# Research Availability of Devices Based on Wireless Networks

Nurzhan Bazhayev, Ilya Lebedev, Irina Krivtsova, Igor Zikratov
ITMO University
Saint-Petersburg, Russian Federation
nurzhan_nfs@hotmail.com, {lebedev, ikr, zikratov}@cit.ifmo.ru

***Abstract*—The wireless self-organizing network under attack was considered. The aim was to organize "a broadcast storm" in order to determine the availability of individual units, and the ability to carry out their functional tasks in an information exposure. A number of conditions for the organization of this type of attack by a potential intruder information security were identified. The analysis of system availability of devices based on wireless technologies was conducted. A model depending functioning of the system in the normal state and the implementation of an information system on the impact from a potential intruder was shown. The analytical modeling of self-organizing wireless network functioning normally and carrying out attacks aimed at organizing "broadcast storm." An experiment that provides obtaining statistical information on the work of the self-organizing network of remote devices was disclosed. The results of the experiment of a typical attack system, to transmit data via a broadcast network scanning package. A qualitative idea of the proximity of theoretical and experimental distributions of packet loss probability for different values of the intensities of the noise packets from the offending information security was checked.**

## I. Introduction

A permanent decline in the cost of wireless devices and improvement of quality indicators of time, energy and information characteristics of sensors makes these technologies very promising. The flexible architecture, increase the computing power of individual units can not only shift from standard wired devices, but also build self-sufficient with respect to multi-agent systems, carrying out the reception, processing, analysis of the received and transmitted data.

The implementation of self-organizing wireless networks is accompanied by the need to address other problematic issues of information security [1], [2].

Among the main vulnerabilities can provide an opportunity to listen to the channel, the premise of "external" packages, the implementation of physical access to the attacker's site, the lack of standardization of intelligent routing algorithms that take into account the state of the network. A large number of devices that provide an intelligent transmission, collection, processing data packets, their relative remoteness, autonomy of operation, dynamically changing topology, weak study models, methods and algorithms for concurrent detection of incorrect information from the compromised node determines the difficulty of creating the classic protection systems [3], [4], [5].

Some of the main potential vulnerabilities associated with the peculiarities of the functioning of the individual units. The need for the exchange of official information in the event of a number of internal and external events is sending broadcast packets between network nodes.

## II. Research statement

A typical network node includes a transceiver, a battery, a processing module which may be connected various detectors. In view of such a structure is necessary to effectively address the problems related to the conservation of energy, providing processing power and throughput characteristics of channels [6]. The combined solution of these problems leads to the presence of most of the protocols of a number of problematic issues implosion, and the blind overlay resources, making such technologies vulnerable to a series of attacks by hackers [7], [8].

Based on the features and operation of wireless networks using the recommended settings to optimize operation of the remote node wireless sensor network may exercise "a broadcast storm" [9], [10], [11].

The technology of this attack is associated with vulnerabilities that lead to a large increase in the service pack on the network. In the simplest case, if you allow the rules defined by the system administrator, then wheeled traffic growth can be generated broadcast messages. Analysis [6], [8], [10] brings out a number of conditions in the configuration settings for this type of attack:

- the absence of restrictions on the time to live;
- the presence of rules that allow to transmit a frame to the broadcast address to all except the node from which he resigned;
- the introduction of devices, continuously generating the message.

Especially it should be noted that to carry out destructive influences the potential infringer may have minimal capacity to dispatch bad frames. The result is a waste of resources to the reception, transmission, processing overhead, which is under load a wireless sensor network not only performs its functions, but also becomes unmanageable [9]. There is no possibility of rapid access and autonomous control devices

that are non-stop responding to events in the network. There is a threat to the implementation of the availability of a wireless sensor network devices due to deliberate action on the part of the attacker, to increase the number of broadcast and other service messages, resulting in blocked access to communication channels and nodes of the computer system. The vast majority of models describing the place in a wireless network processes that information does not include the possibility of exposure to a potential attacker.

