http://doi.org/10.35784/iapgos.3076 *received: 20.09.2022 | revised: 10.12.2022 | accepted: 15.12.2022 | available online: 30.12.2022*

MONITORING OF LINK-LEVEL CONGESTION IN TELECOMMUNICATION SYSTEMS USING INFORMATION CRITERIA

Natalia Yakymchuk, Yosyp Selepyna, Mykola Yevsiuk, Stanislav Prystupa, Serhii Moroz
Lutsk National Technical University, Faculty of Computer and Information Technologies/ Department of Electronics and Telecommunications, Lutsk, Ukraine

Abstract. *The successful functioning of telecommunication networks largely depends on the effectiveness of algorithms for detection and protection against overloads. The article describes the main differences that arise when forecasting, monitoring and managing congestion at the node level and at the channel level. An algorithm for detecting congestion by estimating the entropy of time distributions of traffic parameters is proposed. The entropy measures of data sets for various types of model distribution, in particular for the Pareto distribution, which optimally describes the behavior of self-similar random processes, were calculated and analyzed. The advantages of this approach include scalability, sensitivity to changes in distributions of traffic characteristics and ease of implementation and accessible interpretation*.

Keywords: telecommunication systems, self-similarity factor of network traffic, congestion detection

MONITOROWANIE PRZECIĄŻEŃ NA POZIOMIE ŁĄCZA W SYSTEMACH TELEKOMUNIKACYJNYCH Z WYKORZYSTANIEM KRYTERIÓW INFORMACYJNYCH

Streszczenie. *Pomyślne funkcjonowanie sieci telekomunikacyjnych w dużej mierze zależy od skuteczności algorytmów wykrywania i ochrony przed przeciążeniami. W artykule opisano główne różnice, jakie pojawiają się przy prognozowaniu, monitorowaniu i zarządzaniu przeciążeniami na poziomie węzła i na poziomie kanału. Zaproponowano algorytm wykrywania przeciążeń poprzez estymację entropii rozkładów czasowych parametrów ruchu. Obliczono i przeanalizowano miary entropii zbiorów danych dla różnych typów rozkładów modelowych, w szczególności dla rozkładu Pareto, który optymalnie opisuje zachowanie samopodobnych procesów losowych. Do zalet tego podejścia należy skalowalność, wrażliwość na zmiany rozkładów parametrów ruchu oraz łatwość implementacji i przystępnej interpretacji.*

Słowa kluczowe: systemy telekomunikacyjne, współczynnik samopodobieństwa ruchu sieciowego, wykrywanie przeciążeń

Introduction

In accordance with modern standards of network management systems and concepts of the development of the networks themselves, there is a need to determine the state of the system in its mode of operation. The most popular model provides that network components can accept only two states: „serviceable" (able to work) and „refuse" („disrepair"). The state of a network component is a random value that does not depend on the state of other components [20].

A crucial state of a network (computer, telecommunication, etc.) is the state of overloading of individual network nodes, data transmission routes, and autonomous network segments. Typical symptoms of congestion are packet loss, excessive packet delay, and reduced quality of service (QoS) in the network. This state can be taken by mistake for equipment refusal (and vice versa). Therefore, control and removal of overloads are important tasks of a statistical character [14].

Node-level congestion is detected by examining the buffer utilization and the interval between the consecutive data packets. Because a congestion condition usually occurs when the traffic load on a particular node exceeds the available buffer capacity of that node. If, when monitoring buffer occupancy, a load of 70% or higher was obtained, the interval between two consecutive packets is checked. Obviously, if the interval is small, the chances of buffer overflow will be high, which will increase the probability of packet loss. A large interval indicates that the node's bandwidth will be sufficient for the given traffic flow [10, 11].

Link-level congestion happens because of the unfair utilization of network resources. Link-level congestion is monitored through channel utilization. In this case, network flows are analyzed and not individual network packets (network flows are one-way meta-information about network packets that have the same source and destination IP address and ports, as well as the IP protocol type) [3, 4].

