UDC 681.326:681.51 **doi: 10.26906/SUNZ.2020.4.122**

O. Makogon[1], O. Dychko[1], O. Isakov[1], R. Lazuta[2], H. Osmak[2], L. Trotsko[2]

[1] Military Institute of Tank Troops of National Technical University, Kharkov, Ukraine
[2] Military Institute of Telecommunications and Informatization named after Heroes of Kruty, Ukraine

SIMULATION AN UNRELIABLE WIRELESS SENSOR NETWORK MOT BY A HETEROGENEOUS QUEUING NETWORK

Abstract. The subject matter of the article is the operation of a wireless sensor network in an unfriendly environment. The **goal** of the study is the simulation of processes occurring in wireless sensor networks, a comprehensive description of their main modes of operation and the analysis of "bottlenecks" to improve the reliability of the network and minimize threats to its information security. **The tasks** to be solved are: based on the analysis of the technology for building a wireless sensor network and the functioning of its elements; to determine the reliability characteristics that have an impact on information security; to determine the structure of the Queuing network similar in structure to the wireless sensor network as an object of research; to determine the main characteristics of the sensor network mot as a Queuing network; to determine analytical dependencies for finding the characteristics of an unreliable wireless sensor network mot. General scientific and special **methods** of scientific knowledge are used. The obtained **results** allow us to understand and study the processes occurring in wireless queuing networks and to predict network operation in a hostile environment. The ability to estimate the number of packets lost gives you an understanding of the reliability of network mots. **Conclusions.** Wireless sensor networks can be defined as distributed communication systems. The reliability characteristics of their structural elements have an impact on information security. The wireless sensor network may be simulated by the queuing network. The main characteristics of the sensor network mot can be defined as the characteristics of the queuing network. These analytical dependencies allow you to determine the characteristics of the unreliable node needed to analyze the "bottlenecks", to improve the reliability of the network and minimize threats to the wireless sensor network information security.

Keywords: wireless sensor network, unreliable mot, queuing network, reliability characteristics, information security threats.

Introduction

Formulation of the problem and research tasks. Today, wireless sensor networks (WSN) have defined a new class of distributed communication systems, the use of which in the military sphere is appropriate for determining the location of mobile targets, the territorial spread of chemical weapons, and so on**.**

In general, the WSN refers to networks consisting of a set of wireless information mots located in space and designed to monitor the parameters of the environment or objects are located in it.

The configuration of the wireless sensor network should be flexible and change depending on the current position in space and power supply capabilities. Sensory nodes usually function in an unfriendly environment. Due to the discharge of power supplies, the buffer overflow of lost packets may cause network mots to shut down.

Under these circumstances, it becomes problematic to predict the behavior of the network under different operating modes and make an estimate of the number of losses, which is necessary to understand the accuracy and reliability of calculations that take place in the process of collecting data by mot sensors and countering threats and attacks.

Thus, the question of study the WNS characteristics, analysis of their properties and development of methods for evaluating the basic characteristics and determining ways to improve the reliability of the functioning of the nodes are **relevant.**

Analysis of recent research and publications. To date, the classification of sensor networks has been carried out, their main properties have been determined, and software products for implementing a particular network architecture have been analyzed [1-11]. In [12] it was shown that wireless networks are more difficult to protect due to the use of an open environment as a data carrier and the broadcast nature of wireless connections.

Of particular interest are such networks characteristics as the mathematical expectation of the requirements number and the mathematical expectation (ME) characteristics, we should note the mathematical expectation of the lost packages number.

The goal of this issue is the simulation of processes occurring in wireless sensor networks, a comprehensive description of their main modes of operation and the analysis of "bottlenecks" to improve the reliability of the network and minimize threats to its information security

To achieve this goal, it is proposed to model an unreliable sensor network node using a heterogeneous Queuing network.

This **goal** defined the following research tasks:

– based on the analysis of the technology for building a wireless sensor network and the functioning of its elements;

– to determine the reliability characteristics that have an impact on information security; to determine the structure of the Queuing network similar in structure to the wireless sensor network as an object of research;

– to determine the main characteristics of the sensor network mot as a Queuing network;

– to determine analytical dependencies for finding the characteristics of an unreliable wireless sensor network mot.

General scientific and special **methods** of scientific knowledge are used.

