INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2017, VOL. 63, NO. 2, PP. 201–207
Manuscript received December 8, 2016; revised April, 2017. DOI: 10.1515/eletel-2017-0027

RBCP-WSN: The Reliable Biderectional Control Protocol for Wireless Sensor Networks

Marcin Golański, Radosław O. Schoeneich, Dawid Zgid, Marek Franciszkiewicz, and Michał Kucharski

***Abstract*—This paper presents the Reliable Bidirectional Control Protocol (RBCP) protocol, which is a transport protocol for Wireless Sensor Networks (WSN), focused on managing sensors' behaviour. It aims to be a utility for reliable control data transferring from source to destination unit in the network. Considering the related studies on transport protocols, which are mostly dedicated to a single-direction reliable data transport, RBCP is the answer for the lack of control mechanisms in WSNs based on bidirectional communication. The first part of this paper is focused on general presentation of the proposed solution. In the next part, evaluation of the idea and final functionality are discussed. It will finally show the results of undergone testing stage.**

***Keywords*—Routing Protocols, MANET, WSN**

I. Introduction

THE growing need to process large amounts of information from the environment contributes to the development of wireless sensor networks (WSN). This process is an integral part of the Ambient Intelligence (AmI)[1] - environment combined with user-aware ICT solutions. Sensor networks are built to be in order to facilitate the monitoring of conditions over large areas. The functionality of the sensors allows to capture a very different data e.g. prevailing weather conditions, changes in position of an object or human health condition. Examination of time-varying phenomena in conjunction with the extensive functionality of nodes makes sensor networks popular in a wide scope of military, industrial, and household applications [2]. Regardless of the application, collected data require fast processing and phenomenon of anomalies response. Hence there is a need for mechanisms to control the operation of nodes in the network. This leads to the need for a separate control channel with strictly defined rules of communication.

The current technology with progressive miniaturization of electromechanical devices Micro Electro-Mechanical Systems (MEMS) provides low-cost, wireless and energy-efficient solutions to build a network infrastructure. These advantages allow to build an extensive network with relatively very low cost of creation. Due to the size and battery power, sensors are devices with very limited performance, therefore well known in most networks TCP/IP is inefficient in usage.

The main task of the sensor nodes in the network is to collect and transfer data to the destination sink-node. The sink-node very often has role not only a simple destination but also it aggregates and processes the data. The direction of the data is usually to the destination, but in some situations there is a need to establish reverse communication channels to source-nodes. The two-way communication is dedicated for control and manage the work of the nodes in the networks.

This paper presents the bidirectional control protocol for Wireless Sensor Networks. The main feature of the protocol is a high reliability in two-way control instructions communication. The proposed algorithm allows for modification of the work for individual nodes and the entire network. Particular emphasis is placed on the implementation of a reliable bi-directional communication sink-source-sink.

Marcin Golański, Radosław O. Schoeneich, Dawid Zgid, Marek Franciszkiewicz and Michał Kucharski are with the Institute of Telecommunications, Warsaw University of Technology, Warsaw, Poland (e-mail: mgolanski, rschoeneich@tele.pw.edu.pl).

II. Communication in WSN - State of the Art

A characteristic feature of the WSN is a periodic transmission measurements by sensors in the direction of the sink-node. The proper communication in a highly unstable radio environment is affected by both: internal network parameters and external factors. The most important are: (a) the number of nodes; (b) size of network area; (c) the period of sending data; (d) weather conditions; (e) radio interference from other devices; (f) shielding architectural barriers and landforms.

To optimize the exchange of data, dedicated communication protocols in the network and transport layer of WSN stack are used. Protocols determine a behaviour of nodes in the network, and introduce mechanisms for minimization data transmission losses. The network is overload and transmission errors resistant. The need for reliable communication relates both down as well as up-link. Due to the large amount of collected information, there are introduced solutions to control the network. Therefore, the mechanisms are required for the bidirectional mode of operation.