Thus, in order to ensure information security (IS) of the wireless sensor network, there is a problem of probabilistic assessment of the availability of the devices under attack such as "broadcast storm".

## II. MODELING OF THE IMPACT ON THE SYSTEM

Carrying out an attack on the part of the attacker is reduced to increase the intensity of the receipt of applications, leading to the inability to service the total message flow device. Such a condition can occur in case of a configurable device when filling a buffer having a predetermined volume or unavailable channels, resulting in a loss of the application. There is a threat to the availability associated with limitations on authorized access to network elements, stored information, information flows, services and applications due to events affecting the network [10].

To simplify the model we consider relatively simple, do not have high processing power for the wireless sensor network, for example, a Zigbee technology, with limited functionality, receiving and transmitting a small limited range of types of messages without a priority with pre-configured parameters. A service duration depends on the number of events in a predetermined time interval. Assuming that the device claims arrival process is a poisson process, and the duration of service is distributed exponentially, it becomes possible to consider the processes of collection, processing and transmission of information, as the queuing system M / M / 1 / n.

Features a hardware implementation of autonomous wireless remote nodes suggest a buffer of input messages, which allows you to store several messages received for processing. Fig. 1 shows the transmission of data packets from A to B via the node C.

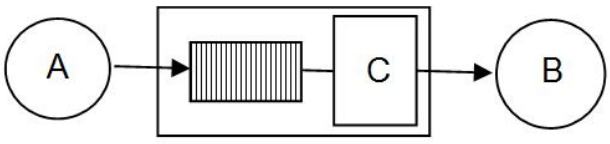



Fig. 1. The transmission scheme of information packets from A to B, via the wireless network node

Assuming that the process of receipt of applications is a Poisson process, and the duration of service is distributed exponentially, it becomes possible to consider the processes of collecting, processing and transmitting information, such as queuing system M / M / 1 / n.

Applying the theory of queuing systems can be assumed that the probability of packet loss during transmission from A to B via one device C will be determined by the formula (1):

$$P_{loss} = \rho^n \frac{1-\rho}{1-\rho^{n+1}}, \ \rho = \frac{\lambda}{\mu} \qquad (1)$$

where in $\lambda$ - the input flow, $\mu$ is the intensity of the service, n - the size of the input buffer processing device.

Fig.2 and Fig.3 shows the dependence of the probability of loss of information packets passing through one device.

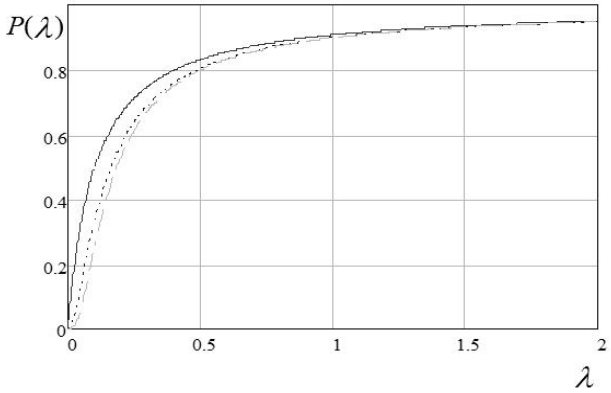



Fig.2. Dependence of the probability of loss of information when changing the package $\lambda$ - is the intensity of input

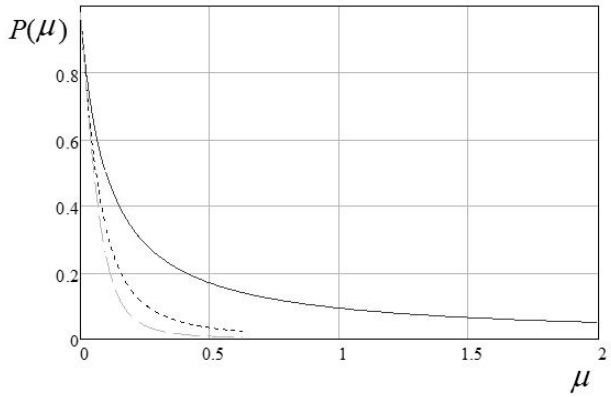



Fig. 3. Dependence of the probability of loss of the information packet at change $\mu$ - is the intensity of service

The curves shown in Fig.2 and Fig.3 may be useful for evaluating the optimum size of a package handling devices in a wireless network as the amount of transmitted and received bytes, impact on the possible number of simultaneously stored in the buffer device messaging service rate and the intensity of the input messages.

