International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Protection of Wireless Sensor Network and Container for Communication in the Arctic

Alexey Lagunov, Dmitry Fedin

Abstract*: Currently, the Arctic is attracting the attention of many states. The nature of the circumpolar region has many dangers for the person who will work in this region. Global warming causes many negative processes. To study them, we created a container and a sensor network. The system we have created allows monitoring the state of natural processes in the Arctic. The sensory and telecommunications network system is also at risk from intruders. In this article, we investigated the attacks that could threaten the sensory network and proposed several measures to eliminate them. We identified three main problems of the network in the Arctic: the problem of power supply, the problem of the communication channel, and the problem of data reliability. We proposed a series of measures to solve these problems. We conclude that other researchers may use the security measures we have proposed in similar sensor systems in the Arctic.

***Keywords* : sensor, monitoring, protection, networks, Arctic.**

I. INTRODUCTION

The Arctic occupies a huge territory: the Northern circumpolar region of the Globe, the Arctic ocean, its seas and islands, the Northern part of the continents of Eurasia and North America (Fig.1).

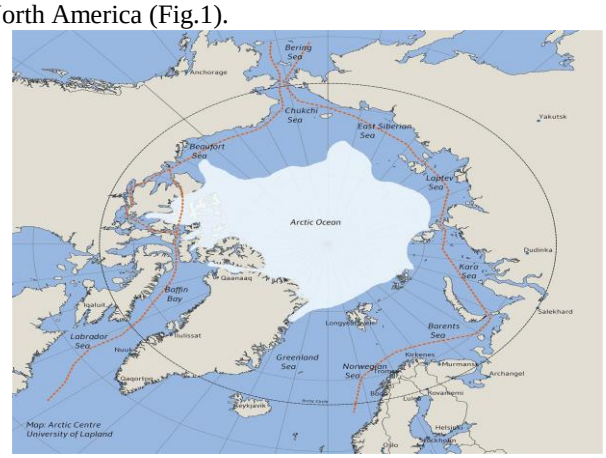

Fig. 1.Arctic Seaways [1].

Manuscript published on 30 September 2019
***** Correspondence Author
Alexey Lagunov *, Department of Fundamental and Applied Physics of the Higher School of Natural Sciences and Technologies Northern (Arctic) Federal University named after M.V. Lomonosov, Severnaya Dvina Emb. 17, Arkhangelsk, Russia, 163002. Email: a.lagunov@narfu.ru
Dmitry Fedin, Company "Lema", Okrugnoe Shosse 3-1, Arkhangelsk, Russia, 163045. Email: d.fedin@hunterhelp.ru

Currently, Arctic becomes one of the most strategically important regions on the planet, and states make serious steps to protect their northern geopolitical interests, for example [2, 3, 4]. It occurs inevitably due to a quarter of the world's oil, and gas reserves are admittedly located in the Arctic [5, 6]; due to the Northern Sea Route can significantly reduce the time of delivery of goods from east to west and back [7]; and so on. At the same time, Arctic region is sensitive to temperature changes, especially, over last decade, for example [8, 9, 10], including variety and uncertainty of local realizations in both statistical [11] and nonlinear [12] terms. These circumstances lead to specific scientific and engineering problems which are not typical for other regions even with similar low-temperature seasons.

New hazards have arisen in the Arctic in recent years. Climate change leads to the threat of sea-level rise [13]. The average air temperature is rising, and the volume of glaciers in Greenland and Antarctica is decreasing. The level of the World's oceans increases by an average of 3 mm every year. As a result of these natural processes, there is a decrease in the area of Islands in the Arctic ocean; the coastline is changing. This phenomenon can create problems for shipping.

Arctic strengthening is the maximum development of warming in the Arctic compared to global warming [14]. The restructuring of the circulation system in the Arctic leads to a sharp reduction in the amount of Arctic ice at the end of the summer period. The reduction of sea ice is the most discussed manifestation of modern warming in the Arctic. The absolute minimum of the area covered by sea ice occurred on September 2012. Scientists have never seen such a reduction in ice area before. The minimum value was 3.37 million km^2 on 22-25 September 2012 (Fig.2).

Ice thickness is the most difficult for mass measurements of sea ice cover. Researchers are developing and improving measurement methods and conducting them from airplanes, submarines, and anchor ice installations, but the full picture is not yet available [16].

