Paper

Self-organization and Routing Algorithms for the Purpose of the Sensor Network Monitoring Environmental Conditions on a Given Area

Krzysztof Bronk[1], Adam Lipka[1], Błażej Wereszko[1], Jerzy Żurek[2], and Krzysztof Żurek[1]

[1] *Wireless Systems and Networks Department, National Institute of Telecommunications, Gdańsk, Poland*
[2] *National Institute of Telecommunications, Warsaw, Poland*

Abstract—The article describes an implementation of wireless sensor network (WSN) based on the IEEE 802.15.4-2006 standard, which was designed to monitor environmental conditions (e.g. temperature, humidity, light intensity, etc.) on a given area. To carry out this task, a self-organization algorithm called KNeighbors was selected. It exhibits low computational complexity and is satisfactory with respect to energy consumption. Additionally, the authors proposed a novel routing algorithm and some modifications to the MAC layer of the IEEE 802.15.4 standard. The article discusses the selected algorithms and procedures that were implemented in the network.

Keywords—network management, network self-organization, sensor networks.

1. Introduction

One of the main benefits of the sensor networks is the fact they offer a myriad of various applications. In fact it is also one of the reasons why they evolve so dynamically. The applications or purposes for which a sensor network is intended to be used determine the requirements such network needs to satisfy. The engineer is faced with a complex problem of selecting the most suitable hardware and software platforms as well as the algorithms and parameters which should ensure the correct – i.e. compliant with the predefined criteria – operation of the sensor network.

The selected mean of communications between the nodes should always reflect the network's characteristics, the method of data acquisition and also the method this data will be used in the future. The most common techniques employed in the wireless sensor networks (WSNs) are the ZigBee and 6LoWPAN, which are based on the IEEE 802.15.4 standard. Identification of the optimal self-organization and routing algorithms is also one the most crucial stages of the WSN development.

In the last years, many algorithms of the transport layer have been proposed, which in assumption should ensure the reliability and congestion control. Some of them have been designed for the node-sink transmission (ESRT [1], RMST [2]), the others for the sink-nodes transmission (GARUDA [3], PSFQ [4]) or for both directions (ART [5], STCP [6]). The comparative study of these protocols can be found in paper [7].

In contrast to the algorithms mentioned above, the algorithm proposed in this paper is used to collect data from as many nodes as possible and the loss of some packets is acceptable, because it does not result in data degradation for the whole monitored area. These assumptions were taken into account during development process. A query is sent from the sink node and answers are sent back by every node to which the query arrived. In the proposed solution, there is no mechanism for ensuring reliability of transmission between node and sink. The reliability is achieved in every hop by sending ACK in MAC layer. Congestion control is also made locally by time-out periods in nodes or by changing the packet destination node.

The following paper describes a practical implementation of the sensor network based on the IEEE 802.15.4-2006 standard, which was built for monitoring of environmental conditions (e.g. temperature, air humidity, light intensity) on a defined area. This network may operate efficiently even when some of the nodes cannot communicate or are damaged. Due to the purpose of the proposed WSN, it should satisfy the following requirements:

- long operational time,
- low sensitivity to communication problems with single nodes,
- scalability and remote configurability,
- communication with the network using the Internet,
- resistance to dynamic modifications of the topology (changes of the nodes' quantity and their location) and operational conditions,
- low price of the network node.

To satisfy the above, several assumptions have been formulated:

- the network configuration can be modified dynamically (via self-organization procedures), depending on the number of nodes and the transmission parameters,

Table 1
Functions performed by the nodes

Node type	Function
Master node, connected to the Internet	1. It receives: a request for data and parameters of the network configuration. 2. It sends a request for measurement data to the slave nodes. 3. The request mentioned in "2" additionally includes the network parameters. 4. It formats the received data. 5. It does not participate in the network self-organization. 6. It acts as a server for the network data.
Slave node, equipped with sensors and GPS	1. At master's request, it sends the measurement data from the sensors and the GPS-based position. 2. It participates in the network self-organization.
Slave node, without sensors	1. It passes data packets from other network nodes. 2. It participates in the network self-organization.

- nodes should be powered using solar power systems,
- network should be configurable remotely through commands transmitted by the primary node,
- the primary node should be connected to the Internet,
- the master-slave architecture should be utilized, where the primary (master) node demands the data, and the other (slave) nodes respond by sending the required data (measurement results) to the master,
- routing should be based on the self-organization procedure,
- hardware requirements for the node's processor should be kept low,
- information (data) is collected from each and every network node (nodes have not assigned IP addresses so it is not possible to collect the data from a specific node).

To implement those assumptions, the authors created their own, novel routing algorithm. Additionally, they proposed some modifications of the 802.15.4 MAC layer. In the next step, those algorithms and procedures have been implemented on a hardware platform designed and built for the purpose of this project, and the resulting solution has been subjected to a measurement campaign. The whole process of the WSN development and testing has been described in the subsequent sections.

2. Architecture of the Proposed Network

The research process was initiated by a review of the existing solutions. In paper [8], the authors analyzed the following self-organization algorithms: LMST (Local Minimum Spanning Tree) [9], CBTC (Cone-Based Topology Control) [10], DistRNG (Distributed Relative Neighbor Group) [11], KNeighbors (k-Neighbors) [12], LINT (Local Information No Topology) [13] and LILT (Local Information Link-state Topology) [13]. In that paper it was shown the KNeighbor algorithm will be the most suitable one to be implemented in the target sensor network. Its major benefits are: a relatively low energy consumption and implementation simplicity. Moreover, it exhibits low computational complexity, since it does not require a precise calculation of the nodes' position or the signal's direction of arrival. With a sufficient number of neighbors (6 or more), alternative routes (of packet transmission) can be ensured in case of nodes' failure. In this way, the problem of losing a full connectivity in the network can be substantially marginalized.

On the basis of the initial assumptions and requirements for the projected WSN and using the simulation comparative analysis of several self-organization algorithms [8]–[13], a general concept of the network architecture was developed [14].

The discussed sensor network is composed of two types of nodes:

– master node,

– slave nodes.

Functions performed by those are listed in Table 1.

The packets transmitted in the network are assigned a type denoted by an ASCII code inserted in the first payload's byte (MAC payload) of each packet. Designations of the packets and their brief description can be found in Table 2. The terms "packet" and "command" are used interchangeably in the following text.

After the reception of the packet, the node checks its type and acts accordingly. Table 2 includes all the commands to be used in the network. The ACK column indicates

Table 2
Commands transmitted in the network

Packet designation	Description	ACK	Number of bytes
W	The packet sent by a node that is searching for its neighbors. The recipient verifies the quality of the received command and if it is above a threshold, responds by sending an "A" type packet. The "W" packet includes the value of power it was transmitted with.	No	50
A	A response for the "W" packet. It contains: • LQI value (range 0–255) of the received "W" packet, which indicates the quality of connection, • ID from the "W" packet, • the value of power the "A" packet was transmitted with.	No	4
O	A packet which contains measurement data obtained by the node, including position information from the GPS.	Yes	Max. 80
o	A packet which contains measurement data sent to the master node. The "o" command is a response to the "s" command. The packet is transmitted with a maximum power.	Yes	Max. 80
S	A request for measurement data sent by the network node to its neighbors. The packet also contains network configuration parameters.	No	13
s	A request for measurement data sent by the master node. The packet is transmitted with a maximum power and it contains network configuration parameters.	Yes	4

whether the transmission of a certain packet has to be acknowledged by the recipient (by ACK frame), or not.

2.1. Network Layer Model

The following subchapter introduces the communication protocols of the self-organization and network layers, which manage the packet routing. The physical and MAC layers are generally compliant with the IEEE 802.15.4 standard [15], with the exception of some MAC layer modifications: the number of attempts to transmit a packet has been increased and the mechanism of power control has been altered.
The layer model of the discussed sensor network is presented in Fig. 1.

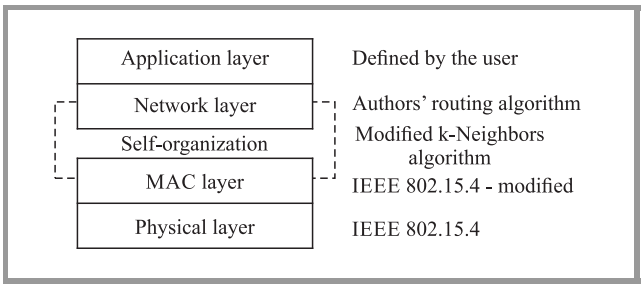

Fig. 1. Network's layer model.