Namely: the position of Queuing theory and fundamentals of systems modeling, distribution of stationary probabilities by an open inhomogeneous queuing network (QN), principles of sensor networks operation. In addition, descriptions of analytical models of network systems and their construction were used.

Main material

1. Technologies in the wireless sensor network. Let's consider a homogeneous self-organizing distributed monitoring and control WSN intended, for example, for monitoring and managing processes and resources. We will assume that each sensor WSN mot consists of a computing device, receiver, sensors, and power supply.

The computing device consists of a microprocessor and memory.

The microprocessor is designed to analyze and convert data from adjacent network nodes and sensors from that node. Programs and data are stored in the memory of the computing device. The receiver is proposed to be considered as a radio transceiver designed to organize the radio interface between the nodes of the sensor network. The sensor is designed to convert a controlled value (electrical voltage, electric current, temperature, pressure, illumination, oscillations, etc.) into a signal that is easy to measure and convert with a microprocessor.

There are usually several types of sensors in a single sensor network mot. The power supply unit is designed to ensure the operation of all electrical circuits of the sensor network node. Failure of the power supply unit causes the entire mot to stop working. Replacing the power supply unit restores the health of the network mot. Network nodes are able to relay messages from each other in turn, providing a significant area of coverage over the 802.15.4/ZigBee short-range radio Protocol [4, 13].

2. Simulation of a Queuing system (QS). As it is known, a QN is a set of interconnected Queuing systems provide for the reception, storage, processing and issuance of requests received by the service system during the operation of the network. from service sources. QS is also divided into open, closed and mixed. Open ones provide for servicing requirements received from the infinite capacity source and returning back to the source [14]**.**

As the subject matter it is proposed an open Queuing Network consists of two Queuing systems and three classes of requirements.

For ease of presentation, all data in the sensor network node, as well as data entering and exiting the node, will be called requirements. Let's define the requirements of the first, second, and third classes. First-class requirements from node sensors are sent to the microprocessor for processing. The second class of requirements are sent from the network to the host receiver. Requirements of the first and second classes that have been processed by the microprocessor become requirements of the third class and are relayed to the network. To the microprocessor and the queue of requirements for processing in the microprocessor, we will put the QS S_1 in accordance with a single device (service channel), an unlimited queue and the LCFS service discipline (the last one came – the first one was serviced).

The receiver-transmitter along with the queue of packets to it in the model will display the QS S_2 with one device and an unlimited queue with the FCFS service discipline (first come – first served).

Let's assume that from the source S0, the system S_1 receives a Poisson flow of first-class requirements with the intensity of first-class requirements with the intensity λ_{01}.

The requirements that come to the microprocessor from the node's sensors will be considered first – class requirements, and those that are received by the node's transmitter from neighboring nodes will be considered second-class requirements, respectively.

The duration of servicing first-class requirements by the S_1 system is an exponentially distributed random variable with the parameter μ_{11}.

After completing service in the S_1 system, the requirements change their class from first to third and enter the S_2 system.

A Poisson stream of second-class requirements with an intensity of λ_{02} and third-class requirements from the S_1 system is sent to the S_2 service system from the source. The service duration of the second and third class requirements in the S_2 system is an exponentially distributed random variable with the parameter μ_{12}.

After completing service in the S_2 system, second-class requirements enter the S_1 system, and third-class requirements leave the Queuing network. The duration of servicing second-class requirements by the S_1 system is an exponentially distributed random variable with the parameter μ_{12}.

After completing service in the S_1 system, the requirements change their class from second to third and enter the S_2 system.

When the system is functioning, it is possible to create queues for processing packets in the packet processor.

In QN terminology, this phenomenon will correspond to the presence of a buffer with the requirements of the first and second class for the S_1 QS. Similarly, we assume that the buffer in QS S_2 can contain m_2 of requirements of the first and second classes [14]. The structure of the sensor network mot as a Queuing network is shown in Fig. 1.

3. The Characteristics of an unreliable sensor network mot will be determined using the stationary characteristics of the Queuing network.

The state of the Queuing network is determined by a vector $q = (q_{11}, q_{12}, q_{22}, q_{23})$, here q11, q12 – the number of requirements in QS S_1 of the first and second class, respectively; q22, q23 – the number of requirements in the QS S_2 of the second and third class, respectively. The stationary probabilities q_{11}, q_{12}, q_{22}, q_{23} are uniquely determined by the characteristics of

the systems and can be calculated by known methods, based on the fact that the corresponding values λ_{01}, λ_{02}, μ_{11}, and μ_{12} are known.

