computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

# MARKOV MODEL OF WIRELESS SENSOR NETWORK AVAILABILITY

**Maryna Kolisnyk [1], Dmytro Kochkar [2], Vyacheslav Kharchenko [1]**

[1] National aerospace university "Kharkiv Aviation Institute", Chkalov str. 17, Kharkiv, Ukraine, 61070, m.kolisnyk@csn.khai.edu, v.kharchenko@csn.khai.edu, www.khai.edu
[2] Metakon company, Kharkiv, Serpova str., 4, d.kochkar@csn.khai.edu, www.khai.edu

**Paper history:**
Received 12 May 2020
Received in revised form 08 August 2020
Accepted 04 September 2020
Available online 27 September 2020

**Keywords:**
Wireless sensor network;
Forest fire monitoring;
Availability function;
Coverage availability factor;
Model-based testing.

**Abstract:** The use of wireless sensor networks (WSN) in industry and for forest fire detection has recently become increasingly popular. Assessment of the availability of such networks is an important task, since they perform essential functions in critical situations. Sensor networks can be used to prevent and detect forest fires, and they must meet high availability requirements. Various options for organizing the WSN system are considered - with and without recovery. For such systems, the paper evaluates the probability of no-failure operation, as well as the readiness function, taking into account the network coverage ratio. In the paper the Markov WSN model for evaluating its availability function is developed taking into account the network coverage area. The obtained graphical dependencies allow us to evaluate how a change in the failure rate of sensors or system equipment affects the availability function value. The goal of this paper is to obtain metrics to assess the availability of system for monitoring forest by WSN and the availability function of a network using the Markov models. A special metric, so-called coverage availability factor is suggested in this paper taking into account different combinations of sensor failures which influence on completeness of monitoring forest fires.



## 1. INTRODUCTION

Wireless sensor networks (WSN) are actively used in various areas of production, recently these types of networks have been used to implement the Internet of things, in particular, the industrial Internet of things. This paper proposes the use of WSN for the prevention and detection of forest fires. For a downward fire in a forest, WSNs are often used. Smoke and temperature detectors track the start of a fire. This information is transmitted over the network to the appropriate fire fighting services. Each sensor has its own transmission range. If these sensors are identical, then trees can affect the communication range (as a natural obstacle to the signal), therefore, it is necessary to take into account the network coverage area (coverage ratio), as well as the probability of failure of sensors or system equipment. The authors of this paper propose to consider the option of organizing a network without recovery (in difficult thickets) and the option of a system with the possibility of recovery. For a non-recoverable system, it is advisable to assess the system reliability index P(t), for a recoverable system - the availability function.

The goal of this paper is to propose the metrics for assessing the availability of the system for monitoring forest fires by WSN and the availability function of a network using the Markov models and assessment of probability system uptime and availability function of WSN considering failures of system equipment and sensors.

## 2. WORK RELATED ANALYSIS

The issues of creating such networks were raised in the scientific works of many authors. In particular, in [1] the authors addressed the issues of ensuring energy efficiency of sensors in such networks. In [2], the size of the wireless sensor

This paper has been submitted fir the Open Special Issue on Green Mobile Computing and IoT Systems. Assessment, Modeling, Assurance.