The self-organization layer is located between the MAC and the network layer. The direct output of the self-organization procedure in a given network node is a table of its neighbors, later utilized by the network layer for routing.

2.1.1. Self-organization Layer

In the discussed network, the term "self-organization" should be understood as the node's activity which results in a list of neighbors connected with that node through a radio link of a certain quality with minimum node's transmit power. As it was mentioned, the output of the self-organization procedure is a table with neighbors' addresses and the current value of transmitted power, which will be used to send data request packets ("S" type packets) and data packets ("O" type packets). A given node in a given moment can generally communicate only with its neighbors. There are, however, two exceptions to this rule:

– any node within the range of the master node can attempt to communicate directly with it,

– a node, which does not have any neighbors, is still capable of sending messages.

As it was mentioned previously, the KNeighbor algorithm [12] has been selected as the most suitable one to be implemented in the discussed sensor network, due to its simplicity and satisfactory performance [16]. The general algorithm of neighbor searching is depicted in Fig. 2.
The procedure of the self-organization is initiated in each node after the time Ts, which is one of the network parameters. After the node has been powered on, the first self-organization starts after a random time in the range of 0 to Ts. This approach was taken to reduce the probability that self-organization procedures performed by neighboring nodes will overlap.

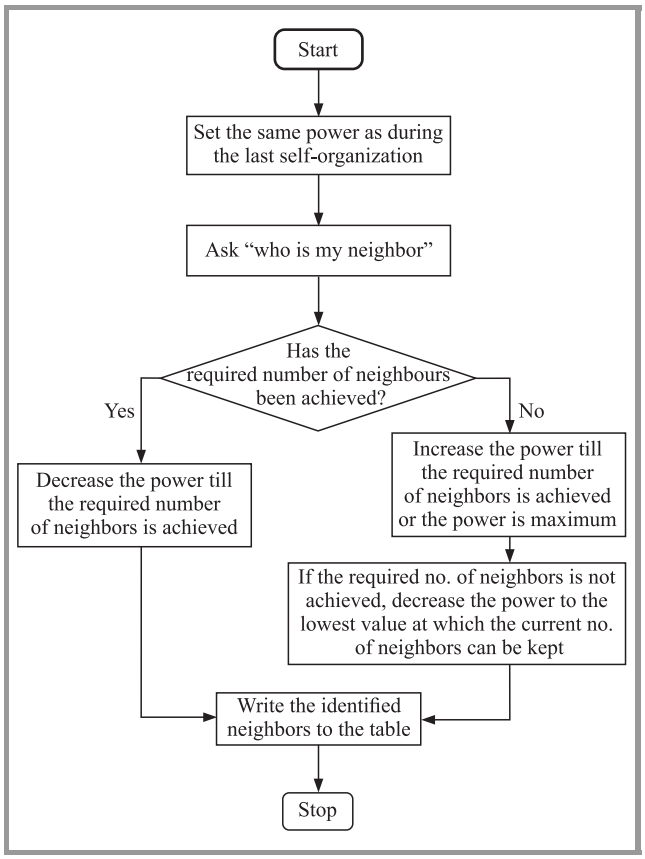

Fig. 2. *k*-Neighbors self-organization algorithm.

The node searching for its neighbors performs the following tasks:

- it sets the transmitter power to the value used during the previous self-organization,
- it sends the "W" packet (with 45 additional bytes to improve the link quality assessment),
- it waits for approx. 1 s, and during this period it collects responses from the neighboring nodes,
- it checks how many nodes actually responded for the "W" packet,
- if the number of the nodes that responded is too small, it increases the transmitted power and resends the "W" packet,
- If the required number of neighbors has been found, it decreases transmitted power and keeps resending the "W" packet. This procedure is repeated until further power decrease would cause the number of neighbors dropping below the desired threshold.

The node, which receives the "W" packet, acts according to the following procedure:

- it evaluates the quality of the received "W" packet;
- if the quality is better than the assumed threshold, it responds (by sending the "A" packet to the "W" packet-sender) with the transceiver power set to the value contained in the received "W" packet. The response also includes the LQI of the received "W" packet.

The procedure of the self-organization ends when:

- the node reaches the minimum or maximum power,
- the number of identified neighbors is at least equal to the desired threshold and any further decrease of the transmitted power would reduce the number of responding nodes.

The result of the self-organization is a table of the node's neighbors and the transmitted power obtained during the procedure. The determination of the transmitted power before sending the "W" and "A" packets is performed in the link layer, which is a modification of the 802.15.4 standard.

2.1.2. Example of Self-organization Procedure

A sample procedure of the self-organization procedure is shown in Fig. 3. The following network configuration parameters have been assumed:

– maximum number of neighbors to be found: MAX_N = 3,

– minimum expected transmission LQI: MIN_LQI = = 30.

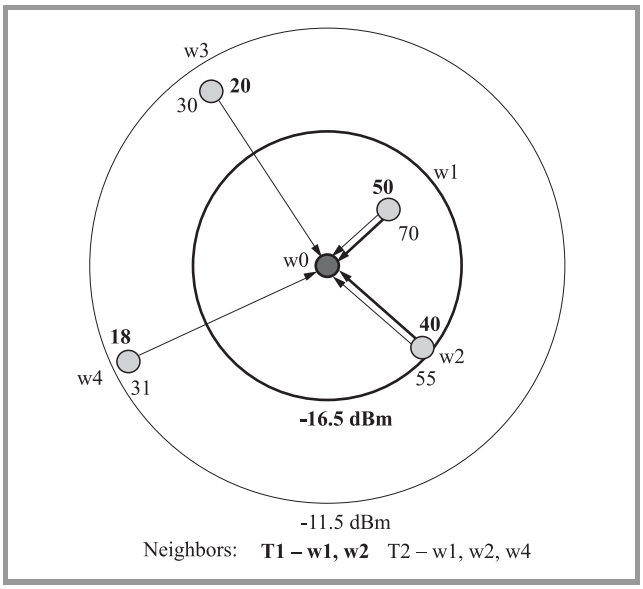

Fig. 3. Sample self-organization procedure.

In the instant T1, the w0 node initiates the procedure, by sending the "W" packet with a power of –16.5 dBm and a recipient address set to broadcast.
The packet is received by every node shown in the Fig. 3, with the following values of LQI: 50 at w1 node, 40 at w2 node, 20 at w3 node and 18 at w4 node. The LQI value

exceeded LQI_MIN only in the cases of w1 and w2 nodes, so only these two respond by sending the "A" packet to the n0 node.
After 1 s, the w0 node checks, how many nodes responded. Since only 2 did, w0 increases transmitted power to –11.5 dBm and resends the "W" packet in the instant T2. In this case, the LQIs were as follows: 70 at w1, 55 at w2, 30 at w3, 31 at w4. Therefore, all of these nodes respond with the "A" packet addressed to the w0 node.
While receiving the "A" packets, the w0 node adds nodes with the highest LQI to its neighbors list. As a result, the searching procedure ends with w1, w2 and w4 nodes identified as w0's neighbors and the transmitted power set to –11.5 dBm.

2.1.3. Network Layer

The network layer is responsible for the routing of packets with measurement data ("O" and "o" packets) and packets with data request ("S" and "s" packets). For the proposed sensor network, the authors created their own novel routing algorithms which should ensure:

- distribution of data requests and configuration parameters to as many nodes as possible,
- delivery of packets with data to the master node.

To make sending the data possible in the network, each node needs to know a specific address called *RoutingNode* (RN). It is the node's address, to which all the measurement data should be sent. The method used for RN's selection will be discussed later.
In the following paragraphs, novel routing algorithms, proposed by the authors, for different types of packets will be introduced.

2.1.4. Request for measurement data sent by the Master Node

The request for measurement data is sent by the master node to the broadcast address, i.e. 0xFFFF. This command is marked as "s" and is transmitted with maximum power. The command contains the following fields:

- "s" packet identification (8 bits),
- message ID, 16-bits random number,
- number of hops, increased by 1 after every successive packet transmission (16 bits),
- network configuration fields discussed in the following part.