1. Literature review

The hidden disadvantage of overloads is that they reinforce themselves according to the principle of feedback [6]. If a collision occurs at a particular location on the network, if the client times out, the client will often resend requests. This increases the load on the system [22, 24]. If the call graph in a service-oriented architecture is deep enough (that is, a client calls a service that calls other services, and those call other services), and each level has several retries, then the load at the lower level will cause a cascading increase their number and the exponential increase in load [19].

Then, all the work already done by the server on this request will be wasted. And in the case of system overload, when resources are limited, it cannot afford to lose resources [8].

In order to monitor the risks of the occurrence of such situations, it is necessary to monitor the time parameters of the traffic flow constantly. However, the analysis of the averaged values of the traffic characteristics gives us a smoothed view of the process, in which it is not possible to track the appearance of load fluctuations, which are characteristic of heterogeneous traffic „Triple Play" (voice + video + data) or „Quadruple Play" (voice + video + data + mobile subscribers) [23].

The specific characteristics of such traffic are explained by the high degree of the grouping of packets at client sites, in routers, and in switching nodes of information communication networks. Even if the source generates a regular stream of packets, the data is delivered to the consumer in bursts interspersed with idle intervals. The reasons for this are the limited speed of network devices, insufficient volume of buffers, etc. To detect this kind of anomaly, an analysis at the level of total traffic is required, based on the use of statistical methods and information theory [21].

Entropy analysis is one of the types of behavioral methods for detecting anomalies, unlike wavelet analysis and spectral analysis; it is not characterized by the complexity of implementation and the requirements for big-time expenditures. Information analysis gives us a statistical criterion for determining anomalous traffic behavior. Today, methods for detecting DOS/DDoS attacks and some types of virus programs have been developed. The method of dividing traffic into unique network flows and calculating the entropy of a set of these flows by the IP address of the source has shown its effectiveness [2, 9].

By comparing the predicted entropy values with the real ones, a decision is made about whether the traffic belongs to a standard type, a DOS attack of a certain intensity, or peak values of legitimate traffic [1]. Estimating the entropy of the number of packets within a time window for network flows can be a tool for detecting „scanning" attacks [15].

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Utwór dostępny jest na licencji Creative Commons Uznanie autorstwa – Na tych samych warunkach 4.0 Miedzynarodowe.

2. Researches methodology

The main statistical characteristics of the random process of traffic transmission lead to gross errors in the assessment and prediction of system behavior. Options are possible when the average load values of network nodes over a long period are approximately the same, but the internal structure of the processes that take place is different [16, 17].

One type of traffic can change smoothly over time; the other can be characterized by significant bursts of activity, while the dependence on probabilities will be low. The choice of the distribution law for the characterization of random processes of information transmission is of great importance.

The numerical characteristic of the distribution, which can be a measure of its uncertainty, is the entropy of the distribution law. For the discrete distribution of the increase

$$H(m) = -\sum_{i=1}^{m} p_i \, log p_i \quad (1)$$

where p_i is the probability of the i state of the system, m is the number of all possible states of the system.

From the entropy properties, it can be seen that the entropy of the experiment with maximum uncertainty is maximum and minimum in the fully „determined" experiment. Entropy is in a certain sense additive: when uncertainty increases due to an increase in the number of outcomes, entropy increases, and the increase in entropy is proportional to the probability of additional outcomes. These properties show that the entropy defined by relation (1) is a reasonable measure of the uncertainty of a stochastic experiment with a finite number of outcomes.

Entropy does not depend on significance, which is a random value, but only on their probabilities, in fact, one is interested not in the absolute value of entropy, but in comparing the entropies of different laws. We will form a strategy for finding overloads based on the information criterion [5, 7].