The issue related to reliable data transport in wireless networks with data-packet communication is the subject of many studies focusing on improving the efficiency of the transport mechanism [3]. Ad-hoc Transport Protocol [4] is control protocol designed for ad-hoc networks. The protocol was created for point-to-point communication. It contains procedures such as communication creation and constant bit rate data communication. Unfortunately, the main procedures are not applicable in WSN due to energy limitations. There exists WSN transport protocols with reliable data delivery mechanisms, most of them are one-way communication. The ESRT [5] and RMST [6] was designed for communication between sensor sources and sink-node. On the other hand there are protocols with up-stream communications like GARUDA [7] and PSFQ [8] protocols. The example of bi-directional

	ESRT	RMST	PSFQ
Reliability	uplink	uplink NACK	downlink NACK
Retransmission	-	yes	yes
Excessive data flow control	yes	no	no
	GARUDA	**ART**	**STCP**
Reliability	downlink NACK	bidirectional ACK/NACK	bidirectional ACK/NACK
Retransmission	yes	yes	yes
Excessive data flow control	no		yes

Fig. 1. Comparison of transport protocols

communication protocol is ART [9] and the management protocol data transfer network is STPC [10]. The comparison of available protocols in terms of selected properties was presented in Figure 1.

As was stated earlier, the Event-to-Sink Reliable Transport [5] protocol allows for reliable data transfer from sensor nodes to the sink-node. The algorithm focuses on messages detection, and then transfer it to the sink with predefined characteristics. The task of the protocol is non-standard data transmission collected by nodes. The reliability of communication is determined based on the number of received packets. The ESRT protocol selects the period of data sent by the source nodes so as to maintain a constant level of delivery reliability. It is done by response rate of nodes in the network based on measurement data load. The traffic volumes indicated by the marker in sent packets.

Another solution used for data transfer Reliable Multi-Segment Transport protocol [6]. RMST is based on the Direct Diffusion [11]. Protocol operation is based on sending a Negative Acknowledge packet. The protocol is used for transmission of large amounts of data. Nodes receiving packets make decisions about the retransmit need of message fragments.

The Pump Slowly Fetch Quickly [8] is a protocol based on a set of additional mechanisms for communication between the source of the message and the receiving node. The mechanisms include error correction in hop-by-hop data exchange, messages buffering within the network, and correction query by use of NACK packets. The packet-send event causes rapid retransmissions even before moment of the next message retransmission form the source, what is called Pump procedure. The solution develop error correction mechanism which is used to recover lost messages. The PSFQ protocol ensures the continuity of sequential data received. The protocol disadvantages include: lack of resistance to the loss of individual packets, and the lack of mechanisms for network overload caused by excessive data flow.

GARUDA [7] is the next example of works carried out over reliable communication. The protocol operation is focused on virtual network infrastructure. Selected nodes in the network are assigned as servers responsible for lost packets recovery. Mechanisms available in the protocol allow for creation and management of virtual set of nodes. The protocol quickly recovers lost data. It works in two stages: in the first phase the lost data are recovered by communication with the central node, in the second stage lost packets are recovered by transmission with other nodes.

The example of bidirectional communication algorithm is Asymmetric Reliable Transport, proposed in [9]. The ART is one of the first reliable transport protocols in WSN networks. The protocol provides the error correction mechanism and introduces a procedures for monitoring the network traffic volume. Operation of the protocol is based on a hierarchical nodes arrangement. The responsibility for packet delivery in destination node lies with the individual node at higher level in hierarchy. The message receive by higher-level node, regardless of the direction of transmission, is sufficient factor for certainty of delivery. All function allow sensors make the operation balanced, and helps in reducing energy consumption.

The last solution strictly related to the bidirectional transmission control in WSN is the Sensor Transmission Control Protocol [10]. The protocol belongs to specialized transport protocols set which can be used independently of protocols in the other layers. Most of the functions of the protocol is managed by the base station the data sink node. The SCTP offers a graduated control over the data loss and the data congestion.

With the best authors knowledge none of these solutions are fully meet the objectives and functions required by the protocol for managing the bidirectional communication of the WSN nodes, which is the justification for our work.

III. The Reliable Biderectional Control Protocol for WSN

In this chapter we introduce the Reliable Bidirectional Control Protocol (RBCP) for data transmission and full bidirectional network nodes control. In our solution we merge the functionality of the data link layer and the network layer which allows to significantly reduce the communication overhead. This unified cross layer communication schema with simple and efficient data transport algorithm consist of the proposed solution.

Dedicated protocol provides direct communication between the sink and source nodes. Additionally it is enhanced by the return channel and dedicated functions for network behaviour modifications. Dedicated protocol is a tool for implementing in sensor network that allows for network control from scratch. This means the implementation of a set of mechanisms allowing layered communication and influencing nodes behaviour. We proposed, that based on the data at the sink-node analysis, the first operations using a reliable algorithm can be done.

