UDC: 534.843:004.9 https://doi.org/10.15407/jai2023.01.123

FORMATION OF WIRELESS SENSOR NETWORK PROTECTION SYSTEM PARAMETERS FOR INTRUSION DETECTION IN THE FORM OF FALSE EVENT FLOWS

O. Belej
Lviv Polytechnic National University, Ukraine
5 Mytropolyt Andrei str., Building 4, Room 324, Lviv 79015
oleksandr.i.belei@lpnu.ua
https://orcid.org/0000-0003-4150-7425

Annotation. Wireless sensor networks with stationary and mobile sensor nodes are studied. For mobile nodes, in addition to sensor nodes, the influence of node movement speed on the duration of the network life cycle for mobile AdHoc networks was also studied. When studying the impact of erroneous events on the sensor field, it was established that providing sensor nodes with mobility allows increasing the life cycle of the network. A model of intrusion into a wireless sensor network with the aim of shortening its life cycle has been developed, which differs from known models in that false event streams are used to achieve this goal. The model is developed based on typical geometric, quantitative and energy parameters of wireless sensor networks using a basic clustering algorithm for a homogeneous mobile sensor network under conditions of Poisson network intrusion and deterministic error event flows.

It is established that the duration of the life cycle of a wireless sensor network can significantly depend on the type of the flow of erroneous events and, other things being equal, under the influence of a deterministic flow can be almost half as long as under the influence of a flow of erroneous events. the impact of the flow of false events. the Poisson flow effect. Detection of false events in a wireless sensor network can be considered as a target tracking task, and to detect false events with a given probability, taking into account the limited capabilities of sensor nodes, it is advisable to use the architectural characteristics of the network, the distribution of the density of nodes on the sensor field.

Keywords: protection system, software complex, wireless sensor network, model, flow of false events, life cycle.

Introduction

The development of communication networks now and in the long term is based on the concept of the Internet of Things. This concept is based on the idea that the most significant part of the customer base of communication networks will be things. Implementation of the concept of the Internet of Things involves fundamental changes in the architecture of communication networks, services and network security. Infrastructural communication networks are transforming and self-organizing, machine-machine services are appearing that are provided without human intervention, in the field of network security, along with traditional types of attacks and intrusions, new ones are appearing due to the novelty of network architecture and services. These qualitative changes are the result of quantitative changes in the customer communication base. Many more things lead to the prospect of trillions of communication networks, and projections suggest the emergence of up to 50 trillion things that are elements of communication networks.

Despite the rather large number of cluster master node selection algorithms for wireless sensor networks, research in this field continues actively. In recent years, new works have appeared dedicated to algorithms for selecting the main node of a wireless sensor network cluster in n-dimensional space [1, 2, 3]. At the same time, the main indicators to be studied have not changed compared to the works in the field of wireless sensor networks on an airplane. This is, as before, the duration of the life cycle of the network and the residual energy.

Currently, another class of wireless sensor networks is emerging - flying sensor networks, the use of which allows expanding the application of wireless sensor networks to tasks such as monitoring and data collection from vineyards, monitoring the condition of building roofs [4, 5].

The technological basis for realizing the concept of the Internet of Things at the moment is wireless sensor networks, which are also called penetrating sensor networks

due to the targeted use of sensor nodes. The study of wireless sensor networks is one of the most common areas of scientific activity in the field of telecommunication systems, networks and devices worldwide since the first decade of the 21st century.

Wireless sensor networks are often used to monitor and protect areas from intrusions. The paper proposes and investigates a new type of intrusion into wireless sensor networks based on the generation of spurious event streams. Considering the above, the research topic is relevant.

Problem statement

In addition to known parameters such as losses, delays, several new parameters are used to evaluate the performance quality of wireless sensor networks. Two closely related are life cycle duration and residual energy. In wireless sensor networks, there may often be no opportunity to recover the energy spent on the operation of the network, and therefore the duration of the life cycle and residual energy are important assessments of the quality of operation for such networks. However, the duration of the life cycle, which always depends only on the residual energy. As mentioned above, wireless sensor networks are often used to monitor space, environment, production processes. At the same time, the most important parameter is the share of space coverage, which allows obtaining information in the necessary and sufficient volume. Therefore, for such tasks, the duration of the life cycle is defined as the duration during which a wireless sensor network provides a given share of space coverage, despite the number of sensor nodes that continue to perform their functions. In target tracking tasks, the life cycle can be defined as the duration of operation of a wireless sensor network during which the sensor nodes ensure target detection with a given probability.

The miniature size and low cost of such Internet of Things as sensor nodes, as well as the self-organization of these nodes into a network, have contributed to the emergence of new methods of intrusion into Internet of Things applications, which have been called cloning. For cloning, both individual nodes, as well as sensor fields in general, and its fragments are suitable. At the same time, two cloning scenarios can be defined. In the first (Fig. 1), the cloned network or its fragments are located directly on the territory of the sensor field, and in the second scenario, the cloned network forms a new field (Fig. 2), which is located near the legal sensor field. The second scenario should find wide application for flying sensor networks.

To detect cloned sensor fields or their fragments, the characteristics of the traffic circulating in the network or the method of creating unique patterns can be used.

