

Hidden node avoidance mechanism for IEEE 802.15.4 wireless sensor networks

Uroš Pešović¹, Jože Mohorko², Siniša Randić¹, Žarko Čučej²

¹University of Kragujevac, Faculty of Technical Sciences Čačak, Serbia

²University of Maribor, Faculty of Electrical Engineering and Computer Science, Slovenia

Abstract: IEEE 802.15.4 is the standard for short range Wireless Personal Area Networks (WPAN). It is targeted for battery powered applications where a long battery life is the main requirement. Most of the device energy is spent for radio communication, where packet collision, caused due to a hidden node problem, is one of the main sources of unnecessary energy waste. IEEE 802.15.4 standard does not originally provide any protection from hidden node collisions. This paper shows influences of hidden node problem on the overall network performances and presents the RTS/CTS handshake mechanism which can be successfully used to prevent hidden node collisions in IEEE 802.15.4 wireless networks.

Key words: Hidden node, Wireless sensor network, IEEE 802.15.4, MAC, RTS/CTS

Mehanizem izogibanja problema skritega vozlišča v IEEE 802.15.4 brezžičnih senzorskih omrežjih

Povzetek: IEEE 802.15.4 standard, za brezžična osebna omrežja (WPAN), je namenjen za aplikacije s baterijskim napajanjem, kjer je pomembna dolga življenjska doba baterije. Tovrstne naprave porabijo večino energije za radijsko komuniciranje. Eden izmed najpomembnejših vzrokov za nepotrebno porabo energije predstavlja problem skritih vozlišč, zaradi katerega prihaja do trkov paketov. Standard IEEE 802.15.4 originalno ne ponuja mehanizmov zaščite pred trki paketov. V tem članku smo prikazali rezultate analize vpliva problema skritih vozlišč na zmogljivost omrežja ter predstavili RTS/CTS mehanizem rokovanja, ki predstavlja eden izmed uspešnih pristopov preprečevanja trkov paketov, ki nastajajo zaradi skritih vozlišč v IEEE 802.15.4 brezžičnih omrežjih.

Ključne besede: Skrito vozlišče, Brezžično senzorsko omrežje, IEEE 802.15.4, MAC, RTS/CTS

* Corresponding Author's e-mail: uros.pesovic@ftn.kg.ac.rs

1. Introduction

Wireless sensor networks (WSN) consist of a large number of autonomous battery-powered sensor devices, referred as *nodes*. They are capable to measure an environmental event, process and transmit collected data to a central node in network. One of the main goals in the wireless sensor networks design process is to minimize overall power consumption in order to achieve months or even years of autonomy operation with the use of a single set of batteries. WSN power consumption can be reduced through a careful selection of low power devices and by suitable communication protocols, which permit usage of long periods of inactivity to take full advantage of low power modes of the device; known as sleep mode.

Much of the node's energy is used for radio transmission, which needs to be efficient in order to increase service life of sensor nodes. There are several sources of unnecessary energy waste during radio communication such as: idle listening, overhearing, protocol's overhead, packet loss due to collisions, etc [1]. One of the biggest sources of energy waste is packet collision. Packet collision represents situation when two nodes transmit packets at the same time, which results in partial or complete distortion of packet on the recipient node. Collided packets cannot be received and they need to be discarded and retransmitted again.

1.1 Problem formulation

IEEE 802.15.4 standard [2] uses blind backoff CSMA/CA (Carrier Sense Medium Access with Collision Avoid-

ance) channel access mechanism, where device checks the state of the channel before any transmission. If it ensures that channel is free, it can start the transmission; if not it will retry the entire procedure after some time. This approach works fine only when all nodes hear each other, which is a rare case in WSN. In most cases, network's coverage area is much larger than the coverage area of a single node. A well-defined coverage area does not exist for wireless media because propagation characteristics are dynamic and uncertain. In that case, the node is not capable to discover what is happening beyond its receiver radio range and its transmission can lead to occurrence of hidden node collision. Hidden node collision occurs when two nodes A and C (Figure 1.) are communicating with node B, although they are not aware of each other's existence since they are not in radio range. According to papers [3] and [4], the probability that two randomly distributed nodes, in the radio range of central node, cannot hear each other is as high as 41%.