New dangerous hydrometeorological phenomena appeared in the Arctic. A tsunami of ice struck Central Canada and the North of the United States on January 2014. This phenomenon shocked residents who left their homes in panic. Seawater, driven by strong winds (in the Arctic wind speed can reach 40 m/s) can flood the low shores of the Arctic ocean seas. The water drags the ice, throwing them ashore [17].

Another problem is the melting of permafrost, which leads, first, to the subsidence of the soil, and, secondly, to the release of greenhouse gas methane [18].

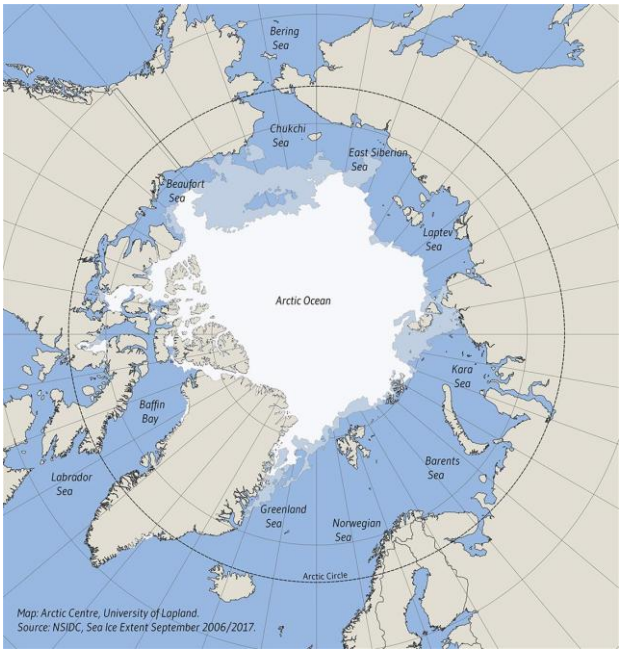

Fig. 2.Arctic Sea Ice Extent 2006-2017 [15].

There is no exact answer to how the climate will change in the future, so there is a need for constant monitoring of natural processes in the Arctic. NARFU [19] together with the Nordic countries in the framework of the Kolarctic program "Ice Operations" is conducting a study of the above and other phenomena in the Arctic [20]. Project objective: to contribute to the industrial development of the North-Eastern Barents sea territories (to support the development of environmentally safe production activities and to contribute to the development of offshore platform projects for the Arctic territories).

A person can conduct research in the Arctic, but it is associated with a number of dangers for his life: polar night and polar day lasting 3-5 months, which have a negative impact on the human psyche; magnetic storms that cause short-term health disorder; low air temperatures during the polar night in combination with strong winds create extremely adverse conditions; sharp variability of weather conditions in time and space due to the influence of local features.

In connection with the above, for the study of dangerous changes in the Arctic, it is best to use a sensor network that allows you to collect all the necessary data automatically. We can not use the wired network of sensors, as adverse conditions such as ice movement, soil subsidence due to permafrost melting, strong winds can damage the cable.

We believe that in the Arctic, it is best to use a wireless sensor network. The first chapter contains a description of the network build. The second chapter is devoted to the safety of the network, as even in the Arctic sensor network cannot always be safe.

II. TELECOMMUNICATION NETWORK

A. Container

To provide the expedition with telecommunications, our team developed a container project. We have compiled a technical task for the development of a remote data collection and control system in a stand-alone platform. Requirements for the software part of the data acquisition and control system:

1. The system must ensure the autonomy of the platform.
2. Developers should organize the collection of data from all key devices connected to the system: Satellite iDirect X3 modem, Hybrid charge controller, Inverter, Wi-fi router, Video server, Weather station, GPS data.
3. To ensure maximum operating time, in case of the insufficient battery, the system should alternately reduce the power consumption of the devices (if possible) or disconnect the devices from the power source at the established priority.
4. For the current monitoring of the readings of the system, a web interface must be implemented, with secure access from the internal network.
5. To monitor the system, collect statistics, service information, remote configuration, and support the device must have the ability to access the internal network (or Internet) the customer.
6. The device must accumulate the necessary information and store it for a period (month, year, five years).
7. The device should inform about all abnormal situations, the local system operator, as well as the remote administrator
8. The way of warning about emergencies (fully discharged batteries in the absence of energy generation, a sharp decrease (increase) in the temperature in the heating cabinet) is e-mail, SMS-message when there is a femtocell, a radio signal (to the personnel's radio, for example) autonomous container.
9. The system should send a notification about the need to connect a diesel/gas generator, or another energy source to the local operator.