A mot that can stop working during operation (for example, due to a failure of the mot's power supply) will be considered unreliable.

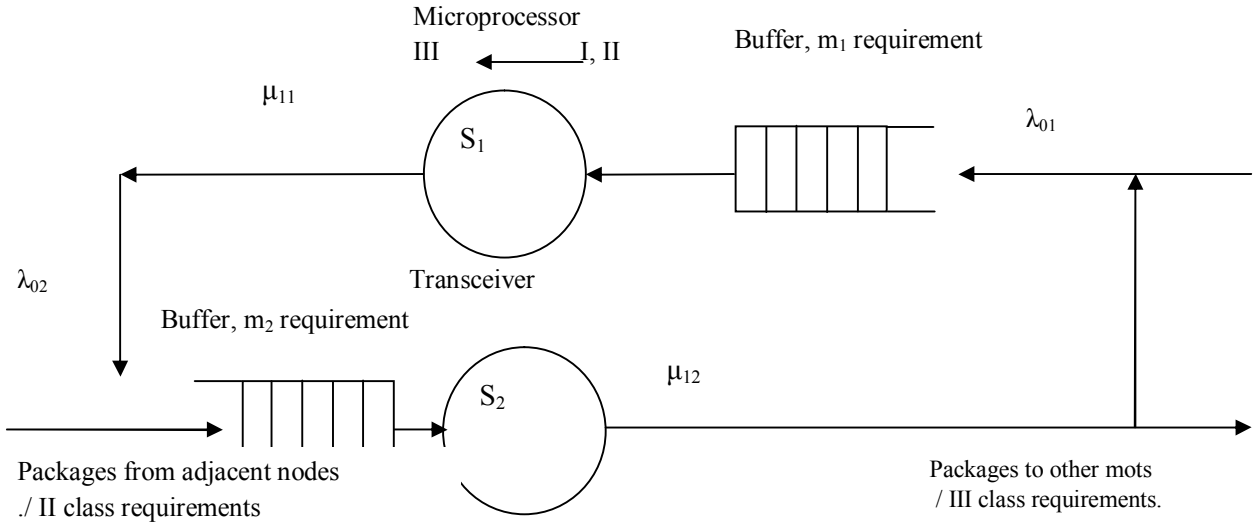

Fig. 1. The structure of the node of the sensor network as a Queuing network

Based on this, we will determine the main characteristics of the sensor network mot as a Queuing network:

– ME of the S_1 systems requirements number;
– ME of the S_2 systems requirements number;
– service network response time;
– ME of the requirements stay time in the S_1 system;
– ME of the requirements stay time in the S_2 system;
– ME of the lost packages number.

The probability that the S_1system is q_{11}, q_{12} and equirements given by

$$P_1(q_{11}) = P_1(q_{12}) = \left(1-\frac{\lambda_{01}}{\mu_{11}}-\frac{\lambda_{02}}{\mu_{12}}\right)\left(1-\frac{\lambda_{01}+2\lambda_{02}}{\mu_2}\right)\times \quad (1)$$

$$\times\left(\frac{\lambda_{01}}{\mu_{11}}\right)^{q_{11}}\left(\frac{\lambda_{02}}{\mu_{12}}\right)^{q_{12}}\left(\frac{\lambda_{01}+2\lambda_{02}}{\mu_2}\right)^{q_2};$$

$$P_1(q_{11}) = P_1(q_{12}) = \left(1-\frac{\lambda_{01}}{\mu_{11}}-\frac{\lambda_{02}}{\mu_{12}}\right)\left(1-\frac{\lambda_{01}+2\lambda_{02}}{\mu_2}\right); \quad (2)$$

$$q_{11},\ q_{12} = 0,\ 1,2,....$$

The probability that the system S_2 is $q_2 = q_{22} + q_{23}$ requirements is determined similarly by the expression

$$P_2(q_2) = \left(1-\frac{\lambda_0+\lambda_{02}}{\mu_2}\right)\left(\frac{\lambda_0+\lambda_{02}}{\mu_2}\right)^{q}, \quad .(3)$$