In the process of transmitting information in a wireless network information flow passes through several such devices.

To estimate the probability of packet loss, passing by k units expression (1) takes the form:

$$P_{loss} = 1-(1-\rho^n \frac{1-\rho}{1-\rho^{n+1}})^k \quad (2)$$

Fig.4 and Fig.5 show graphs of the probability of loss of the information packet that passes through multiple devices.

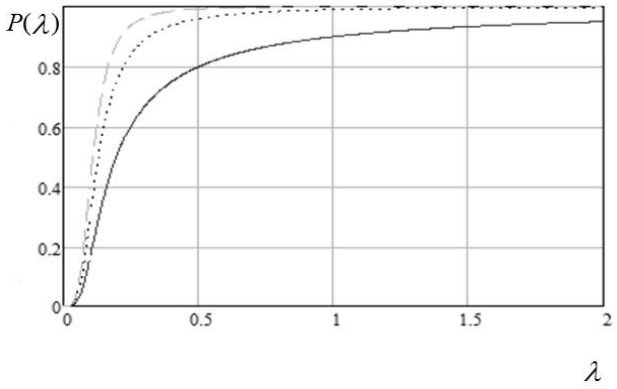



Fig. 4. The dependence of the probability of loss of information when changing the package $\lambda$ - is the intensity of the input stream

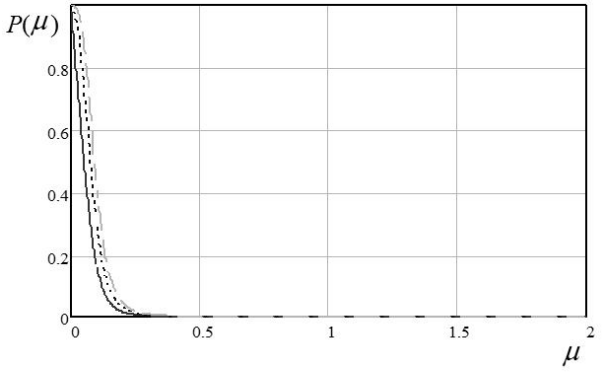



Fig. 5. The dependence of the probability of loss of the information packet at change $\mu$ - is the intensity of service

Most probabilistic models implemented evaluation systems does not imply the existence of a potential attacker, whose actions are aimed at exploiting vulnerabilities used protocols and system components.

However, a certain openness and accessibility of the network allow an attacker to perform actions to increase the intensity distribution of frames that do not contain the correct information, a bad checksum, the wrong title, which lead to an unjustified waste of resources on the part of the system.

Fig.6 shows the effect on the sequence of the chain of devices that transmit data packets to the intensity $\lambda_p$. An attacker on the network increases the number of events causing the generation of broadcast frames, with intensity $\lambda_{sh}$.

Received broadcast frame is processed by a wireless network and is relayed to the next node. In the presence of a powerful transmitter, a plurality of nodes at the same time affecting the wireless network, there is a growing junk traffic network.