The RBCP provides the communication organization between nodes. At the network creation moment, nodes are unaware their network topology and structure of connections to neighbouring units. Therefore the tree is created based on radio connections and hierarchical relations between nodes. The communication organization, besides the use in RBCP protocol, introduces arrangement of the data transmission. The message delivery is done by forwarding hop-by-hop. This means that packets are transported from node to node based on the parent-child scheme. The advantage of this structure is reducing amount of transmitted data in the network.

A. Assumptions

Main assumptions and initial conditions are: (a) after-specific network nodes do not know the topology; (b) the findings encapsulation of distribution of the nodes during the operation of the algorithm is fixed topology of the nodes; (c) the transfer of data is done by the so-called. flooding - flooding packets neighbours; (d) messages are disseminated in the network, until it will reach the destination; (e) each node has its own identifier, works with a specific clock rate, and has a simple pseudo-random number generator; (e) all nodes in the network are synchronized in terms of start at the same time; (f) nodes have sufficient resources for computing; (g) the communication is one-sided, there is no acknowledgement packets or answers.

B. TinyOS Medium Access Protocol

We decided to use standard MAC [12] [13] [14] protocol implemented in TinyOS [15] operating system for RBCP purpose. The most important procedure of the MAC for RBCP performance is the back-off procedure. The procedure helps in minimizing data packet loss during the establishing of network connections and correct data transmissions. While the channel is busy due to other transmissions, the next transmission will take place after time back-off procedure. Functions of the MAC protocol are used for the organization of communication of the nodes. The details of this function are described in [16].

C. Routing protocol

Wireless sensor network self organization starts at the time of first sensor start-up. The initial connections topology is created. At this stage, each node has information about the possible connections only to its parent-node - to the node with lower value TTL. Both sink-node and other sensors do not know the connections between nodes which are not within their sight. On parallel paths to each node in the network are created. In this process the path creation is distinguished by the following steps:

Step 1 The sink-node sends a start packet with the value of TTL = TTLsink. Other nodes in the network are in the listening mode at this time.

Step 2 After receiving the packet by the nodes in the first level of the visibility (1 hop), the TTL value is checked the TTL value and identifier idsink available in the message is stored in node memory. After then a TTL value is increased by 1 (TTLcurr = TTLprev + 1), and they replace the TTL parameter in received packet. In addition the information about the node identifier idnode is included to the message. The modified packet is broadcast in the network. Figure 2 presents the initial phase of the algorithm.

Step 3 At the next hop, a first received packet by the node is a source of information for the path creation. The procedure for packet content modification is similar to those in step 2, and then the packet is forwarded into the network, as we present in Figure 3. Information about the higher level neighbourhood are stored in the modes memory.

Step 4 If during tw period after sending the modified message with updated path, the node does not receive a packet

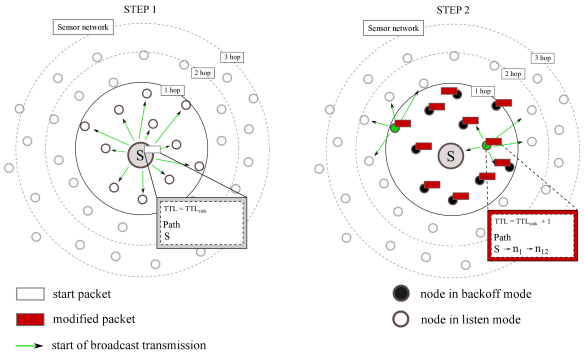

Fig. 2. A tree creation: initial phase example

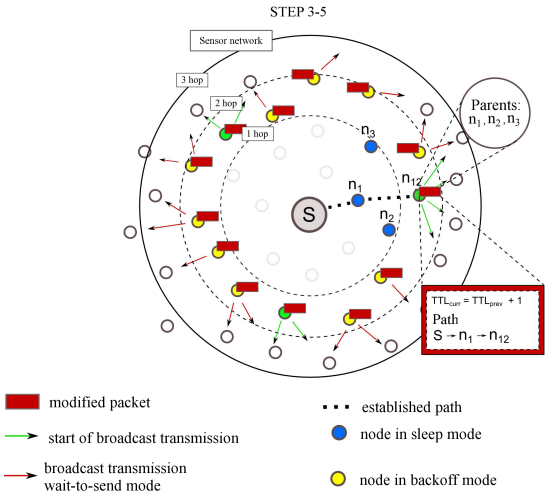

Fig. 3. A creation of tree connections

with a higher TTL value, it is regarded as an edge of the network. The node has the role of the leaf in the tree.