Hardware requirements for data acquisition and control systems:

1. The operating temperature range of the system is -40...+50°C (we placed the device in a heating cabinet with a constant temperature of 10°C, but not lower than 0°C).
2. Operating voltage of systems: 12-24 V.
3. The system must have the on/off means of the connected devices, the minimum number of switches: 5.
4. The system should contain all interfaces for connecting to devices that researchers regularly install on an autonomous platform.
5. The GPS transmitter can be optionally installed in the system to determine the current location of the device, as well as sending the device coordinates in the event of an SOS signal.
6. The set of the complex must provide for the presence of devices/instruments for determining the vertical and horizontal horizons (necessary for proper installation of the antenna).

Based on these requirements and the study [21], a container was created (Fig.3).

Fig. 3. Container.

B. Structure Scheme of Telecommunication Network

We placed the container structure in Fig.4. Information is exchanged with the "mainland" through satellite communications with a satellite that is in geostationary orbit. Communication is carried out in the Ku-range. The antenna has a diameter of 1.8 meters. To decode the signal, use the iDirect Evolution X3 modem.

The modem sends a signal to the Mikrotik Router BOARD 951G-2HnD. All container systems are managed using a single-board computer Udoo [22]. We installed two wind generators and six solar panels in the container. The required amount of electricity, this system can produce only in the period from May to September. The rest of the time, it is necessary to connect a gas generator to the container. Researchers organize most expeditions in the summer and can use the container at full capacity. The delay in the removal of the container in October led to its complete shut-down. We were forced to replace the batteries to restore system performance.

