

THE APPLICATION OF REDUNDANCY IN LEACH PROTOCOL

Volodymyr Mosorov, Sebastian Biedron, Taras Panskyi

Lodz University of Technology, Institute of Applied Computer Science

Abstract. Nowadays wireless sensor networks have gained much popularity due to their flexibility. This progress has enabled the use of sensor nodes on an unprecedented scale and opened new opportunities for the so-called ubiquitous computerization. The total freedom of nodes distribution within the wireless sensor network (WSN), where the wireless characteristic is one of the greatest advantages of WSN, implies its greatest weaknesses. To overcome this challenge specialized routing protocols, such as many different version of LEACH, were ushered in so as to make effective use of the energy of the nodes themselves. This article aims to show the functioning of a new author's solution, called IIS-LEACH, which uses redundancy as a basic element in increasing the reliability of WSN networks.

Keywords: LEACH, reliability, node, IIS-LEACH

ZASTOSOWANIE NADMIAROWOŚCI W PROTOKOLE LEACH

Streszczenie. W dzisiejszych czasach bezprzewodowe sieci czujników zyskują coraz to większą popularność ze względu na swoją elastyczność. Postęp ten, umożliwił zastosowanie węzłów sensorowych na niespotykaną dotąd skalę i otworzył nowe możliwości dla tzw. wszechobecnej komputeryzacji. Całkowita dowolność w rozmieszczeniu węzłów jak i jego bezprzewodowy charakter, stanowiący jedną z największych zalet wykorzystania bezprzewodowych sieci sensorowych, implikuje jego największą słabość – ograniczenia związane z mobilnymi źródłami zasilania oraz nowymi problemami w zachowaniu niezawodności sieci. W celu efektywnego wykorzystania energii węzłów, zaczęto stosować wyspecjalizowane protokoły routingu takie jak LEACH. Celem tego artykułu będzie pokazanie nowej, zmodyfikowanej wersji tego protokołu o nazwie IIS-LEACH.

Słowa kluczowe: LEACH, niezawodność, sensor, IIS-LEACH

Introduction

Technological progress in the twenty-first century, which resulted in the development of fields such as digital electronics, miniaturization and wireless communication devices, enabled the construction of multi-functional, economical and low-cost wireless sensor networks (WSN). Sensor networks are a new branch network, which largely differs from traditional wireless networks and IEEE 802.11 networks, such as mobile phones networks and MANET (ang. Mobile ad-hoc network) [4]. Self-organization of these networks, the management of mobility and routing has been designed so that as much as possible to ensure an appropriate level of QoS communication with the optimum use of the resources.

The first concept of such a network was proposed by Kristofer Pister, who began research in the late twentieth century as a professor at the University of California at Berkeley. Very important of further studies of wireless sensor network had rapid development of nanotechnology that was a consequence of the emergence of sensors that reach the size of up to 2.5 millimeters [7].

Sensor networks are usually homogeneous networks. Apart from base stations all nodes are identical and perform the same role. The nodes are arranged in so-called field sensors. Their number depends on the purpose of the network, and may consist from several to tens of thousands sensors. Sensor network nodes can be equipped with various types of measuring devices, which leads to perform different functions. This type of network is used to monitor the change in the weather, the state of the patient or even follow deformations or vibrations in the construction industry, where it may become an early warning system [1, 2]. This could prevent of disasters, accidents and contribute to improve the design and technology.

Putting these small devices often in such sensitive areas requires equipment protocols and algorithms used in a sensor network with the ability to quickly self-organize, and reliability features.

It should be noted that a large part of the sensor network is not possible to replace or attach the power source, and therefore the problem of use and optimal energy management is a priority in the sensor network. Such devices are usually equipped with a power supply (1.2 V). Battery consumption is equivalent to the damaged node. Depending on the construction of a network the loss of one or more nodes forces the network to reconfigure their connections. This leads to changes in the network topology and the need for re-alignment. Reconfiguration can drain more energy from still active nodes which in turn will lead to further instability. Therefore, power management becomes enormous importance. New

improvements and solutions in the construction of the nodes have to allow inter alia their longer life. There are attempts to recover energy from the surrounding environment. Paul Wright developed nodes obtaining up to 200 mW of power from vibrations reaching the sensor.