To carry out the analysis procedure of congestion detection by estimating the entropy of time series, it is necessary to select the parameters of the assessment. To do this, consider the following criteria:

1) The length of the sliding window. This is the size of the interval in which point values of entropy time series are calculated. Small windows are very sensitive, and on the one hand, this will increase the detection rate, on the other hand, the frequency of false alarms will also increase. This will lead to the implementation of a traffic restriction policy, which will negatively affect the quality of the service. Large windows are relatively insensitive, which leads to the opposite effect. Windows of 5 to 10 minutes are used as a compromise.

2) The overlap size of sliding windows. Overlapping sliding windows results in a more detailed time series. We want to make our system respond as quickly as possible to sudden changes, so we chose a relative overlap of 80%.

3) The size of the sliding window for calculating variances. We decided to set the size of the sliding window to calculate the standard deviation up to 24 hours. Most often, such a sliding window covers the entire seasonal cycle. In other cases, we recommend choosing windows that are multiple 24 hours.

Each combination of parameters involves a trade-off: high detection rate at the expense of many false positives or vice versa.

To simulate traffic, we will use the distribution of traffic falling into a time window of fixed duration, using the ratio of transmission delay to the maximum permissible transmission interval or successful data transmission of one of the network nodes as a probability [18].

The main idea of the algorithm is to constantly make short-term predictions and determine the difference between the predictions and the actually observed entropy value. Entropy serves as an indicator of the equilibrium of the process. Thus, sharp changes in entropy indicate a qualitative change in the structure (through changes in the distributions of characteristics) of the system [12, 13].

The analysis of the time characteristics of the network is based on the model or geometric distribution of the probability of sending a packet by each terminal node of an autonomous network segment. In the case of a mixed (heterogeneous) network, each device is allocated an approximately equal time interval in traffic.

As emphasized above, entropy is the most general measure of evaluating the efficiency of information transmission for probability distributions belonging to at least one type (in this case – to the discrete type). Let us present the comparative entropy characteristics of model distributions.

1. The geometric distribution is inextricably linked with the binomial distribution. The difference is that the binomial random variable determines the probability m of success in trials n, while the geometric random variable determines the probability n of trials up to the first success (including the first success).

2. A random variable uniformly distributed on [$-a; a$] has the highest entropy among all random variables distributed on [$-a; a$].

3. The exponential distribution with the parameter λ has the largest entropy among all distributions defined on the semi-axis $[0; \infty]$ with mathematical expectation λ.

4. On the entire straight line, among all distributions with fixed mathematical expectation and variance, the normal distribution has the greatest entropy.

The entropy of a discrete source is always positive. Differential entropy $H(x)$, unlike the entropy of sources of discrete messages, can take positive, negative, and zero values. Differential entropy, in contrast to the usual entropy of a discrete source, is not a measure of its own information contained in an ensemble of values of a random variable. It depends on the scale X and can take negative values because the information meaning has not the absolute value of the differential entropy, but the difference between two differential entropies, which explains its name.

Differential entropy does not change when all possible values of a random variable are changed to a constant value. Indeed, the scale X does not change, and equality is fair:

$$h(x + C) = -\int_{-\infty}^{\infty} w(x + C) log_2 w(x + C) d(x + C) = \\ = -\int_{-\infty}^{\infty} w(x) log_2 w(x) d(x) \quad (2)$$

From this it follows that it does not depend on the mathematical expectation of a random variable, since changing all values $x+C$ to x, we thereby change its average to C, that is, the mathematical expectation.

Differential entropy is additive, i.e. for the union $x \cup y$ of independent random variables and the equality holds:

$$H(x \cup y) = H(x) + H(y) \quad (3)$$

For example, consider the subnet shown in Fig. 1. As a result of overlapping traffic flows, the bandwidth of the channel is not sufficient to ensure the required quality of service. Routers L, G, B, C, J are overloaded. Identifying these channels and removing them from the network will avoid information loss. For this purpose, a possible route of the virtual channel bypassing congested lines is established (shown by a dashed line).