network coverage area was considered to ensure efficient data transfer. In [3] the authors made a detailed analysis of various types of faults in a WSN service availability in WSN through the use of fault tolerance techniques. In [4] the authors analyzed the different models of collecting information from wireless sensor networks and proposed a model for information gathering. In paper [5], the author analyzed the routing process, types of vulnerabilities, and various types of attacks (black holes in two popular protocols based on LAR and DREAM locations) with the aim of disrupting the routing process or launching a DoS attack, and estimated the channel throughput when attacked. In [6], the author conducted an investigation of the OSLR protocol with simulated routing table overflows and spoofing attacks. The author in [7] proposed an extended version of exude detector technology, which makes it possible to calculate the packet loss rate for individual nodes of the MANET network. In [8], the author investigated the routing protocol of the multipath distance vector (AOMDV) in the MANET network under the influence of flooding attacks and other types of attacks. In [9], the author presented a study of various attacks and their impact on routing in the MANET network. In [10], the author performed an analysis of protocol vulnerabilities and routing methods when launching attacks. In [11], the author presented simulations and estimates of the performance and throughput of ZRP (Zone Routing Protocol), AODV (Vector Distance on Demand Protocol), and HWMP (Hybrid Wireless Network Protocol) for attacks of a gray hole, black hole, and jellyfish. In [12], the author proposed a secure routing algorithm for recognizing and rejecting a black hole attack. In [13], the author presented an analysis of the throughput of DSR and AODV in a black hole attack by changing the universality of mobile nodes on the network. In [14], the author simulated a black hole attack, a flood attack using the AODV (Ad hoc on Demand Distance Vector) protocol to test their influence on this protocol using the NS-2 network simulator. In [15], Jayashree S Patil introduced an integrated technology for attack audit and risk assessment in MANET routing. Many authors in their scientific works considered various aspects of the implementation of WSN, assessing the coverage area, and their reliability. The scientific novelty of this paper is the development of metrics for assessing the reliability of such networks, taking into account the network coverage ratio, for which two options for organizing a network are considered - a non-recoverable network in the event of a sensor or system equipment failure, and a network with the ability to recover from a failure.

## 3. ASSESSMENT OF UNRECOVERABLE WSN PROBABILITY OF UPTIME

Consider the option of organizing a WSN provided that in case of sensor failure it is almost impossible to restore them due to the difficulty of accessing them in the forest or the wetland where they were installed. The probability of uptime was taken as an indicator of the reliability of the considered network. The assumptions were made when evaluating the probability of uptime that the failure flow of sensors and system equipment obey the exponential distribution law. When calculating the probability of failure-free operation of a WSN of 10 sensors, both sensors and system equipment were sorted due to the possible failure options. The system in question is assumed to be unrecoverable. Consider a wireless sensor network, which consists of 10 sensors of the same type (identical). Assume that a network failure occurs if 5 sensors fail. The assumption was accepted of an exponential law of distribution of the flow of failures.

Assume that there can be no simultaneous failure of the sensor and system equipment. If the sensor fails, the system remains operational. A variant of the state of the system was considered in case of failure of half of the sensors. The sensors should be located so that a failure of two adjacent sensors is not possible, and failure of any set (up to five) of sensors does not lead to a system failure.

The logical-probabilistic method of finding the probability of uptime was applied. An enumeration of options of the system states made it possible to obtain an analytical expression for obtaining the probability of failure-free operation. The resulting formula allows us to determine P(t) at different failure rates of the same type of sensors (equally reliable and identical).

$$\begin{aligned} P(t) = {} & 950 \cdot pc(t)^4 \cdot po(t)^5 + 172 \cdot po(t)^5 \cdot pc(t) \\ & + 675 \cdot pc(t)^2 \cdot po(t)^4 \\ & + 677 \cdot pc(t)^4 \cdot po(t)^2 \\ & + 1010 \cdot pc(t)^3 \cdot po(t)^3 \\ & + 178 \cdot pc(t)^5 \cdot po(t) - 20 \cdot po(t)^5 \\ & - 94 \cdot pc(t) \cdot po(t)^4 \\ & - 190 \cdot pc(t)^2 \cdot po(t)^3 \\ & - 190 \cdot pc(t)^3 \cdot po(t)^2 \\ & - 94 \cdot pc(t)^4 \cdot po(t) - 20 \cdot pc(t)^5 \\ & - po(t)^4 - 2 \cdot po(t) \cdot pc(t)^3), \end{aligned}$$

$$po(t) = exp(-\lambda o \cdot t), pc(t) = exp(-\lambda c \cdot t)$$

For simulation the following values of the failure rate of sensors were chosen $\lambda c = 10^{-4}$ 1/hour, system equipment $\lambda o = 10^{-6}$ 1/hour (graph a) and $\lambda c = 10^{-5}$ 1/hour, system equipment $\lambda o = 10^{-7}$ 1/hour (graph b). Simulation results for presented initial data are shown in Fig. 1.

