PERFORMANCES AND LIMITATIONS OF UNSLOTTED CSMA/CA MEDIA ACCESS IN IEEE 802.15.4 NETWORKS

Žarko F. Čučej

University of Maribor, Slovenia

Key words: wireless sensor network, standard IEEE 802.15.4, media access control, modeling, simulation

Abstract: Standard IEEE 802.15.4 offers three topology types and two channel access modes: slotted and unslotted CSMA/CA. The majority of a research work targets the performance of the slotted CSMA, despite the fact that wireless sensor networks are, by nature, intended to be multi-hop networks, where unslotted CSMA is the preferred media access control. This article analyzes the performance and limitations of the slotted CSMA channel access mechanism found in IEEE 802.15.4 devices. For this purpose, we have developed a model of a wireless sensor network node for the simulation-program OPNET.

Zmogljivosti in omejitve mehanizma dostopa do medija CSMA/CD brez rež v omrežjih IEEE 802.15.4

Kjučne besede: brezžična senzorska omrežja, standard IEEE 802.15.4, dostop do prenosnega medija, modeliranje, simulacije

Izvleček: Standard IEEE 802.15.4 določa tri topologije povezav omrežij in dva načina dostopa do prenosnega medija: CSMA/CA v definiranih režah in CSMA/CA v poljubnem času. Glavnina raziskav je usmerjena v mehanizme dostopa, ki so lahko aktivni le znotraj definiranih in med uporabniki omrežja sinhroniziranimi časovnimi intervali – režami, čeprav je dejstvo, da so brezžična radijska omrežja po naravi namenjena več-etapnemu prometu, kateremu je inherentna lastnost svobodni dostop do medija brez omejevanja s časovnimi režami.

V članku analiziramo zmogljivosti in omejitve dostopa do prenosnega medija brez organizacije časovnih rež, kot ga določa standard IEEE 802.15.4. V ta namen smo za simulacijski program OPNET razvili simulacijski model vozlišča v brezžičnem senzorskem omrežju.

1. Introduction

Wireless Sensor Networks (WSN) have two main advantages over wired networks:

1. the nodes can be mobile, and
2. they can be simply deployed in areas of interest, and at low-cost.

Both advantages require the following from network nodes: sensors with the ability to communicate with each other or with some central station. Their radio signals, on the one hand should have an autonomous energy source able to provide long-term sensor operations without maintenance, and on the other hand, have the capability of self-organization within the network.

A typical WSN consists of a large number, even a few thousand, nodes equipped with different types of sensors, microprocessors, radio transceivers etc, with goal of collecting measured data by sensors and transferring it through one or more data sinks, called User Access Point (UAP) or a Base Station (BS), to the end users of WSN services. The random-deployment of sensors, for example in battlefields or in plantations, usually means that the positions of the nodes are neither known exactly nor accessible for maintenance and local administration. Consequently, they should have the capabilities for self-organization on an ad-hoc multi-hop network fashion where, under normal working circumstances, the majority of traffic flows towards BS /1/

Within the implementation of WSN, the standard IEEE 802.15.4 developed by a working group for Wireless Personal Area Network (WPAN) /2/, is very popular. For example, the ZigBee alliance /3/ built their wireless sensor network solution on top of the 802.15.4 standard, which they used for the physical and medium access layer. ZigBee found its application area within home automation, plantations monitoring, health care, etc and even in the military field, where it is used, for example, for remote battlefield and Base-Camps, where surveillance became simpler and possible using wireless technology /4/. ZigBee's current focus is on defining a general-purpose, inexpensive, self-organizing mesh network that can be used for industrial control, embedded sensing, medical data collection, smoke and intruder warning systems, building automation, home automation, etc. The resulting network use very small amounts of power – individual devices would have to have a battery life of at least two years to pass ZigBee certification.

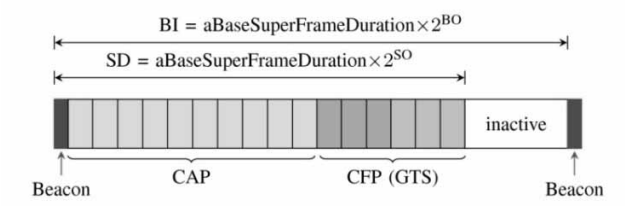
This article evaluates the multihop properties of the IEEE 802.15.4 standard through simulations in OPNET, using our own simulation model (SPaRCMosquitoModel), based on a WSN node prototype named SPaRCMosquito.