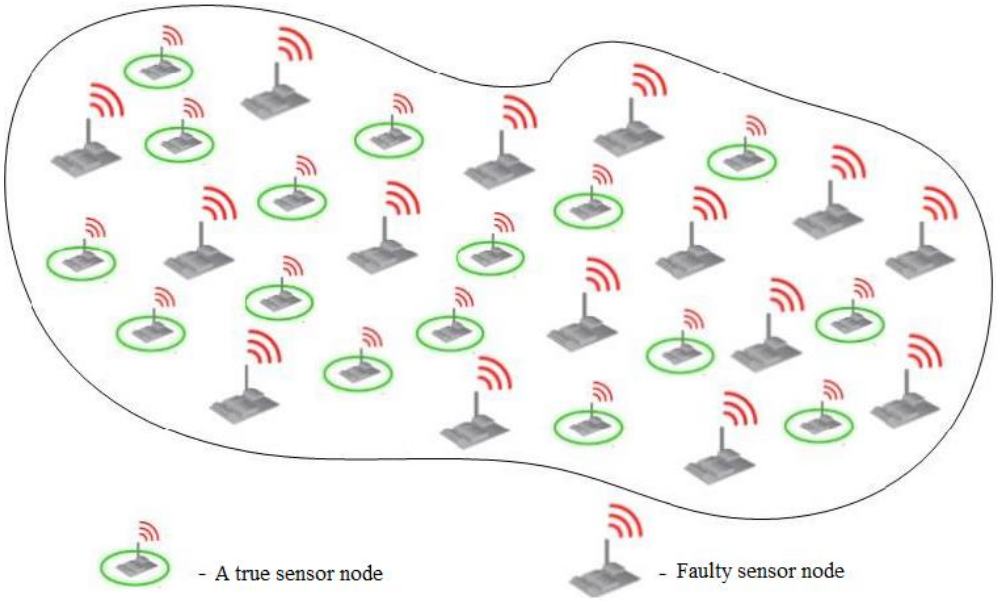

Fig. 1. Cloning of the sensor field or its fragment near the legal field

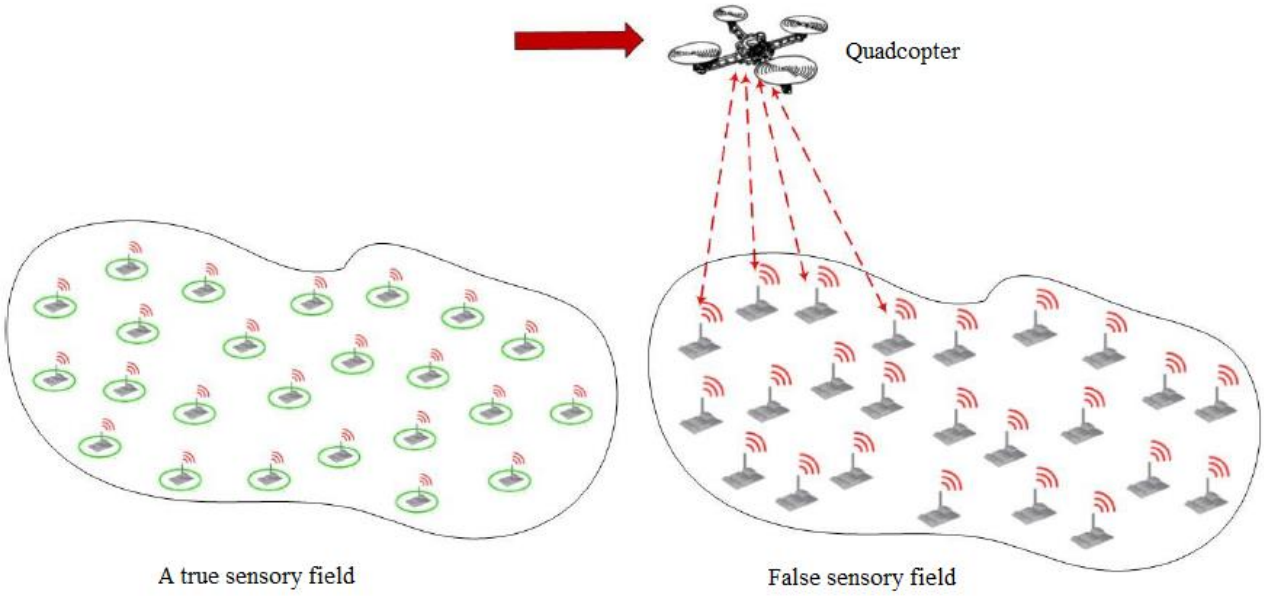

Fig. 2. Cloning of a sensor field or its fragment by creating a cloned field directly next to the legal one

The most general model will be used in further studies to determine the impact of various streams of erroneous events on a wireless sensor network, where the duration of the network's life cycle is determined by the moment of death of the last sensor node. When determining the optimal density of sensor nodes for the protection of a wireless sensor network against the flow of false events, the duration of the life cycle is determined as a target surveillance network, i.e. as the duration of operation of a wireless sensor network during which sensor nodes ensure target detection with a given probability.

To study the intrusions of streams of false events into sensor networks, we will use a model of the network, which receives a Poissonian or deterministic stream of false events. In addition, the duration of the life cycle of the investigated network, which is the main parameter to be found in the research process, is determined by the moment of death of the last sensor node.

In recent years, a lot of attention has been paid to mobile wireless sensor networks MWSN (Mobile Wireless Sensor Networks). Therefore, mobile sensor nodes will be considered along with stationary sensor nodes in the model of intrusion into sensor networks of false event streams. In MWSN studies, the speed of movement of the sensor node is, as a rule, 2 m/s. This speed value corresponds to a fast pedestrian. We will use this speed value as a base in the model. In the classification of self-organizing networks, an important place is occupied by Mobile Ad Hoc Networks (MANETs), which differ from MWSNs both in the number of nodes in the network and in the speed of node movement. For MANETs, the travel speed is chosen from 8-10 m/s (average vehicle speed in an urban environment) and above, which is determined by MANET applications such as Vehicular Ad Hoc Networks (VANET). The speed range from 2 m/s to 8 m/s as a boundary between MWSN and MANET will also be considered in the model, but for MWSN, the basic value of sensor node movement speed is 2 m/s.

Wireless sensor networks can be homogeneous and heterogeneous. Since sensor nodes are quite simple devices, as a rule, research on sensor networks uses the concept of a homogeneous network consisting of a set of sensor nodes with the same initial characteristics, such as the radius of action of the sensor node, initial energy, energy consumption for information transmission, etc. n. In the model under development, the sensor network will be considered as homogeneous.

As mentioned in the first chapter, in order to increase the residual energy and

duration of the life cycle of sensor networks, various clustering algorithms are used in their construction. The LEACH (Low Energy Adaptive Cluster Hierarchy) algorithm is the most well-known and widely used in wireless sensor network research. The use of the LEACH algorithm is based on the rule according to which a sensor node that was the master node in the previous life cycle of the sensor network cannot be it in the current cycle. Such a seemingly simple rule provides a 7-fold increase in the life cycle of a wireless sensor network compared to a random selection of a master node. A modification of the LEACH algorithm called LEACH-M was developed for mobile sensor networks. For a study involving both stationary and mobile sensor nodes, there is no fundamental difference in using LEACH or LEACH-M for mobile nodes. Therefore, the LEACH algorithm is always used when clustering the investigated network.

As in all typical models of wireless sensor networks, the radius of the sensor node is assumed to be 25 m, the energy reserve in each node is 2 J, the energy consumption for reception is 50 nJ/bit, for transmission - 50 nJ/bit and additionally 100 pJ/sq.m . The location of the gateway is chosen in the center of the plane, and its size is 200x200 m. When modeling, as it is customary for sensor networks, the duration of the life cycle of the sensor network is measured in rounds or iterations. At the same time, one iteration equals 1 second, and the ratio between rounds and iterations is 1:5 (one round has 5 iterations). The period during which the life cycle of a wireless sensor network is investigated, as in the basic work of LEACH, is chosen to last 1000s. Note that the main node is subject to rotation in each round.

Thus, the following model is developed to study the intrusions of false event streams on a wireless sensor network. 100 mobile nodes are initially distributed randomly on a plane measuring 200 by 200 meters. The radius of action of the sensor node is 25 m, the average speed is from 2 m/s (fast pedestrian) to 10 m/s (car in urban conditions), the energy reserve in each node is 2 J, the energy consumption for reception is 50 nJ/bit, for transmission – 50 nJ/bit and additionally 100 pJ/sq.m. All sensor nodes are homogeneous, i.e. have the same range and initial energy characteristics. According to the practice of using the LEACH algorithm, the share of the main nodes is defined as 5% of the total number of sensor nodes. The gateway is located in the center of the network.

The specified network is affected by intrusions as streams of false events. The influence of Poissonian and deterministic flows is studied and compared. The values of life cycle parameters of the attacked sensor network for self-similar flows with a Hurst parameter from 0.5 (Poissonian flow) to 1 (deterministic flow) will be within the interval of the obtained values for Poissonian and deterministic flows. The intensity of the flow of false events varies from one to 10 events per second. The speed of movement of the moving sensor nodes of the model varies from 2 m/s to 10 m/s. False events are materialized in the form of false objects penetrating the territory of the sensor network. When a false object is detected by the sensor node, information about the false event is transmitted to the gateway and this object is destroyed.

Research is carried out by the method of simulation modeling, the software is written in the C# language.

In Fig. 3-6 show screenshots illustrating the initial state of the network, the process of its clustering, the state of the network with half of the living nodes, and the state of the network before the death of the last nodes. Erroneous objects occupying an increasing space of the sensor field as the sensor nodes die are depicted by black dots, the main nodes are shown in green, and the sensor nodes – members of the cluster – are shown in pink.