At the same time, a compromise is reached between the host and the subnet during the establishment of a virtual channel, which determines the volume and form of traffic, the required quality of service and other parameters. As fulfillment of its part of the agreement, the subnet usually reserves resources in the path of the channel being created. These resources include memory for buffers and router tables and line bandwidth. With this approach, the occurrence of congestion in the new virtual channel is unlikely, since all the necessary resources have been reserved and their availability is guaranteed.

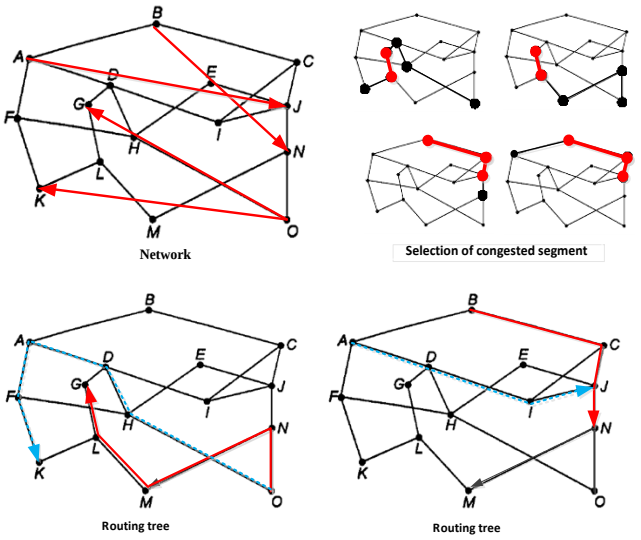

Fig. 1. Link-level congestion

In the case of the geometric distribution, we carry out independent transmissions of the test packet until „success" appears. To calculate entropy $H_G(x)$ let's make a state diagram with the probability of „success" $p < 1$ and „failure" $q < 1$. Obviously $p + q = 1$.

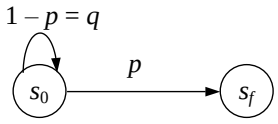

Fig. 2. System states

The system is in the initial state S_0. Having achieved success, it passes into an irreversible (absorbing) state S_f (Fig. 2). Thus, the random process is not transitive (not transitional to the previous state). The graph of transitions has the following form (Fig. 3). S_+ – transition state upon the success of the test; S_- – transition state in case of test failure; $H_{Gi}(x)$, $i = 1, 2, \ldots, n, \ldots$ is the entropy of the distribution upon success at the i step.

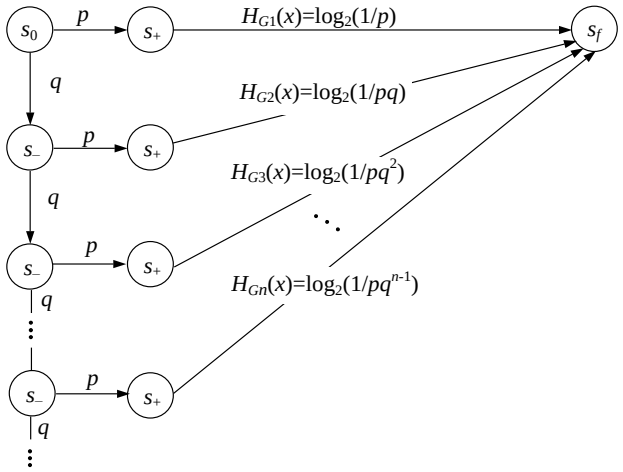

Fig. 3. The graph of transitions

Then the current entropy of the geometric distribution would be calculated using the following formulas:

$$\begin{gathered} H_G(x) = -plog_2p - pqlog_2(pq) - \cdots - pq^{n-1}log_2(pq^{n-1}) = \\ = -(1 + q + \cdots + q^{n-1} + \cdots)plog_2p - \\ -pq(1 + 2q + \cdots + +nq^{n-1})log_2q; \\ 1 + q + \cdots + q^{n-1} + \cdots = \frac{1}{1-q} \\ 1 + 2q + \cdots + nq^{n-1} + (n+1)q^n = \frac{1}{(1-q)^2} \\ H_G(x) = -log_2p - pq\frac{1}{(1-q)^2}log_2q = -log_2p - \frac{q}{p}log_2q \end{gathered} \tag{4}$$