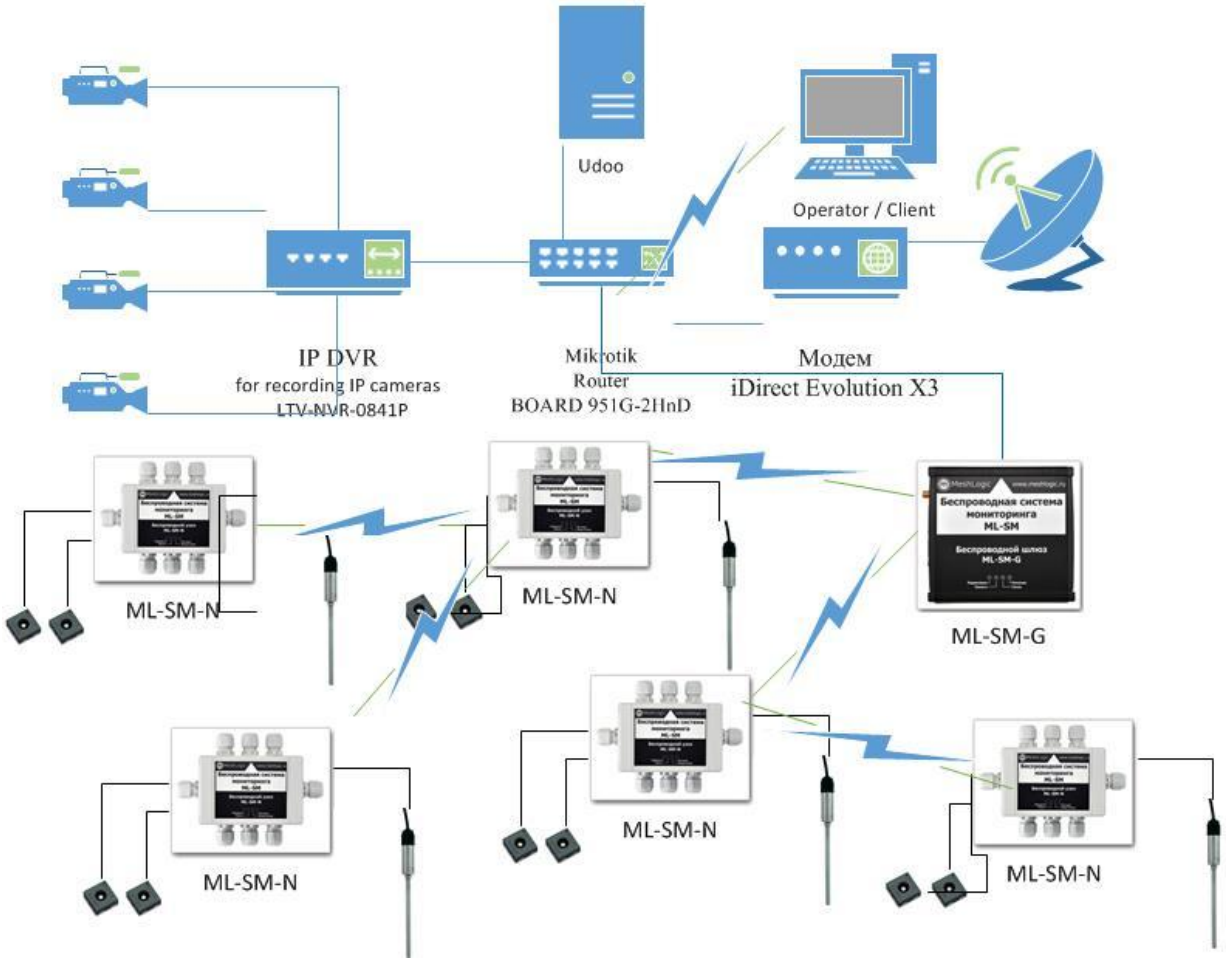

Fig. 4.Block diagram of a telecommunication network.

A big problem for researchers is polar bears. We equipped the system with four cameras for monitoring the environment and timely detection of polar bears.

We used the ML - SM monitoring system to organize the wireless network [23]. The hardware-software complex ML-SM includes ml-SM-N wireless nodes, ML-SM-Sx interface modules, sensors, ML-SM-G wireless gateway, server, specialized software.

The developer placed the ML-SM-N wireless node (Table I) in a plastic case with IP66 protection. In the same case, there are boards of modules of ml-SM-Sx interface and elements of Autonomous power supply.

The universal modular design of the wireless node ML-SM-N allows you to install up to 4 mezzanine modules in each node to pair with different types of sensors in any order and arbitrary combinations. We used the temperature and relative humidity sensors of the Sensirion SHTx family with the ML-SM-S1W interface module and the thermocouple with the ML-SM-STC interface module.

We installed thermocouples in GrUT-03 [24] to measure the temperature distribution in the soil in depth. The complex is designed to study the temperature dependence of vertical sections of soils in the Arctic.

Table- I: Typical ML-SM-N modul specifications

Parameter	Value
Radio channel type	IEEE 802.15.4
Frequency range	2400...2483.5 MHz
Transmitter output power	Up to 20 dBm (100 mW)
Receiver sensitivity	-98 dBm
Supply voltage	from 3 to 36 V DC (1 W)
Transmission / standby consumption current	21 mA / 9 µA
Management Interface	UART (LVCMOS)
UART interface speed	from 9600 to 921600 bps
Temperature range	-40...85°C
Number of measurement channels	up to 64 external sensors per node
Measurement period	from 1 second to 24 hours

The ML-SM-G wireless gateway has IP20 enclosure protection. We placed it in a special Cabinet together with other communication equipment. The design and execution of wireless nodes, interface modules, and gateways ensure their performance in a wide range of climatic parameters with an operating temperature range from -40 to +85 · C. The temperature Range allows the use of equipment in the Arctic.

We used as the server computer Udoo, installing the software for complex ML-SM. Main advantages of the network:

- fully multistage network topology;
- all nodes are equal and are routers;
- self-organization and automatic route search;
- resistance to channel interference;
- high scalability and reliability of data delivery;
- possible to work all nodes from independent sources of supply.

By the period specified in the system settings (we chose one hour for our monitoring task), the ML-SM-N wireless nodes automatically perform normalization and analog-to-digital conversion of signals from external sensors connected to it. They carry out the primary processing of the measurement results and their transmission over the radio channel gateway ML-SM-G. They have received from wireless nodes ML-SM-N data gateway ML-SM-G stores in non-volatile memory, noting the time of their receipt and other service information for unambiguous subsequent recovery of the collected data from the archive. Thus, the gateway performs the function of an Autonomous recorder of readings coming from distributed sensors. Further, with the help of special software information from the gateway archive is downloaded to the server and transmitted via the satellite channel.