Step 5 A leaf, based on packet information received from its parent, has full information about the intermediate nodes in the route from the sink-node. This information is provided to the sink-node, therefore each node sends a message to each parent as is shown in Figure 4. Every time the packet arrives to the parent node, the acknowledge ACK message is sent. After the time t_ack the packet with route information is retransmitted.

Step 6 The sink-node collects maintenance information. It is done be receiving information from neighbouring children and parents at the communication tree. The return-path can be set using different routes. This is due to receive multiple packets from the same node, but passing through other intermediate nodes.

D. Data Transfer

The goal of the algorithm is the fastest communication between sink and leaf and in the reverse order. Bi-directional data exchange of RBCP protocol is divided into two phases: up and down the network.

1) Up the network: The sink-node sends packet to all nodes network which contains: the TTL value, the source identifier idsrc = idsink, the destination identifier iddest, a message priority MP parameter, and the payload. The TTL value specifies

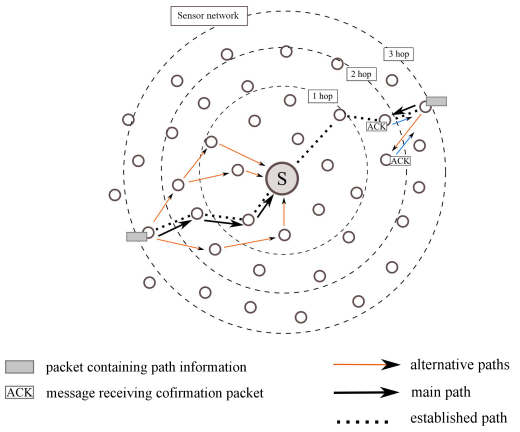

Fig. 4. Run-off packages of routes to individual nodes in the network - the concept III

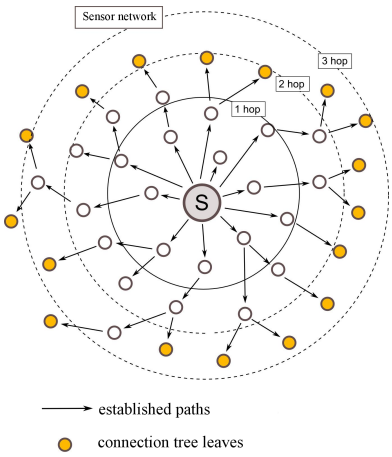

Fig. 5. Created tree connections

the number of levels through which the message must pass. At each level the TTL is decreased by 1, and it is done until TTL is equal 0 at the destination node. The MP parameter is placed in the message header as additional fields. It determines the priority of the message and has influence on the behaviour of nodes at the time of the messages transmission. Network operation which depends on the MP parameter is described later in this chapter. The payload contains instructions for node controlling or a single requests. In addition, the sink node extends message payload by return path. Such prepared message is sent into the network.

2) Down the network: Message information received by the node are basis for a response. The decision for the response is taken based on the Response parameter. The zero response value means control message without response required. If the Response is set to 1, it begins response procedure. The response message contains: the TTL value which is set to the number of levels in the reverse path, the packet source identifier which is set to id of node, the destination identifier which is set to id of sink, and the value of Message Priority which is set to the same as received from the sink-node. Furthermore the message contains nodes response for sink-node instructions.

The network behaviour is strictly dependent on the MP parameter and can take the values equal 0, 1, 2. If message priority is equal 0 then the message is considered as a standard control instruction. In this case, the fast bidirectional communication is not required. The message with data is sent to the sink-node based on source-routed path, but without a mechanism that increases the probability of getting in a shorter period of time. If message priority is equal 1, the message has priority in sending. Sensor nodes within the radio range of the sender are forcing back-off procedure. Their own data are postponed. This method minimizes the medium access competition. For message priority equal 2 the control packet is sent in similar way to the MP = 1 parameter. Nodes participating in the downlink transmission are informed about a sleep mode suspend, resulting in active participation in transmission to the end of the cycle. This allows for fast transfer of data between the source to sink-node. Thus it eliminates the collision possibility in the channel and delays associated with the random time of the back-off procedure.

