© Rajba S., Karpinski M., Korchenko O. Generalized models, construction methodology and the application of secure wireless sensor networks with random network parameters // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 120-125.

GENERALIZED MODELS, CONSTRUCTION METHODOLOGY AND THE APPLICATION OF SECURE WIRELESS SENSOR NETWORKS WITH RANDOM NETWORK PARAMETERS

Stanislaw Rajba[1], Mikolaj Karpinski[2], Oleksandr Korchenko[3]

[1]*University of Bielsko-Biala, Poland*
[2]*University of Bielsko-Biala & State Higher Vocational School in Nowy Sacz, Poland*
[3]*National Aviation University, Ukraine*

RAJBA Stanislaw W., Candidate of Science (PhD)

Date and place of birth: 1952, Iłownica, Poland.
Education: Wrocław University of Technology, 1977.
Research interests: telecommunication, fiber optic communication, computer network, electronics.
Current position & Functions: Associate Professor at Electrical Engineering and Automatic Dept.
Publications: author and co-author of 39 publications.
E-mail: rajbas@ath.bielsko.pl

KARPINSKI Mikolaj P., Doctor of Science (DSc)

Date and place of birth: 1958, Baley, Chita Oblast, Russia.
Education: Lviv Polytechnic Institute, 1980.
Research interests: cybersecurity, computer systems and wireless networks, especially their security, in particular cryptographic methods of information security, lighting engineering and electric & photometric measurements.
Current position & Functions: Head of Computer Science Division since 2009.
Publications: over 100 scientific publications including monographs, papers in domestic & foreign scientific journals, international conferences proceedings, patents etc.
E-mail: mkarpinski@ath.bielsko.pl

KORCHENKO Oleksandr G., Doctor of Science (DSc)

Date and place of birth: 1961, Kyiv, Ukraine.
Education: Kyiv Institute of Civil Aviation Engineers (National Aviation University since 2000), 1983.
Research interests: information & aviation security.
Current position & Functions: Head of IT-Security Academic Department since 2004.
Publications: over 270 scientific publications including monographs, vocabularies, textbooks, papers in domestic & foreign scientific journals, patents etc.
E-mail: icaocentre@nau.edu.ua

Abstract. *A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions and to cooperatively pass their data through the network to a main location. In computer science and telecommunications, WSN are an active research area. In the paper an analysis of models of WSN with random access is presented. In these models, the parameters characterizing the network can be random. We presented the methodology of selection of the network model for practical application. We give an example of application of this methodology for the selection of the network model that supports the safety of maintenance work on the building.*

Key words: *Wireless Sensor Network, Poisson process, probability of collision, methodology of network model selection.*

1. Introduction

The wireless measurement is a very fast growing area of research. The wireless sensor network (WSN) is a specific use of radio communications systems where many stations nodes transmit the information to a base station (sink) [1]. It requires a completely different approach to radio communications than traditional systems, or even ad hoc networks [2]. You can list a number of important factors affecting the design of the WSN network. These are:

bands and communication frequencies, the demand for power supply (for example: for the purposes of communication and data processing), reducing external (environmental) as well as, hardware limitations, scalability, fault tolerance range. On the one hand the WSN network is characterized by the architectural and communication specificity associated with the system requirements, and on the other hand with the requirements of the radio propagation conditions. Among them: the mobility of the network nodes, configuration changes, the changing environmental conditions, algorithms for single-hop and multi-hop networks, often self-learning [3]. Basically, the use of WSN in specific applications often requires individual solutions to many complex problems. A specific class of network WSN is using some probabilistic solutions that can be applied to both randomized algorithms access, process control network [4] and probabilistic analysis on the wireless network [5]. Randomized algorithms play an important role in any type of distributed system, they lead to faster and simpler solutions [6, 7]. In the case of wireless networks there are essentially four main topics of probabilistic analysis: (1) related to energy saving [8], (2) related to design and analysis - random access or random sending [9, 10], (3) probabilistic network performance analysis (assuming random network topology), and (4) probabilistic analysis of randomized algorithms [11-13].

In this study, there has been presented a methodology of model selection WSN with random access in order to protect restoration works of sacral object. There has been designated the probability of transmitted information packets collision and security level of transmitted information in the security of carried construction works context.

2. Probabilistic network model

We modeled our wireless network using a Poisson process. Mathematically the process N is described by so called counter process N_t or $N(t)$ of rate $\lambda > 0$. The counter tells the number of events that have occurred in the interval $[0, t]$ $(t \geq 0)$.