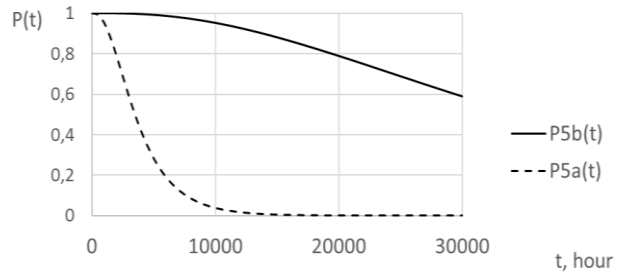


**Figure 1 – Graph of dependence of WSN P(t) on changing the failure rate of system equipment λ0**

The research of graphical dependencies showed that the value of the probability of failure-free operation (P(t)) of an unrecoverable system substantially depends on the reliability of sensors and on the reliability of system equipment. We can observe a strong drop in the P(t) already during the first 5000 hours of operation at values of failure intensities $\lambda c = 10^{-4}$ 1/hour, system equipment $\lambda o = 10^{-6}$ 1/hour. With a decrease in the values of failure rates by an order of $\lambda c = 10^{-5}$ 1/hour, system equipment $\lambda o = 10^{-7}$ 1/hour, the P(t) value increases, after 10,000 hours of operation of the system its value of 0.95 is reached. This value of P(t) does not meet the requirements for ensuring the reliability of the system, therefore, measures must be taken to increase reliability. Let us consider a similar system with restoring and evaluate its reliability indicators.

## 4. AVAILABILITY INDICATORS

Consider the variant of a recoverable system after a failure. Availability function *AC(t)* is the coefficient/function of availability (the probability that at any moment of time if the system is in a working state; prevention modes are not considered).

For WSN, the concept of a good working state is multi-level and is determined by the coverage ratio

$$\alpha_{\text{п}} = {}^{n_{\text{pc}}}/_{n}.$$

In case of sensor failures, the system degrades.

In the event of system equipment failure (SO), a complete system failure occurs. Therefore, the expression can be refined.

$$\alpha_{\text{п}} = \begin{cases} \frac{n_{\text{pc}}}{n}, if\ SO\ in\ good\ working\ state, \\ 0, if\ SO\ failure. \end{cases}$$

Then introduce the availability factor of coverage ACc(t,αп), which is a function of two variables.

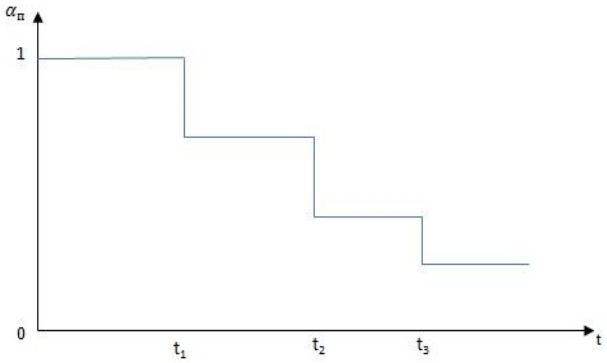


**Figure 2 – Graphics of dependence $\alpha_{\text{п}} = f(t)$**

Then we introduce the availability factor of the coverage ACгп(t,αп), which is a function of two variables t and αп.

Then ACгп(t, 1) is the full coverage availability factor, and ACгп(t,αп, 0<αп<1) - partial coverage.

System requirements may apply:

a) the total coverage, αп≥αпreq;

and to the maximum relative value of the uncovered area (of the forest massif)

$$\Delta\bar{\alpha}_{\text{п}\,max} \le \Delta\bar{\alpha}_{\text{п доп}}.$$

Then we have the coverage availability factor, which is a function of the three variables ACгп(t,αп, $\Delta\bar{\alpha}_{\text{п}\,max}$), $\Delta\bar{\alpha}_{\text{п}\,max}$ - defined as $\Delta\bar{\alpha}_{\text{п}\,max} = \max_{o=1,r}\{\Delta\bar{\alpha}_{\text{п}\,j}\}$, where r is the number of non-coverage zones consisting of one, two, .... areas with failed sensors.