2. Standard IEEE 802.15.4

The IEEE 802.15.4-2003 Low-Rate Wireless Personal Area Network (WPAN) standard specifies the lower protocol layers: the physical layer (PHY), and the media access

control (MAC) portion of the data link layer (DLL). This standard specifies operations within the unlicensed 2,4 GHz (worldwide), 915 MHz (Americas), and 868 MHz (Europe) industrial, scientific, and medical (ISM) bands, where is defined 16, 10 and one channel, respectively. Channel bandwidth is 5 MHz. The raw, over-the-air data rate is 250 kb/s per channel in the 2,4 GHz band, 40 kb/s per channel in the 915 MHz, and 20 kb/s in the 868 MHz band. The transmission range is between 10 and 75 meters, and the output power of the radios is generally 0 dBm (1 mW) /5/.

The basic channel access mode is Carrier Sense, Multiple Access/Collision Avoidance" (CSMA/CA) channel access /6/. Their usage depends on their operating modes: beacon and non-beacon modes. In the beacon mode network, the coordinator creates a beacon message, called super frame, on which every client node is synchronized /5/. Super frame (Fig. 1) is divided on two types of slots and on an inactive period /2/.



Legend:

CAP	Contention Access Period	BO/ SO	Beacon/Superframe Order
CFP	Contention Free Period	BI	Beacon Interval
GTS	Guaranteed Time Slots	SD	Superframe Duration

Fig. 1: Slotted CSMA/CA media access algorithm.

The first ten slots after beacon form so-called Contention Access Period (CAP), where the client uses a slotted CSMA/CA media access mechanism, which is similar to slotted Aloha media access control. CAP follows the Contention Free Period which, by definition, does not use CSMA. The same is valid for the beacon, which doesn't use any media access mechanism.

A. Non-beacon mode

The beacon mode is inappropriate for the multi-hop network, even though there are some scheduling techniques which propose the use of beacon mode in multi-hop networks /7/. The non-beacon mode standard specifies the use of unslotted CSMA/CA access mechanism (Fig. 2.)

Which, due to the specifics of WSN, differs from other IEEE 802.11x CSMA/CA mechanisms.

B. Non-beacon mode

The unslotted CSMA/CA mechanism uses random back-off time before sampling the channel (CCA). If the channel is found to be idle the node transmits data, otherwise it

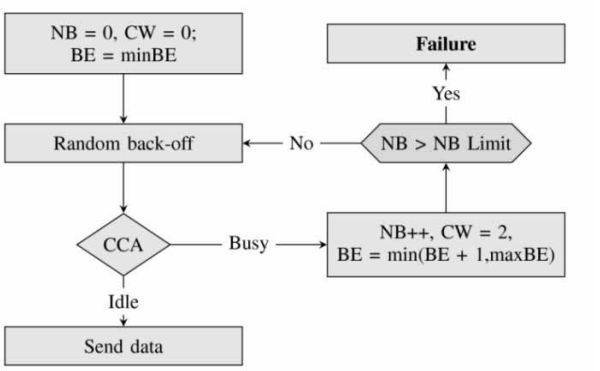


Fig. 2: Unslotted CSMA/CA media access control procedure. NB: Number of Backoffs, BE: Backoff Exponent, CW: Contention Window, CCA: Clear Channel Assessment.

repeats the back-off sequence until the channel is idle (or NB > NB Limit, see Fig. 2). The longest time to be channel accessed when channels is in the idle state considering initial back-off period and CCA sampling can be calculated as:

$$\text{backoff} + \text{CCA} = (2^3 - 1)\cdot\text{UBP} + \text{CCA} = 3{,}768 \text{ ms} \quad (1)$$

where CCA is defined as eight modulation symbol periods, and UBP (Unit Backoff Period) as 20 modulation symbol periods. A length of one modulation symbol period is determined by QPSK modulation and its duration is 1250 kHz = 16 micro second.