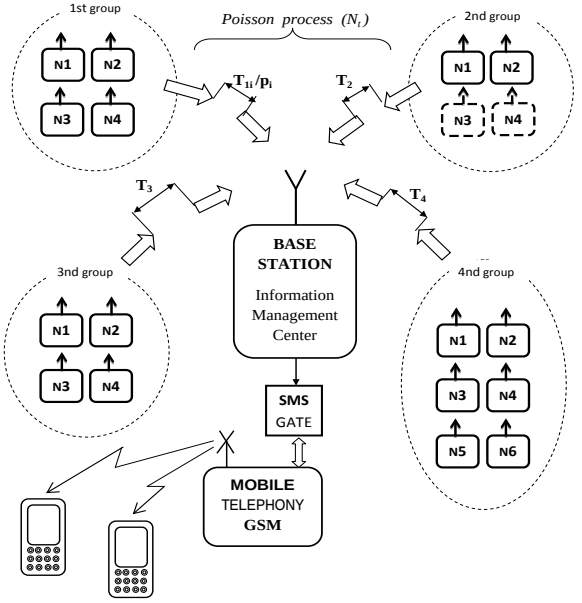

Fig. 1. Model safety evaluation of information transmission in securing restoration works of sacred object

N has independent increments (the number of occurrences counted in disjoint intervals are independent from each other), such that $N(t) - N(s)$ has the Poisson $(\lambda (t-s))$ distribution.

Let us state our main assumptions. There are some number nodes observing a dynamical system and reporting to a central location over the wireless sensor network with one radio channel. For simplicity, we assume that our sensor network is a single-hop network with star topology. We also assume every node (sender-sensor) always has packet ready for transmission. We assume that nodes send probe packets (a communication protocol) at poissonian times (Poisson Arrivals See Time Averages PASTA). Duration of the communication protocol is t_p. We say that a collision occurs in time interval s, if there exist at least two nodes which start sending within this interval with the difference between the beginning of their sending times not exceeding the value of t_p. Let $P(A_s)$ denote the probability of collisions (or the collision probability) in the time interval s. We proved the following theorem on the probability of collisions [4, 14].

Theorem 1. Let $N(t)$ be a Poisson process with the rate $\lambda>0$, representing the time counter of transmissions of nodes. Then the probability of collisions in the time interval of s length $(s > t_p)$ is given by the formula

$$P(A_s) = \sum_{j=2}^{\infty} e^{-\lambda s} \frac{(\lambda s)^j}{j!} [1 - (1 - j\frac{t_p}{s})_+^j], \qquad (1)$$

where t_p is the duration time of a protocol.

In [4, 13] we consider the case, when there are n identical nodes, with the same average time between transmissions of a node. In [13] we give some conditional probability of collisions, and in [4] unconditional probability of collisions.

Theorem 2. ([4]) Let n be the number of nodes and let T be the average time between transmissions of a node. Then the probability of collisions in the interval of s length $(s > t_p)$ is given by the formula (1) with $\lambda = n/T$.

In [14] we study the case, when the average times between transmissions of nodes are not necessarily the same. In [14] can be found the following theorem on the probability of collisions in this case.

Theorem 3. Let n be the number of nodes. Assume that all nodes are divided into k groups $(1 \leq k \leq n)$, such that $n = n_1 + n_k$, where n_i is the number of nodes from the i–th group and T_i is the average time between transmissions of each node from the i–th group $(i = 1, 2, \ldots k)$. Then the probability of collisions in the interval of s length $(s > t_p)$ is given by (1) with λ given by the formula

$$\lambda = \lambda(k; n_1, ..., n_k; T_1, ..., T_k) = \sum_{i=1}^{k} \frac{n_i}{T_i}. \qquad (2)$$

Note that, by denoting $x_i = n_i / n$, we obtain that $n_i = x_i n \quad (i = 1, 2, ..., k)$. In [15] we replace deterministic network parameters $n; k; x_1, ..., x_k; T_1, ..., T_k$ by random variables. Then, assuming, that these network parameters are random variables, we obtain formulas for the collision probability. for different cases.

In this paper we replace deterministic network parameters $n_1, ..., n_k; T_1, ..., T_k$ by random variables and we obtain new formula for the collision probability.