Moreover, there are attempts to generate energy from light, heat and electromagnetic fields. An important factor is the proper usage of energy. Most resource is used for two tasks: data collection and communication. Pre-processing of data already in the memory of the sensor allows limiting energy-drain transmission to a minimum. Helpful is also a sensor configuration in such a way that it enter into a state of latency [3]. Sensor wakes up only to the collection, processing or data transmitting. Thereby, drastic solution significantly extends the life of the node. Despite of this, the device can run out of energy or may be damaged.

In some cases, when several sensors are damage it could separate the network into two parts that do not interact. The easiest way to prevent the degradation of a network is a dense arrangement of nodes. This solution will create a lot of potential routes for data transfer. With such a large number of connections data transmission in a disorganized manner would be a big waste of energy. Therefore, instead of a broadcast communication in the network data routing has been applied [5].

The purpose of this article is to use the redundancy in WSN using the original solution in the LEACH protocol. Redundancy in the protocol enables a reliable transmission of information to the base station. Presented IIS-LEACH protocol is a new technique to increase security in the exchange of information in WSN networks.

1. Node in a sensor network

The WSN is built from any number of sensors called nodes. Each node may be assigned different tasks, which results in a high diversity of the nodes and their structure. All nodes within a sensor network share similar features and modules. Each sensor has a power, transmission, measurement, and calculation module. A simplified diagram of the construction of a single node is shown in Figure 1.

The measurement module consists of a sensor that examines the surroundings and is the smallest element of the device. Figure 2 shows a configuration of the MEMS (Micro-Electro-Mechanical Systems). Other sensors can measure, e.g. temperature, humidity, radioactivity, speed, motion, chemical composition. The type of the measured parameter depends on the type of the sensor used. Some sensor network nodes allow the use of several types of sensors.

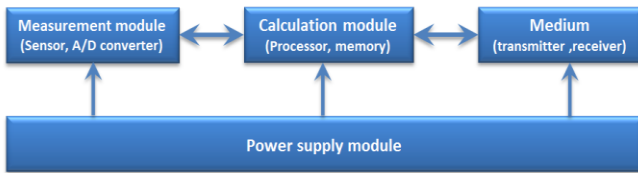


Fig. 1. Schema of a WSN node

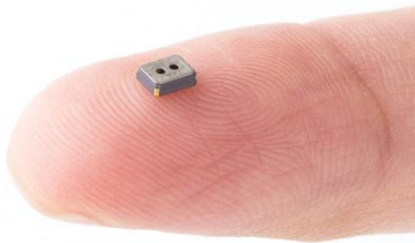


Fig. 2. FIGARO TGS8100 sensor (H_2 , CO, cigarette smoke) [8]

Having completed the measurement the sensor transmits the data to the A/D converter. The purpose of the converter is to convert the signal to the digital form and forward it on. Sensor networks can be designed so that they are alert even on stand-by. This solution is applied when the network is to be continuously alert or respond to specific events only. For example, if we are interested in measuring the concentration of CO in the air, we can use appropriate filters so that we can set the sensitivity of the device. Then, the signal processed by the sensor must first penetrate through the filter. When it has met the specific requirements, the signal is passed and starts the process of activating the device.

The calculation module is one of the most important parts of the device. Its main purpose is to control the tasks and perform calculations. The module consists of a PCB board on which a microcontroller or microprocessor is integrated with the memory, interfaces and permanent record memory. The ROM, RAM and Flash memories are small in size and at best reach the size of 1 megabyte.

The medium is the most resource-consuming part of the sensor. The media are utilised by the nodes to communicate and transfer data between themselves.

The power supply module is primarily the energy storage element. The power supply system is the weakest link in the functioning of the entire platform. Depending on the size and purpose of the device different solutions are applied. Larger devices have replaceable power sources: batteries, rechargeable connectors, and many other solutions. Smaller devices are equipped with non-replaceable energy sources, solar cells and mechanisms harvesting energy from vibration or temperature differences. Still, new solutions are being sought to resolve the energy issue. Figure 4 shows energy consumption of a node in the subsequent stages.