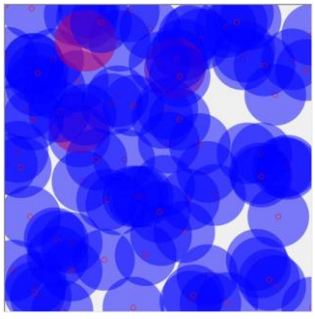

Fig. 3. Sensor field before clustering

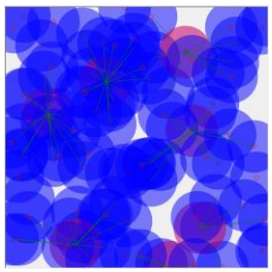

Fig. 4. Clustered wireless sensor network

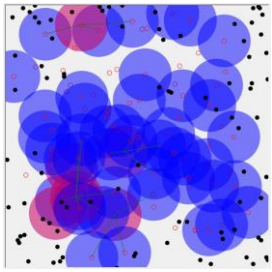

Fig. 5. Sensory field with half of living nodes

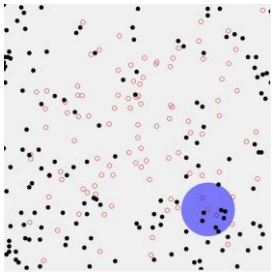

Fig. 6. The sensory field before the death of the last sensory node

In Fig. 7 presents the simulation results for the Poisson flow of false events with different intensity and different values of the movement speed of sensor nodes.

Analysis of the results shown in fig. 5, shows that streams of false events can significantly reduce the life cycle of a wireless sensor network.

Analysis of the last publications

Cloud technologies play a key role in network architecture in realizing the concept of the Internet of Things. Indeed, most often the Internet of Things has limited computing capabilities, and the use of cloud resources is the only option for efficient network organization. At the same time, data transmitted to the cloud can be of interest to various attackers. The security of the network of such a structure in the conditions of the widespread distribution of clouds cannot be guaranteed by many indicators, and the most modern approach proposed in [6] is to create false clouds.

It is predicted that the extraordinary amount of IoT will require self-organization when building networks. In addition, in many applications of the Internet of Things concept, the nodes of such networks are very simple physically and have low cost.

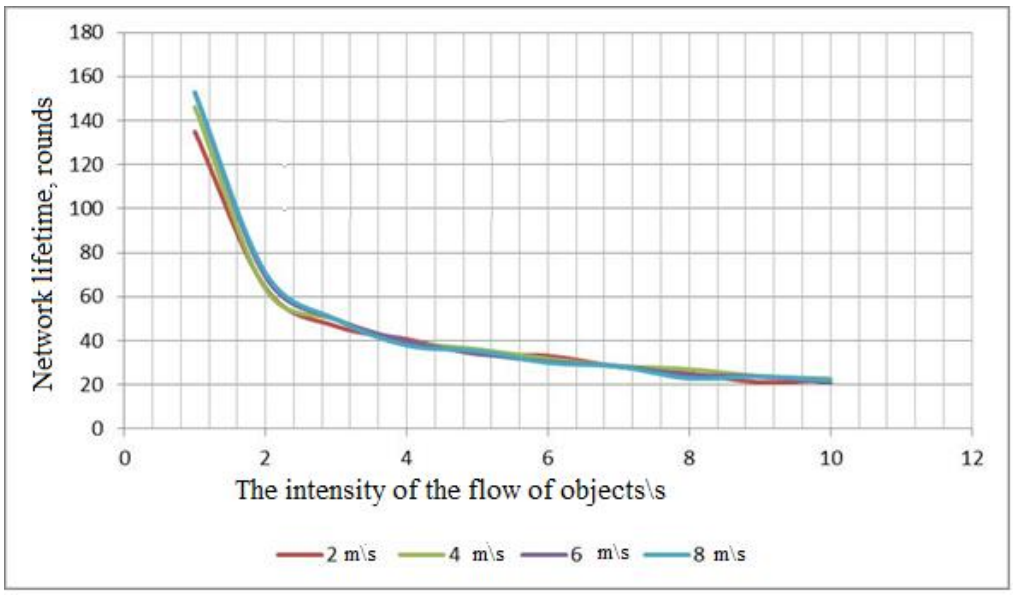

Fig. 7. The duration of the life cycle of a wireless sensor network under the influence of Poisson flow and different values of the movement speed of sensor nodes

Therefore, another direction of creating fake structures in Internet of Things application networks is cloning elements of such networks.

A real work is devoted to the study of erroneous event streams and their impact on wireless sensor networks. Next, we'll cover the basics of false clouds and cloning, which also apply to false IoT structures.

The concept and implementation systems of false clouds are presented in [7]. There are also protection systems against the collection of information by false clouds. In order to gain access to confidential data that goes from a regular Internet thing to the cloud, it is suggested to use systems for cloning packages and sending them to a duplicate cloud (fake cloud).

To send data to the Internet cloud, a thing must have a connection to an access point of a public communication network. Interception and redirection of data can be implemented in the immediate vicinity of the "Internet thing - access point" communication channel [8]. The protection system against the use of false clouds based on the application of hybrid encryption algorithms (RSA-512 and AES-128) requires a relatively large computing power of the Internet of Things and cannot be implemented for things with a CPU bitrate, because as well as devices with a small amount of memory.

In [9], a method for creating unique patterns of Internet of Things network traffic is proposed, which can be used both in low-power Internet of Things with a microcontroller and in more powerful things with microprocessors.

The miniaturized size and low cost of such Internet of Things as sensor nodes, as well as the self-organization of these nodes into a network, have contributed to the emergence of new methods of penetration into Internet of Things applications, which have come to be known as cloning. . Cloning of individual sensor nodes is considered [10]. However, both individual nodes and sensor fields as a whole and its fragments are suitable for cloning.

The analysis of research conducted in the field of building wireless sensor networks showed that the main efforts are aimed at increasing the life cycle of wireless sensor networks by reducing energy costs and increasing residual energy.

The aim of research

The work is devoted to the problems of providing secure wireless sensor networks, which gives grounds for a detailed study of the effects on the energy system of these networks and the development of protection systems against intrusions into wireless sensor networks associated with attempts to reduce the life cycle of a wireless sensor network by reducing residual energy.

The main material

We proposed the following model for conducting research. False objects move from the side of the boundary d (Fig. 8). At the same time, the point at which the object enters the sensor field is random, and the value in y is distributed uniformly on the segment [0; h] (Fig. 7). The point of exit of the object from the sensory field has similar properties: the value yout is distributed evenly on the segment [0; h].

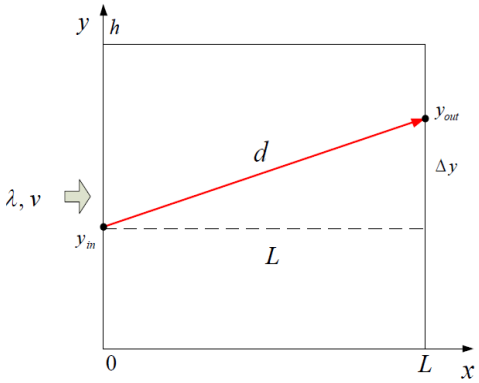

Fig. 8. Model of the trajectory of the flow of false events in the sensory field

The distance traveled by object d can be calculated as follows:

$$d = \sqrt{L^2 - (y_{out} - y_{in})^2} = \sqrt{L^2}\ , \qquad (1)$$

Since the values in y and out y have a uniform probability distribution, their difference Δy has a Simpson distribution (triangular distribution) on the interval [0; h]:

$$f(y) = \begin{cases} 0 & y < 0 \\ 2\dfrac{(h-y)}{h^2} & 0 \le y \le h \\ 0 & y \ge h \end{cases}, \qquad (2)$$

Then the probability density of the distance traveled by the object can be defined as:

$$f(\omega)=\begin{cases}0\\ 2\dfrac{\omega}{h^2}\left(\dfrac{h}{\sqrt{\omega^2-L^2}}-1\right)\\ 0\end{cases}, \qquad (3)$$

The corresponding probability density is shown in Fig. 9.