The procedure of the "s" packet routing is shown in Fig. 4. The node which received the "s" packet, sets the master's address as its RN and sends its measurement data at this address. This node also sends the received "s" packet to its neighbors, but the packet type is changed to "S". It is the only case when the RoutingNode is not one of the neighbors. The master node is not a neighbor of any node, because it does not participate in the self-organization procedures. Consequently, it cannot be added to any neighbors' list.

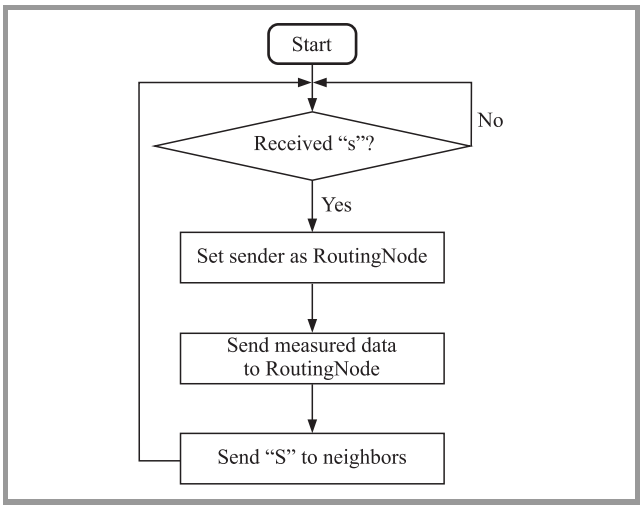

Fig. 4. Routing of the data request sent by the master node.

2.1.5. Request for data Sent by the Slave Node

A slave node is any node in the network that is not a master node. Every node that received the "s" packet, sends its measurement data back to the sender and then – if the node has neighbors – it sends the "S" packet to them. Data requests originated by the slave node are treated differently than the packets from the master:

- they do not need to be sent with maximum power,
- packet sender will not be set as RN, if it is not the recipient's neighbor.

The procedure of the "S" packet routing is shown in Fig. 5. The node, which receives the "S" packet, acts according to the following procedure:

- it checks if the number of hops is less or greater than the maximum acceptable value; if it is greater, the nodes will ignore the message;
- it reads the ID and checks if it has already received a message with an identical ID. If it has not, it writes the ID to the table; on the other hand, if such an ID is already in the table – another RN is selected;
- it checks if the sender is its neighbor; if yes – it sets the sender as RN;
- it sends its measurement data to the RN;
- it increases the number of hops by 1;
- it sends "S" to its neighbors.

2.1.6. Sending Measurement Data

Measurement data ("O" or "o" packets) are always sent to the RoutingNode: with the same transmitted power as the one used during the previous self-organization, or with

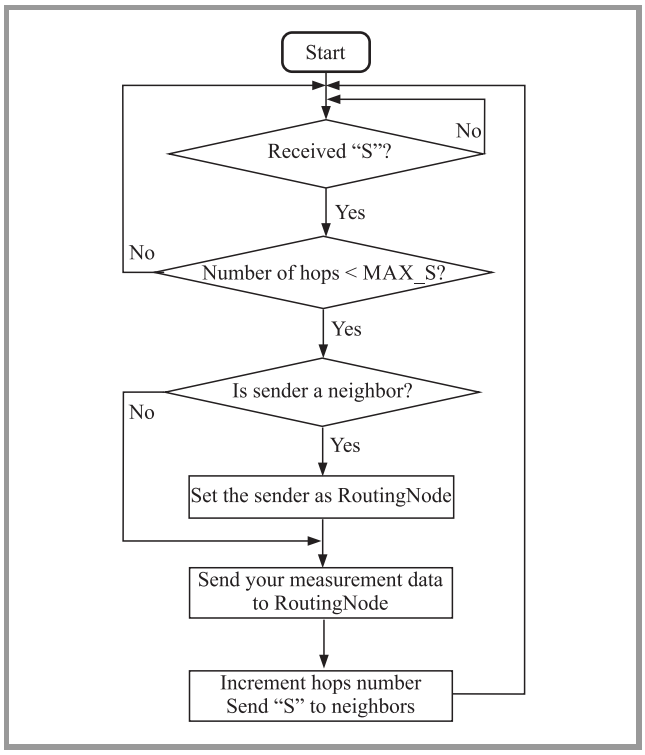

Fig. 5. Routing of the "S" packets.

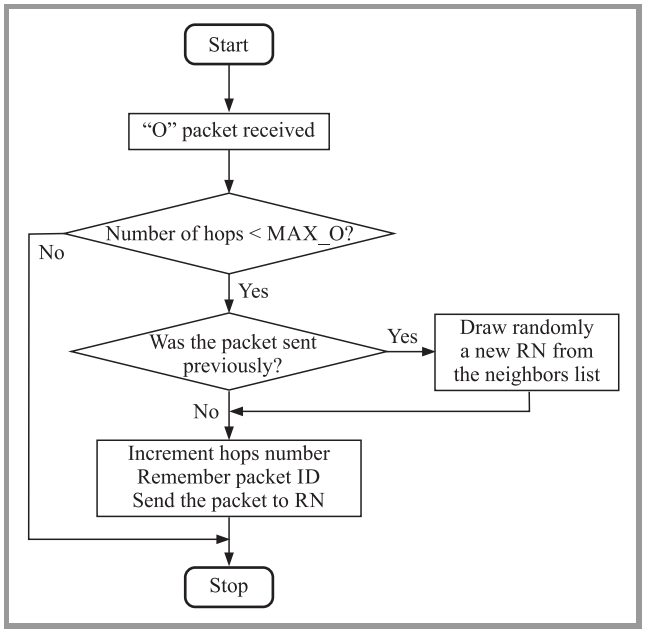

Fig. 6. Routing of the measurement data packets.

maximum power if the data is addressed to the master node. The routing of the packets carrying the measurement data is depicted in Fig. 6.

2.1.7. Determination of the RoutingNode

The RoutingNode is selected in the following way:

- it is the master node, from which the "s" packet was received,
- it is the neighbor node, from which the "S" packet was received,
- if the packet with measurement data is returned to sender, a different neighbor node has to be selected as RN,
- if the node which does not have any neighbors receives the "S" packet, it sets the packet sender as RN.

Measurement data packets have a hop counter, which is incremented (increased by 1) after every successive packet transmission. If the hop counter value in the packet is greater than the accepted threshold, such a packet will be ignored by the node that received it. The "o" packet (sent directly to the master node) should always have the hop counter value set at zero.

2.1.8. Exchange of Data Request Packets and Data Packets – Sample Scenario

In this scenario, it was assumed that in a given moment of time, only one node can be granted access to the radio channel. It was also assumed that nodes have the following neighbors:

Node w1: w4 and w2,

Node w2: w3, w4 and w5,

Node w3: w2 and w5,

Node w4: w1, w2, w5,

Node w5: w2, w3 and w4.