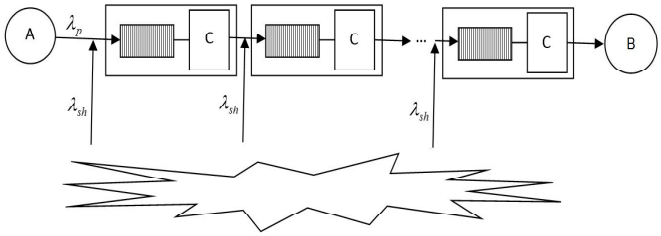



Fig. 6. Impact on the chain of devices

Using expressions (1) and (2) the probability of packet loss in the network, subject to a broadcast storm, is given by:

$$\begin{cases} P_{loss} = 1-\left(1-\left(\frac{\lambda_p+\lambda_{sh}}{\mu}\right)^n \frac{1-\left(\frac{\lambda_p+\lambda_{sh}}{\mu}\right)}{1-\left(\frac{\lambda_p+\lambda_{sh}}{\mu}\right)^{n+1}}\right)\prod_{k=2}^{m}\left(1-\left(\frac{\mu+k\lambda_{sh}}{\mu}\right)^n \frac{1-\left(\frac{\mu+k\lambda_{sh}}{\mu}\right)}{1-\left(\frac{\mu+k\lambda_{sh}}{\mu}\right)^{n+1}}\right), k \geq 2 \\ P_{loss} = 1-\left(1-\left(\frac{\lambda_p+\lambda_{sh}}{\mu}\right)^n \frac{1-\left(\frac{\lambda_p+\lambda_{sh}}{\mu}\right)}{1-\left(\frac{\lambda_p+\lambda_{sh}}{\mu}\right)^{n+1}}\right), k=1 \end{cases} \quad (3)$$

where in $\lambda_p$ - is the intensity of the useful traffic, $\lambda_{sh}$ - the intensity of the noise of traffic, $\mu$ - is the intensity of service, $n$ - the size of the input buffer processing device, $k$ - is the number of devices found in the path of the package.

Fig.7, Fig.8, Fig.9 show the dependence of the probability of loss from the package, $\lambda_p$ is the intensity of the useful traffic, $\lambda_{sh}$ is the intensity of the noise of traffic, $\mu$ is the intensity of service.

Despite the possibility of limiting the admitted assumptions characteristic of the mathematical apparatus of SMO, such models allow us to estimate the probability state of the system and levels of indicators specific to its operation in harsh conditions and environments, taking into account the intruder. With regard to consideration the type of attack, the model takes into account the possibility of the person carrying out the impact on the intensity of the events causing the generation of broadcast packets.

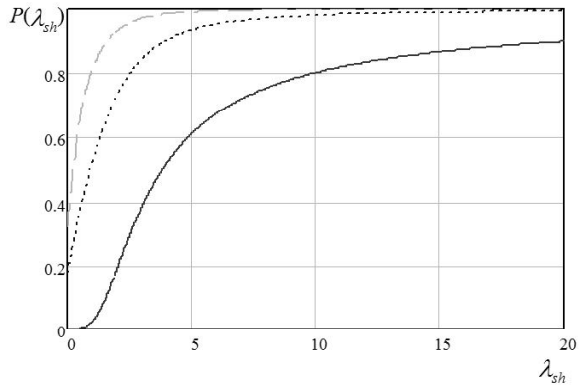



Fig. 7. Dependence of the probability of loss of information when changing the package, $\lambda_{sh}$ - is the intensity of the noise of traffic

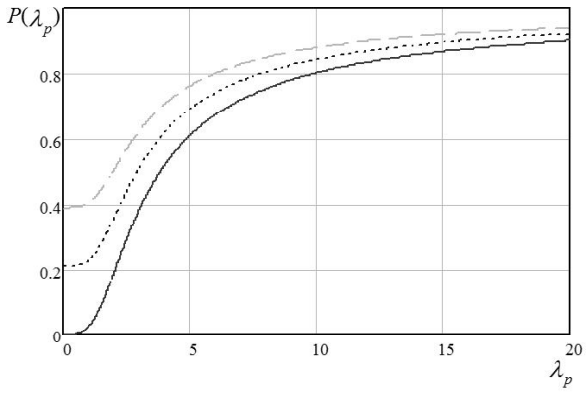



Fig. 8. Dependence of the probability of loss of information when changing the package, $\lambda_p$ - is the intensity of the useful traffic