From (3) it is possible to determine the mathematical expectation of the distance traveled by the object before crossing the boundary of the sensory field:

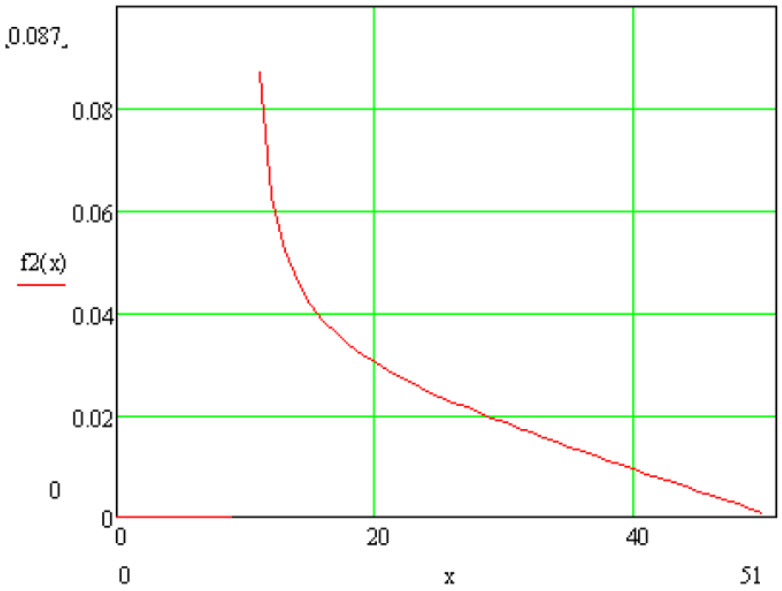

Fig. 9. Probability density of the distance traveled by the flow of false events

$$\hat{\omega}=\sqrt{L^2+h^2}+\frac{L^2}{h}\ln\left(\frac{\sqrt{L^2+h^2}+h}{L}\right)+, \qquad (4)$$
$$+\frac{2}{3h^2}\left(L^3-\sqrt{(L^2+h^2)^3}\right)$$

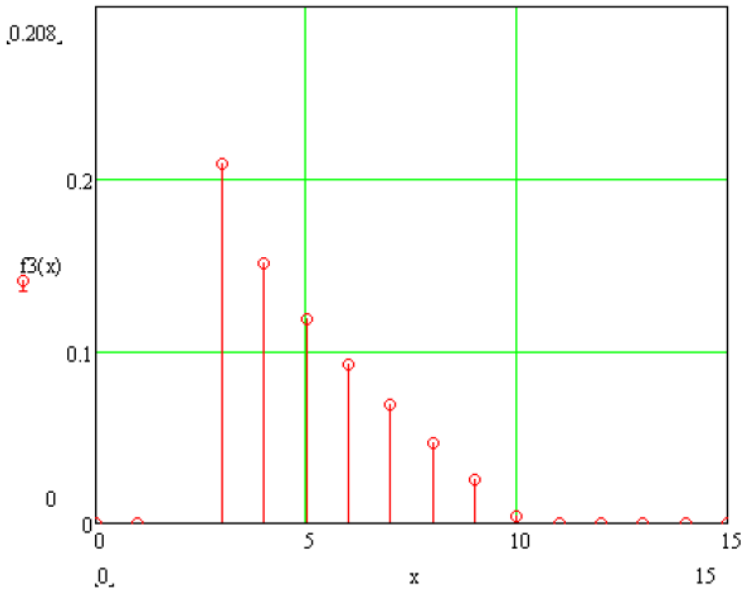

Fig. 10. Probability density of the number of messages

Passing through the sensor field, the object falls into the detection zones of a certain number of nodes, as a result of which each of these nodes produces a message that is transmitted over the network. The number of produced messages affects the parameters of the network's functioning, because during the transmission of a message, network nodes consume energy, the reserve of which is limited. The number of nodes on the path of the object can be estimated based on the properties of the sensory field:

$$\overline{m} = 2r\rho \cdot \hat{\omega}, \qquad (5)$$

Taking into account (4) and (5), it is possible to determine the probability density of the number of messages transmitted when the object passes through the sensor field as:

$$f(m) = \begin{cases} 0 & m < 2L\rho r \\ \dfrac{m}{2(\rho r)^2} \cdot \left(\dfrac{h}{\left(\dfrac{m}{2(\rho r)} \right)^2} - 1 \right) & 2L\rho \le m \le 2\rho r\sqrt{L^2 + h^2} \\ 0 & m > 2\rho r\sqrt{L^2 + h^2} \end{cases}, \qquad (6)$$

The mathematical expectation of the number of messages will then be equal:

$$\overline{m} = 2\rho r\sqrt{L^2 + h^2} + \frac{4\rho r}{3h^2}(L^3 - \sqrt{(L^2 + h^2)^3}) + \\ + \frac{2L^2\rho r}{h} \ln\left(\frac{\sqrt{L^2 + h^2} + h}{L} \right), \qquad (7)$$

From (7), it is possible to determine the energy consumption of sensor nodes and, accordingly, the life cycle of the sensor network.

A wireless sensor network intrusion model is developed to reduce the network lifecycle, which differs from the known ones in that it uses spurious event streams to achieve this goal. The model is developed on the basis of typical geometric, quantitative and energy parameters of wireless sensor networks using a basic clustering algorithm for a homogeneous mobile sensor network under network intrusion of Poisson and deterministic flows of false events.

Discussing

To confirm the results obtained in the work, a number of additional experiments were conducted aimed at evaluating the dependence of the informativeness of features on the following characteristics of the network:

-topologies;

-packet generation periods;

-degrees of randomness in choosing destination addresses.

The informativeness of the features of the cluster tree was evaluated. The results are shown in Fig. 11. It can be concluded that there is a tendency to a general increase in the informativeness of signs with an increase in the period of statistics collection. In addition, the existence of signs capable of separating abnormal behavior from normal behavior is once again confirmed.

To compare the most informative features for different topologies (cellular network and cluster tree), the maximum period of statistics collection was chosen - 360T.

In Fig. 12 presents the most informative features.

Fig. 13 shows the dependence of the features of the discretization parameter for the cluster tree topology network.

When analyzing the results, the following conclusions can be drawn:

1. In the case, the informativeness of features for the "cluster tree" network topology is higher than the informativeness for a cellular network;

2. For a network with a "cluster tree" topology and a cellular network, for the most part, the same features are informative.

The following experiment is implemented by assigning to each node the eigenvalues of the mathematical expectation for normal distributions that determine the period of packet generation. Mathematical expectations in the first case are the same and equal to 10 (which was considered above), in the second case they are assigned arbitrarily.