In the absence of failures:

$$\alpha_{\text{п}} = 1, \Delta\bar{\alpha}_{\text{п}} = 0.$$

With one failed sensor:

$$n_p = n - 1, \alpha_{\text{п}} = \frac{n-1}{n},$$
$$\Delta\bar{\alpha}_{\text{п}\,max} = 1/n.$$

With two failed sensors:

$$n_p = n - 2, \alpha_{\text{п}} = (n-2)/n,$$
$$\Delta\bar{\alpha}_{\text{п}\,max} = 2/n.$$

In case of a failure of SO:

$$\Delta\bar{\alpha}_{\text{п}\,max} = 1.$$

## 5. DEVELOPMENT OF CCM AVAILABILITY MODELS

### 5.1 AVAILABILITY MODELS WITH NO REQUIREMENTS FOR $\Delta\overline{\alpha}_{\Pi\,max}$

We consider the simplest failures of sensors with a rate of λc and system equipment with a rate of λ0. In the absence of duplication, the reliability of the system:

$$P_{\text{CCM}}(t) = P_o(t) \cdot \prod_{i=1}^{n} p_{ci}(t).$$

Assumptions in the paper are the following ones: the network uses the same sensors, the same routers, the coverage area is 113 m, and the sensors with their own control system are located in the network. As a problem statement, we select a forest area of 1130 m2 in which the sensors are located to determine the fire (sensors that record the temperature increase in the event of a fire). Considering the radius of action of 6.4 m, as well as the overlap zone of 80 cm, we believe that the number of sensors covering a given area is 10. Let us introduce the concept of system failure: consider a failure as failure of 5 sensors. Coverage availability factor takes into account the coverage area and failures rates of system equipment and sensors. Two adjacent sensors cannot fail in the system.

Consider the simplest flow of the failures of sensors with the rate of λc and system equipment with the rate of λ0.

With the simplest recovery flows are with the rates μc and μ0 with perfect control of sensors and system equipment (routers).

Each sensor can transmit a signal to the system equipment. The monitoring system is considered as ideal, the flow of system and sensor failures is the simplest due to the Poisson distribution law. The network topology is either a star or a tree.

Assumptions for the developed model are the following [16-25]:

- the flow of failures of sensors and system equipment obey Poisson distribution according to the results of monitoring and diagnostics, testing corrected secondary error (the result of the accumulation of the effects of primary errors and defects, software backdoors);
- the process, which occurs in the system, is a process without aftereffect, every time in the future behavior of the system depends only on the state of the system at this time and does not depend on how the system reached that state. Therefore, the process has the Markov property. In Fig. 4 the graph of a Markov model of WSN is shown.

When calculating the availability function, the value of the failure rate of the system equipment was determined taking into account the failure of the network coordinator and router.

To determine the AC(t), the mathematical apparatus of the Markov models was used. On the state graph of the transition rates from one state to another, the network coverage indicator α and the failure rate of the system equipment λ0 and sensors λc, as well as the recovery rate of the system equipment μ0 and sensors μc after failure, are taken into account. The states of the Markov model graph: 1 - the system is operational, 2 - 1 sensor has failed, the rest ones are operational, 3 - the system equipment has failed, etc. The number of sensors in the network is 10. The Markov model of WSN functioning is presented in Fig. 3 in the case of the system equipment and sensors failure, which has the following states: well functioning state (1); states 2-11– sensors failed; states 12-21 – system equipment failed; n = 10, $\lambda 0 = 10^{-5}$ 1/h, $\lambda c = 10^{-4}$ 1/h, μ0 = 0,1667 1/h, μc = 0.0417 1/h.