The IEEE 802.15.4 standard specifies a 127 bytes long MAC frame (data + header). Standard header is 25 bytes long. When using short addressing field (16 bits), the overhead is reduced to 13 bytes, leaving 114 bytes to payload /2/. Considering five bytes for Start of Frame Delimiter (SFD), one byte for data length (LEN) and MAC frame length, the duration of PHY frame is:

$$\frac{MACframe + \text{SFD} + \text{LEN}}{250\times10^3} = \frac{(127+5+1)8}{250\times10^3} = 4{,}256 \text{ ms} \quad (2)$$

Minimum time of MCU used for process the data is called turnaround time (TAT). In 802.15.4 standard the TAT is 0,192 ms. Inter frame separation period depends on PHY frame length. When sending frames shorter than 18 bytes, the short IFS (SIFS) is used (the length of SIFS is period of 12 symbols), and when frames are longer, the long IFS (LIFS) is used (the length of LIFS is period of 40 symbols). Acknowledge frame in IEEE 802.15.4 is 11 bytes in length and needs 0,352 ms of time to be send. Of course ACK duration of waiting period must be considered – normally it should not exceed 0,864 ms.

In the worst case scenario for traffic throughput all above elements should be considered when sending one frame. Without using ACK communications, which doesn't use CSMA/CA media access, the total time for sending one frame is around 6,816 ms, giving effective data rate approximately 133,8 kb/s, and with ACK communication this time is around 8,032 ms giving effective rate approximately 113,6 kb/s.

C. Open issues in non-beacon mode

The IEEE 802.15.4 faces with two significant problems, the both already known from 802.11x standard: hidden node and expose node problems.

The hidden-node problem is, in practice, solved with RTS/CTS frames /8/ in both networks 802.11x and 802.15.4 /9/, /10/. Some previous simulations stated that nearly 35 % of all traffic represents the control RTS/CTS packets /9/, /11/. On the other hand, without RTS/CTS packets, the network falls into congestion and only a low percentage of actual data is transmitted /9/, /11/.

In the case of the RTS/CTS frame usage channel saturation is about 48 % of the channels capability (120 kb/s). The use of RTS/CTS packets solves the hidden node problem, but the exposed node problem remain unresolved /9/ - /11/.

IEEE 802.15.4 does not consider any protocol or solution for either the hidden-node problem or the exposed-node problem.

3. Node model for OPNET

The OPNET model named "SPaRCMosquitoModel`` has been developed from a physical wireless sensor node, designed and created in the SpaRC[1] laboratory (Fig. 3).

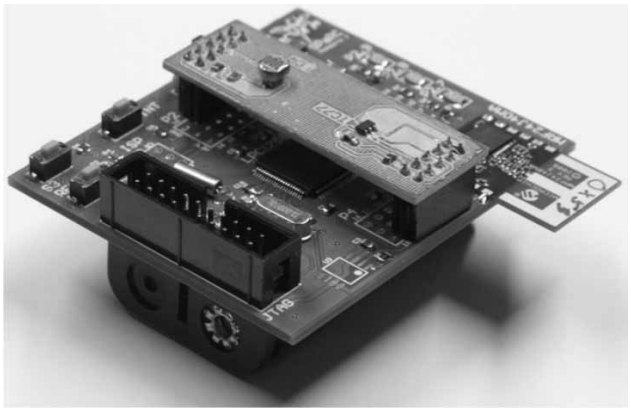


Fig. 3: WSN node SPaRCMosquito.

Calculations in simulations are based on real hardware data. Power consumption in simulations is calculated from measurements of real power consumption of the radio module MRF24J40 and CC2420, Cortex MCU, memory and integrated interface circuits. The figure 4 shows selection of data for simulation considering exact parameters as stated in data sheets.

The OPNET node model implements Physical layer, MAC layer with CSMA/CA access mechanism, routing and topology layers, a dispatcher and a data layer with source and sink processes at the top. The independent Battery process serves for separate calculation of power consumptions for CPU, sensors, and radio (Fig. 5).