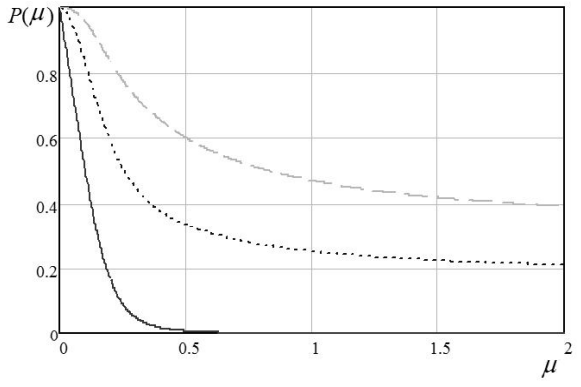



Fig. 9. Dependence of the probability of loss of the information packet at change, $\mu$ - is the intensity of service

## III. EXPERIMENT

To implement the experiment was configured wireless network based devices Telegesis, presented in Fig.10, consisting of several units. From device A to device B transmitted messages at a rate of 250 kbit/sec. A node C contained sniffer generating broadcasts.

The purpose of the experiment was to obtain quantitative availability terminal. As used metric of lost packets. Each node can accept messages only from two sites, one of which was the sniffer sends broadcast packets, and the other - the node providing data traffic by relaying all received packets. On the terminal node received packets are analyzed and determined by the statistics of lost and unrecognized messages.

The percentage of lost and unrecognized information packets in the configured communication channel for the speed of 250 kbit/sec at a frequency of generation of 14 packs, query nodes in the network, in the second of the sniffer is shown in Fig.11 and Fig.12.

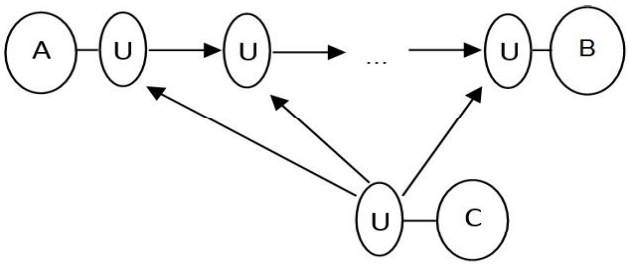



Fig. 10. The scheme of the system for the experiment

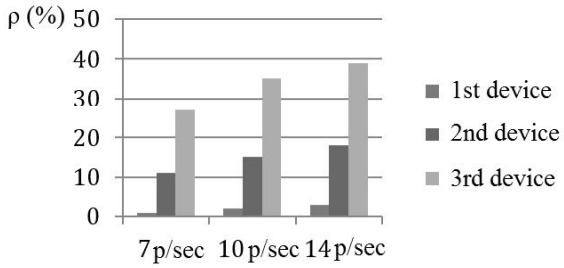



Fig. 11. A packets loss p (%), depending on the number of devices, the transmission frequency broadcast type AT + N

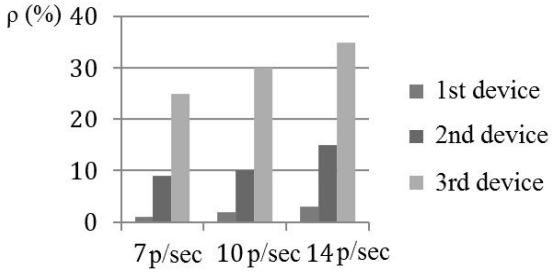
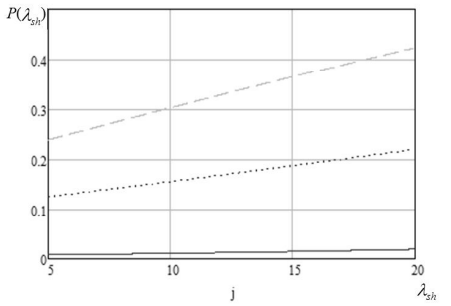



Fig. 12. A packets loss p (%) depending on the number of devices, the transmission frequency broadcast type AT + SN: 00