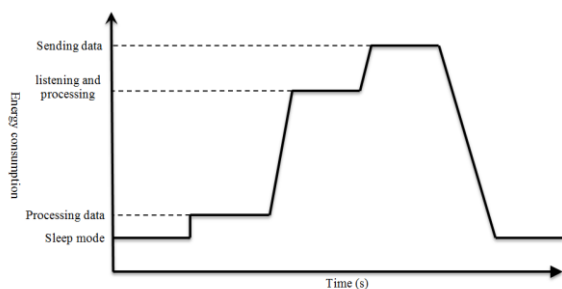


Fig. 3. Phases of energy consumption of a node

Software is one of the most important elements in the structure of the sensor, whose task is to monitor and manage the modules. The operating system which can be stored in the node's microcontroller memory can ensure response to incidents and concurrent

performance of many activities conducted within sensor networks. A node can utilise, e.g. scheduler software, databases, wireless communications maintenance programme, networking programme, power management programme, and even encryption technology ensuring data confidentiality.

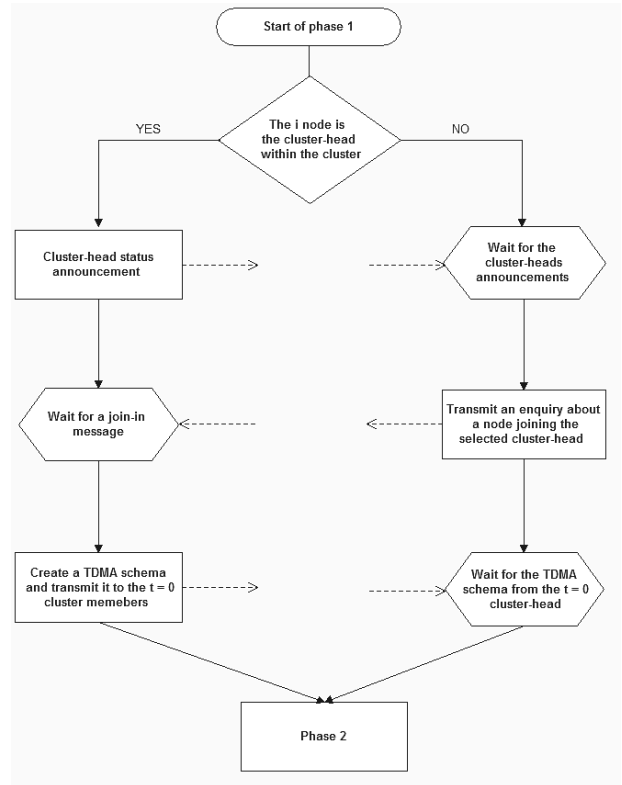


Fig. 4. Cluster-heads selection in the LEACH protocol

2. LEACH protocol

Low Energy Adaptive Clustering Hierarchy (LEACH) is a protocol that operates based on hierarchical routing protocols. The protocol creates a so-called “cluster” comprised of a group of sensors which communicate with one and the same cluster-head. The cluster-heads are selected in a random rotation, which has greatly helped to reduce energy consumption and uniformly distribute the energy load between individual network nodes. The LEACH protocol utilises location coordinates to achieve appropriate network scalability and data aggregation, which enables reduction of the amount of data flowing to the cluster-head.

The functioning of LEACH protocol [6]:

- The first phase comprises clusters formation and cluster-heads selection. Each node generates a random number between 0 and 1. If the number turns out to be less than the threshold value $T(n)$ the node becomes the cluster-head of the cluster. The $T(n)$ value is calculated as follows:

$$T(n) = \begin{cases} \frac{p}{1 - p \cdot \text{mod}(\frac{1}{p})} & n \in G \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

where, p – expected number of nodes to become cluster-heads, G – set of nodes participating in the selection process.

The newly selected cluster-head transmit a message/communication to all the nodes within the network. The nodes join those cluster-heads from which they receive the most powerful signal. When all the information regarding affiliation with the cluster-head has been transmitted, the cluster-head assigns to the sensor nodes time slots that are consistent with the TDMA technique that enable them to transmit data.

- The second phase consists in collecting and transferring data to the cluster-head that aggregate and transmit them to the base station. During this phase the nodes within the cluster perform

their tasks and then transmit the results to the cluster-head at the designated time slots. The data are transmitted to the database by the cluster-heads which aggregate the data to all the nodes within the cluster. After sometime within the WSN, the network once again passes through the first phase. In the communication process, each cluster code utilises a different CDMA code, which minimises the interference issue.