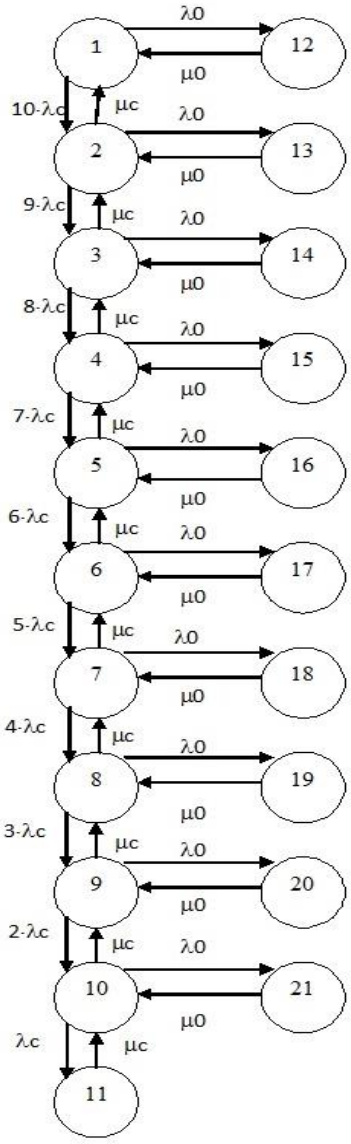


**Figure 3 – Graph of the Markov model of WSN considering failures of system equipment and sensors**

A system of linear differential equations of the Kolmogorov-Chapmen was composed and solved in the paper under the initial conditions:

$$\sum_{i=1}^{21} P_i(t) = 1; P1(0) = 1. \quad (1)$$

An important criterion of WSN availability is the availability function AC(t), that is defined as the sum of the probabilities of up-states. Availability function AC(t) is determined by equation:

$$AC(t) = P1(t)+P2(t)+P3(t)+P4(t)+P5(t). \quad (2)$$

Pi(t) – probabilities of WSN up-states. In case of 5 sensors failures a coverage factor will not be acceptable.

Availability function of WSN has been received by solving the system of Kolmogorov-Chapmen equations.

$$\frac{dP_1(t)}{dt} = \mu_0 \cdot P_{12}(t) + \mu_c \cdot P_2(t) - P_1(t) \cdot (\lambda_0 + 10 \cdot \lambda_c);$$

$$\frac{dP_2(t)}{dt} = 10 \cdot \lambda_c \cdot P_1(t) + \mu_c \cdot P_3(t) + \mu_0 \cdot P_{13}(t) - P_2(t) \cdot (\lambda_0 + \mu_c + 9 \cdot \lambda_c);$$

$$\frac{dP_3(t)}{dt} = 9 \cdot \lambda_c \cdot P_2(t) + \mu_c \cdot P_4(t) + \mu_0 \cdot P_{14}(t) - P_3(t) \cdot (\lambda_0 + \mu_c + 8 \cdot \lambda_c);$$

$$\frac{dP_4(t)}{dt} = 8 \cdot \lambda_c \cdot P_3(t) + \mu_c \cdot P_5(t) + \mu_0 \cdot P_{15}(t) - P_4(t) \cdot (\lambda_0 + \mu_c + 7 \cdot \lambda_c);$$

$$\frac{dP_5(t)}{dt} = 7 \cdot \lambda_c \cdot P_4(t) + \mu_c \cdot P_6(t) + \mu_0 \cdot P_{16}(t) - P_5(t) \cdot (\lambda_0 + \mu_c + 6 \cdot \lambda_c);$$

$$\frac{dP_6(t)}{dt} = 6 \cdot \lambda_c \cdot P_5(t) + \mu_c \cdot P_7(t) + \mu_0 \cdot P_{17}(t) - P_6(t) \cdot (\lambda_0 + \mu_c + 5 \cdot \lambda_c);$$

...