III. SENSOR NETWORK SECURITY

We placed the container and sensor network in the Arctic on Novaya Zemlya Island. The system is configured and operates further automatically without interference from the staff. Engineers go to the site only if there is a malfunction or malfunction of the equipment. The system is controlled remotely via a telecommunication channel, which leads to a decrease in security. We made the container according to the scheme resistant to vandalism. We can monitor the situation with the help of 4 video cameras, which are available on the container.

Sensor network and telecommunications require configuration to protect against an intruder. We divided potential violators into three main categories:

1. Curious. A person who discovers a container with a sensor network in the Arctic may try to break the network out of curiosity. Most curious people do not pose a serious threat to network security. But if they use special programs and hacker tips, they can detect vulnerabilities. Most often, curious people report their findings to the owners of the container and the network, helping to improve security.

2. Hunters for communication channels. In the Arctic, there are practically no high-quality communication channels, as they are very expensive. Satellite communication channels with geostationary satellites can only be used up to 78°N [25]. The lack of a communication channel pushes these people to try to use a foreign network to transfer various content to the network. According to international law, any attempt to penetrate someone else's network has serious consequences, including imprisonment, but there are few people in the Arctic, so hunters often go unpunished.

3. Criminals. The third category is the most dangerous. Its representatives know and know how best to perform such a hack. They are attracted by the anonymity of the sensor network and the availability of out-of-band access channels. In the sensor network, which has a large number of devices connected to the network, it is very difficult to track through which device data transfer occurred. They make the strongest attacks by a group of people who have a fairly good education in the field of computer technology and are not hearsay familiar with the principles of radiophysics. Criminals can cause significant damage to the system by disabling it or replacing the data, which can lead to false data from the sensors.

We must be aware of the different types of attacks that can be used by intruders to create a sensor network protection system. Attacking a system is an action or a set of actions by an attacker aimed at gaining access to an information system [26].

We distinguish the following elements for which the threats of violators in Artik are most significant:

1. The problem of power. The attacker attacks the settings of the power-saving mode. The problem of energy saving is very acute in the Arctic [27]. Most often, electricity is produced using a gas generator. We use solar panels and wind generators; we use batteries to power the sensors. Typically, ML-SM-N modules are in standby mode and have low power consumption. Only at the moment of data transmission for a short period, the module becomes active. An attacker could fill the communication channel with unauthorized traffic or floods the communication session with fake frames. In this case, the module will be inactive mode until it transfers data.

For a long time, the module is inactive mode leads to large power consumption, which leads the module to a non-working state.

2. The problem of the communication channel. The attacker attacks the communication channel. The problem of communication channels is also very acute in the Arctic [25]. It is necessary to use several special measures to increase the throughput of the communication channel [28]. We use a fairly narrow communication channel due to the high cost and low data transfer rate. Therefore, if the intruder will use our communication channel, then our system may not get access to the channel.

3. The problem of data reliability. An attacker performs an attack aimed at violating data integrity or replacing data with other data. Based on incorrect data, the contractor may make the wrong decision, which can lead to a serious threat to the Arctic environment or the safety of countries that work in the Arctic.

We analyzed primary sources on the security of sensor networks and identified the most common types of attacks [29-32]. We have distributed these attacks to the levels of the standard OSI model. The analysis of primary sources also made it possible to identify several measures that allow counteracting attacks (Fig.5).