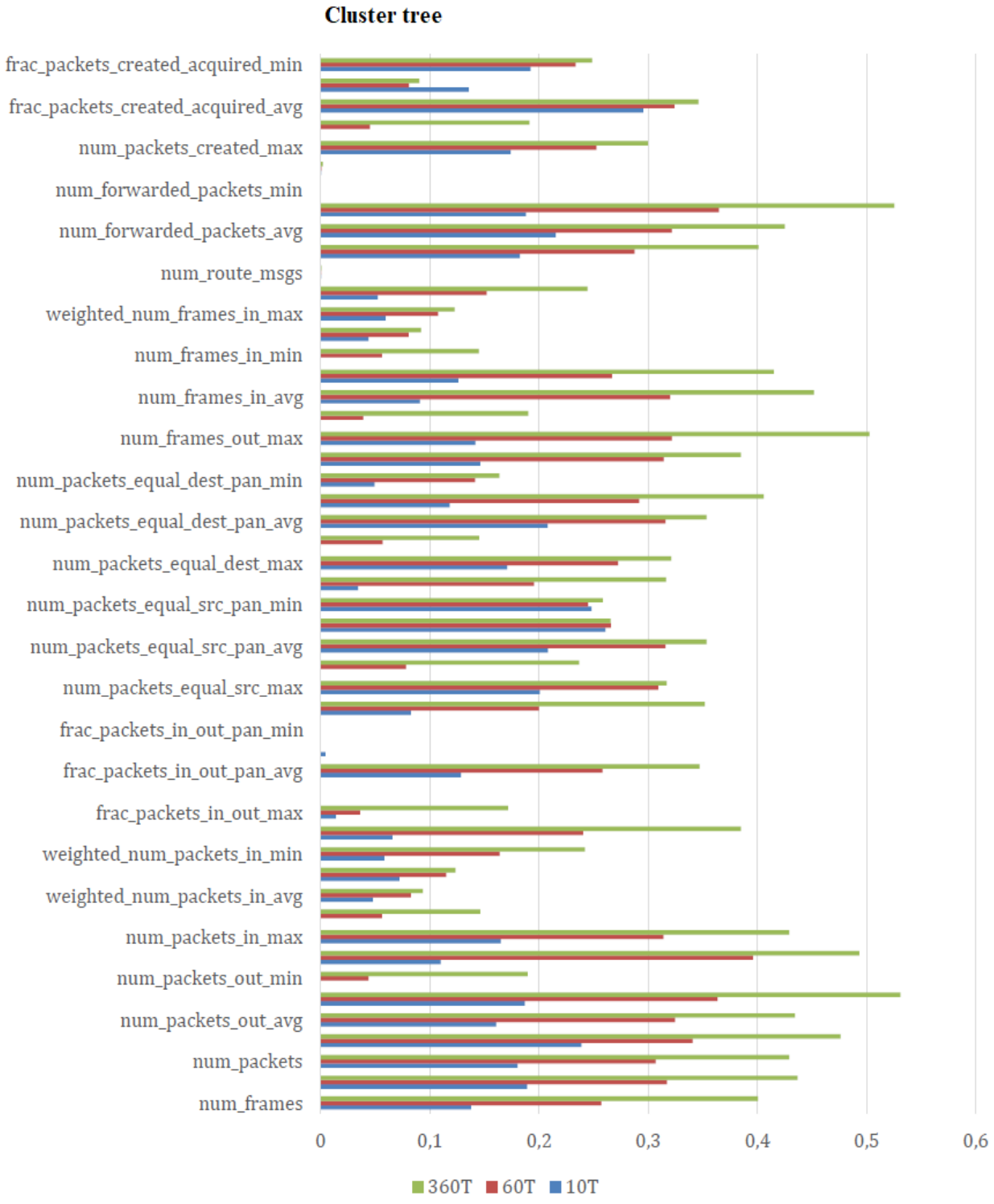

Fig. 11. Informativeness of features for the "cluster tree" topology network according to Shannon's method