$$\frac{dP_{20}(t)}{dt} = \lambda_0 \cdot P_9(t) - \mu_0 \cdot P_{20}(t);$$

$$\frac{dP_{21}(t)}{dt} = \lambda_0 \cdot P_{10}(t) - \mu_0 \cdot P_{21}(t).$$

## 5.2 SIMULATION RESULTS

On the basis of the analysis of statistical data the main indicator of WSN availability AC(t) was assessed with the change in values of failure rates of system equipment - λ0 and sensors - λc and graphs, shown in Fig. 4 and Fig. 5 were built. As an example, graphical dependencies for the WSN AC(t) were given, taking into account failures of system equipment and sensors. The dependences of the system AC(t) on the transition rates to different states (λij, μij, where i = $\overline{1,21}$, j = $\overline{1,21}$) were constructed, which depend on events occurrence time. Fig. 4 and Fig. 5 show the change in AC(t) of WSN due to the change in the transition rates from one state to another in the Markov model. A research of the WSN system AC(t) in possible states of failures of system equipment and sensors and coverage zone was carried out.

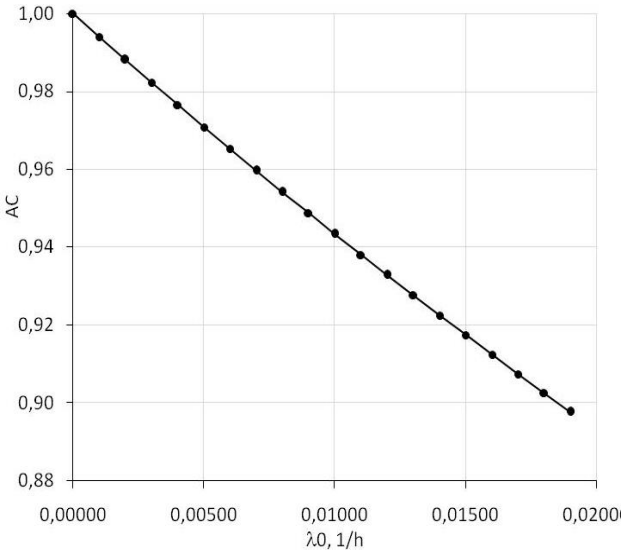


**Figure 4 – Graph of dependence of WSN AC on changing the failure rate of system equipment λ0**

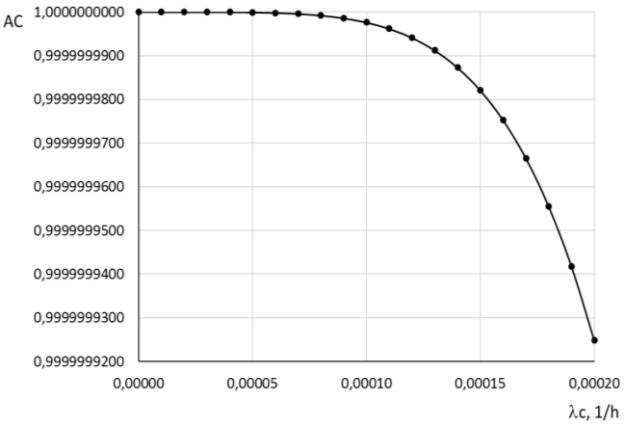


**Figure 5 – Graph of dependence of WSN AC on changing the failure rate of sensors λc**

The obtained graphical dependencies make it possible to evaluate how a change in the failure rate of sensors or system equipment affects the value of the availability function. If the failure rate of the sensors is 0.0002 1/h, then the value of the AC decreases from a value of 1 to 0.99999992 - slightly. If the failure rate of the system equipment is 0.0002 1/h, then the value of the AC is reduced from a value of 0.99999 to 0.9988. Thus, the availability of the system is highly dependent on the reliability of the system equipment, and the failure of one sensor does not significantly affect its availability.

## 6. CONCLUSION AND THE FUTURE WORK

In this paper metrics were obtained to assess the availability of forest fires WSN monitoring system and the availability function of a network using the Markov models. Also the assessment of probability system uptime and availability function of WSN was proposed considering failures of system equipment and sensors.

The paper presents an approach to a comprehensive assessment of the availability of a WSN system, taking into account the availability function and network coverage ratio. Two variants of the system are considered - without recovery and with recovery.