Figure 6 presents an example of the algorithm for different values of the message priority parameter. The message with MP = 0 is treated as an ordinary data packet. In Figure 6.a the packet is held by intermediate nodes until the radio channel is free. The medium occupancy is caused by the neighbouring node transmission. Random back-off times introduce additional delay in packet delivery to the destination node. The MP = 1 results in a lengthening back-off procedure among individuals who are within radio range of nodes that route the message. The message from the source-node to the sink-node causes analogous behaviour of nodes in the network (see Fig. 6.b).

In the third priority stage the data exchange (MP = 2) there are two stages of operations as shown in Figure 6.c. The message with instructions is transmitted in accordance with the diagram in the MP = 1 case. The difference lies in information for neighbouring nodes about an active mode extension until the next cycle start. A destination node starts of sending response data after the end of active time. All nodes on the return path are in the listening mode. The delay are only caused by the transfer of packets between intermediate nodes. Other nodes in the network are in the sleep mode at this time. A transmitting node is switching to the sleep mode after receiving the acknowledge from a node on a higher-level.

IV. Simulation Results

This chapter presents the results of simulation tests carried out on the reliability of RBCP protocol operation. We investigate the control messages influence for the number of delivered packets, the average delay of control packets for three values of the message priority parameter, and we examine the effect of control messages for the duration of data transmission to the sink-node.

The TOSSIM [17] as a simulation tool has been used, our implementation has been prepared using NesC[18] [19]. We assume for retransmission maximum of 3 attempts to send a data packet. For control packets, retransmissions are performed until receiving an acknowledge. Control messages are sent by

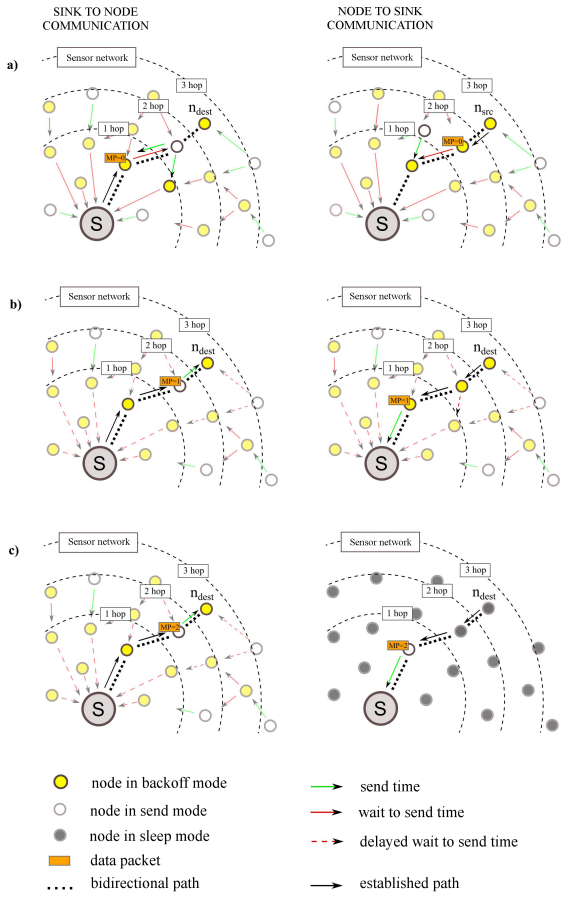

Fig. 6. The impact of Message Priority on the network behaviour for MP = 0, MP = 1, MP = 2

sink-node to the destination randomly selected. The maximum waiting time for the answer is equal to three times the value of the nodes cycle. All tests were performed on 100 different networks with 100 nodes.

Simulation parameters are presented in Figure 7. The node activity time is equal to 15% of entire cycle. Time values in the node operation mode was adopted based on the default operating times of SMAC protocol [20]. The simulation time was set to 100 second. The cycle time is defined as nodes working cycle and includes nodes active time and a sleep period. The awake time is defined as as a time at which the node has active radio transceiver. The csend parameter describes the period of control messages sending and is multiple of the cycle_time. The cchanel parameter equals 1 for control channel simulation or 0 for simulations without this channel. The MP message priority describes the version of RBCP protocol. The pp parameter describes both the intensity of data packets in the network and the percentage of nodes sending data packets in the simulated network. The dfactor parameter is scaling factor, which helps in tests for different physical dimensions of networks and their suppression.