$$q_2 = 0,\ 1,2,....$$

ME of the S_1 systems requirements number

$$\overline{q}_{11} = \sum_{n=1}^{\infty} n \sum_{m=0}^{\infty} P_1(n,m) \quad (4)$$

$$\overline{q}_1 = P_1(0,0)\cdot\sum_{n=1}^{\infty}\sum_{m=0}^{n}\binom{n}{m}\left(\frac{\lambda_{01}}{\mu_{11}}\right)^{m}\left(\frac{\lambda_{02}}{\mu_{12}}\right)^{n-m}; \quad (5)$$

$$q_{11} = q_{12} = 0,1,2,3.....$$

Accordingly, the mathematical expectation of the S_2 systems requirements number number of requi-?ements in the system S_2

$$\overline{q_2} = \sum_{k=1}^{\infty} P_2(k). \quad (6)$$

Service network response time

$$\overline{\tau_2} = \frac{\overline{q_1}+\overline{q_2}}{\lambda_0}. \quad (7)$$

ME of the requirements stay time in the S_1 system

$$\overline{u_1} = \frac{\overline{q_1}}{\lambda_0}. \quad (8)$$

ME of the requirements stay time in the S_2 system

$$\overline{u_2} = \frac{\overline{q_2}}{\lambda_{01}+2\lambda_{02}}. \quad (9)$$

Mathematical expectation of the lost packages number Q could be received from sensors to a mot when disabled

$$Q = \frac{\overline{q_2}}{\lambda_{01}+2\lambda_{02}}. \quad (10)$$

We assume that the recovery time of a node is a random variable that obeys the exponential distribution law with parameter β.

Then Q can be determined by the formula [15].

$$Q = \lambda_{01}/\beta. \quad (11)$$

Thus, the analytical dependencies (1) - (11) make it possible to determine the characteristics of the unreliable node required for the analysis of "bottlenecks", to increase the reliability of the network operation and to minimize threats to the WSN information security.

Conclusions

1. Wireless sensor networks can be defined as distributed communication systems. The reliability characteristics of their structural elements have an impact on information security.

2. The wireless sensor network may be simulated by the Queuing Network.

3. The main characteristics of the sensor network mot can be defined as the characteristics of the Queuing Network.

4. These analytical dependencies allow you to determine the characteristics of the unreliable node needed to analyze the "bottlenecks", to improve the reliability of the network and minimize threats to the wireless sensor network information security.