In specialized networks, these assumptions are not fully fulfilled. As noted above, network traffic is usually heterogeneous (voice, video, data) and self-similar in nature. Its statistical characteristics can no longer be described by traditional. In this case, distributions with so-called „heavy tails" (Pareto, Weibull, gamma, and beta distributions) are used.

3. Results

Distributions with heavy tails are distributions in which large but rare events (outliers) cannot be neglected. All commonly used heavy-tailed distributions are subexponential.

Let us define the differential entropy for the exponential distribution. This distribution is widely used to determine the failure rate in electronic equipment.

$$\begin{gathered} f(x) = k \cdot e^{-kx}, x > 0 \\ h(x) = -\int_0^\infty k \cdot e^{-kx}(log_2k - k \cdot x \cdot log_2e)dx = \\ = -log_2k\int_0^\infty k \cdot e^{-kx}dx + log_2e\int_0^\infty x \cdot k \cdot e^{-kx}dx = \\ = -log_2k + log_2e = log_2\frac{e}{k} \end{gathered} \tag{5}$$

The total entropy for the exponential distribution is:

$$H(x) = h(x) - log_2\Delta x = log_2\frac{e}{k\Delta x} \tag{6}$$

The dependence of the entropy of the exponential distribution on the probability p of successful data transmission of one of the network nodes was calculated (Fig. 4). It can be seen that when the probability of success is set higher, the entropy of the distribution decreases, therefore, the required resource for data exchange decreases.

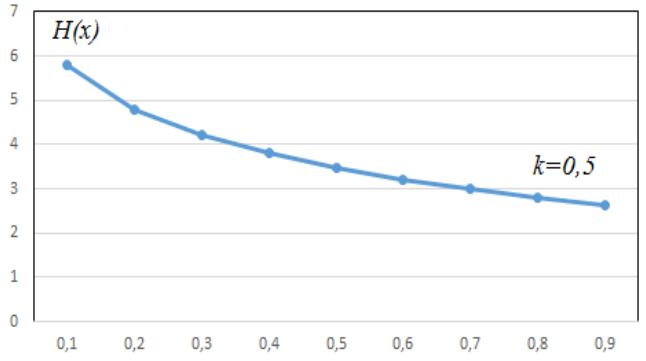

Fig. 4. Dependence of the entropy of the exponential distribution on the probability p of successful data transmission

To analyze the influence of the self-similarity factor of network traffic, an expression for the current entropy of the Pareto distribution as a typical distribution with „heavy tails" characteristic of self-similar traffic is derived:

$$H_p(x) = c\frac{log_2c}{ln2} \times \frac{x^{-c}}{-c-1} + (c-1)\left[x^{-c}log_2x - \frac{x^{-c}}{cln2}\right] \tag{7}$$

where c is a shape parameter.

At Fig. 5 shows graphs of the differential entropy of the Pareto distribution for the shape parameters 0.5 and 1. It can be seen that when the values x change, the entropy first decreases and then increases, which is explained by the influence of the „heavy tail" of the distribution. From the graphs presented in Fig. 5, it is seen that the total cost of Internet traffic increases when using the standard method, and when using the proposed method remains constant. This is due to the fact that when using the method described above, the flow of traffic occurs only when determining the correction factor on the first day of measurements. Further measurement of the bit rate of the Internet connection takes place without active data exchange, so traffic costs do not increase.