Figure 7a depicts 13 subsequent steps of the scenario (numbers in brackets next to the arrows indicate the step's number), additionally all the events are presented in Fig. 7b.
In the first instant of time, the master node transmits the "s" packet which is received by nodes w1, w2 and w3. These three nodes set the master's address as RN.
In the next instant of time, the node w1 is granted access to the radio link and sends the measurement data obtained by its sensors to the RN. After that, it sends the "S" packet to the node w4. W4 sets the address of w1 to be its RN. In the fourth instant of time, the node w4 sends its measurement data back to w1.
The precise time sequence of the whole procedure is shown in Fig. 7b. The numbers visible in the first column are the numbers of subsequent steps.
In the procedure depicted in Fig. 7, the w5 node received the "S" packet from the w4 node, and the w4 node had previously received this same packet from w1 – consequently there were two hops of the packet ("S" was originally sent from the master, which constituted the zeroth hop). As a result, number 2 (number of hops) is inserted by w4 to the specific field of the "S" packet.
One can observe, the message containing data from w5 took the longest path. It was delivered to w0 via nodes w4 and w1. The heaviest traffic was served at node w1, which sent its own data and the data from nodes w5 and w4. Obviously, the channel access is granted randomly, so

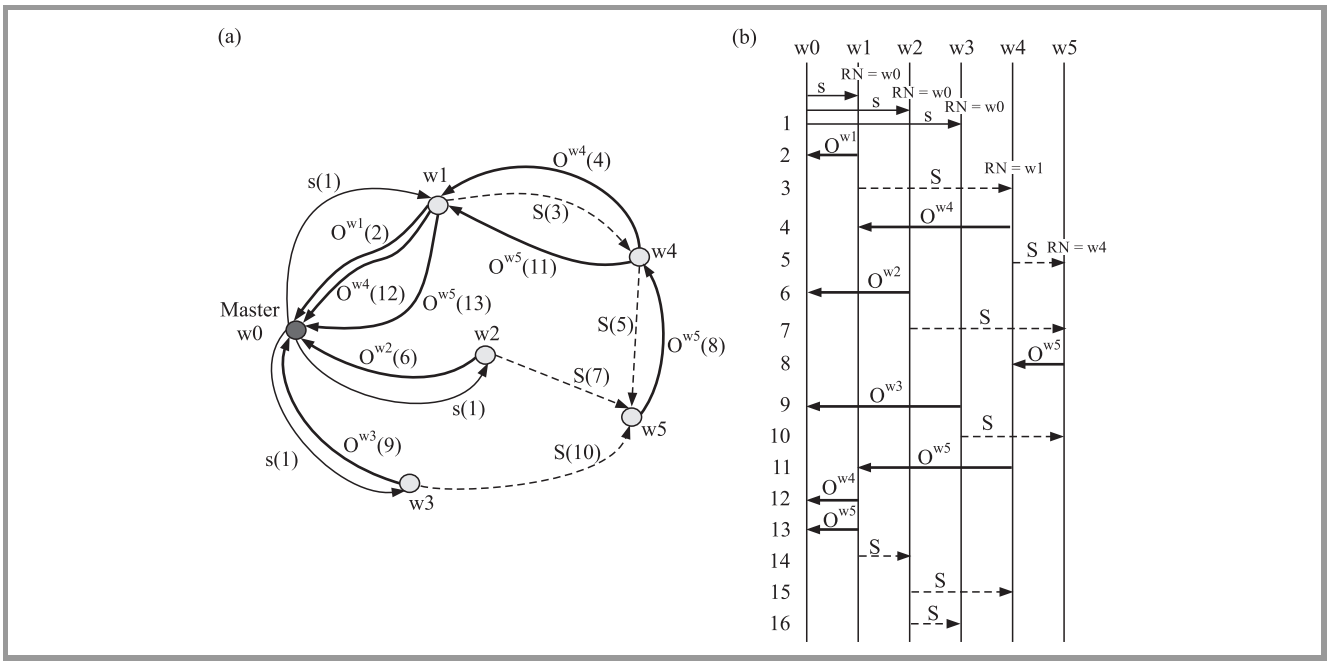

Fig. 7. Data routing scenario.

Table 3
Structure of the "S" and "s" data request packet

No.	Field	Description	Example	Bytes
1	Packet type	Data request command	"S"	1
2	MAX_S	Maximum number of hops for the "S" packet	100	2
3	MAX_O	Maximum number of hops for the "O" packet	200	2
4	T_S	Time between self-organization procedures, max. 72 hours	10	2
5	T_GPS	Time between position readings from the GPS, max. 72 hours	30	2
6	LQI_MIN	Minimum LQI in the self-organization procedure	20	1
7	MAX_N	Maximum number of neighbors, from 1 to 10	3	1
8	CRC	CRC checksum	0x1C	1
			Total	12

in the next steps, the routing can be handled in a different way.

2.2. Network Configuration

One of the main features of the presented sensor network is the capability to be configured remotely, which also ensures a certain level of scalability. The network configuration is performed through a distribution of the "S" and "s" packets, which contain fields with the network's parameters. The structure of the data request packets is introduced in Table 3.

The MAX_S field defines the maximum number of hops for the "S" packet. This parameter allows to modify the range of the packet distribution and consequently to modify the area from which the data can be collected.

The MAX_O field defines the maximum number of hops for the "O" packet.

The T_S field defines the time that has to elapse between two subsequent self-organization procedures. To determine the value of this parameter, the changes of nodes' positions should be considered: if the nodes are moving, self-organization should occur more frequently than in the case of fixed nodes.

The T_GPS field defines how often the position is read from the GPS receiver. After the position has been obtained, the receiver is switched off (or goes into idle mode) to reduce power consumption of the node.

The LQI_MIN field contains a value (in the range of 1 to 255) defining a minimum LQI at which the node will still respond to the "W" packet sent by another node. Besides the MAX_N, this parameter is the most crucial with respect to the resulting network topology. A low value of LQI_MIN results in a greater number of neighbors (i.e. bigger network connectivity), but at the same time it might result in a low quality of connections between the nodes.

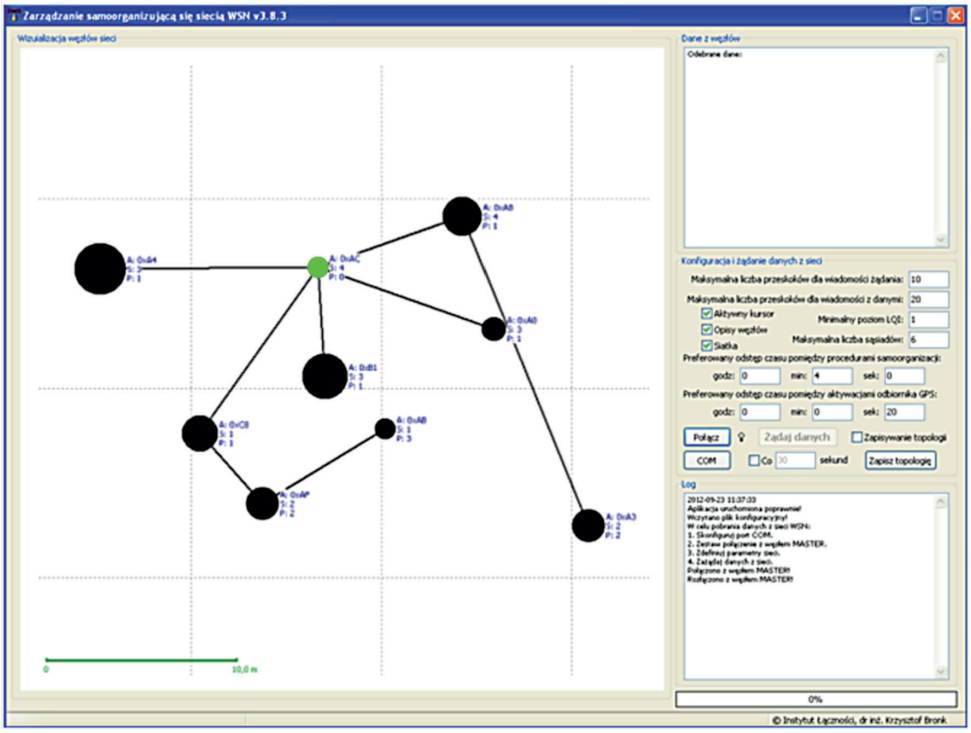

Fig. 8. Software tool for the network management. (See color pictures online at www.nit.eu/publications/journal-jtit)

The MAX_N field defines the maximum number of neighbors that can be found in the self-organization procedure.

As it was previously mentioned, the network topologies resulting from the self-organization mostly depend on the MAX_N and LQI_MIN parameters (when the nodes' position and terrain condition are known and remain constant). Low value of the MAX_N can lead to local clusters of nodes that remain "hidden" and separated from the rest of the network. On the other hand, high values of this parameter make the self-organization procedure longer and increase the nodes' transmitted power, which may result in heavy traffic and increase of the network interference. These two factors will in turn worsen the self-organization efficiency so the node will possibly be able to discover fewer neighbors than it was supposed to.

2.3. Hardware Implementation

On the basis of all the assumptions, simulations results [8] and concepts discussed above, as well as the analysis of the relevant references and state of the art, a hardware implementation of the wireless sensor network has been created. The network comprises of ten RCB128RFA1 radio modules with additional sensors, and one master node connected to the Internet. To enable acquisition of the data from the network and its visualization and also to facilitate network configuration, a software tool for network management was developed. The user interface of the tool is depicted in Fig. 8.