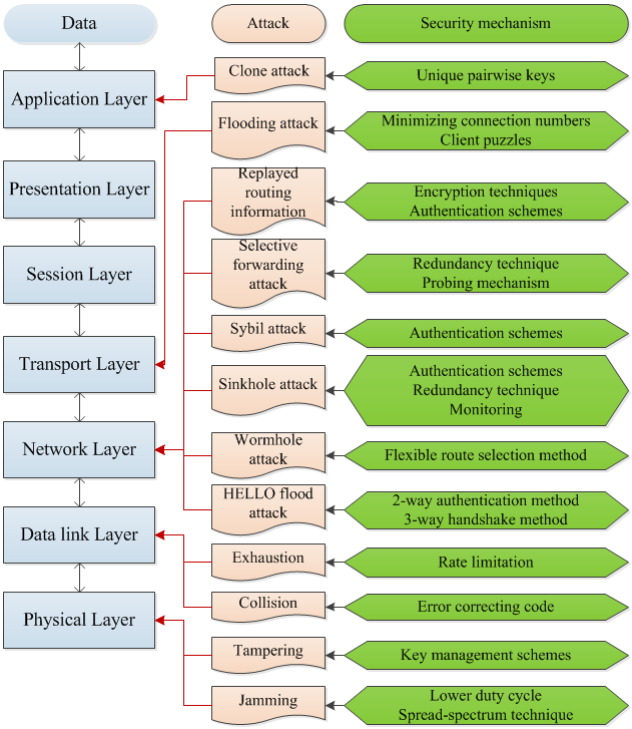

Fig. 5.Attacks and security mechanisms according to the OSI levels.

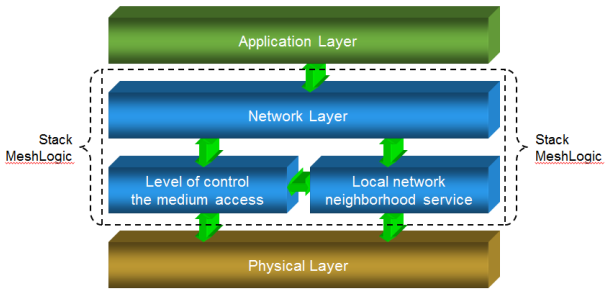

Fig. 6.Stack Protocols Platform MeshLogic.

In general, the container telecommunications system uses all seven levels of the OSI model. The sensor network on the MeshLogic platform uses the Network Layer and Data Link Layer (Fig.6). The system is most vulnerable at these levels. As can be seen from Fig.5 on the Network Layer, attackers carry out the greatest number of attacks. The authors of the source [33] proposed several measures to improve the security of the sensor network. The figure, graph, the chart can be written as per given below schedule.

In general, the following measures can be recommended to improve the security of the sensor network in Artik:

- reduce the radio coverage area (correctly, if the signal does not go beyond the limits of the controlled area);
- set a new administrator password (other than the default one);
- Enable filtering by MAC address;
- change the standard network identifier (SSID) and change it periodically;
- Activate intra-network encryption;
- change encryption keys on time;
- install firewalls and antiviruses;
- Ensure the implementation of traffic filtering algorithms on firewalls;
- establish a special scheme for backing up equipment and backing up software installed on the network;
- to periodically monitor the equipment operating in the network.

IV. CONCLUSION

The Arctic occupies a vast territory. This region is of interest to many states since this region has large reserves of minerals. At the same time, there are quite unfavorable conditions for researchers and workers in the Arctic. In addition to cold and strong winds, new dangers have recently appeared. These include melting ice, melting permafrost, ice storms, changing the thickness of the ice, and outlines of the coast. All this creates a danger to humans, vessels, and mechanisms.

It is difficult for a person to explore the Arctic as the harsh conditions adversely affect the health and mental state of the researcher. The best option is to replace a person with automatic monitoring systems. We have created one of these systems, consisting of a container and a sensor network. The system can function in the Arctic without human service for quite a long time.

But in the Arctic, there is a danger to the work of the system by the person. We have identified three categories of people who can harm the system: Curious, Hunters for communication channels, Criminals. We analyzed the sources and identified several attacks on various levels of the OSI model, and also identified measures that help protect the sensor network from the actions of intruders.

We identified three problems that are most important for the Arctic: The problem of power; The problem of the communication channel; The problem of data reliability. We have proposed solutions for these problems. We believe that other researchers may use the safety measures we have developed in similar systems in the Arctic.