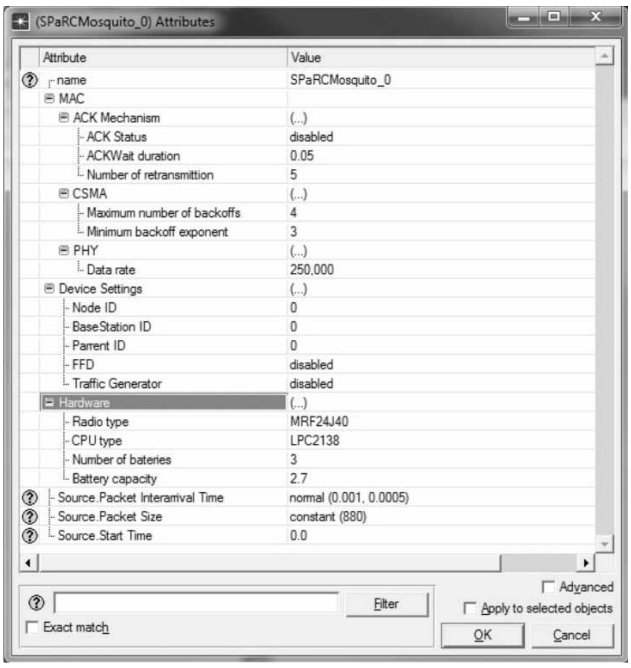


Fig. 4: Parameter selections for SPaRCMosquito OPNET model.

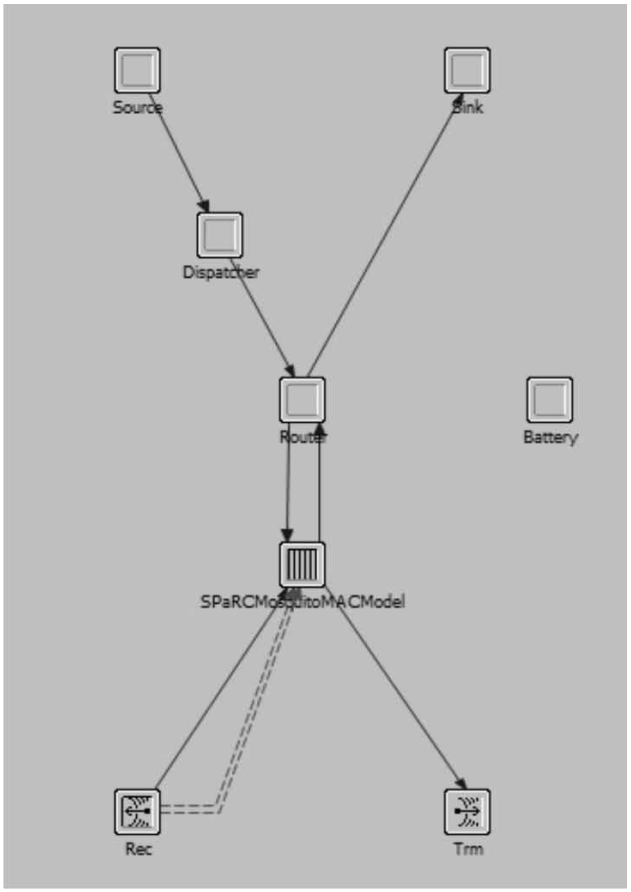


Fig. 5: Parameter selections for SPaRCMosquito OPNET model.

The source process is the data generator. Data is generated based on packet inter-arrival time and size selected in

1 *Laboratory for Signal Processing and Remote Control, \http://sparc.feri.uni-mb.si/*

node Attributes windows (Fig: 4). When created, the data packet is sent to the dispatcher process. The dispatcher process selects the targeted address (receiving node). In current setups around 95 % of data is sent towards the base-station. The rest of a packets are sent to random nodes within the network.

The routing process adds routing information to the packet (next hop destination) and sends data to MAC process, which allocates the channel and sends the data to TX process. TX process sends the data over the "air" simulated by one from many communication channel models provided within the OPNET. Packets are received in MAC process via the RX process. The consistency of a packet is done during the MAC process (CRC is checked, packet types and addresses are examined). If the packet is consistent then it is forwarded to the routing process. Inconsistent packets, ACK packets, and others are dropped in the MAC layer. The routing-process checks if the frame destination address is equal to node address. If it is, sends the data to the sink module, otherwise it calculates the next hop address and sends the data to MAC process, where it is treated like every other data packet.