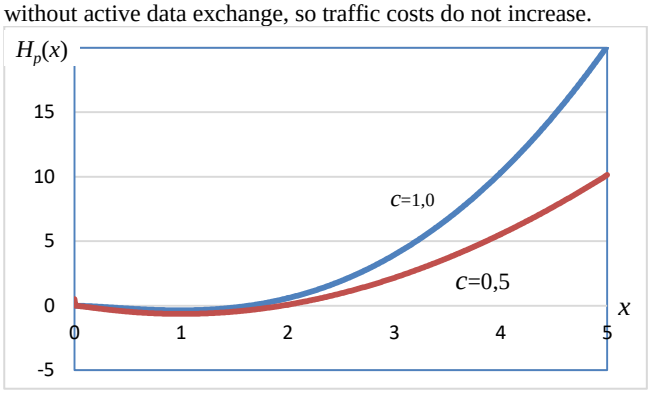

Fig. 5. Dependence of the entropy of the Pareto distribution for various parameters of the form

Note that when calculating entropy measures, you can use different parameters of model distributions. At the same time, comparative estimates based on entropy will be universal and clear.

The advantages of this approach include scalability (the proposed methods are able to use aggregated data, which makes it possible to use it in arbitrarily complex and highly loaded networks), sensitivity to changes in distributions of traffic characteristics and ease of implementation, and accessible interpretation (quickly ready to go, no need for training data).

In conclusion, it is necessary to note the main advantage of the described method: it allows you to effectively use the above methods in the study of networks operating at high load (with network utilization coefficients close to unity, i.e. on the verge of saturation), for their analytical modeling at arbitrary (in particular, small or normal) load.

In any case, congestion detection is the mechanism that usually initiates the procedure for launching management policies.

Congestion problems can be reduced by the fair distribution of resources in the network in identified areas. The composite routing metric is composed of the consumed energy (λ) of the sensor node, the participation level (η) of the sensor node, and the signal quality (Ω) between the sensor nodes. Amongst these three routing metrics, λ and η represent the characteristics of the sensor node, whereas, Ω represents the quality of the link between the sensor nodes. Each metric in the composite routing metric.

The mechanism must maintain routing entries in the routing table according to the least hops criterion to implement the shortest path to the receiver. Because there is a possibility that an inefficiently long route will be chosen to reduce congestion, which will increase the ETE delay. Due to the use of multiple paths, problems such as route coupling, contention, and channel access rate can occur, which can reduce network performance.

The goal of all congestion control methods is to limit the length of queues at nodes. Nevertheless, no method of dealing with the load provides a theoretical ideal. However, a good congestion control strategy avoids the collapse of bandwidth, bringing it closer to the ideal.

4. Conclusions

In the paper peculiarities of the occurrence of overloads in telecommunication networks at the node level and at the channel level are analyzed. The main causes and consequences of overloads are considered. A strategy for finding overloads based on the information criterion is proposed. The criteria for the selection of parameters for the evaluation of the congestion detection procedure by evaluating the entropy of time series have been determined. The entropy measures of data sets for various types of model distribution, in particular for the Pareto distribution, which optimally describes the behavior of self-similar random processes, were calculated and analyzed. The entropy of the Pareto distribution for the self-similarity coefficient of network traffic for various parameters of the form is presented.

In contrast to the methods of monitoring congestion in network nodes, the management of which consists in discarding redundant packets and limiting the speed of information transmission, which leads to a noticeable decrease in QOS parameters, the development of methods for detecting network congestion at the channel level will allow the application of a flow management policy based on the principle of „fair resources distribution". This will guarantee regulated quality indicators of consumer service. The estimation of the entropy of the proposed parameters of the time series will allow us to describe and predict the behavior of multimedia traffic data flows with higher quality, which belongs to the type of self-similar processes and is poorly described by traditional model distributions.

References

[1] Airehrour D., Gutierrez J. A., Ray S. K.: SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Generation Computer Systems 93, 2019, 860–876 [http://doi.org/10.1016/j.future.2018.03.021].