The visualization of the network activity includes the following factors:

- the node's position calculated using the GPS data,
- the size of the node corresponds to the node's transmitted power,
- nodes are depicted by three different colors: green – a node that transmits directly to the master, black – other nodes, red – nodes whose power voltage is below 3.225 V.
- the nodes which exchange data with one another are connected with lines.

2.3.1. Master Node

The master node (see Fig. 9) is implemented using the Ethernet module with the RTL8019AS controller and the

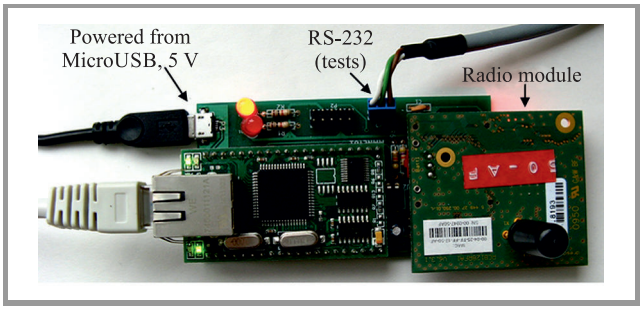

Fig. 9. Master node with the Ethernet interface.

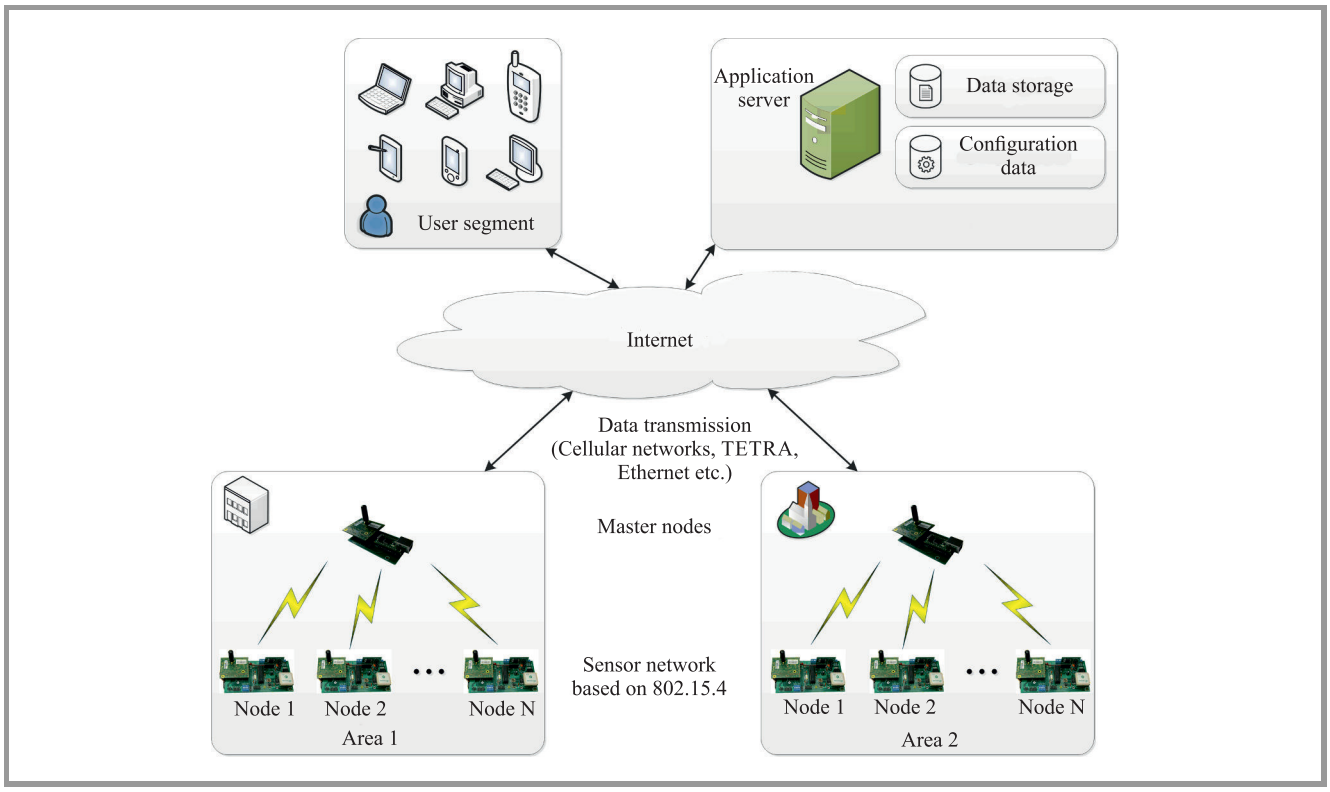

Fig. 10. Connection of the sensor network to the Internet.

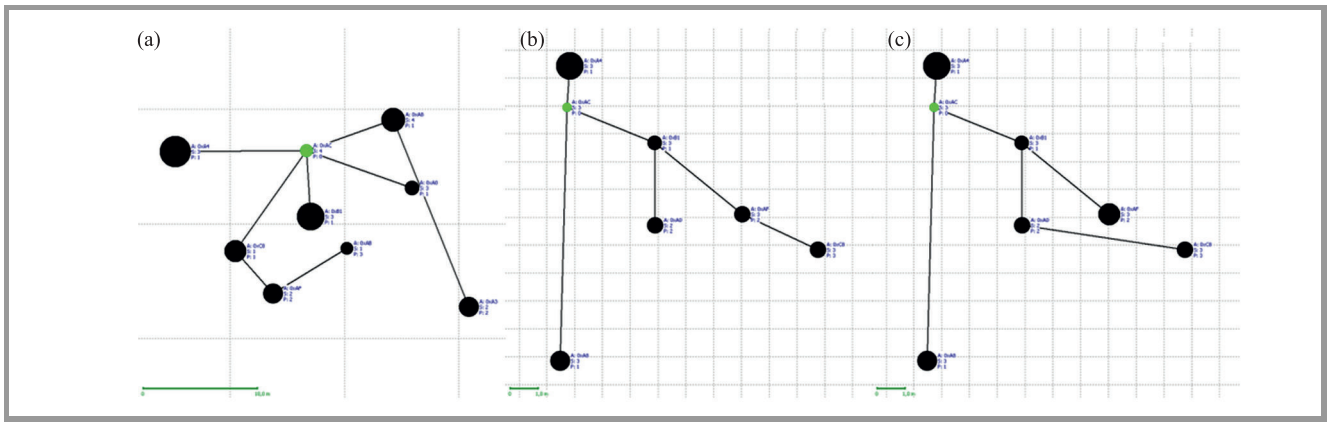

Fig. 11. Sample topologies created during the WSN measurements.

RCB128RFA1 radio module by the Dresden Elektronik. Both these components have been assembled on a single printed circuit board. The node is powered with 5 V from the microUSB port.

The Ethernet module operates under control of the real time system FreeRTOS with the TCP/IP stack called LwIP (A Lightweight TCP/IP stack [17]).

2.3.2. Connecting the Network to the Internet

The proposed network is connected to the Internet through the master node. This approach is illustrated in Fig. 10. As it has been previously mentioned, in the discussed network, no node-to-node communication has been employed, i.e. it is not possible to communicate with a specific network node. Instead the authors utilized the master-to-node communication. In this case, establishing a connection to the master is essentially establishing a connection with the whole network, and consequently, in the best-case scenario, data from all the nodes can be collected. Such an approach was taken due to the target purpose of the proposed network (monitoring of the environmental parameters on large areas), in which the ability to obtain the data from as many nodes as possible is the top priority.