Denote

$$W(\lambda,s)=\sum_{j=2}^{\infty}e^{-\lambda s}\frac{(\lambda s)^j}{j!}[1-(1-j\frac{t_p}{s})_+^j]. \quad (3)$$

Then, the probability of collisions, given in Theorem 3, can be written in the form

$$P(A_s)=W(\lambda,s). \quad (4)$$

Where λ is given by (2). Consider now, in place of deterministic parameters $n_1,...,n_k;T_1,...,T_k$ random variables $\nu_1,...,\nu_k;\tau_1,...,\tau_k$. Next, we replace λ by the random variable given by the formula $\Lambda=\Lambda(k;\nu_1,...,\nu_k;\tau_1,...,\tau_k)=\sum_{i=1}^{k}\frac{\nu_i}{\tau_i}$. Taking into account that the probability of collision can be regarded as the expectation of $W(\Lambda,s)$, we obtain the formula for the probability of collision

$$P(A_s)=E(W(\Lambda))=E(\sum_{j=2}^{\infty}e^{-\Lambda s}\frac{(\Lambda s)^j}{j!}[1-(1-j\frac{t_p}{s})_+^j]). \quad (5)$$

3. Metodology

The choice of a mathematical model of wireless sensor network with random access is strictly connected with task type dedicated to WSN. The following diagram presents the methodology of selecting the correct model to a dedicated task. There has been specified below 12 characteristic features which decide what path we move in the diagram (Fig. 2), and which model finally we will choose:

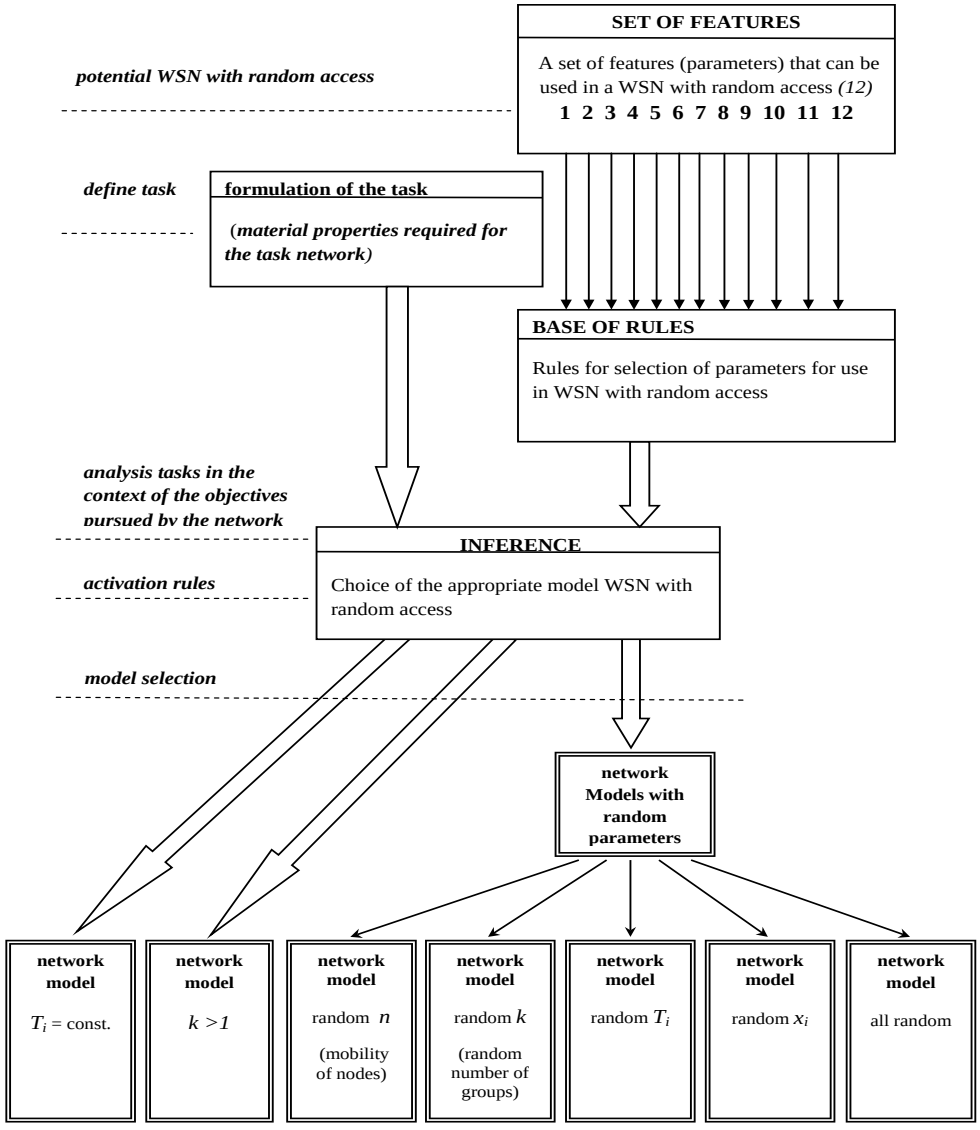

Fig. 2. Methodology of network model selection suited to the task

There has been specified below 12 characteristic features which decide what path we move in the diagram (Fig. 2), and which model finally we will choose:

