information messages between remote objects and identification of the data transmission channel, interrupted randomly by fragmentation-defragmentation processes of this flow as a result of the stochastic appearance and disappearance of traces from meteors burning in the ionosphere, which are used as passive repeaters of VHF radio signals that carry out energy contact between correspondents of a computer network. The problem is posed to implement an algorithm for discontinuous transmission of a continuous data stream over a meteor communication network without distortion and loss of transmitted messages without the inclusion of redundant signs, which contributes to a more rational use of the limited telecommunication resource of the meteor communication network. It is shown that to ensure a reliable exchange of information data between remote infrastructure facilities of the Northern Sea Route, a meteor trail can be used, which will provide a statistically stable connection with the fulfillment of the requirements for the probability of receiving false signals while maintaining the integrity of messages, provided that this type of communication between correspondents is discontinuous.

The meteoric communication network (MCN) is one of the elements of information telecommunications in the Arctic of Russia and is designed to automate the processes of transmitting messages over an intermittent channel [1-3]. As part of infotelecommunications, MCN plays the role of a statistically stable telecommunications exchange of information data between remote objects. It provides data transmission over intermittent stochastically appearing energy contacts on the VHF between the correspondents of the ship traffic management system (STMS) as a means of exchanging formalized information, when carrying out automated monitoring of the operability of STMS technical means (such as buoys, luminous signs, etc.), which can be located from the control centre at a distance of 1500-2000 km, in order to ensure the safety of the transport and technological process in the Arctic region, in particular, on the Northern Sea Route (figure 1). However, it is necessary to take into account the factor that when using this type of communication there is a high probability of false signal generation to identify a correspondent in the network, as well as violation of the integrity of the transmitted information data stream, which significantly reduces the quality of communication.
Figure 1. - A variant of the meteor communication network (MCN) topology of the Northern Sea Route: MSCC - Marine Rescue Coordination Centre (Dikson), MSPC - Marine Rescue Sub-Centre.

It is proposed to preserve the integrity of the transmitted information data stream due to the complex application of a composite complex signal of scanning the ionosphere for the simultaneous joint solution of three interrelated tasks, which are to ensure: clock synchronization of digital devices of correspondents; frame synchronization when exchanging digital passwords; correct identification of correspondents. In addition, the retransmission of the last two information characters of the previous fragment of the stream of transmitted messages occurs in the best communication conditions, which increases the level of protection against errors in the transmitted information data [5].

The essence of messaging in MCN is as follows. Unformalized information is entered by the operator of the automated control system (ACS) from a workstation connected to a computer. Formalized and non-formalized information for transmission via the data transmission channel to MCN is accumulated in the computer memory in the form of separate messages. This kind of information in a computer is accumulated and formed using the seven-element ASC II code (recommendation of the International Telecommunication Union). In this form, it is transmitted to the appropriate recipient via MCN. The intermittent channel of the radio meteoric link, as a rule, does not allow, during one energy contact (the existence of a meteor channel) between the correspondents, to transmit the entire message to the addressee in full [4,5]. Therefore, when the meteor channel disappears, the transmission of the message is suspended until a new meteor trail appears, which will provide the next energy contact between the correspondents, which is necessary to continue the data transmission. When it is restored, the data stream transfer resumes. As a result of the discontinuous transmission mode, the entire information data stream is divided into fragments, the length of which is determined by a random stream of meteors leaving trails necessary for relaying VHF radio signals. At the moments of breaks in the data transmission stream, distortion and loss of individual characters (seven-element code blocks) of information data are possible. To eliminate distortions and losses of individual characters in the transmitted data stream, the proposed algorithm contains a block for forming a stitching structure and a counter of transmitted characters in transmission, similar blocks are also used in reception.