2.3.3. Initial Measurements of the Network

The network management software tool allows to collect data from the network and to perform network configuration. Additionally, the master node acts as a Webserver

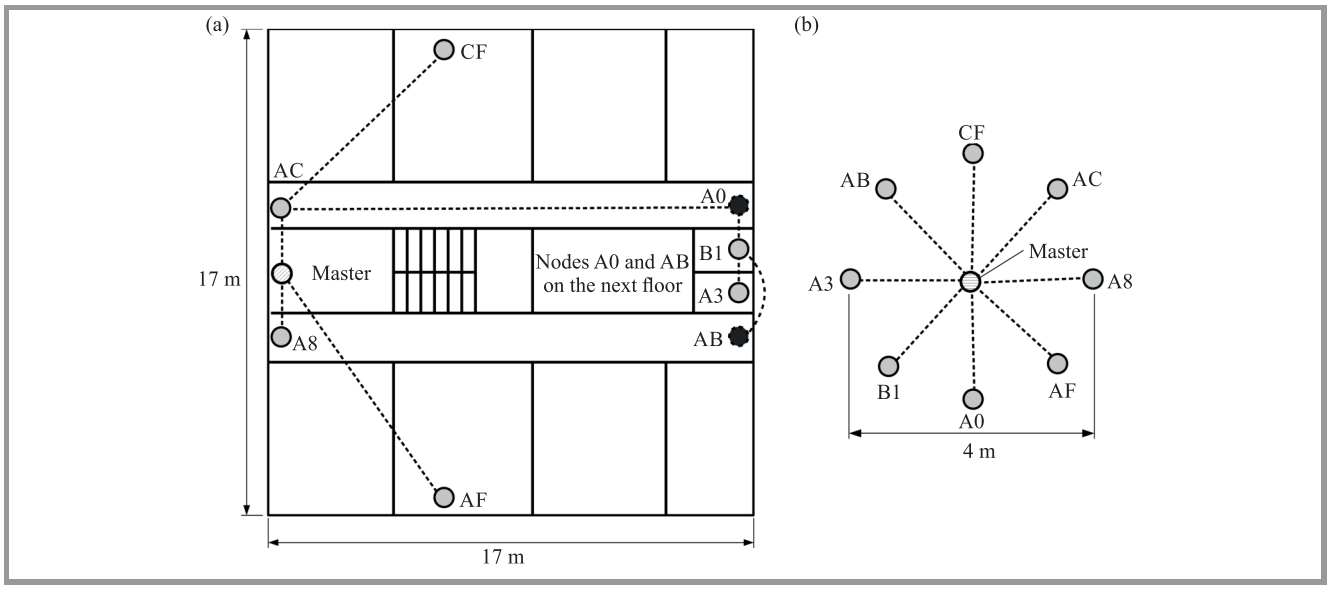

Fig. 12. Network topologies.

to enable remote observation of the parameters measured by the sensor nodes. The acquired data are presented in the table and can be accessed e.g. in an Internet browser.
A few examples of the topologies obtained during the tests are depicted in Fig. 11.
These topologies are generated in the software tool on the basis of the received data. The black circles represent the nodes and their size (diameter) is proportional to the transmitted power. Obviously, the greater the diameter, the higher the transmitter power. In this particular case the largest diameter is equivalent to the power of 3.5 dBm. Green circles are the nodes communicating directly with the master node. Their diameter corresponds to the power determined in the self-organization procedure, but the transmission to the master is always performed with the maximum power. Positions of the nodes are obtained from GPS receiver mounted on every node. The lines between nodes denote the paths over which packets are routed.
It should be stated, Fig. 11a, depicts a scenario where nodes were located on a rectangular plane of 17×17 m (the roof of the National Institute of Telecommunications (NIT) building in Gdańsk), whereas in the cases of Figs. 11b and 11c, the nodes were located in rooms and corridors of the same building. As we can observe, Figs. 11b and 11c depict the same arrangement of the nodes, but two different paths of the packets originating from the rightmost node.

3. Functional Network Tests

3.1. Network Configuration During the Tests

The measurement tests of the resulting sensor network have been performed in the NIT office in Gdańsk, using eight slave nodes and one master node. The tests have been carried out for two network's configurations: the mesh (Fig. 12a) and the star (Fig. 12b).

The mesh topology was obtained by placing the nodes in different rooms on the same floor, with the exception of nodes A0[1] and AB, which were located on a higher level. By doing so, some of the nodes were outside the master node's range and data requests could be delivered to them only via other nodes in the network.
On the other hand, the star topology was obtained by placing all the nodes in the same room, approximately 2 meters from the master node. Consequently, all the nodes were in the master's range and each of the node was in the range of all other nodes. The tests of the star topology were performed for the purpose of comparison with the mesh.
All the simulations have been carried out using the following network settings:

- requested number of neighbors: 1, 2, 3, 4 and 5,
- maximum number of hops for the request packets: 10,
- maximum number of hops for the data packets: 12,
- minimum LQI: 50,
- maximum number of attempts to send the message: 2,
- self-organization procedure initiated every 120 s,
- data requests from the network sent every 15 s.

The measurement series have been repeated ten times, and each of them comprised approx. 200 requests being sent to the network, which accounted for a total of roughly 2000 requests.

3.2. Measurements Results

In this section, the measurements results – averaged for the entire network – are presented. The testing procedure

[1]In the paper, in order to address the node, only the last byte of its 8-byte address was used. It could be done, because the nodes' addresses only differed in this last byte.

covered such parameters as: the delay, number of packets, number of hops, availability and number of discovered neighbors. Additionally, the availability was analyzed separately for every network's node.

3.2.1. Delay

The delay in the network – measured by the software application – is defined as the time that elapsed from the moment the data request packet was prepared (by the application) to the moment the data packet was received. According to that definition, the following "events" account for the delay: (a) packet processing by the computer, (b) packet multi-hop transmission, (c) packet processing by the recipient node, (d) transmission of the response and its reception by the master node, (e) packet forming and its transmission to the computer via the USART interface and (f) time needed by the computer to deliver the packet to the software application.
The tests performed for the scenario of the connectivity with just one node, show that the minimum reachable delay for this configuration is 218 ms. That analysis was performed using the exact same computer that was later employed in the actual measurements of the network (2-cores Pentium R 3.4 GHz processor, 64-bit Windows 7).

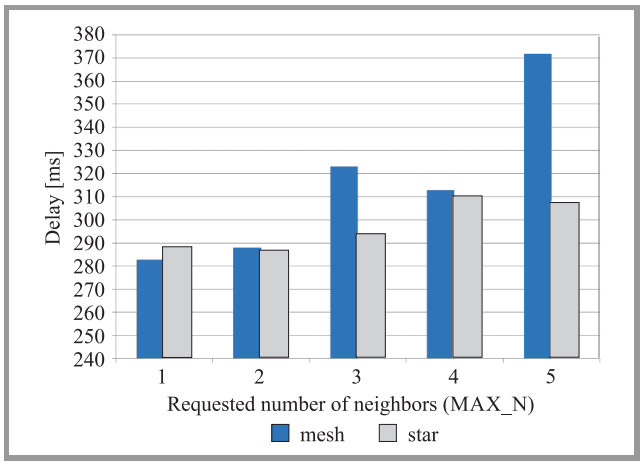

Fig. 13. Average delay in the network.

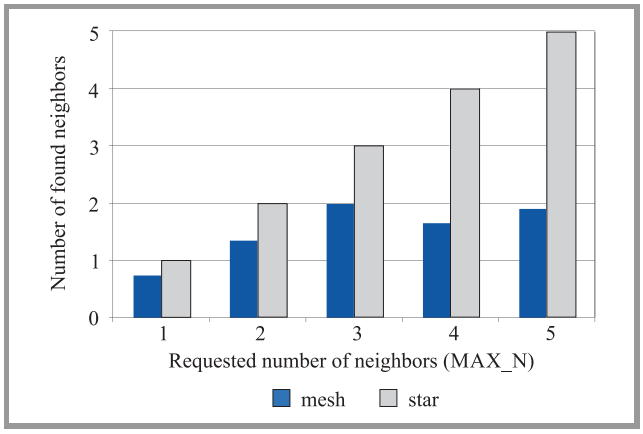

Fig. 14. Number of discovered neighbors.

The measured values of the delay are presented in Fig. 13. The delay for the mesh topology increases as the number of neighbors increases, with the only exception being the case of 4 neighbors. It can be explained by the fact that when the requested number of neighbors is 4 (MAX_N=4), the number of actually discovered neighbors drops (see Fig. 14), which decreases the number of transmitted messages and consequently – reduces the delay in the network as well.