1) T – the average time between transmissions (selected by the necessary frequency of measurements by sensors attached to the node).

2) t_p – duration of transmitting a packet by node. (conditioned by the number of sensors connected to node, selected protocol with required binary word length for information record about required resolution, available bandwidth on a radio channel).

3) n – number of nodes required for task implementation.

4) Nodes mobility.

5) Expected transmission quality (required probability of collision).

6) The necessity of the nodes division into groups according to the criterion of the average time between transmissions.

7) The required number of sensors connected to node (associated with selection of protocol and conditioned dispatching of radio channel bandwidth).

8) Communication protocol selection (according to conditions mentioned above).

9) Available or required radio channel bandwidth.

10) Required constant intensity (frequency) of studied phenomena observation by the network.

11) Required variable intensity (frequency) of studied phenomena observation by the network.

12) Necessity to randomize some or all of the network parameters according to proposed models.

4. Model safety evaluation of information transmission in securing restoration works of sacred object

In thesis there has been presented an issue of using wireless sensor network with random access for secure surveillance restoration work on the sacral historic object in Rudzica. Sacral object in Rudzica was built over 200 years ago on a small hill (Fig. 3). After a while from the right side below there was formed a road causing a grounds setoff. Over the years, it has noted that the ground on which stays the object is a small landslide, which is moving towards the road. It caused cracks in the walls especially in a ceiling of the object (Fig. 4). This situation was getting worse and threatened a construction catastrophe.

Facility rescue project was prepared, which consisted of earthworks involving foundations improvement as well as abutment elements building which would protect the area for further landslides.

Fig. 3. Church in Rudzica - the object of restoration works protected by wireless sensor network with random access

There has been also provided binding (hooking) of opposite walls by screws which protect the ceiling against collapse.

Fig. 4. The crack in ceiling

Excavations execution in strained environment of the object is especially dangerous and the whole process of completing a task requires continuous supervision. Electronic surveillance should be mobile and without major inconvenience for the maintenance and guaranteeing secure communication of information to a monitoring station (base station). The base station records displacement sensors indications, angles, as well as rainfall, especially dangerous during open pit works in ground. Indications are transmitted via wireless nodes. Nodes in part were moved during works according to needs, as well as their number was changing. The base station elaborates obtained data and in emergency situations generates alarms via GSM mobile telephone network via SMS Gateway. SMS messages are sent as an alarm in order to recall the construction supervision in dangerous situations (excessive movements of soil, cracks in walls, too much rain). The works were planned in the period for 6 months starting from April, when due to climatic conditions there can be carried out field works, while the average monthly rainfall in the first two months are relatively low [16] guaranteeing construction safety. In works security were used wireless sensor network with random access as a simple solution, little troublesome for building works (e.g., no cables, with changing measurement points) with high required mobility of nodes (along with measuring points). To the restoration task accomplishment it was selected model of wireless sensor network with random access (see model selection) it was also adjusted net for the necessary measurements. The purpose of the used network is to provide security in conservation work execution. However, in order to obtain such guarantee, it needs to be examining a security of information transmission in network.

For practical application of the network model for restoration works supervision (fig. 1) it was set a number of nodes groups $k = 4$.

In first group, number of nodes $n_1 = 4$,

The first group of nodes Table 1

o.n.	**w**	T_{1i}	p	Attention
	[mm/h]	[s]		
1	**0-0,8**	28800	0,7	
2	**0,8-1,6**	3600	0,2	State increased risk
3	**> 1,6**	600	0,1	State of alarm
	$n_1 = 4$			

there are random times between transmissions with distributed random variable dependent on rainfall shown in Table 1 (includes 4 nodes at the corners of the object equipped with rainfall sensors and inclinometers).