REFERENCES

1. Sergiyevskiy, M. "Wireless Sensor Networks", [Online], available at: http://www.compress.ru/Article.aspx?id=17950.
2. *Karl, H and Willig, A (2005). Protocols and Architectures for Wireless Sensor Networks.* John Wiley & Sons, Ltd., Hoboken, US.
3. Karabutov, A. "Sensor Networks", [Online], available at: http://offline.computerra.ru/2004/553/35459/.
4. Xiang, L., (2013), "Design Of Household Control System Based On ZigBee, GSM and TCP/IP Protocol, *10th IEEE International Conference on Control and Automation (ICCA),* pp. 1372-1375.
5. Кучук Н.Г., Гавриленко С.Ю., Лукова-Чуйко Н.В., Собчук В.В. Перерозподіл інформаційних потоків у гіперконвергентній системі / С.Ю. Гавриленко. *Сучасні інформаційні системи*. 2019. Т. 3, № 2. С. 116-121. DOI: https://doi.org/10.20998/2522-9052.2019.2.20
6. Nechausov A., Mamusuĉ I., Kuchuk N. Synthesis of the air pollution level control system on the basis of hyperconvergent infrastructures. *Сучасні інформаційні системи*. 2017. Т. 1, № 2. С. 21-26. DOI: https://doi.org/10.20998/2522-9052.2017.2.04
7. Mozhaiev M., Kuchuk N., Usatenko M. (2019) The method of jitter determining in the telecommunication network of a computer system on a special software platform. *Innovative technologies and scientific solutions for industries*, 2019. Vol. 4 (10), pp. 134-140. doi: https://doi.org/10.30837/2522-9818.2019.10.134
8. Зиков І. С., Кучук Н. Г., Шматков С. І. Синтез архітектури комп'ютерної системи управління транзакціями e-learning. *Сучасні інформаційні системи*. 2018. Т. 2, № 3. С. 60–66. DOI: https://doi.org/10.20998/2522-9052.2018.3.10
9. Гахов Р.П. Моделирование трафика беспроводной сети передачи данных / Р. П. Гахов, Н. Г. Кучук// Научные ведомости БелГУ. – 2014. – № 1 (172). – Вып. 29(1). – С. 175-181.
10. Свиридов А. С., Коваленко А. А., Кучук Г. А. Метод перерозподілу пропускної здатності критичної ділянки мережі на основі удосконалення ON/OFF-моделі трафіку. *Сучасні інформаційні системи*. 2018. Т. 2, № 2. С. 139–144. DOI: https://doi.org/10.20998/2522-9052.2018.2.24
11. Кучук Н. Г. Метод зменшення часу доступу до слабкоструктурованих даних / Н. Г. Кучук, В. Ю. Мерлак, В. В. Скородєлов // *Сучасні інформаційні системи = Advanced Information Systems*. – 2020. – Т. 4, № 1. – С. 97-102. doi: https://doi.org/10.20998/2522-9052.2020.1.14
12. Korchenko, O. Alyeksander M., Nadzhi Abdu and Petrenko, O. (2016), "Analysis of threats and mechanisms for ensuring information security in sensor networks", *Zakhyst informatsiyi,* Vol. 18, no1, pp. 48-56.
13. Stetsenko, I.V. (2010), *Modelyuvannya system: navch. posib.* [Systems Modeling: Tutorial. tool.],: CHDTU, Cherkasy, UA.
14. Tananko, I. Ye. and Dolgov, V. I. (2018), Fundamentals of system modeling: textbook. allowance, Nauka, Saratov, RU.
15. Lozhkovs′kyy, A.H. (2010), *Teoriya masovoho obsluhovuvannya v telekomunikatsiyakh* [Queuing theory in telecommunications], Odes′ka natsional′na akademiya zv″yazku, Odesa, UA.

Received (Надійшла) 16.09.2020
Accepted for publication (Прийнята до друку) 28.10.2020

Моделювання ненадійного вузла бездротової сенсорної мережі неоднорідною мережею масового обслуговування

О. А. Макогон, О. О. Дичко, О. В. Ісаков, Р. Р. Лазута , О. Ю. Осьмак, Л. Г. Троцько

Анотація. Предметом вивчення в статті є функціонування бездротової сенсорної мережі в недружньому середовищі. **Метою дослідження** є моделювання процесів, які відбуваються у бездротових сенсорних мережах, всебічного опису їх основних режимів роботи та аналізу "вузьких" місць задля підвищення надійності функціонування мережі та мінімізації загроз її інформаційної безпеки. **Задачі:** на основі аналізу технології побудови бездротової сенсорної мережі та процесів функціонування її елементів визначити характеристики надійності, що мають вплив на інформаційну безпеку; визначити структуру мережі масового обслуговування, подібну за структурою до бездротової сенсорної мережі як об'єкту дослідження; визначити основні характеристики вузла сенсорної мережі як мережі масового обслуговування; визначити аналітичні залежності для знаходження характеристик ненадійного вузла бездротової сенсорної мережі. Методологічною основою дослідження стали загальнонаукові та спеціальні **методи** наукового пізнання. Отримані **результати дослідження** дозволяють зрозуміти та вивчити процеси, що відбуваються у бездротових мережах масового обслуговування та спрогнозувати поведінку мережі у недружньому середовищі. Можливість зробити оцінку числа загублених пакетів дає розуміння надійності роботи вузлів мережі. **Висновки.** Бездротові сенсорні мережі можуть бути визначені як розподілені комунікаційні системи**.** Характеристики надійності їх структурних елементів мають вплив на інформаційну безпеку. Бездротова сенсорна мережа може бути смодельована мережею масового обслуговування. Основні характеристики вузла сенсорної мережі можуть бути визначені як характеристики мережі масового обслуговування. Приведені аналітичні залежності дозволяють визначити характеристик ненадійного вузла, необхідних для аналізу "вузьких" місць, підвищення надійності функціонування мережі та мінімізації загроз інформаційної безпеки бездротової сенсорної мережі.

Ключові слова: бездротова сенсорна мережа, ненадійний вузол, мережа масового обслуговування, характеристики надійності, загрози інформаційної безпеки.