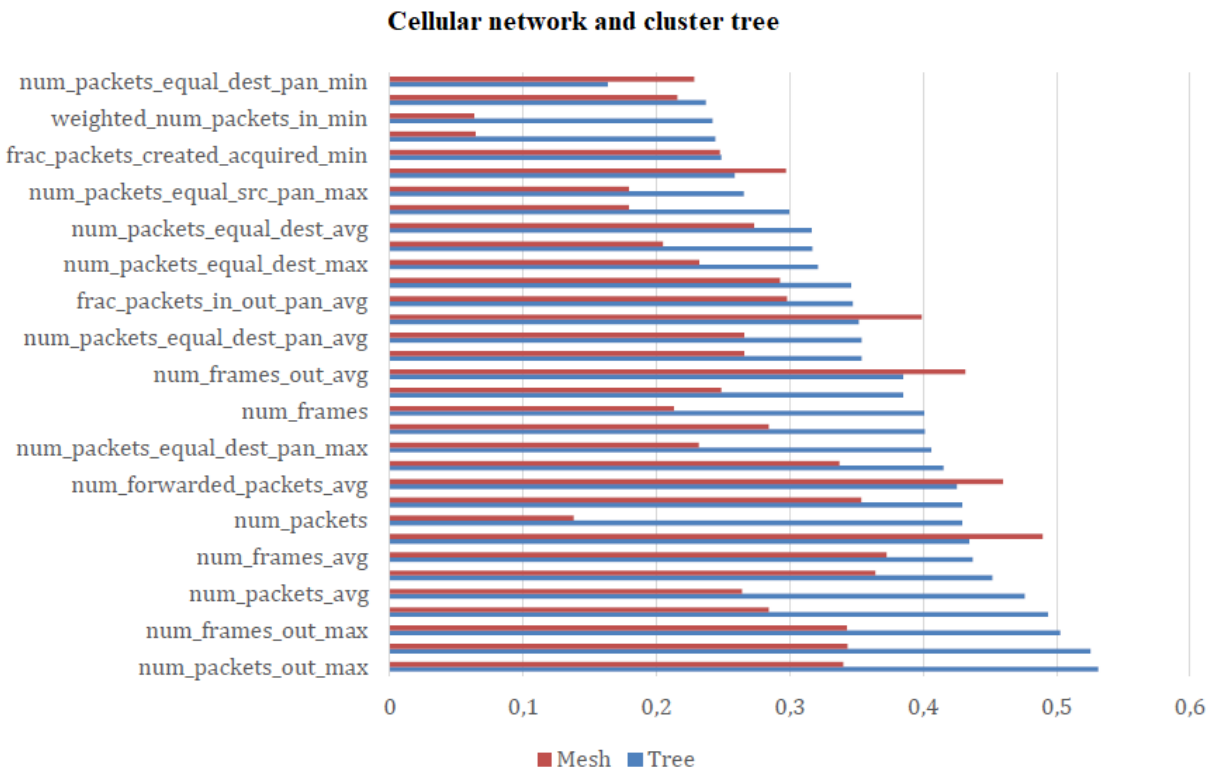

Fig. 12. Informative features for cluster tree and cellular network topology

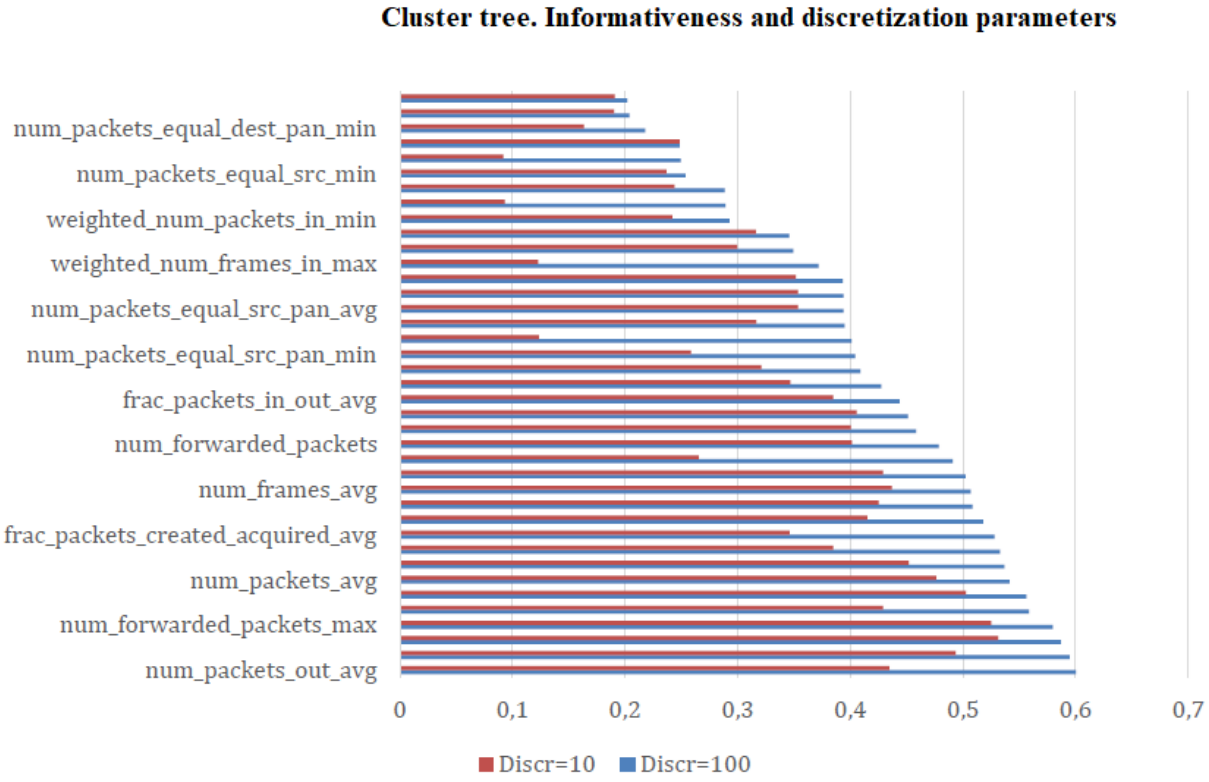

Fig. 13. Informativeness and the discretization parameter in a network with a "cluster tree" topology

The second part of the experiment consists in assigning to each node of the network (with the exception of one - the coordinator) an address to which all packets generated by this node are sent. Message forwarding routes are configured so that selective forwarding, retransmission, and funnel attacks make sense.

It is worth noting that for the case of deterministic forwarding, attacks such as elective_forward_dest and repeated_transmission_dest are not simulated, since these attacks in such networks are reduced to the usual selective forwarding and repeated transmission.

The generalized results of the experiment are presented in fig. 14. Just as in the case of the cluster tree and cellular network comparison, features that do not belong to the rank of non-informative are depicted. It is worth noting that scores were obtained by three methods of assessing informativeness for any pair of "normal-abnormal behavior" classes. These results are not given in the work due to the large volume of information. The general conclusion is the same as for the similar assessment of the tree-like structure: for most types of attacks there are absolutely informative features, which theoretically determines the high accuracy of classification methods based on algorithm compositions.

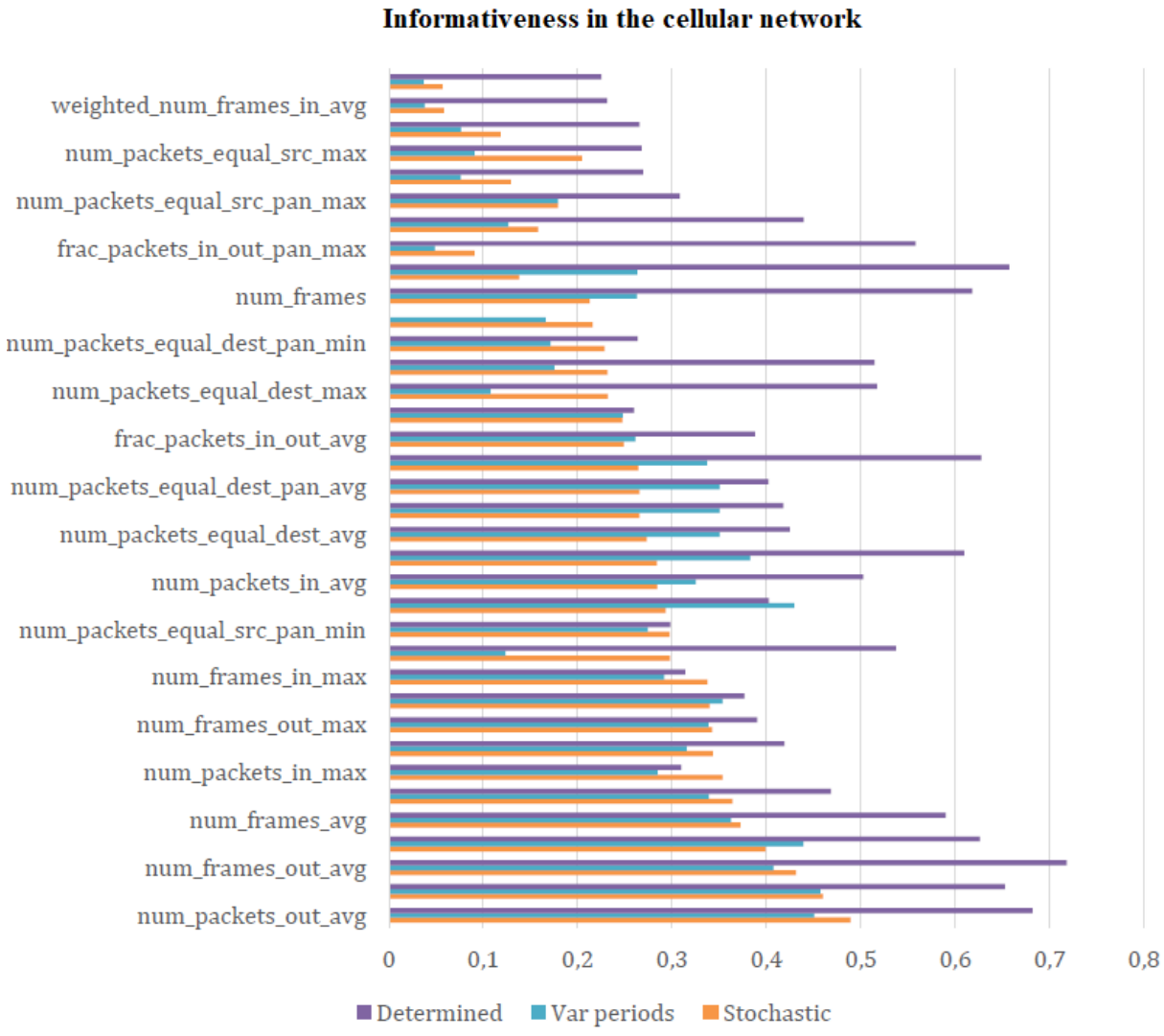

Fig. 14. Informativeness of features in a network with a porous topology depending on various network parameters