The most important process for our simulation purposes is the "SPaRCMosquitoMACModel" (MAC model) – the model that implements CSMA-CA channel access. The SPaRCMosquitoMACModel (Fig. 6) is, as

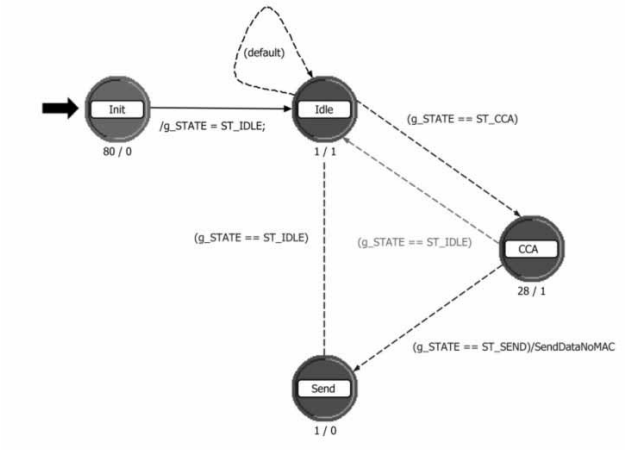


Fig. 6: SPaRCMosquitoMACModel process.

All others process models in OPNET based on the "state machine concept`` . In the idle state (Fig. 6), MAC process waits for the data from upper Network layer (from Routing process) or from lower Physical layer (from RX process).

If the data is passed from the upper layer, the model queues the data and starts the transmit protocol. The transmit protocol is based on a media accessed control procedure (Fig. 2). CCA scan duration is then simulated. During simulation, only two CCA samples are made: at the start and at the end of a CCA procedure which is 8 symbol-periods in length. If the medium is found to be idle, the data is sent. Alternatively, a new back-off duration is calculated and CCA sampling is repeated (Fig.2).

4. Network analysis by simulation in OPNET

For testing IEEE 802.15.4 throughput by simulations in OPNET the three scenarios were created:

1. scenario of the calculation for the worst case traffic throughput,
2. the traffic in the star topology (Fig. 7a), and
3. the traffic with 7 nodes creating a 6 hop network (Fig. 7b).

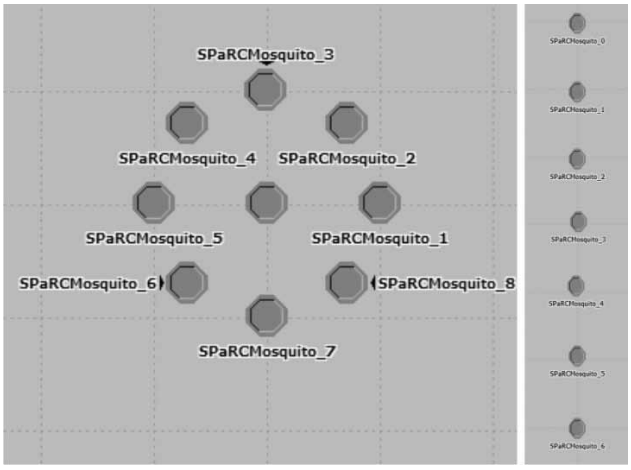


Fig. 7: SPaRCMosquitoMACModel process.

Traffic generators in the simulation scenario use normal distribution for packet inter-arrival times. Two parameters can be changed: mean outcome, defining the base time for data creation, and variance, defining the scattering. If, for example, the mean outcome is set at 0,5 and the variation to 0,1, a packet will be generated every 0,5 s within a possible variation of 0,1 s. Inversing the mean outcome give us the number of packets per second (mean outcome 0.5 means 2 packets/second), and vice-versa.

A. Throughput between two nodes

A comparison of the calculated results for the worst case scenario as it is described in subsection II-B with simulation of "real-life`` traffic with Gaussian pdf shows that simulation results give approximately 10 % to 20 % better throughput (Tab. 1).

Tabela 1: Comparison of computed worst case throughput and simulated average throughput between two nodes.