For an unrecoverable WSN system consisting of 10 identical sensors and system equipment, an analytical expression was obtained to estimate the probability of failure-free operation of such a system based on enumeration of possible states of the system, which can be used for various failure rates of system equipment and equally reliable sensors.

For the WSN system being restored, analytical expressions are proposed that take into account the network coverage coefficient and the value of the availability function for a system consisting of n sensors. The study of the WSN availability function depending on different values of the failure rates of both sensors and system equipment was carried out for a system of 10 sensors.

To assess the availability of WSN, metrics and a the Markov model were proposed taking into account failures and recovery of network equipment and sensors.

The conducted research allows us to estimate the network availability function when the failure rate of system equipment and network sensors is changed.

In the future, a study will be conducted on changes in the value of the availability function when cyber-attacks affect system equipment and sensors of the WSN and it can be possible to consider a system with different reliability of sensors.

## 7. ACKNOWLEDGEMENTS

This research is supported by the project STARC (Methodology of SusTAinable Development and InfoRmation Technologies of Green COmputing and Communication) funded by the Ministry of Education and Science of Ukraine.

## 8. REFERENCES

[1] A.N. Zelenin, V.A. Vlasova "Analysis of the power cycles of the nodes of wireless sensor networks," *East European Journal of Advanced Technologies,* vol. 3, issue 9 (57), pp. 13-17, 2012.

[2] P. Galkin, "Model of reducing the power consumption for node of wireless sensor network in embedded control systems," *Proceedings of the 2018 IEEE International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T),* October 2018, pp. 252-256.

[3] T.V. Sudarshan, B.N. Manjesh, "A survey on heterogeneous wireless sensor networks," *International Journal of Engineering Research & Technology (IJERT*). vol. 4, issue 4, pp. 1303-1306, 2015.

[4] S. Mishra, L. Jena, A. Pradhan, "Fault tolerance in wireless sensor networks," *International Journal of Advanced Research in Computer Science and Software Engineering Research Paper,* vol. 2, issue 10, pp. 146-152, 2012.

[5] E.M. Shakshuki, N. Kang, T.R. Sheltami, "EAACK – A secure intrusion-detection system for MANETs," *Proceedings of IEEE Transactions on Industrial Electronics,* vol. 60, issue 3, pp. 1089-1098, March 2013.

[6] K. Liu, J. Deng, P. K. Varshney, K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *Proceedings of IEEE Transactions on Mobile Computing,* vol. 6, issue 5, pp. 536–550, May 2007.

[7] S. Marti, T.J. Giuli, K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *Proceedings of the 6th ACM International Conference on Mobile Computing and Networking,* Boston, MA, 2000, pp. 255–265.

[8] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," *Proceedings of the International Conference on Multimedia Systems*, vol. 15, issue 5, October 2009, pp. 273–282.

[9] R. Balakrishnan, "An acknowledgement based approach for the detection of routing misbehavior in MANETs," *IEEE Transactions on Mobile Computing*, vol. 6, issue 5, May 2007, pp. 536–550.

[10] V. Desai, N. Shekokar, "Performance evaluation of OLSR protocol in MANET under

the influence of routing attack," *Proceedings of the 2014 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, December 2014, pp. 138-143.

[11] K. Kumar, V. Laxmi, K. Srinivasa Rao, "Identifying the behavior: Nodes, route and collusion attack's in MANET," *Proceedings of the 2014 IEEE International Conference on Contemporary Computing and Informatics (IC3I)*, Mysore, India, November 2014, pp. 124-129.

[12] Sukiswo, M. R. Rifquddin, "Performance of AOMDV routing protocol under rushing and flooding attacks in MANET," *Proceedings of the 20l5 2nd International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE)*, Semarang, Indonesia, October 2015, pp. 386–390.

[13] S. Rani, "Performance analysis of security attacks and improvements of routing protocols in MANET," *Proceedings of the 2015 Second International Conference on Computer Science, Computer Engineering, and Social Media (CSCESM)*, Lodz, Poland, September 2015, pp. 163-169.