3. Redundancy in LEACH protocol

Sensor networks, given the arrangement of sensors in the field, are exposed to many risks [13, 14]. They can result from intentional damage or random failure during functioning.

In most applications, a sensor network has limited energy resources and computing capabilities of individual nodes compared to cable IP networks, so it is important to ensure an adequate level of reliability, to the environmental problems or for example hostile attack, that they can perform their functions and continue to collect data and transfer it to the base station [9].

LEACH protocol, unfortunately, does not have the mechanisms implemented in its design to ensure reliable communication in the event of random failure of the cluster-head in the cluster. Nodes in case of cluster-head failure will be still sending to it their data [11, 12].

The selection of cluster-head is determined by random system without taking the residual energy of nodes into account, so once a node with less energy is selected to be cluster-head, its energy will dissipate quickly, and then the nodes within this cluster will lose touch with its cluster-head and sink [10]. In other words, it will accelerate energy dissipation, shorten the lifetime of the network, and at worst put the network out of action.

3.1. IIS-LEACH

One of the new developments presented in modified version of LEACH called IIS-LEACH provides that much needed reliability. The functioning of the protocol IIS-LEACH as in the case of LEACH protocol consists of two phases:

Phase 1. In phase one the base station starts transmitting the test signal to all the nodes. On this basis each node calculates its distance from the base station using the following formula [14]:

$$FSPL (dB) = 20\log_{10}(d) + 20\log_{10}(f) + K \quad (2)$$

where, d – distance, f – frequency, K – constant that depends on the units used for d and f , $FSPL$ – Free Space Path Loss. For d and f in meters and kilohertz, respectively, the constant becomes – 87.55. For d, f in meters and megahertz, respectively, the constant becomes – 27.55. For d and f in kilometers and megahertz, respectively, the constant becomes – 32.45.

$$d = 10(\text{Free Space Path Loss} - K - 20\log_{10}(f)) / 20 \quad (3)$$

The cluster-head is selected according to the following selection algorithm [6, 8]:

$$k = \sum_{i=1}^N P_i(t) * 1 \quad (4)$$

where, k – number of clusters during each round, N – number of nodes in the network, $P_i(t)$ – is the probability with which node i elects itself to be cluster-head at the beginning of the round $r+1$ which starts at time t .

$$P_i(t) = \begin{cases} \frac{k}{N - k * (r \bmod \frac{N}{k})} & C_i(t) = 1 \\ 0 & C_i(t) = 0 \end{cases} \quad (5)$$

where, $C_i(t)$ determines whether node i has been a cluster-head in most recent $(r \bmod (N/k))$ rounds.

Once the cluster-heads N has been selected, it is transmitted to all the other nodes information of their existence. While receiving this information the nodes decide which cluster they want to join. Their choice is primarily informed by the strength of the signal received from the cluster-heads. In the next step sensor nodes

inform the selected cluster-heads that they will be members of their clusters by sending a message with information about their power supply status, distance from base station and cluster-head N . Having received such applications, each cluster-head selects its supplementary node, like shown in Figure 5, where the selection criterion is the shortest distance from the cluster-head and the appropriate condition of the power source calculated according to the following formula:

$$SM + LM + PD + SD < PS \quad (6)$$

where, SM – energy consumption during standby mode, LM – energy consumption during listening mode, PD – energy consumption during processing data, PS – power supply status, SD – energy consumption during sending data:

$$SD = E_{ss} d \epsilon_{amp} \quad (7)$$

Phase 2. During phase two of the WSN network the protocol based on IIS-LEACH sets the supplementary node in the listening watch mode to collect information from the other nodes in the same way as the cluster-head. At the end of the second phase the cluster-head informs the listening node that it has sent collected data to the base station. If the cluster-head were damaged, the listening node after a certain time (t) would send the collected data to the base station