Figure 8 presents the packet delivery ratio (PDR) with respect to the simulation dfactor parameter. We observe, the increasing dimensions of the simulation area causes a decrease in the packet delivery ratio value. For the control channel RBCP, the distance increase results in changes of tree

Name	Value	Unit
sim_time	100	h
cycle_time	1000	ms
awake_time	150	ms
csend	3	-
cchannel	[0,1]	-
mp	[0,1,2]	-
pp	50	-
dfactor	[30,40,...,100]	m

Fig. 7. Simulation parameters

structure. There is a fewer neighbouring units and alternative routes. Following this, a larger number of nodes are involved in the packet transmission, resulting in less output at these points. Since control messages are sent with the highest priority, the packet containing the measurement data can be rejected in case of the retransmissions, but this situation is rare.

PDR metric values for each MP are very close to each other. In the case of sensor networks operating without a control channel, the packet is transmitted much more times by a greater number of nodes due to limitations in neighbourhood nodes. This results in a longer route and consequently a greater chance for losing the packet in high noise conditions.

The value of MP = 1 with dfactor = 50 parameter is smaller then other MP parameters. This is due to back-off procedure usage on the nodes not participating in the control messages exchange, and a relatively high density of nodes in the network. This means that the sensors transmitted data measurements must wait for a random period of time and only after the transmission attempt. This can increase the number of attempts to send the packet because the back-off procedure may be initiated before the end time of the activity nodes. Then the packet will be retransmitted in the next cycle or, rejected after a certain number attempts to send.

Although the back-off mechanism is present for MP = 2, control messages replies are not sent during the activity nodes. This results in the highest value of PDR metrics for all values of the dfactor parameter. The lowest values of PDR occurs are for networks without RBCP protocol. Increasing dfactor results in increasing number of data measurement packets sent. This is due to greater distances between nodes and the reduction of interferences in the transmission medium. Consequences are more frequent data measurement data sending and lower nodes ability for packets forwarding towards the sink-node.

Figure 9 presents PDR metric changes for control packets with increasing dfactor parameter. Control messages are transmitted from the sink-node to the source-node. For RBCP protocol usage the number of control packets sent decreases with increasing distance between nodes. This is due to the intensive increase of data packets and acknowledge packets required. On the other hand, when the control channel is not in use, the number of packets sent is on a constant level. PDR metric values without control channel are significantly lower than with the RBCP. The PDR metric values decrease with increasing distance between the nodes and increase number of