[14] R. Kamal Kapur, S. Kumar Khatri, "Analysis of attacks on routing protocols in MANETs," *Proceedings of the 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA)*, Ghaziabad, India, March 2015, pp. 791-798.

[15] A. Chandra, S. Thakur, "Performance evaluation of hybrid routing protocols against network layer attacks in MANET," *Proceedings of the 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015*), Dehradun, India, 2015, pp. 207-211.

[16] S. R. Deshmukh, P. N. Chatur, N. B. Bhople, "AODV-based secure routing against black hole attack in MANET," *Proceedings of the IEEE International Conference on Recent Trends in Electronics Information Communication Technology*, India, May 2016, pp. 1960-1964.

[17] L. Mejaeleov, E. O. Ochola, "Effect of varying node mobility in the analysis of black hole attack on MANET reactive routing protocols," *Proceedings of the Information Security for South Africa (ISSA)*, Johannesburg, South Africa, August 2016, pp. 62-68.

[18] H. Moudni, M. Er-Rouidi, H. Mouncif, B. El Hadadi, "Performance analysis of AODV routing protocol in MANET under the influence of routing attacks," *Proceedings of the 2016 International Conference on Electrical and Information Technologies (ICEIT 2016)*, Tangiers, Morocco, 2016, pp. 191-196.

[19] J. S. Pati, K. V. N. Sunitha, "A combined technique for attack monitoring and risk assessment in MANET routing," *Proceedings of the 2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN)*, Hyderabad, India, July 2016, pp. 1-11.

[20] M. Dener, C. Bostancioglu, "Smart technologies with wireless sensor networks," *World Conference on Technology, Innovation and Entrepreneurship, Procedia. Social and Behavioral Sciences*, vol. 195, pp. 1915-1921, 2015.

[21] M. Rouse, "Wireless sensor network (WSN)", Techtarget. [Online]. Available at: https://searchdatacenter.techtarget.com/definition/sensor-network.

[22] S. Atanasov, "An overview of wireless communication technologies used in wireless sensor networks," *Proceedings of the International Scientific Conference eRA-8. Technologies used in wireless sensor networks*, TEI Piraeus, Athens, Greece, September 2013, pp. 11-18.

[23] *Enabling technologies for Wireless Sensor Networks*. VTT technical research centre of Finland LTD, June 2017, 14 p. [Online]. Available at: https://www.vttresearch.com/Documents/Smart%20industry/EEES/updates_201610/technology/technology_sensor_network.pdf.

[24] V. Kharchenko, D. Kochkar, O. Orekhov, "Monitoring network-based infrastructure for forest fire detection," *Proceedings of the Modelling, Monitoring and Management of Forest Fires III*, Great Britain, 2012, pp. 91–100.

[25] M. Kolisnyk, V. Kharchenko, I. Piskachova, "The research of the model of smart office availability considering patches on the router firewall software," *Proceedings of the 2018 IEEE 9th International Conference on dependable systems, services and technologies (DESSERT*), May 2018, pp. 176–182.

***Dr. Maryna Kolisnyk*** *- Doctor of Philosophy (Ph.D.), Associate professor of Dept. of "Computer systems, networks and cybersecurity", Faculty of radioelectronics, computer systems and infocommunications, National Aerospace University "Kharkiv Aviation Institute", Ukraine. Research areas: dependability, reliability, cybersecurity of IoT based and WSN systems.*

***Dmytro Kochkar****, SEO in Lisinfo. Graduated Dept. of "Computer systems, networks and cybersecurity", Faculty of radioelectronics, computer systems and infocommunications, National Aerospace University "Kharkiv Aviation Institute", Ukraine in 2000. Research areas: WSN systems, systems of firefighting and video control.*

***Prof. Vyacheslav Kharchenko,*** *Doctor of Sciences, Professor of Dept. of «Computer systems, networks and cybersecurity», Faculty of radioelectronics, computer systems and infocommunications, National Aerospace University "Kharkiv Aviation Institute", Ukraine. Research areas: dependability, cybersecurity, resilience, safety, reliability of critical infrastructure systems.*