REFERENCES

1. "Arctic Seaways," Arctic Centre, University of Lapland, Official site. Available: https://www.arcticcentre.org/EN/arcticregion/Maps/Seaways.
2. "US demands shared use of Russia's Northern Sea Route," 2018, [Online]. Available: https://www.rt.com/business/423913-northern-sea-route-us/.
3. V. Ingimundarson, "The geopolitics of the 'future return': Britain's century-long challenges to Norway's control over the spitsbergen archipelago," *International History Review*, Vol. 40 (4), pp. 893-915, 2018, DOI: 10.1080/07075332.2017.1345773.
4. V. V. Kovalev, V. V. Kasyanov, Y. S. Bortsov, Goloborod'ko A. Y. , T. D. Skudnova, "The increase in geopolitical competition as a challenge (threat) to Russia's national security," *European Research Studies Journal*, Vol. 20 (4), pp. 499-508, 2017.
5. M. Motomura, "Perspectives on oil and gas development in the russian arctic*," Russia's Far North: The Contested Energy Frontier*, pp. 27-42, 2018, DOI: 10.4324/9781315121772.
6. G.-C. Zhang, H.-J. Qu, C. Zhao, F.-L. Zhang, Z. Zhao, "Giant discoveries of oil and gas exploration in global deepwaters in 40 years and the prospect of exploration", *Natural Gas Geoscience*, 28 (10), pp. 1447-1477, 2017, DOI: 10.11764/j.issn.1672-1926.2017.08.008.
7. A. Buixadé Farré, et al., "Commercial Arctic shipping through the Northeast Passage: routes, resources, governance, technology, and infrastructure", *Polar Geography*, Vol. 37 (4), pp. 298-324, 2014. DOI: 10.1080/1088937X.2014.965769
8. M. Nuttal, "Tipping points and the human world: living with change and thinking about the future," *AMBIO*, Vol. 41, pp.96-105, 2012.
9. S. Goldenberg, *Arctic sea ice extent breaks record low for winter*, 2016, [Online]. Available: https://www.theguardian.com/environment/2016/mar/28/arctic-sea-ice-record-low-winter.
10. C.Welch, *Arctic Sea Ice Is Second-Lowest on Record*, 2018, [Online]. Available: https://news.nationalgeographic.com/2018/03/winter-arctic-sea-ice-second-lowest-record-spd/.
11. Yu. Kolokolov and A. Monovskaya, "Multidimensional analysis of dynamics of annual warming-cooling cycles on the basis of index model of temperature observations," Proc. the 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 24-26 September 2015, Warsaw, Poland, v.2, pp.631-637.
12. Y. Kolokolov and A. Monovskaya, "Guess-work and reasonings on centennial evolution of surface air temperature in Russia. Part II: Is it possible to research both local peculiarities and regional tendencies from the bifurcation analysis viewpoint?" Int. J. of Bifurcation and Chaos 26, 1650071, 2016.
13. N. S.Fučkar, V. Guemas, N. C. Johnson, F. J. Doblas-Reyes, "Dynamical prediction of Arctic sea ice modes of variability," *Climate Dynamics*, Vol. 52 (5-6), pp. 3157-3173, 2019, DOI: 10.1007/s00382-018-4318-9.
14. J. Robson, et al., "Recent multivariate changes in the North Atlantic climate system, with a focus on 2005–2016", International Journal of Climatology, Vol.38 (14), pp. 5050-5076, 2018, DOI: 10.1002/joc.5815.
15. "Arctic Sea Ice Extent 2006-2017", Arctic Centre, University of Lapland, Official site. Available: https://www.arcticcentre.org/EN/arcticregion/Maps/Sea-Ice.
16. A. Lagunov, D. Fedin, A. Tyagunin, "Using UAVs for remote study of ice in the arctic with a view to laying the optimal route vessel", in *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Paper № 6933168, pp. 1293-1299, 2014, DOI: 10.15439/2014F226.
17. V. Heller, F. Chen, M. Brühl, R. Gabl, X. Chen, G. Wolters, H. Fuchs, "Large-scale experiments into the tsunamigenic potential of different iceberg calving mechanisms," *Scientific Reports*, Vol. 9 (1), Article N 861, 2019, DOI: 10.1038/s41598-018-36634-3.
18. M. T. Jorgenson, G. V. Frost, D. Dissing, "Drivers of landscape changes in coastal ecosystems on the Yukon-Kuskokwim Delta, Alaska," *Remote Sensing*, Vol. 10 (8), N 1280, 2018, DOI: 10.3390/rs10081280.
19. Northern (Arctic) Federal University, Official site. Available: http://NARFU.ru/en/
20. Ice Operations (KO2100 ICEOP), Kolarctic, Official site. Available: https://kolarctic.info/projects-2/.