Traffic	calculated	simulated
non-ACK communication	~133,8 kb/s	155 kb/s
ACK	111 kb/s	~130 kb/s

This is expected results since the CSMA/CA mechanism implemented in ZigBee is accommodated for sparse traffic. Consequently calculated worst case throughput is actually upper bound for guaranteed utilization of raw channel capacity. Maximal throughput is obtained, when backoff

time is zero. In this case, as follows from calculation, the maximal throughput is approximately two times higher as at worst case scenario. Consequently, randomly generated traffic, obeying Gaussian pdf, should be clos to worst case scenario.

B. Single-hop network

Four single hop simulation groups were prepared: net-work with No-Acknowledgement and Acknowledgement settings simulated with two different node transmitting powers. Packets are generated on every node except base station in the middle of a circle (Fig. 7a). Packet generation is done via normal distribution with mean-value as the inverse number of packets per second and variation as half of the mean-value (Fig: 8).

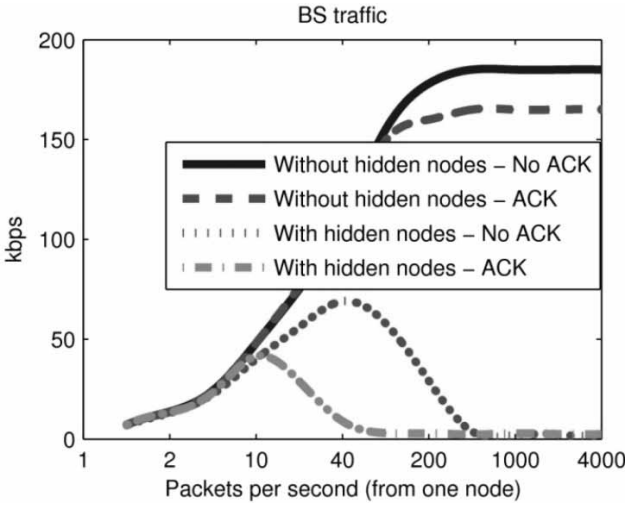


Fig. 8: Channel saturation.

In the first two simulations all nodes are in the same collision domain – no hidden nodes are present. The second simulation involves hidden nodes. This is accomplished by the selection of a transmission power, which enables 66,7 % of nodes to be visible to each other, and 33,3 % nodes to be hidden from certain nodes.

When considering the graphs (Fig. 4) it can be seen that without the hidden nodes' presence, the network throughput grows and stays saturated. The saturation limit for networks is acknowledged to be expectedly lower, as shown in Fig. 4 – acknowledgement frames must be sent from the receiver to the sender.

When dealing with hidden nodes, it can be seen that throughput rises to the point of maximum traffic still allowed and then drastically falls to a few received packets per second. Of course, the traffic with no acknowledges is again more successful. Sending ACK packets increases the chance of collision during the data send.

C. Multi-hop network

No-Acknowledge traffic setting was selected for multi-hop communication. The transmitting power was reduced to the levels can only hear the next node in chain (in scenario simulation radio sight was limited to 510 m; nodes were 500 m apart).

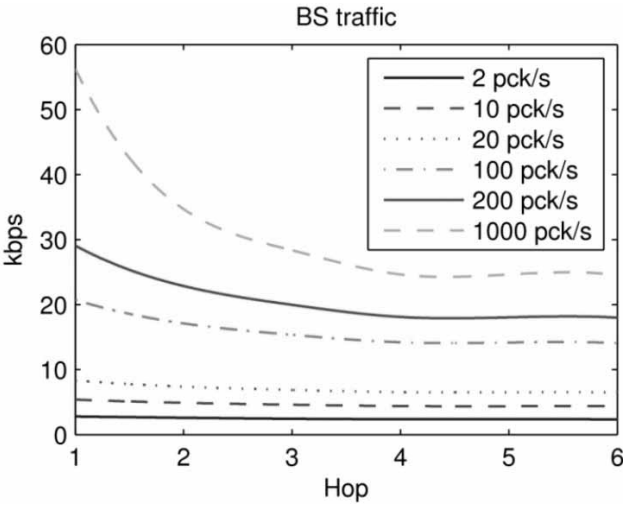


Fig. 9: Multihop saturation.