[2] Alashhab A. A., Zahid M. S. M., Azim M. A., Daha M. Y., Isyaku B., Ali S.: A Survey of Low Rate DDoS Detection Techniques Based on Machine Learning in Software-Defined Networks. Symmetry 14, 2022, 1563 [http://doi.org/10.3390/sym14081563].

[3] Bakhovskyy P. et al.: Stages of the Virtual Technical Functions Concept Networks Development. Cagáˇnová et al. (eds.): Advances in Industrial Internet of Things, Engineering and Management. EAI/Springer Innovations in Communication and Computing, 2021, 119–135 [http://doi.org/10.1007/978-3-030-69705-1_7].

[4] Bedin A., Chiariotti F., Kucera S., Zanella A.: Optimal Latency-Oriented Coding and Scheduling in Parallel Queuing Systems. IEEE Transactions on Communications 70(10), 2022, 6471–6488 [http://doi.org/10.1109/TCOMM.2022.3200105].

[5] Chughtai O., Badruddin N., Rehan M., Khan A.: Congestion Detection and Alleviation in Multihop Wireless Sensor Networks. Wireless Communications and Mobile Computing 2017, 9243019 [http://doi.org/10.1155/2017/9243019].

[6] Desai R. M., Patil B. P., Sharma D. P.: Learning based route management in mobile ad hoc networks. Indonesian Journal of Electrical Engineering and Computer Science 7(3), 2017, 718–723 [http://doi.org/10.11591/ijeecs.v7.i3.pp718-723].

[7] Desmoulins N., Fouque P.A., Onete C., Sanders O.: Pattern Matching on Encrypted Streams. ASIACRYPT 2018. Lecture Notes in Computer Science 11272, Springer, Cham. [http://doi.org/10.1007/978-3-030-03326-2_5].

[8] Divitskyi A., Salnyk S., Hol V., Sydorkin P., Storchak A.: Development of a model of a subsystem for forecasting changes in data transmission routes in special purpose mobile radio networks. Eastern-European Journal of Enterprise Technologies 3(9), 2021, 116–125 [http://doi.org/10.15587/1729-4061.2021.235609].

[9] Dobkach L.: Analysis of methods for recognizing computer attacks. Legal informatics 1, 2020, 67–75 [http://doi.org/10/21681/1944-1404-2020-1-67-75].

[10] Durairaj M., Hirudhaya Mary Asha J.: The Internet of Things (IoT) Routing Security – A Study. International Conference on Communication, Computing and Electronics Systems. Lecture Notes in Electrical Engineering 637. Springer, Singapore 2020 [http://doi.org/10.1007/978-981-15-2612-1_58].

[11] Hasan N., Mishra A, Ray A. K.: Fuzzy logic based cross-layer design to improve Quality of Service in Mobile ad-hoc networks for Next-gen Cyber Physical System. Engineering Science and Technology, an International Journal 35, 2022, 101099 [http://doi.org/10.1016/j.jestch.2022.101099].

[12] Hui W., Zijian C., Bo H.: A Network Intrusion Detection System Based on Convolutional Neural Network. Journal of Intelligent & Fuzzy Systems 38(6), 2020, 7623–7637 [http://doi.org/10.3233/JIFS-179833].

[13] Mangelkar S., Dhage S., Nimkar A.: A comparative study on RPL attacks and security solutions. International Conference on Intelligent Computing and Control (I2C2), 2017, 1–6 [http://doi.org/10.1109/I2C2.2017.8321851].