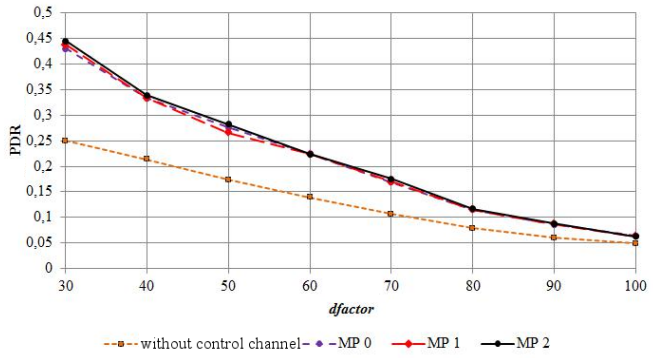

Fig. 8. Packet Delivery Ratio

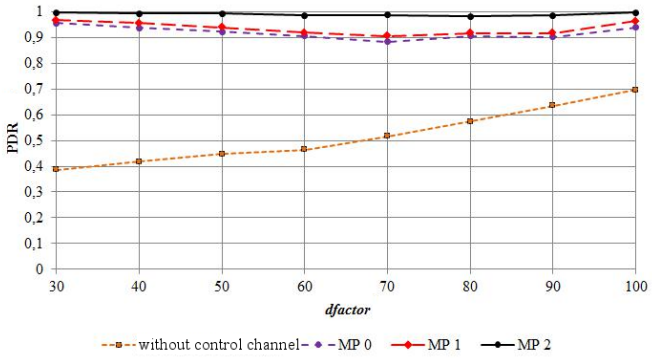

Fig. 10. PDR for control response messages

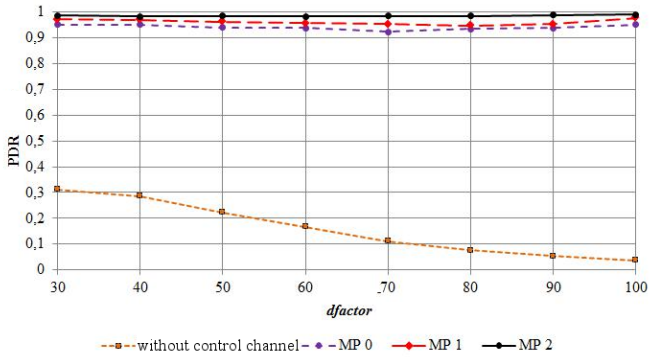

Fig. 9. The PDR for control packets

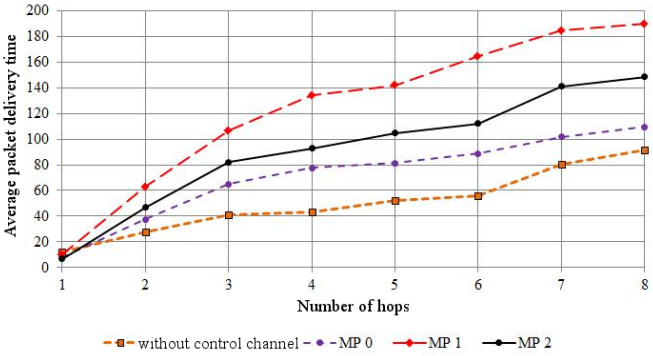

Fig. 11. Average packet delivery time

packets in the network. The most of packets are transmitted close to sink-node within the third or fourth hop. The visible impact of back-off procedure is for MP = 1 and MP = 2.

Figure 10 presents PDR metric results for response to control messages. Values of PDR are constant and much more better for all our solutions then for networks operating without a control channel. Most of the control messages reaches to nodes located near the sink-node, so replies following mainly from this nodes. With increasing value of the dfactor parameter and successful transmission, there is a greater chance for succeed packet delivery. A few percent drop of PDR for MP = 0 and 1, for dfactor 60, 70 is due to the tree structure of network topology. The reduction of the transfer ability occurs at points where nodes are connected to multiple upper level tree neighbours.

Results of RBCP with parameter MP = 2 are very good. The number of responses is almost equal to the number of control packets. The difference between them is due to the presence of high power noise in the transmission channel.

The average packet delivery delay was simulated for similar network parameters, with some differences. We propose the cycle_time = 120 sec., awake time = 5 sec., and dfactor = 60 meters.

The results of average packet delivery time were presented in Figure 11. Number of hops corresponds to the most common number and the maximum number of hops in the network tree. All values of the metric increases with increasing number of hops.

Average time for messages delivery is the shortest for solution without channel control for one cycle. It uses flooding, and does not guarantee the selection of the shortest path to the destination node. The number of hops significantly exceeds the graph scale, the restricted number of hops was introduced for comparison.

The average time results for MP = 0 represents the average time of packet transmission on the tree. The RBCP mode MP = 1 has the highest average delivery time. This is due to intentional delays made by nodes transmitting packets and additional delays caused by response messages transmission. The MP = 2 series is a compromise between the other modes MP. The average packet delivery time is longer than the standard MP = 0 due to the back-off procedure forcing. Responses for control messages are not sent during the nodes activity, thus the average delay is lower for MP = 1.

The Figure 12 presents the average time of control packet response delay. The shortest delivery time offers RBCP with MP = 2. The responses to control packets are sent not in the time of nodes activity. For this reason, the packet delivery time is dependent only by receive of the acknowledgement and delays associated with noise presence in the transmission channel.

V. Conclusions

The aim of this paper is to present the Reliable Bidirectional Control Protocol. The protocol is designed for control and management of nodes in WSN networks. The proposed

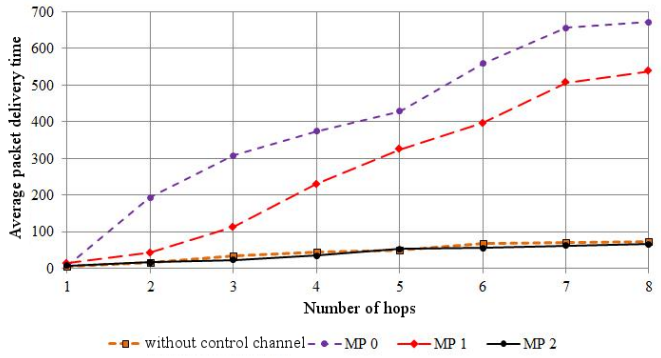

Fig. 12. Average latency of response packet delivery delay for control packets

solution in three versions (MP = 1, 2, 3) was extensively tested using simulation tools. The results of the simulations suggests the different usage. The RBCP with MP=1 can be used in networks where average packet delivery time is important. The MP = 1 version may be used (relative to the mode MP = 2) in cased where packets could not be transmitted after the time of the nodes activity. The solution for MP = 2 offers the best results consider simulation metrics, the cost is less energy efficiency.