Packets were generated in the same manner as in the single-hop simulation (via normal distribution with mean value as the inverse number of packets per second, and variation as half of the mean-value) only on the last node in the chain (Fig. 3b.: SPaRCMosquito_6). Other nodes only resent data towards the base-station (Fig. 3b: SPaRCMosquito_0).

From the simulation results (Fig. 5.), it can be seen that the data rate in each hop decreases. Data rate decreasing can be clearly seen with 1000 packets/second where, in the first hop data rate drastically decreased (about 38 %), but at the last hop the decrease is hardly noticeable (2 %).

5. Conclusion

The goal of this simulation was to define the limits for data rate within IEEE 802.15.4 based networks.

IEEE 802.15.4 standards are intended for low power low data rate wireless sensor networks, meaning that sensor nodes only send a few messages per second and the upper data rate limit is never reached. Due to the lack of standardized hardware supporting higher data rates, the IEEE 802.15.4 standardized hardware is often used as PHY layer for higher data rates.

It can be assumed that IEEE 802.15.4 is intended for those networks without hidden nodes which is, in practice, very hard (or often impossible) to achieve. From the simulation point of view the data rate in channel must not exceed 40 kb/s in order to achieve stable and useful communication but, in practice, this data rate falls down to less than 20 kb/s.

Wireless sensor networks based on IEEE 802.15.4 would tend to use the minimum number of hops as possible if the

data rates are high, regardless of the energy efficiency hypothesis which claims that shorter hops provide greater energy-efficiency than a few longer jumps – when using high data rates, energy must be sacrificed at the data rate's expense.

Network traffic should be evenly distributed over the network in order to achieve better throughput and efficiency.

6. Acknowledgement

This work was financial supported by Research programs ARRS, P2-0065 "Telematics`` financed by Slovenian Ministry of Higher Education, Science and Technology.

References

/1/ H. Dai and R. Han, "A node-centric load balancing algorithm for wireless sensor networks." in Proc. of the Global Telecommunications Conference, vol. 1, San Jose, Ca, USA, January 2003, pp. 548–552.

/2/ IEEE 802.15 WPAN Task Group 4. IEEE 802.15.4. standard. /Online/. Available: http://www.ieee802.org/15/pub/TG4.html

/3/ Zigbee alliance. /Online/. Available: http://www.zigbee.org/

/4/ B. Ames, "Electronics are central to 21st century warfare tactics," Military and Aerospace Electronics, 2004.

/5/ A comprehensive simulation study of slotted CSMA/CA for IEEE 802.15.4 wireless sensor networks, 2006. /Online/. Available:http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1704149

/6/ L. Kleinrock, Fouad, and A. Tobagi, "Carrier sense multiple-access modes and their throughput-delay characteristics," IEEE Trans. Comm, vol. 23, pp. 1400–1416, 1983.

/7/ B. Carballido Villaverde, R. De Paz Alberola, Rodolfo. Susan, and P. Dirk, "Experimental Evaluation of Beacon Scheduling Mechanisms for Multihop IEEE," in Proc. of the Fourth International Conference on Sensor Technologies and Applications, vol. 1, August 2010, pp. 229–234.

/8/ R. S, C. J. B, and S. D, "RTS/CTS-induced congestion in ad hoc wireless LANs," in WCNC, vol. 3, March 2003, pp. 1516–1521.

/9/ K. Benkič, "Prometno uravnoteženi usmerjevalni algoritmi za brezži˘cna senzorska omrežja," Ph.D. dissertation, Univerza v Mariboru, Fakulteta za elektrotehniko, ra˘cunalništvo in informatiko, Maribor, Slovenia, 2010.

/10/ K. P, "Maca - a new channel access method for packet radio," in ARRL/CRRL Amateur Radio 9th Computer Networking Conference, vol. ?, Lake Buena Vista, FL, USA, ? 1900, pp. 134–140.

/11/ U. Pešović, "Hidden node avoidance mechanism for IEEE 802.15.4/zigbee wireless sensor networks," Master of Science thesis, Univerza v Mariboru, Fakulteta za elektrotehniko, ra˘cunalništvo in informatiko, Maribor, Slovenia, 2009.

Žarko F. Čučej
University of Maribor, Slovenia
elektronska pošta: zarko.cucej@uni-mb.si

Prispelo: 03.01.2011 *Sprejeto: 23.08.2011*