## IV. ANALYSIS OF THE RESULTS OF THE EXPERIMENT

Comparing charts theoretical probability of packet $P_{loss}$ (Fig. 13) with histograms in Fig.11 and Fig.12, you can make a qualitative idea of the proximity of theoretical and experimental distributions of packet loss probability for different values $\lambda_{sh}$.




| Parameter | Value for the experiment |
|---|---|
| $\lambda_p$ | 120 messages per second |
| $\lambda_{sh}$ | 1 to 15 |
| $\mu$ | 180 messages per second |
| $n$ | 10 messages |
| $k$ | 1,2,3 |

Fig. 13. Model according to the experimental values

Fig.14 shows histograms of the experimental values of packet loss for different values $\lambda_{sh}$. for k = 3 devices.

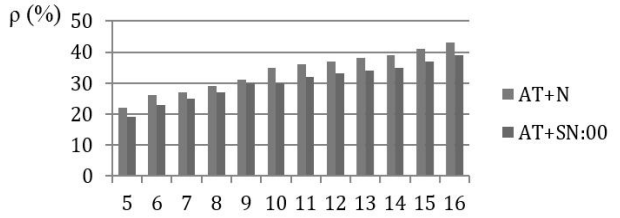



Fig. 14. The experimental values of losses parquet ρ (%) of broadcast messages for k = 3

Testing statistical hypothesis that received the experimental distribution is different from the theoretical, carried out at the level of significance $\alpha$ = 0,05 for Pearson ($\chi^2$ 2 - criterion):

$$\chi_v^2 = \sum_{j=1}^{l} \frac{(n_j^* - np_j)^2}{np_j} \qquad (4)$$

when the number of degrees of freedom $v$= 9, n = 100 sample volume.

It is known [12] that the number of events in npj formula (4) in the intervals $\lambda_{sh}$ expected parameter values may be equal to two, if l ≥10. Therefore, in accordance with the formula (3), for example, k = 3 $\lambda_{sh}$ = 5. The critical value for the corresponding table [12] found a criterion and still $\chi^2_{cr}$ = 16.919, the experimental value $\chi^2_{ex}$ criterion is calculated using the formula (4), while the inequality $\chi^2_{ex} < \chi^2_{кр}$.

It follows that at the level of significance $\alpha$ = 0,05 can be argued that the discrepancies between the theoretical and experimental $P_{loss}$ probability distributions of packet loss in the network, a broadcast storm-prone, at various specified values of intensity noise of traffic $\lambda_{sh}$ not statistically significant.

Thus, the assumption of the Poisson flow of the process of receiving applications and exponential distribution service time confirmed by the data of the statistical analysis of wireless networks load.

## VI. Conclusion

The widespread emergence of wireless networks, the ability to detect them outside the controlled area, making them an attractive target for attempts at various kinds of attacks. A potential attacker with the scanner of radio, protocol scanner software to decode the dongle has sufficient capacity for the organization of eavesdropping, radio coverage and creating a false access point wireless sensor network.

The implementation of a large number of projects on the basis of technology Bluetooth, ZigBee, WiFi, their use in intelligent transport systems, local area networks, sensor networks makes it necessary to provide the required level of security circulating in their data [12], [13], [14], [15].

The proposed model makes it possible to explore the availability of devices, wireless network vulnerable to attack, "broadcast storm" based on the performance of the intensities of the transmitted and received data messages, allowing you to select various settings and thresholds lengths, the buffer size during system configuration, the number of packets, limiting "the limb of one or other system resources." The proposed model takes into account the characteristics of intruder behavior and does not require a significant investment of computational resources, setting up special computational experiments in identifying common patterns in the behavior of the system.

## References

[1] P. Kumar, M. Ylianttila, A. Gurtov, S.-G. Lee, H.-J. Lee, An Efficient and Adaptive Mutual Authentication Framework for Heterogeneous Wireless Sensor Networks-based Applications, *MDPI Sensors*, 14(2), 2732-2755, 2014.