Second group of nodes includes a variable (random) number of nodes v_2. Average time between transmissions is constant and it is T_2 =30 minutes. Random is number of nodes v_2 and has a distribution shown in Table 2 (including 2 to 4 knots, depending on the carried out works, equipped with pressure sensors to control the excavation works).

The second group of nodes Table 2

Number of nodes n_{2l}	2	3	4
Probability q_i	0,3	0,2	0,5
T_2 = 1800 s (const.)			

In a third group of nodes n_3 = 4, the average time between transmissions is constant and it is T_3 = 12 hours (43200 s) (nodes equipped with crack control sensors (fig. 4)).

In a fourth group of nodes n_4 = 6 Average time between transmissions is constant and it is T_3 = 8 hours (28800 s) (strain control in the ceiling).

Fig. 5. Sensor for recording movements of cracked parts of the wall

For presented of practical application case, using the formula (5) for the collision probability we obtain a formula for the probability of collisions in the WSN network of restoration works supervision

$$P(A_s) = \sum_{l=1}^{3}\sum_{m=1}^{3} q_l p_m W(\lambda(k; n_1, n_{2l}, n_3, n_4; T_{1m}, T_2, T_3, T_4)).$$

Using dependence (3) and (4) it was calculated the probability of collisions in network for restoration works supervision by the data presented in Table 1, Table 2 and in the description of parameters for groups 1, 2, 3, 4. In the network communication protocol was used on the duration $t_p = 32 \cdot 10^{-6}$ s. The calculated probability of collision is $P(A_s) = 1,25 \cdot 10^{-7}$. It is a result completely satisfactory, allowing to ensure secure transmission for carrying out restoration works.

6. Conclusion

In the paper are examined models of WSN network with random access, where the individual parameters characterizing the network are randomized. Parameters randomization allows for a better fit of network model for practical use. In chapter 3 presented a set of 12 characteristic features of WSN network with random access, which were systematized in provided diagram. Procedure for selection of network model for particular application consists a selections the appropriate path (Fig. 2). It is an essential element of the procedure for the selection of optimal network model for a specific application. During choosing a model it should be guided by the smallest but the necessary number of transmissions in the operation space of all nodes. The probability of collisions as the main measure of the network quality should be as small as possible. In order to obtain that aim it should by using the scheme (Fig. 2) choose this solution which will reduce total number of transmissions in impact of all nodes area. For example, the division into groups of nodes allow for sensors whose data are rarely needed, to reduce the number of transmissions by node that supports them. Randomization such as the number of nodes accurately reflects situation with mobile nodes which are not always active in receiving base station area. Analyzing the situation of carrying maintenance works in the context of methodological scheme (Fig. 2), established was a network in which operate 4 groups of nodes. In first group we deal with randomization of average time between transmissions, in second group was advisable to randomize the number of nodes. However the service of groups 3 and 4 requires the use deterministic parameters. Obtained result for probability of collision $P(A_s) = 1,25 \cdot 10^{-7}$ is a very good one and guarantee the security in terms of information transmission about the state of object under the restoration. This result is due to a good selection of a model for this task.

References

[1] Wireless sensor networks: a survey / I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci // Computer networks. – 2002. – Vol. 38, No 4. – P. 393-422.

[2] Chatzigiannakis I. Efficient data propagation strategies in wireless sensor networks using a single mobile sink / I. Chatzigiannakis, A. Kinalis, S.E. Nikoletseas // Computer Communications. – 2008. – Vol. 31, No 5. – P. 896-914.

[3] Culler D. Overview of sensor networks / D. Culler, D. Estrin, M. Srivastava // IEEE Computer. – 2004. – Vol. 37, No 8. – P. 41-49.

[4] Rajba S. The probability of collisions in Wireless Sensor Network with random sending / S. Rajba, T. Rajba // Przegląd Elektrotechniczny (Electrical Review). – 2012. – Vol. 88, No 9a. – P. 243-246. – ISSN 0033-2097.

[5] Wattenhofer H. Algorithms for Wireless Sensor Networks (Tutorial) / H. Wattenhofer // Proc. European Workshop on Wireless Sensor Networks. – 2006.

[6] The Role of PASTA in Network Measurement / F. Baccelli, S. Machiraju, D. Veitch, J. Bolot // Computer Communication Review, Proceedings of ACM Sigcomm. – 2006. – Vol. 36, No 4. – P. 231-242.

[7] Rajba S. Wireless sensor network with a random control / S. Rajba // Вісник Національного університету «Львівська політехніка». Серія: Радіоелектроніка та телекомунікації. – 2012. – № 738. – С. 106-111. – ISSN 0321-0499.