21. A. Lagunov, N. Podorojnyak, "The research of the complex of alternative energy to power the satellite container," in *Proceedings of the 17th IEEE International Conference on Smart Technologies, EUROCON 2017*, Paper N 8011137, pp. 370-375, 2017, DOI: 10.1109/EUROCON.2017.8011137.
22. UDOO X86, UDOO, Official site. Available: https://www.udoo.org/udoo-x86/.
23. Wireless monitoring system, MeshLogic, Official site. Available: http://www.meshlogic.ru/system.html.
24. A. Rozevika, A. Volkov, G. Martinov, A. Veselkov, "Development of the hardware-software complex GrUT-03", AIP Conference Proceedings, 2015, Paper N 020080, 2018, DOI: 10.1063/1.5055153.
25. A. Lagunov, A. Surovtsev, V. Terekhin, A. Belugin, D. Korobitsyn, V. Glavatskih, P. Danilochkin, "Features of supply of telecommunications in the arctic," in *Proceedings of the 2014 22nd Telecommunications Forum, TELFOR 2014*, Paper N 7034531, pp. 814-817, 2015, DOI: 10.1109/TELFOR.2014.7034531.
26. Y. M. Amin, A. T. Abdel-Hamid, "A Comprehensive Taxonomy and Analysis of IEEE 802.15.4 Attacks", *Journal of Electrical and Computer Engineering*, Article N 7165952, 2016.
27. V. Terekhin, A. Lagunov, "Telecommunications equipment power supply in the Arctic by means of solar panels," AIP Conference Proceedings, 1767, Paper N 020021, 2016, DOI: 10.1063/1.4962605.
28. O. Ivakhiv, "Information state of system estimation," *International Journal of Computing*, Vol. 15 (1), pp. 33-41, 2016.
29. S. Watts, "Secure authentication is the only solution for vulnerable public wifi," *Computer Fraud and Security*, 2016 (1), pp. 18-20, 2016, DOI: 10.1016/S1361-3723(16)30009-4.
30. Y. Lu, G. Xu, L. Li, Y. Yang, "Anonymous three-factor authenticated key agreement for wireless sensor networks," *Wireless Networks*, Vol. 25 (4), pp. 1461-1475, 2019, DOI: 10.1007/s11276-017-1604-0.
31. X. Tan, S. Su, Z. Huang, X. Guo, Z. Zuo, X. Sun, L. Li, "Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm," *Sensors (Switzerland)*, Vol. 19 (1), Article N 203, 2019, DOI: 10.3390/s19010203.
32. S. R. Rajeswari, V. Seenivasagam, "Comparative Study on Various Authentication Protocols in Wireless Sensor Networks," *Scientific World Journal*, 2016, Review N 6854303, 2016, DOI: 10.1155/2016/6854303.
33. O. Kehret, A. Walz, A. Sikora, "Integration of hardware security modules into a deeply embedded TLS stack," *International Journal of Computing*, Vol. 15 (1), pp. 24-32, 2016.

AUTHORS PROFILE

Alexey Lagunov, Associate Professor of the Department of Fundamental and Applied Physics of the Higher School of Natural Sciences and Technologies Northern (Arctic) Federal University named after M.V. Lomonosov. Educational qualifications: mathematics, State Pedagogical Institute, Arkhangelsk, RUSSIA. PhD, Author of 24 publications. Area of scientific interests: research and construction of telecommunication systems in the Arctic, the study of the possibility of using alternative energy systems to operate in high latitudes, data analysis and construction of information and telecommunication systems for monitoring the environment of the North, the construction of hardware and software systems to protect human life and health in the Arctic, the construction of medical devices.

Dmitry Fedin, Programmer of the company "Lema". Educational qualifications: engineer, Northern (Arctic) Federal University named after M.V. Lomonosov, Arkhangelsk, RUSSIA. Master of physics, author of 4 publications. Area of scientific interests: computer, radio engineering, programming, data analysis, sensor networks, satellite communications, Arctic, telecommunications. programming in the construction of telecommunication systems in the Arctic, configuration and programming of alternative energy systems for operation in high latitudes, data analysis and construction of information and telecommunication systems for monitoring the environment of the North, construction of hardware and software systems for the protection of human life and health in the Arctic, writing software for medical devices.