3.2.2. Number of Discovered Neighbors

The average number of the discovered (found) neighbors is shown in Fig. 14.
In case of the star topology, where each node is in the range of every other node, the nodes are able to discover as many neighbors as required. On the other hand, in case of the mesh topology, the highest average number of neighbors can be found for the parameter MAX_N=3.
In the mesh topology, where the node is in the range of only some of the nodes, neighbors' discovery requires a higher number of requests sent with higher power, which could translate into greater interference inside the network and longer duration of the whole procedure. As a result, the self-organization fails more frequently and the node is then unable to find the required number of neighbors.
Consequently, it might be stated that increasing the MAX_N parameter value can often prove counterproductive and in such a case, the actual neighbors' number will more likely start to drop rather than grow. This observation can be confirmed in Fig. 14 for MAX_N=4 and MAX_N=5. The same picture clearly indicates the optimal value of the MAX_N parameter is 3.

3.2.3. Number of Packets

Figure 15 shows the average number of packets transmitted in the network per single request. The term "packets transmitted in the network" should be understood as every packet sent by the node, including data requests, data packets and messages utilized in the self-organization algorithm.
In case of the star topology, the number of packets grows linearly as the required number of neighbors' increases. It

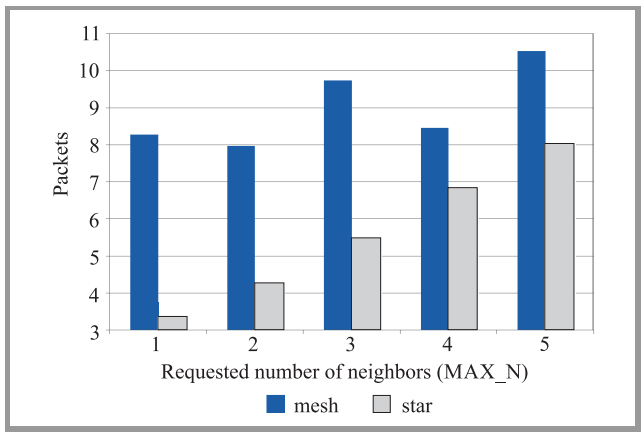

Fig. 15. Number of packets sent in the network per single request.

is caused by the fact that the requests are broadcast to the increasing number of neighbors. Hence, if the required number of neighbors is increased by one, the number of transmitted packets grows accordingly.
For the mesh topology, the growth of the packet number is less significant, which is caused by the problems with finding the required number of neighbors in this particular topology (see Subsection 3.2.2).

3.2.4. Number of Hops

Figure 16 indicates an average number of hops for data packets. If the number of hops is zero, it means the packet is sent directly to the master node. In case of the star topology, hops occur quite rarely, because the nodes send their data directly to the master.

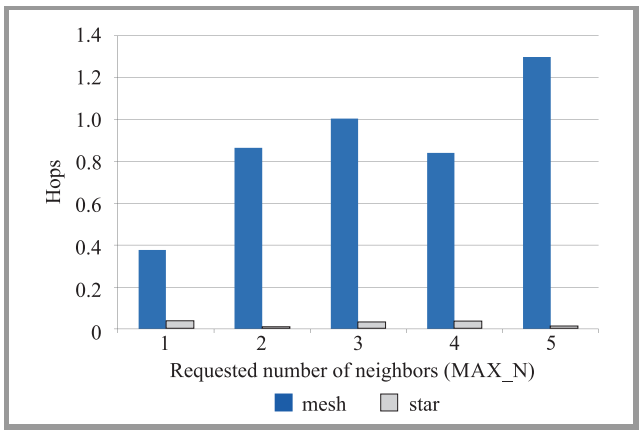

Fig. 16. Average number of hops for data packets.

In case of the mesh topology, the number of hops grows as the MAX_N parameter grows, even though the nodes' positions remain unchanged. This might suggest that the paths for the data messages are not chosen optimally. Unfortunately, this is a weakness of the assumed solution, where the first node from which the data request has been received is appointed to be the node to which the data packets are sent back – without the actual path length to the master node being calculated. On the other hand, that issue has been known already at the development stage and – from a practical point of view – it does not represent any significant problem for the network in its current form and it does not interfere with its primary purpose i.e. environmental parameters' monitoring.

3.2.5. Availability

The node's availability is defined here as a ratio of the number of responses to the number of requests. For example, if 100 requests have been sent to the network, and 80 responses have been received from a certain node, that node's availability is 0.8 (or 80%).
In Fig. 17, the availability for the whole network was presented, whereas in Fig. 18, the same parameter was shown separately for every analyzed node.
The maximum availability is observed for the requested number of neighbors MAX_N=3. For MAX_N<3, local

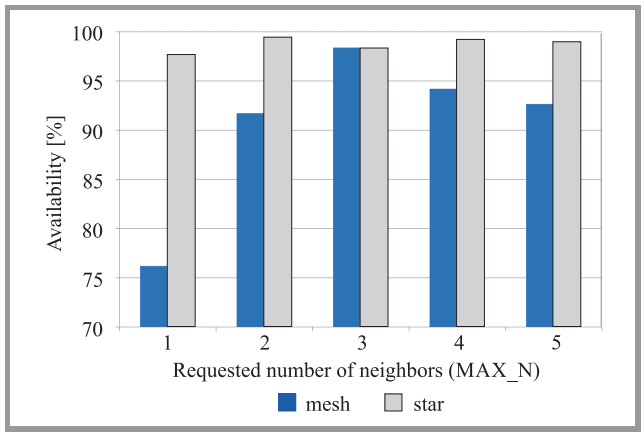

Fig. 17. Nodes' availability in the network.

nodes' clusters are formed, the messages are unable to be transmitted outside this cluster and consequently, they are unable to reach the master node. Obviously, in such a scenario the availability of the nodes belonging to such a cluster drops – it can be observed particularly for the nodes A3 and AB at MAX_N=1 (Fig. 18).

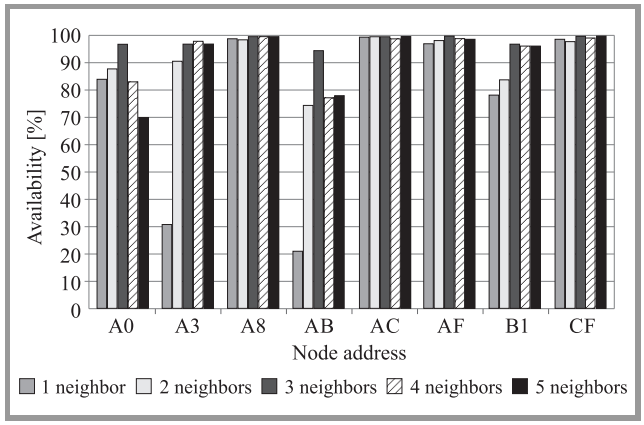

Fig. 18. Availability of every analyzed node.

For MAX_N>3, the number of messages transmitted in the network goes up, which also reduces the nodes' availability. Those mechanisms that occur when MAX_N is not equal to 3 result in the fact that some nodes – especially those far away from the master (i.e. AB, A3, B1 and A0) – lose their connectivity.

4. Conclusions

In the article, a wireless sensor network based on the IEEE 802.15.4-2006 standard has been introduced. The network was developed to monitor various environmental parameters on a defined (potentially large) area. The authors employed the approach in which the data are collected from the whole network via a single primary node, instead of a more common practice where every node is assigned an IP address. Owing to that, the resulting network works efficiently even when some of nodes lose connection or are damaged.

In the network implementation phase, the authors identified the KNeighbors algorithm as the base for the self-organization mechanisms. In comparison to similar algorithms, it exhibits small computational complexity and reasonable energy consumption. Additionally, the authors proposed their own routing algorithm and introduced some modification to the MAC layer of the IEEE 802.15.4 standard, which is one of the main achievements of this work. The article discusses in detail those algorithms and presents the complete network hardware implementation.

The conducted measurement research performed using the hardware platform mentioned above – showed that the implemented self-organization and routing algorithms are effective and allow to maintain connectivity in the network. During the measurement test, the nodes' availability of 98% was observed, but that value strongly depends on the parameter MAX_N (the number of requested neighbors). It is caused by two main mechanisms: for MAX_N$<$3 local groups of nodes occur, and for MAX_N$>$3 the number of packets sent in the network increases.