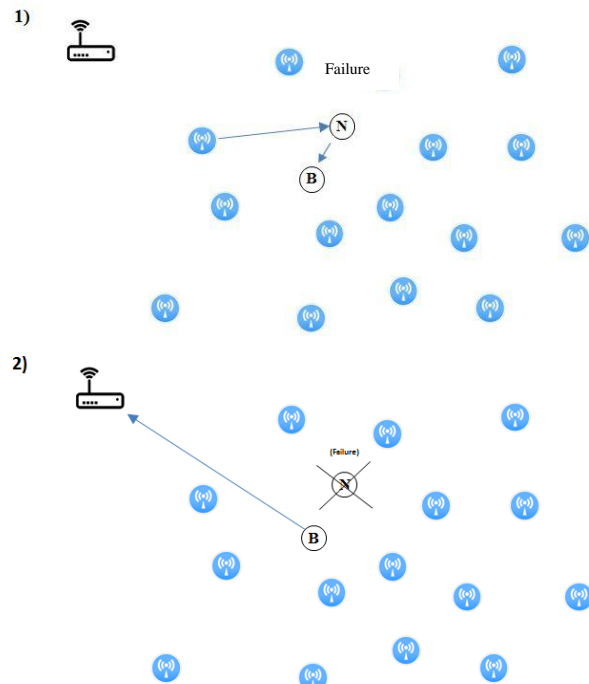


Fig. 5. Redundancy in IIS-LEACH

3.2. Simulation

The present study aims to determine how the life of a network is affected by the number of mobile sensors in the test environment using LEACH and ISS-LEACH protocol. The test involved MATLAB software using parameters from Table. 1. A test environment has been generated in which the nodes are randomly arranged upon the test. Each such node has its mobile source of energy and present energy consumption level, depending on their function and the number and distance of the transmitted data.

In the experiment, we assume:

- after the position of nodes was randomly chosen they do not change it to the end of the test;
- the supplementary node do not gather information from its monitoring equipment;
- authors do not know the physical localization of nodes in network area.

Table 1 Parameters used in test

Parameters	Value
Network area	100 m × 100 m
Number of nodes	100, 200, 300, 400, 500, 600
Number of rounds	1000
Sink location	50, 50
Initial energy	0.5 J
Packet Length	6400 bit
ETX (Transmitter circuit consumption)	0.00000005 J
ERX (Receiver circuit consumption)	0.00000005 J
Amplification energy	0.000000001 J

In the experiment have been selected 1000 rounds to show visible changes in the functioning of LEACH protocol and its proposed version with the option of the redundancy – IIS-LEACH. The number of sensors is increased by 100. The purpose of this amendment is to show how changes the energy system of both protocols, when in the investigated area occurs the placement of a greater number of sensors. The sum of the energy of nodes using the protocol with redundancy IIS-LEACH and standard LEACH is shown in Figure 6. The red curve determines the functioning of the protocol IIS-LEACH. Its total energy of 1000 rounds is slightly lower than the LEACH protocol. This small difference is a result of the redundancy protocol mechanism.

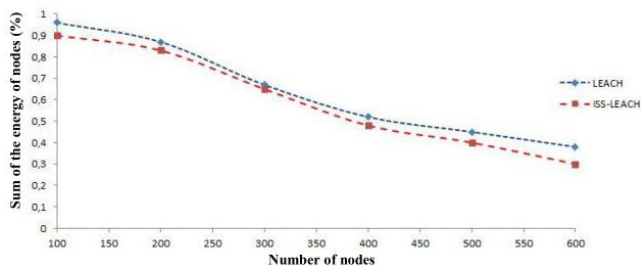


Fig. 6. Sum of energy after 1000 of rounds for networks created from different number of nodes, using IIS-LEACH and LEACH

4. Conclusion

WSN turn out to be a very interesting and forward-looking technology. Its resources and capabilities are negligible, yet the potential of the device is massive. Equipped with appropriate gauging sensors it can acquire any type of data, and with a little help from the other nodes it can process and transmit such data. The nodes can be scattered, nevertheless they will automatically activate and create a network.

Redundancy in LEACH protocol is a very useful option if it is very important periodically collect data from the area and you cannot afford that information will not be delivered. The new protocol provides this functionality, enabling thus its use in situations where the underlying protocol LEACH not meets our expectations. The experiment showed that the battery consumption increased slightly in favour of the reliability of data transmission. The next stage of the development of the said protocol will see the implementation of an even selection of the cluster-head within the cluster.

References

[1] Abbas Z., Javaid N., Khan M.A., Ahmed S., Qasim U., Khan Z.A.: Simulation Analysis of IEEE 802.15.4 Non-beacon Mode at Varying Data Rates. Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012.