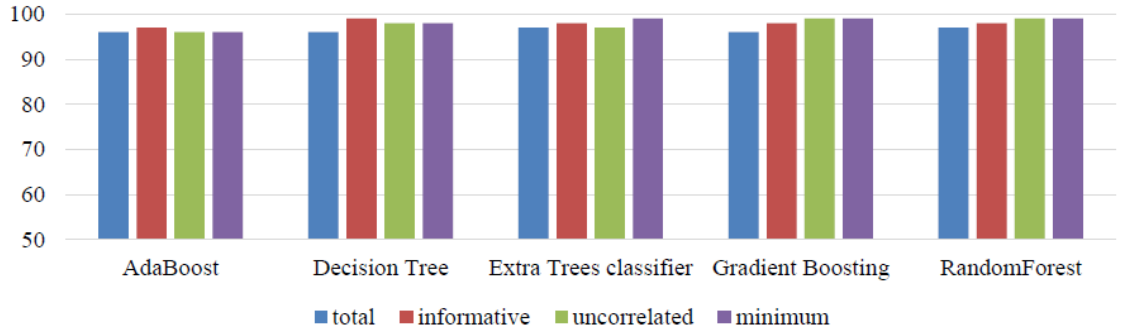

Fig. 15. Accuracy of multiclass classification when cutting off individual cases

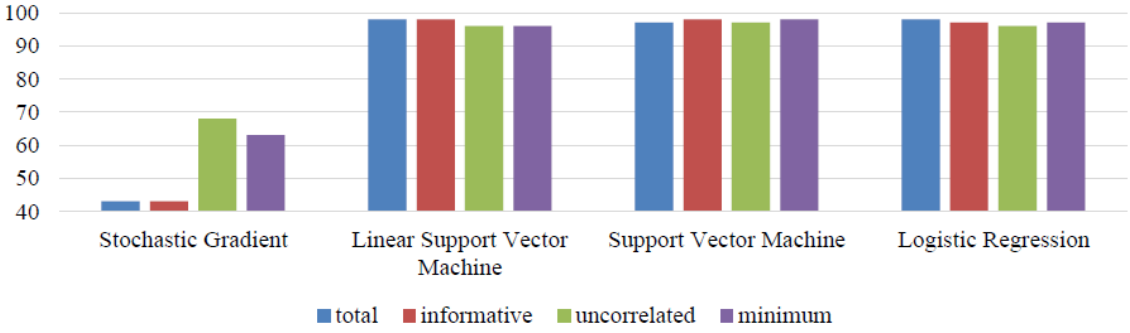

Fig. 16. Accuracy of linear classification when cutting off individual cases

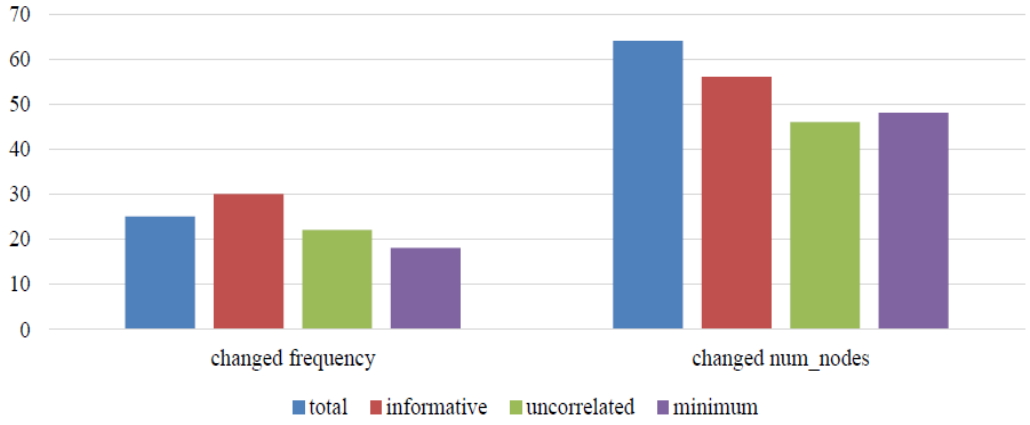

Fig. 17. Accuracy of classification when cutting off private types of streams of false events based on the DecisionTree algorithm

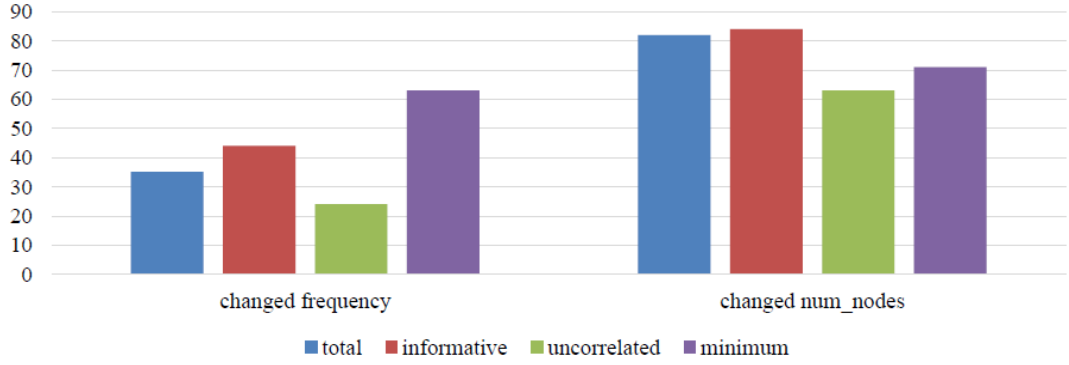

Fig. 18. Accuracy of classification when cutting off private types of streams of false events based on the Random Forest algorithm

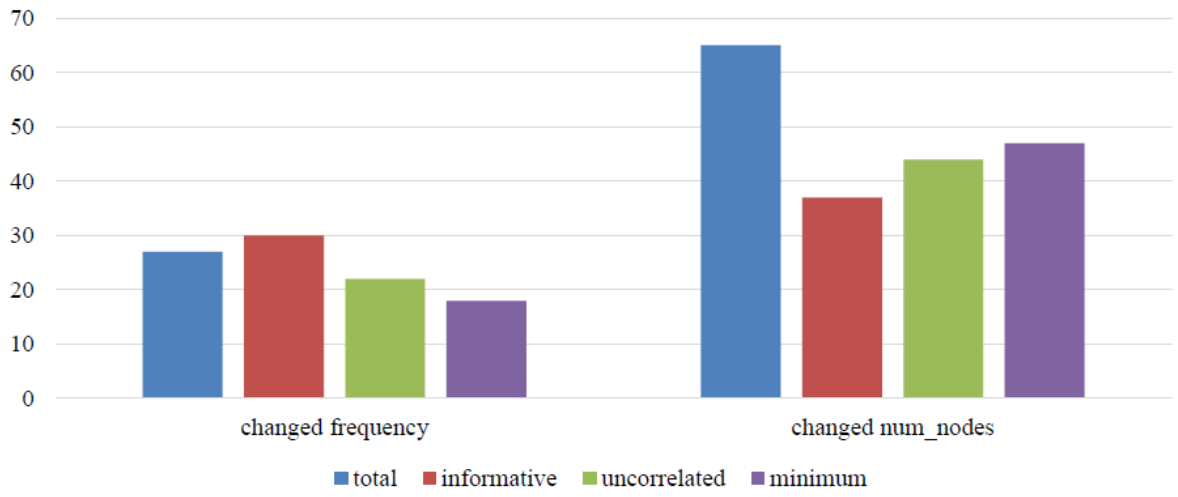

Fig. 19. Accuracy of classification when cutting off private types of streams of false events based on the DecisionTree algorithm