In general, the RBCP protocol provides a high degree of transmission reliability of the requests, control instructions and control responses. The proposed solution is applicable in networks designed for making measurements in environments with large and sudden changes in measured values. The algorithm introduces the reaction for the environment anomaly.

REFERENCES

[1] G. Riva, F. Vatalaro, F. Davide, M. Alcaiz, "Ambient Intelligence," *IOS Press,* 2005.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless Sensor Networks: a Survey," *Computer Networks,* Vol. 38, 2002, pp. 393-422.

[3] F. Wang, Y. Zhang, "Improving TCP Performance over Mobile ad-hoc Networks with Out-of-Order Detection and Response," *in Proceedings of ACM Mobihoc,* 2002, pp. 217-225.

[4] K. Sundaresan, V. Anantharaman, H.-Y. Hsieh, R. Sivakumar, "ATP: a Reliable Transport Protocol for ad-hoc Networks," *in Proceedings of ACM Mobihoc,* 2003, pp. 64-75.

[5] Y. Sankarasubramaniam, O. Akan, I. Akyildiz, "ESRT: Event-to-Sink Reliable Transport in Wireless Sensor Networks," *in Proceedings of ACM MobiHoc,* 2003, pp. 177-188.

[6] F. Stann, J. Heideman, "RMST: Reliable Data Transport in Sensor Networks". *in Proceedings of IEEE SNPA,* 2003, pp. 102-113.

[7] S. Park, R. Vedantham, R. Sivakumar, I. Akyildiz, "A Scalable Approach for Reliable Downstream Data Delivery in Wireless Sensor Networks," *in Proceedings of ACM MobiHoc,* 2004, pp.78-89.

[8] C.-Y. Wan, A.T. Campbell, L. Krishnamurthy, "Pump Slowly, Fetch Quickly (PSFQ): a Reliable Transport Protocol for Sensor Networks,". *IEEE Journal On Selected Areas In Communications,* Vol. 23, No. 4, 2005.

[9] N. Tezcan, W. Wang, "ART: An Asymmetric and Reliable Transport Mechanism for Wireless Sensor Networks," *International Journal of Sensor Networks,* Vol. 2, Issue 3/4, 2007, pp. 188-200.

[10] Y. G. Iyer, S. Gandham, S. Venkatesan, "STCP: A Generic Transport Layer Protocol for Wireless Sensor Networks," *in Proceedings of 14th International Conference on Computer Communications and Networks,* 2005, pp. 449 - 454.

[11] S. Khan, A.-S. K. Pathan, N. A. Alrajeh, "Wireless Sensor Networks: Current Status and Future Trends," *Ch.* 11, 2012, pp. 285-324.

[12] W. Ye, J. Heidemann, D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," *IEEE INFOCOM,* Vol. 3, 2002, pp. 15671576.

[13] W. Ye, J. Heidemann, D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," *IEEE/ACM Transactions on Networking,* 2004, pp. 493506.

[14] T. Van Dam, K. Langendoen, "An Adaptive Energy Efficient MAC Protocol for Wireless Sensor Networks," *in Proceedings of the 1st international conference on Embedded networked sensor systems, SenSys,* 2003, pp. 171 180.

[15] https://github.com/tyll/tinyos-2.x-contrib.

[16] D. Moss, P. Levis, "BoX-MACs: Exploiting Physical and Link Layer Boundaries in LowPower Networking," *Technical Report SING-08-00*, Stanford University, 2008.

[17] P. Levis, N. Lee, M. Welsh, D. Culler, "TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications," *in Proceedings of the 1st international conference on Embedded networked sensor systems,* SenSys, 2003, pp. 126-137.

[18] D. Gay, P. Levis, R. Von Behren, M. Welsh, E. Brewer, D. Culler, "The nesC Language: A Holistic Approach to Networked Embedded Systems," *in Proceedings of Programming Language Design and Implementation (PLDI)*, 2003.

[19] http://nescc.sourceforge.net/

[20] D.E. Boubiche, A. Bilami, "A Defense Strategy against Energy Exhausting Attacks in Wireless Sensor Networks," *Journal Of Emerging Technologies In Web Intelligence,* Vol. 5, 2013, pp.23.