The entire stream of information characters transmitted through the stitching device is numbered both in transmission and in reception from 1 to 127, and then the numbers of the transmitted characters are repeated again from 1 to 127. This numbering was introduced so that during communication interruptions during transmission it was possible. When recovering, transmit in one code block the number of the last transmitted character in the previous communication fragment. The maximum digit 127 is determined by the seven-element information code: 2^{7}-1 = 127. In this case, any number from 1 to 127 is transmitted in one code block. Reducing the number of service characters is necessary because they take away a significant part of the already low telecommunication resource of MCN [6-8]. To eliminate losses and unauthorized insertion of unnecessary information signs, the counters on transmission and reception must work synchronously (figure 2). Since they are triggered start-stop for
each transmitted character on transmission and reception, the number of the last transmitted character can be used to clarify the correctness of the numbers of the transmitted information code blocks.

![Start-stop-synchronous scheme of operation of counters of transmitted (SCH1) and received (SCH2) bytes (fragmentation-defragmentation procedure of the transmitted data stream).](image)

Figure 2. Start-stop-synchronous scheme of operation of counters of transmitted (SCH1) and received (SCH2) bytes (fragmentation-defragmentation procedure of the transmitted data stream).

Since the unit for evaluating the quality of the received analogue VHF radio signals by the level of the received signal has inertia, not only the last, but also the penultimate transmitted information sign can be distorted. Therefore, on the transmitting and receiving sides, there are special storage devices for two information signs so that in the event of the loss of the energy contact of the meteor communication radio line to the VHF, it would be possible to repeat their transmission when it resumes, correctly restore it at the reception and register it in the counter. This takes into account the specificity of the meteor communication, which is as follows: at the beginning of the energy contact between the correspondents the best conditions are created for the error-free transmission of code data blocks, in which the probability of errors is the lowest, and before the interruption of the meteor communication channel, the worst conditions for error-free data transmission are created, and the probability of errors in the received codewords is the highest.

Functionally, the proposed algorithm is implemented as follows. When a new meteor trail appears, the energy contact between the correspondents is restored. It becomes possible to continue transferring the next piece of data. Before the start of its transmission, the number of the last transmitted data character of the previous fragment is transmitted, and after that, the next-to-last and last character of the information data that was transmitted at the end of the previous fragment is repeated. Further, the transmission of the information data stream continues. The retransmitted characters are compared with those already transmitted, and an advantage in choosing to register the received character is given by retransmission. This is how the stream of transmitted information data is stitched.

![Fragmentation-defragmentation of a formalized message.](image)

Figure 3. Fragmentation-defragmentation of a formalized message.

The moments of the beginning and the end of fragmentation-defragmentation (figure 3), that is, restoration of the energy contact and its break, are continuously monitored by the quality control module of the analog radio channel VHF according to the ratio of signal levels and interference at reception (Us / Uh) [9]. Since the data exchange is carried out duplex, then when the ratio of the signal level at the reception drops below a predetermined threshold level (Uthr = Us / Uh), the energy contact between the
correspondents is interrupted by transmitting the STOP TRANSFER service signal from the receiving correspondent to the transmitting one.

At the end of the transmission of the entire information message, the service signal “END OF MESSAGE” is transmitted, after which the structure of the received message is formed, which is then issued to the recipient in the computer and registered in it.

To ensure MCN protection from errors, a special cyclic code \((n, k) = (11,7)\) is used. It allows to detect errors in the received code combinations and automatically correct single errors. If the code block is received with errors, then they are corrected by automatically requesting the retransmission of the code blocks received with errors on the reverse channel of the meteor radio link. The original information seven-element code allows one code block to transmit up to 127 digital numbers, and the 11-element noise-immune code can transmit up to 2047 digital numbers with one code block. Therefore, digital passwords for identifying correspondents in a meteoric communication network can consist of one code block. Moreover, each correspondent of the meteoric communication network has its own digital number (password), which is especially important for more rational use of the MCN bandwidth resource for business purposes. When entering a connection and in the process of identifying correspondents, the digital passwords of the called and calling correspondent are transmitted.