[2] Sridhar, P., Sheikh-Bahaei, S., Xia, S., Jamshidi, Mo. Multi agent simulation using discrete event and soft-computing methodologies // *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics 2*, 2003, pp. 1711-1716

[3] Page J., Zaslavsky A., Indrawan M. Countering security vulnerabilities using a shared security buddy model schema in mobile agent communities // *Proc. of the First International Workshop on Safety and Security in Multi-Agent Systems (SASEMAS 2004)*, 2004. – P. 85–101.

[4] Zikratov., E. Kozlova., T. Zikratova. Vulnerability Analysis robotic systems with swarm intelligence // *Scientific and technical journal of information technologies, mechanics and optics.* – 2013. – № 5 (87). – P. 149–154.

[5] Zikratov, I. Lebedev, A. Gurtov, Trust and Reputation Mechanisms for Multi-agent Robotic Systems, Lecture Notes in Computer Science Volume 8638, 2014, pp 106-120. *(Proc. of the Internet of Things, Smart Spaces, and Next Generation Networks and Systems)*

[6] Wyglinski, A.M., Huang, X., Padir, T., Lai, L., Eisenbarth, T.R., Venkatasubramanian, K. Security of autonomous systems employing embedded computing and sensors//*IEEE Micro 33 (1) 2013,* art. no. 6504448, pp. 80-86

[7] Lebedev I.S., Korzhuk V.M. The Monitoring of Information Security of Remote Devices of Wireless Networks // *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial*

*Intelligence and Lecture Notes in Bioinformatics)* - 2015, Vol. 9247, pp. 3-10

[8] M. Prabhakar, J. N. Singh, G. Mahadevan Nash equilibrium and Marcov chains to enhance game theoretic approach for vanet security. // *International Conference on Advances in Computing, ICAdC 2012;* Bangalore, Karnataka; India; 4 July 2012 through 6 July 2012, Volume 174 AISC, 2013, pp 191-199

[9] Korzun D.G., Nikolaevskiy I., Gurtov A.V. Service Intelligence Support for Medical Sensor Networks in Personalized Mobile Health Systems // *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* - 2015, Vol. 9247, pp. 116-127

[10] Recommendation ITU-T X.805. Security architecture for systems providing end-to-end communications.

[11] Nikolaevskiy I., Lukyanenko A., Polishchuk T., Polishchuk V.M., Gurtov A.V. isBF: Scalable In-Packet Bloom Filter Based Multicast // *Computer Communications - 2015*, Vol. 70, pp. 79-85

[12] E.I. Kulikov. Applied statistical analysis: a manual for universities / E.I. Kulikov. – 2-nd edition., revised and updated. – *M.: Goryachaya liniya-Telecom*, 2008. – pp. 464.

[13] S. Komov. Terms and definitions in the field of information security. – *M., AC-Trasm*, 2009. -304 P.

[14] Kumar P., Gurtov A.V., Linatti J., Ylianttila M., Sain M. Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments // *IEEE Sensors Journal - 2015*, Vol. PP, No. 99, pp. 1

[15] Al-Naggar Y.,Koucheryavy A. Fuzzy Logic and Voronoi Diagram Using for Cluster Head Selection in Ubiquitous Sensor Networks // *Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 14th International Conference, NEW2AN 2014 and 7th Conference*, ruSMART 2014 Saint-Petersburg, Russia, August 27–29, 2014, Proceedings. Springer, LNCS 8638, – PP. 319–330.

[16] Chehri A.,Hussein T. Moutah Survivable and Scalable Wireless Solution for E-health and Emergency Applications. // *In EICS4MED 2011. Proceedings of the 1st International Workshop on Engineering Interactive Computing Systems for Medicine and Health Care.* Pisa, Italy. – 2011. – PP. 25–29

[17] Koucheryavy Y.A., Ometov A.Y., Andreev D.S. On the role of wireless technologies in the development of the Internet of Things. // *Information Technology and Telecommunications*. – 2014. – N 3 (7). – PP. 31–40.