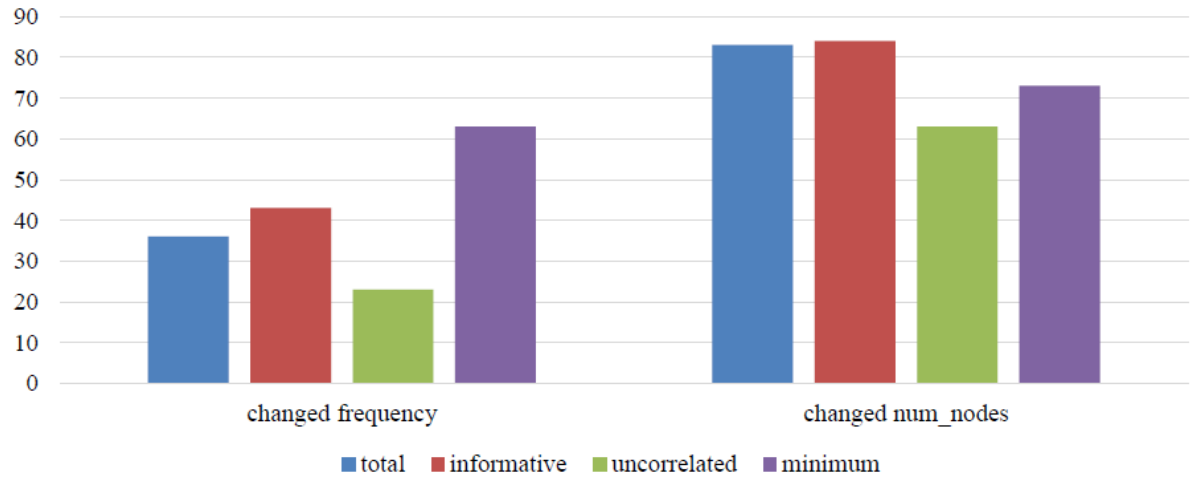

Fig. 20. Accuracy of classification when cutting off private types of streams of false events based on the RandomForest algorithm

In order for an attacking node to be able to carry out an attack, it is necessary that packets with a certain sender or recipient address pass through it. In the case of a network with stochastic addressing, this is quite rare. So, with five nodes in some PAN, only every fifth packet will meet the required condition. At the same time, the attacking node cannot reject all packets corresponding to a certain address and passing through it, because in this case it will be quickly detected by the attacked node. Therefore, most often attackers exert abnormal influence selectively on only part of the packets. As a result, statistically, some types of attacks may not appear even during a one-hour statistics collection period.

The following conclusions emerge from the analysis of the given information:

1. Informativeness of features in a network with deterministic routes is usually higher than informativeness in a stochastic network.

2. The number of informative features in a network with deterministic routes is usually greater than the number in a stochastic network.

3. Informativeness depends little on the ratio of packet generation periods by different nodes, which once again emphasizes the validity of the formula for calculating the cumulative frequency of packet generation.

The inverse size – the average packet generation period – is extremely important

because it partly determines the size of the statistics collection period.

The obtained data show that there is no significant difference with the results of the informativeness assessment. So, it is possible to come to the disappointing conclusion that from most options, regardless of the degree of randomness in the choice of addresses and other parameters, the most informative signs are the same.

As already mentioned earlier, among the classes of behavior there are individual cases of attacks on wireless sensor networks, which in the sample were marked with the suffixes _exact_dest and _exact_src. These special cases correspond to the application of malicious influence to packets corresponding to a specific sender or recipient address.

Consider the accuracy of classification when cutting off variations (private cases) of attacks. The results are shown in fig. 15 and 16.

Therefore, the classification accuracy when cutting off individual cases increases significantly and reaches 97% even for machine learning algorithms that previously did not work well. In this way, an intermediate conclusion can be drawn: the proposed behavior profile model allows determining the behavior of BSM with almost 100% accuracy.

Let's consider the work of classifiers when the number of nodes and average periods of packet generation change. The classifier was trained on a sample obtained for 15 nodes with an average packet generation period of 10 seconds. As test samples were used:

1. Sample obtained for 20 nodes with an average packet generation period of 10 seconds.

2. Sample obtained for 15 nodes with an average packet generation period of 5 seconds.

The classification accuracy for the decision tree and the stochastic forest is presented in Fig. 17 and 18. In fig. 19 and 20 present the classification accuracy when cutting off certain types of streams of false events.

Based on the above, it can be concluded that a change in the number of nodes has a less detrimental effect on the classifier than a change in the average packet generation periods. At the same time, the accuracy of the classification is much lower than that obtained earlier in the case of an unchanged number of nodes and statistical characteristics.

Conclusions

The functionality of the proposed behavior scenario model and identification subsystem was tested for topologies of cellular network and cluster tree, characteristics of the wireless sensor network (packet generation period, degree of randomness in the selection of destination node addresses), changes in the confidence level parameter, and changes in the a priori probability of normal behavior.

The effectiveness of the attack identification process was evaluated using the developed model of the behavior scenario of the identification subsystem on wireless sensor networks in comparison with existing studies. The increase in efficiency is 20%.

The parameters of the system of protection of wireless sensor networks against the flow of false events are determined by changing the structural characteristics of the sensor field, which consists in changing the distribution of the density of sensor nodes compared to a uniform one. It is proved that there is an optimal value of the density of nodes in the first and second regions of the sensor field, which ensures the maximum life time of the sensor network, and the corresponding numerical characteristics are determined for different values of the total number of nodes in the sensor field, as well as under conditions of different ratios of the intensities of false and real flows events

References

1. B. P. Deosarkar, N. S. Yadav and R. P. Yadav, "Clusterhead selection in clustering algorithms for wireless sensor networks: A survey," 2008 International Conference on Computing, Communication and Networking, 2008, pp. 1-8, doi: 10.1109/ICCCNET.2008.4787686.

2. S. Mody, S. Mirkar, R. Ghag and P. Kotecha, "Cluster Head Selection Algorithm For Wireless Sensor Networks Using Machine Learning," 2021 International Conference on Computational

Performance Evaluation (ComPE), 2021, pp. 445-450, doi: 10.1109/ComPE53109.2021.9752264.

3. A. Pang, F. Chao, H. Zhou and J. Zhang, "The Method of Data Collection Based on Multiple Mobile Nodes for Wireless Sensor Network," in IEEE Access, vol. 8, pp. 14704-14713, 2020, doi: 10.1109/ACCESS.2020.2966652.

4. Salam, Abdu & Javaid, Qaisar & Ahmed, Masood. (2020). Bioinspired Mobility-Aware Clustering Optimization in Flying Ad Hoc Sensor Network for Internet of Things: BIMAC-FASNET. Complexity. 20. 1-20. 10.1155/2020/9797650.

5. Pasandideh, F.; da Costa, J.P.J.; Kunst, R.; Islam, N.; Hardjawana, W.; Pignaton de Freitas, E. A Review of Flying Ad Hoc Networks: Key Characteristics, Applications, and Wireless Technologies. *Remote Sens.* 2022, *14*, 4459. https://doi.org/10.3390/rs14184459.

6. K. Hakimzadehy, P. K. Nicholsonz, D. Lugonesz and A. H. Payberahy, "IMITA: Imitation Learning for Generalizing Cloud Orchestration," 2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid), 2021, pp. 237-246, doi: 10.1109/CCGrid51090.2021.00033.

7. D. Moscoso-Montenegro and L. Serpa-Andrade, "Design and experimental tests of a LoRaWAN based beacon system for cyclist with automatic crash detection," 2019 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC), 2019, pp. 1-6, doi: 10.1109/ROPEC48299.2019.9057053.

8. Z. Ma, L. Feng and F. Xu, "Design and Analysis of a Distributed and Demand-Based Backscatter MAC Protocol for Internet of Things Networks," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 1246-1256, Feb. 2019, doi: 10.1109/JIOT.2018.2869015.

9. T. T. Jui, M. N. Hoq, S. Majumdar and M. S. Hossain, "Feature Reduction through Data Preprocessing for Intrusion Detection in IoT Networks," 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2021, pp. 41-50, doi: 10.1109/TPSISA52974.2021.00005.

10. X. Ding, F. Xiao, M. Zhou and Z. Wang, "Active Link Obfuscation to Thwart Link-flooding Attacks for Internet of Things," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 217-224, doi: 10.1109/TrustCom50675.2020.00040.

The article has been sent to the editors 08.11.22.
After processing 11.11.22.