The digital passwords of correspondents are generated in the form of scramblers (Scr) as components of the pseudo-random sequence \(2^{11}-1=2047\). Each scrambler consists of 11 binary symbols. To carry out the process of identifying correspondents in the network, adaptive descramblers are used. It is they that provide imitation protection of the information data transmission channel, the assessment of which can be represented as the probability of \(P_{FI}\) of false generation of the correspondent identification signal via one of the MCN radio links. Accordingly, the following expression can be written: \[P_{FI} = P_{\text{misSC}}P_{\text{misScr2}}P_{\text{misScr1}},\] where \(P_{\text{misSC}}\) is the probability of erroneous formation of a clock synchronization signal at reception, \(P_{\text{misScr2}}\) is the probability of erroneous formation of a portion of the pseudo-random sequence Scr2 (digital password) of the called station; \(P_{\text{misScr1}}\) - the probability of erroneous formation of a section of the pseudo-random sequence Scr1 (digital password) of the calling station.

The proposed algorithm allows to preserve the integrity of the transmitted data stream in the meteor communication network, while ensuring the confidentiality of the connection between correspondents, without requiring the involvement of additional telecommunication resources of the meteor communication network. Consequently, from the point of view of information security, a meteoric communication network is capable of exchanging information data between network correspondents, while ensuring a low probability of transmitting information to those correspondents to whom it is not intended, as well as a low probability that the flow of transmitted information data itself may have false data. At the same time, in the conditions of intermittent energy contact between correspondents in the meteoric communication network, the integrity of the information messages flow transmission is preserved, which, in turn, contributes to the most highly efficient use of the limited radio frequency information resource of the network.

References

[1] Doroshenko V I and Ksenofontov Yu G 2019 The use of meteor communication in the systems of ensuring the safety of infrastructure facilities of the Northern Sea Route Scientific and Technical Journal “Defense Engineering Problems Series 16 Technical means of combating terrorism” 1-2(127-8) 3-11

[2] Skripnik I L 2019 Communication systems based on multiple access technologies for managing the actions of units of the EMERCOM of Russia Proc. of the All-Russian IXth Sci. and Pract.Conf. on Monitoring, Modeling and Forecasting of Natural Hazards and Emergencies (Zheleznogorsk: FGBOU VO Siberian Fire and Rescue Academy of State Fire Service of the Ministry of Emergencies) p 363-9

[3] Martynov V L, Doroshenko V I and Skripnik I L 2020 Meteor communication network in the monitoring system of technical means of navigation safety of the Northern Sea Route Marine
Intellectual Technologies Scientific Magazine 1(2) 118-25

[4] Karpov A V, Sidorov V V and Sulimov A I 2008 Meteoric generation of secret encryption keys to protect open communication channels Informacionnye Tekhnologii I Vichislitel’nye Sistemy (Journal of Information Technologies and Computing Systems) 3

[5] Kachnov A I, Penkin A A and Rybakov A V 2016 Development of a mobile information support system using meteor communication channels Proc. of the Vth Int. Sci.-Technical and Sci.-Methodological Conf. on Actual Problems of Information Telecommunications in Science and Education (St. Petersburg: SUT) p 177-81

[6] Ksenofontov Yu G, Doroshenko V I and Pivovarov A N 2019 Increasing information security of monitoring channels in meteor communication networks in the Arctic of Russia Information Security Problems Computer Systems 3 41-8

[7] Doroshenko V I, Ksenofontov Yu G and Skripnik I L 2020 Telecommunication resource of the information and telecommunication network of meteor communication in the Arctic of Russia Bulletin of Voronezh State Technical University 16(1) 45-55

[8] Blagov D S and Volvenko S V 2010 Increasing the speed of information transmission in meteoric communication systems by using signals of variable duration St. Petersburg State Polytechnical University Journal Computer Science Telecommunications and Control Systems 5(108) 7-13

[9] Kapralov D D and Kirik D I 2018 Stochastic model of a meteor radio channel Proceedings of Telecommunication Universities 4(3)