[2] Ahmed S., Sandhu M.M., Amjad N., Haider A., Akbar M., Ahmad A., Khan Z.A., Qasim U.: iMOD LEACH: improved MODified LEACH Protocol for Wireless Sensor Networks, Journal of Basic and Applied Scientific Research, 2013

[3] Bakr B. A.: LEACH-SM: A Protocol for Extending Wireless Sensor Network Lifetime by Management of Spare Nodes. Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2011, 277–278

[4] Diane L., Kacimi R., Mammeri Z., Niang I.: Energy Optimization based on the Redundancy in WSNs. 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), Dubai, 2013, 1–7 [DOI: 10.1109/WMNC.2013.6548980]

[5] Faludi R.: Building Wireless Sensor Networks, O'Reilly Media, 2010

[6] Hayat S., Javaid N., Khan Z. A., Shareef A., Mahmood A., Bouk S. H.: Energy Efficient MAC Protocols in Wireless Body Area Sensor Networks. 5th International Symposium on Advances of High Performance Computing and Networking (AHPCN-2012), 2012.

[7] Heinzelman W., Chandrakasan A., Balakrishnan H.: Energy-Efficient Communication Protocols for Wireless Microsensor Networks. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, vol. 2, 2000 [DOI: 10.1109/HICSS.2000.926982].

[8] <http://www.figaro.co.jp/en/topic/2014/03/announcement-of-new-mems-type-air-quality-sensor-tgs8100.html> [19.05.2016]

[9] Lewis F.L.: Wireless Sensor Networks, Smart Environments: Technologies, Protocols, and Applications, 2004.

[10] Liao Q., Zhu H.: An Energy Balanced Clustering Algorithm Based on LEACH Protocol. Proceedings of the 2nd International Conference On Systems Engineering and Modeling (ICSEM-13), 2013.

[11] Mursleen M., Singh R.: An Improved LEACH protocol with reduced data redundancy for wireless sensor networks, Vol 5, No 3/2014, 331–341.

[12] Najgebauer A., Dyk M.: Sieci sensorowe dla potrzeb pozyskiwania danych w symulacji wielorozdzielczej. Symulacja w Badaniach i Rozwoju, Vol. 2, No. 4/2011, 197–207

[13] Raed M., Hani B., Abdalraheem A., Ijeh A.: A Survey on LEACH-Based Energy Aware Protocols for Wireless Sensor Networks, Journal of Communications, Vol. 8, No. 3, 2013, 192–206.

[14] Sehgal N., Kaur G.: Improved Cluster Head Selection Using Enhanced LEACH Protocol. International Journal of Engineering and Innovative Technology (IJEIT), Vol. 3, Issue 3/2013, 77–88.

[15] Tahir M., Javaid N., Iqbal A., Khan Z. A., Alrajeh N.: On Adaptive Energy Efficient Transmission in WSNs. International Journal of Distributed Sensor Networks, 2013.

[16] Zhong J., Bertok P.: A Variable Threats Based Self-Organization Scheme for Wireless Sensor Networks. Proceedings of the 2009 Third International Conference on Sensor Technologies and Applications, 2009.

D.Sc. Eng. Volodymyr Mosorov
e-mail: w.mosorow@kis.p.lodz.pl

Volodymyr Mosorov received his Ph.D. in 1998 from the State University of Lviv, Ukraine. V.Mosorov was awarded the title of Doctor of Science from AGH University of Science and Technology Krakow Poland in 2009. He is now an associate professor at the Institute of Applied Computer Science of Lodz University of Technology, Poland. His research interests include data mining and clustering. He has published more than 80 technical articles.



M.Sc. Eng. Sebastian Biedron
e-mail: sbiedron@wpia.uni.lodz.pl

A graduate of the Department of Science and Mathematics at Lodz University. From 2012 year is a court expert at the District Court at the Prague in Warsaw. From 2013, Ph.D. student at the Institute of Applied Computer Science of Lodz University of Technology. Supervisor of the Ph.D. thesis is D.Sc. (dr hab. inż.) Volodymyr Mosorov, prof. PL.



M.Sc. Taras Panskyi
e-mail: tpanski@kis.p.lodz.pl

Graduate of the Electrotechnics Department at the Lviv National Polytechnic University, Ukraine. From 2013, Ph.D. student at the Institute of Applied Computer Science of Lodz University of Technology, Poland. His research interests include data clustering, reliability and availability indexes of embedded systems, educational migration.