[14] Moroz S., Tkachuk A., Khvyshchun M., Prystupa S., Yevsiuk M.: Methods for Ensuring Data Security in Mobile Standards. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska 12(1), 2022, 4–9 [http://doi.org/10.35784/iapgos.2877].
[15] Myneni S., Chowdhary A., Huang D., Alshamrani A.: A distributed deep defense against DDoS attacks with edge computing. Computer Networks 209, 2022, 108874 [http://doi.org/10.1016/j.comnet.2022.108874].
[16] Priyadarshini R., Rabindra K.: A deep learning based intelligent framework to mitigate DDoS attack in fog environment. Journal of King Saud University – Computer and Information Sciences 34(3), 2022, 825–831 [http://doi.org/10.1016/j.jksuci.2019.04.010].
[17] Rafe V., Mohammady S., Cuevas E.: Using Bayesian optimization algorithm for model-based integration testing. Soft Comput 26, 2022, 3503–3525 [http://doi.org/10.1007/s00500-021-06476-9].
[18] Showail A., Tahir R., Zaffar M. F., Noor M. H., Al-Khatib M.: An internet of secure and private things: A service-oriented architecture. Computers & Security 120, 2022, 102776 [http://doi.org/10.1016/j.cose.2022.102776].
[19] Tkachuk A. et al.: Basic Stations Work Optimization in Cellular Communication Network. Advances in Industrial Internet of Things, Engineering and Management, EAI. Springer Innovations in Communication and Computing, 2021, 1–19 [http://doi.org/10.1007/978-3-030-69705-1_1].
[20] Toroshanko Y., Selepyna Y., Yakymchuk N., Cherevyk V.: Control of traffic streams with the multi-rate token bucket, in International Conference on Advanced Information and Communications Technologies AICT 2019, 2019, 352–355 [http://doi.org/10.1109/AIACT.2019.8847860].
[21] Verma A., Ranga V.: Addressing Flooding Attacks in IPv6-based Low Power and Lossy Networks. TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), 2019, 552–557 [http://doi.org/10.1109/TENCON.2019.8929409].
[22] Yin C., Wang H., Yin X. et al.: Improved deep packet inspection in data stream detection. J Supercomput 75, 2019, 4295–4308 [http://doi.org/10.1007/s11227-018-2685-y].
[23] Yungaicela-Naula N., Vargas-Rosales C., Pérez-Díaz J., Carrera D.: A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning. Journal of Network and Computer Applications 205, 2022, 103444 [http://doi.org/10.1016/j.jnca.2022.103444].
[24] Zheng C., Li X., Liu Q., Sun Y., Fang B.: Hashing Incomplete and Unordered Network Streams. Advances in Digital Forensics XIV. DigitalForensics 2018. IFIP Advances in Information and Communication Technology 532. Springer, Cham. 2018 [https://doi.org/10.1007/978-3-319-99277-8_12].

Ph.D. Natalia Yakymchuk
e-mail: n.yakymchuk@lntu.edu.ua

Research interests: diagnostics and control of the telecommunication networks state, end-to-end diagnostics, congestion management.

http://orcid.org/0000-0002-8173-449X

Ph.D. Stanislav Prystupa
e-mail: s.prystupa@lntu.edu.ua

Author of more than 60 scientific papers, 5 patents for utility models. Research interests: design of microelectronic intelligent sensors of physical quantities.

http://orcid.org/0000-0003-3705-1541

Ph.D. Yosyp Selepyna
e-mail: y.selepyna@lntu.edu.ua

Research interests: Modeling of electronic devices and systems. Digital signal processing and coding in telecommunication systems and networks.

http://orcid.org/0000-0002-2421-1844

Ph.D. Serhii Moroz
e-mail: s.moroz@lntu.edu.ua

Author of more than 100 scientific papers, 7 patents for utility models. Research interests: Methodological bases of construction of sensors of physical quantities and measuring modules, Research of info-communication systems in the context of the development of the concept of the Internet of Things.

http://orcid.org/0000-0003-4677-5170

Ph.D. Mykola Yevsiuk
e-mail: m.yevsiuk@lutsk-ntu.com.ua

Research interests: telecommunication networks, radio engineering devices, power supply systems of radio engineering devices and systems. Author and co-author of about 40 scientific articles, two textbooks, two monographs.

http://orcid.org/0000-0002-3768-8959