[8] Younis O. HEED: A Hybrid, Energy-Efficient, Distributed clustering approach for Ad Hoc sensor networks / O. Younis, S. Fahmy // IEEE Transactions on Mobile Computing. – 2004. – Vol. 3, No. 4. – P. 366–379.

[9] Rajba S.W. Random Control of Sending Radio Messages in the Wireless Sensor Network / S. W. Rajba // Informatics and Mathematical Methods in Simulation. – 2012. – Vol. 2, No 2. – P. 113-120. – ISSN 2223-5744.

[10] Xu-Xun L. A Survey on Clustering Routing Protocols in Wireless Sensor Networks / L. Xu-Xun // Sensors. – 2012. – Vol. 12. – No 8. – P. 11113-11153. – ISSN 1424-8220.

[11] Elson J. Random, ephemeral transaction identifiers in dynamic sensor networks / J. Elson, D. Estrin // Distributed Computing Systems: Proceedings 21 International Conference, Mesa, AZ. : thesis. – April 2001. – P. 459–468.

[12] Rajba S. Probabilistic Methods of Controlling Emissions in the Radio Network / S. Rajba, M. Karpinski, O. Korchenko // Informatics and Mathematical Methods in Simulation. – 2013. – Vol. 3, No 4. – P. 314-322. – ISSN 2223-5744.

[13] Rajba S. Wireless sensor converge cast based on random operations procedure / S. Rajba, T. Rajba // PAK. – 2010. – Vol. 56, No 3. – P. 255-258. – ISSN 0032-4140.

[14] Wireless Sensor Networks in Application to Patients Health Monitoring / S. Rajba, T. Rajba, P. Raif, M. Mahmud // IEEE Computational Intelligence in Healthcare and E-health. – Singapore. – 2013. – P. 94-98. – ISBN 978-1-4673-5883-5.

[15] Rajba S. A randomization of parameters in Wireless Sensor Networks / S. Rajba, T. Rajba // Przegląd Elektrotechniczny (Electrical Review). – 2013. – R 89, No 9. – P. 240-244. – ISSN 0033-2097.

[16] Lorenc H. Atlas klimatu Polski. – Warszawa: Instytut Meteorologii i Gospodarki Wodnej. – 2005. – 116 s.

UDC 004.7:62-519:621.391 (045)

Райба С.В., Карпінський М.П., Корченко О.Г. Узагальнені моделі, методологія побудови та застосування захищених безпровідних сенсорних мереж з випадковими мережевими параметрами

Анотація. *Безпроводові сенсорні мережі є просторово розподіленими автономними датчиками для моніторингу фізичних або екологічних умов з метою спільної передачі своїх даних через мережу до основного місця (серверу). В інформатиці і телекомунікаціях, на сьогодні безпроводові сенсорні мережі є активним напрямом наукових досліджень. У статті представлено аналіз моделей безпроводових сенсорних мереж з випадковим доступом. У цих моделях параметри, які характеризують мережу, можуть бути випадковими. Запропоновано методологію вибору моделі мережі для практичного застосування. Наведено приклад застосування цієї методології для вибору моделі мережі, яка підтримує безпеку робіт щодо консервації будівельного об'єкта.*

Ключові слова: *безпроводова сенсорна мережа, потік Пуассона, ймовірність колізії, методологія вибору моделі мережі.*

Райба С.В., Карпинский Н.П., Корченко А.Г. Обобщенные модели, методология построения и применение защищенных беспроводных сенсорных сетей со случайными сетевыми параметрами

Аннотация. *Беспроводные сенсорные сети являются пространственно распределенными автономными датчиками для мониторинга физических или экологических условий с целью совместной передачи своих данных через сеть к основному месту (серверу). В информатике и телекоммуникациях, на сегодня беспроводные сенсорные сети являются активным направлением научных исследований. В статье представлен анализ моделей беспроводных сенсорных сетей со случайным доступом. В этих моделях характеризующие сеть параметры могут быть случайными. Предложена методология выбора модели сети для практического применения. Приведен пример применения этой методологии для выбора модели сети, поддерживающей безопасность работ по консервации строительного объекта.*

Ключевые слова: *беспроводная сенсорная сеть, поток Пуассона, вероятность коллизии, методология выбора модели сети.*

Отримано *15 квітня 2014 року*, затверджено редколегією *20 травня 2014 року*