On the basis of those observations, the following goals for the future network development can be identified:

- the configuration of the network should not be performed "manually". Instead, the adaptive mechanisms should be introduced to identify optimal network parameters;
- the number of transmitted messages should be reduced;
- the shortest path for the data packets should be selected.

The implementation of the above factors will make the network more efficient and will enable to use it in wide range of various applications. Nevertheless, it is necessary to recall one more time the original purpose of the wireless sensor network presented in this article – i.e. the monitoring of environmental conditions on a given area. The tests have proven that for this specific purpose, the network in its current configuration and architecture is more than sufficient and does not require any substantial modifications.

References

[1] Y. Sankarasubramaniam, O. Akan, and I. Akyildiz, "ESRT: Event-to-sink reliable transport in wireless sensor networks", in *Proc. 4th Int. Symp. on Mob. Ad Hoc Netw. & Comput. MobiHoc 2003*, Annapolis, MD, USA, 2003, s. 177–188 (doi: 10.1145/778415.778437).

[2] F. Stann and J. Heideman, "RMST: Reliable data transport in sensor networks", in *Proc. 1st IEEE Int. Worksh. Sensor Netw. Protoc. & Appl. SNPA 2003*, Anchorage, AK, USA, 2003, pp. 102–113.

[3] S. Park, R. Vedantham, R. Sivakumar, and I. Akyildiz, "A scalable approach for reliable downstream data delivery in wireless sensor networks", in *Proc. 5th Int. Symp. on Mob. Ad Hoc Netw. & Comput. MobiHoc 2004*, Tokyo, Japan, 2004, pp. 78–89 (doi: 10.1145/989459.989470).

[4] C.-Y. Wan, A. T. Campbell, and L. Krishnamurthy "PSFQ: A reliable transport protocol for sensor networks", in *Proc. 1st ACM Int. Worksh. on Wirel. Sensor Netw. & Appl. WSNA 2002*, Atlanta, GA, USA, 2002, pp. 1–11 (doi: 10.1145/570738.570740).

[5] N. Tezcan and W. Wang, "ART: An asymmetric and reliable transport mechanism for wireless sensor networks", *Int. J. of Sensor Netw.*, Special Issue on Theoretical and Algorithmic Aspects in Sensor Networks, vol. 2, no. 3-4, pp. 188–200, 2006.

[6] Y. G. Iyer, S. Gandham, and S. Venkatesan, "STCP: A generic transport layer protocol for wireless sensor networks", in *Proc. 14th Int. Conf. on Comp. Commun. & Netw. ICCCN 2005*, San Diego, CA, USA, 2005, pp. 449–454.

[7] A. Karanjawane, A. W. Rohankar, S. D. Mali, and A. A. Agarkar, "Transport layer protocol for urgent data transmission in WSN", *Int. J. of Res. in Engin. & Technol.*, vol. 2, no. 11, pp. 81–89, 2013.

[8] K. Bronk, A. Lipka, and B. Wereszko, "Analysis of the topology control algorithms for the purpose of the hardware implementation", *Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne*, vol. 4, pp. 364–367, 2012 (in Polish).

[9] N. Li, J.C. Hou, and L. Sha, "Design and analysis of an MST-based topology control algorithm", in *Proc. 22nd Ann. Joint Conf. . IEEE Comp. & Commun. INFOCOM 2003*, San Francisco, CA, USA, 2003, pp. 1702–1712.

[10] M. Bahramgiri, M. Hajiaghayi, and V. S. Mirrokni, "Fault-tolerant and 3-dimensional distributed topology control algorithms in wireless multi-hop networks", in *Proc. 11th Int. Conf. on Comp. Commun. & Netw. ICCCN 2002*, Miami, FL, USA, 2002, pp. 392–397.

[11] S. A. Borbash and E. H. Jennings, "Distributed topology control algorithm for multihop wireless networks", in *Proc. Int. Joint Conf. on Neural Netw. IJCNN'02*, Honolulu, Hawaii, USA, 2002, pp. 355–360.

[12] D. M. Blough, M. Leoncini, G. Resta, and P. Santi, "The *k*- Neighbors approach to interference bounded and symmetric topology control in ad hoc network, *IEEE Trans. on Mob. Comput.*, vol. 5, no. 9, pp. 1267–1282, 2006.

[13] K. Wu and W. Liao, "Revisiting topology control for multi-hop wireless ad hoc networks", *IEEE Trans. on Wirel. Commun.*, vol. 7, no. 9, pp. 3498–3506, 2008.

[14] K. Bronk, A. Lipka, B. Wereszko, and K. Żurek, "Hardware implementation of the self-organizing sensor network to monitor of the environmental parameters", *Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne*, vol. 6, pp. 246–249, 2013 (in Polish).

[15] IEEE Std 802.15.4-2006: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE, New York, 2006.

[16] R. Niski, K. Bronk, J. Żurek, A. Lipka, B. Wereszko, and K. Żurek, "A hardware demonstrator of the self-organizing sensor network to monitor condition and hydro-meteorological threats at sea – Stage 1", National Institute of Telecommunications, Gdańsk, 2011 (in Polish).

[17] lwIP 2.0.0 LightweightIPstack [Online]. Available: http://www.nongnu.org/lwip/

Krzysztof Bronk holds Ph.D. (2010) and is an Assistant Professor in National Institute of Telecommunications. He is an author or co-author of more than 30 reviewed scientific articles and publications and about 20 R&D technical documents and studies. His research is mainly centered on the field of radiocommunication systems and networks designing and planning, software defined and cognitive radio systems development, multi-antenna technology, cryptography, propagation analysis, transmission

and coding techniques as well as positioning systems and techniques. His interests includes also multithread and object oriented applications, devices controlling applications, DSP algorithms and quality measurement solutions.
E-mail: K.Bronk@itl.waw.pl
National Institute of Telecommunications
Wireless Systems and Networks Department
Jaśkowa Dolina st 15
80-252 Gdańsk, Poland

Adam Lipka received the M.Sc. and Ph.D. degrees in Telecommunication from the Gdańsk University of Technology in October 2005 and June 2013, respectively. Since January 2006, he has been working in the National Institute of Telecommunications in its Wireless Systems and Networks Department in Gdańsk (currently as an Assistant Professor). His scientific interests include contemporary transmission techniques, MIMO systems and radio waves propagation. He is an author or co-author of over 40 scientific papers and publications.
E-mail: A.Lipka@itl.waw.pl
National Institute of Telecommunications
Wireless Systems and Networks Department
Jaśkowa Dolina st 15
80-252 Gdańsk, Poland

Błażej Wereszko received the M.Sc. in Electronics and Telecommunications from Gdańsk University of Technology in 2011. Since 2010 he works in the Wireless Systems and Networks Department of the National Institute of Telecommunications. His scientific interests focus on wireless communications, radio waves propagation, radiolocation and cognitive radio technology. He is an author or co-author of over 10 scientific papers and publications in the field of radiocommunication.
E-mail: B.Wereszko@itl.waw.pl
National Institute of Telecommunications
Wireless Systems and Networks Department
Jaśkowa Dolina st 15
80-252 Gdańsk, Poland

Jerzy Żurek received his M.Sc. and Ph.D. degrees in Telecommunication from the Gdańsk University of Technology in 1990 and 2005, respectively. Since 2005, he is employed at the National Institute of Telecommunications, Poland, (as an Assistant Professor) and since July 2014 he is also the Director of the Institute. He has also been associated with the Gdynia Maritime University. His research interest includes wireless systems theory, digital signals processing and radio propagation. He is a member of Polish Government delegation to IMO COMSAR Subcommittee in London.
E-mail: J.Zurek@itl.waw.pl
National Institute of Telecommunication
Szachowa st 1
04-894 Warsaw, Poland

Krzysztof Żurek is employed at the National Institute of Telecommunications in Wireless Systems and Networks Department in Gdańsk as an R&D specialist. Currently he is also concluding his Ph.D. thesis at the Gdańsk University of Technology. His research interest include the theory of automatic control, sensor networks and wireless systems.
E-mail: K.Zurek@itl.waw.pl
National Institute of Telecommunication
Wireless Systems and Networks Department
Jaśkowa Dolina st 15
80-252 Gdańsk, Poland