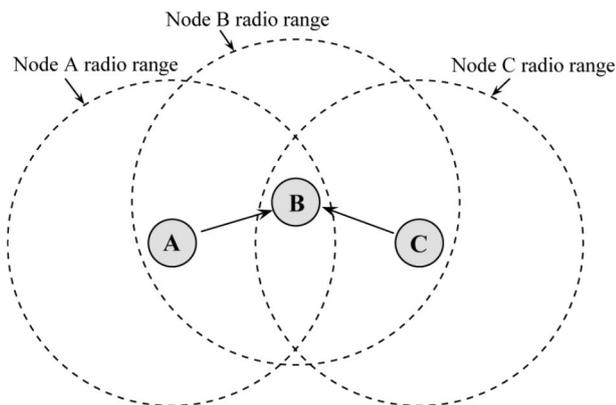


Figure 1: Explanation of hidden node problem

According to CSMA/CA, nodes A and C can start the transmission if they detect an idle channel. Since they cannot hear each other, they can begin the transmission simultaneously, without knowing that they have created packet collision on the node B. In this case, the node B is not able to receive any of the transmitted packets and both packets need to be retransmitted again, which causes unnecessary energy consumption.

IEEE 802.15.4 protocol does not originally provide any protection against the hidden node problem. Since these kinds of networks are designed for the low-rate traffic, occurrence of this phenomenon is rare. Probability of collisions, due to hidden nodes, increases with the increase of network traffic. This kind of scenario is also possible in networks with low-rate traffic, in places that represent traffic bottlenecks, which are usually located near the sink nodes. Occurrence of such events, in some parts of the network, can easily produce a chain reaction, which can affect or even disrupt operation of the entire network.

1.2 Related work

Several solutions to avoid a hidden node problem in WSN have been proposed. Besides the task of elimination of hidden node problem, these solutions need to comply with basic principles of WSN design, hence simplicity and energy efficiency. Solutions for hidden node problem in WSN can be classified into two categories: proactive and reactive approaches. Proactive approaches prevent occurrence of hidden node collision, by use of: busy tone mechanisms [5], carrier sense tuning [6], node grouping [7, 8] or RTS/CTS handshake mechanism [9]. First two approaches are not practical since they require additional hardware radio resources which increase power consumption. Node grouping technique forms network groups in which all devices that participate in one group can hear each other. This solution suffers from frequent group reallocation in networks with mobile nodes. RTS/CTS Handshake mechanism employs channel reservation around transmitter and receiver using RTS/CTS frames. Their uses in IEEE 802.15.4 networks have been proposed in [10], although best to our knowledge, measurements of effectiveness of this solution have not been performed yet. Authors of paper [8] have analyzed a possibility to use RTS/CTS mechanism in WSN networks and have concluded that this method is not particularly suitable for WSN networks. Reactive approaches react only when hidden node collisions happened in order to solve collision chain and to prevent its future occurrence [3].

The main idea behind this research is to analyze the possibility of implementation of RTS/CTS handshake mechanism in IEEE 802.15.4 MAC as a hidden node avoidance mechanism. Since its implementation in IEEE 802.15.4 networks has just been suggested, measurements of its effectiveness are not performed. It is shown that the proposed hidden node avoidance mechanism helps to prevent collisions due to hidden nodes. The main disadvantage of this solution is high packet overhead which increases packet delay and limits channel throughput, which limits its usefulness in IEEE 802.15.4 networks.

2. Influence of hidden node collisions on wireless transmission

In real world communications, modulated signals sent through a channel are received together with some unwanted signals, which are referred to as noise. Noise can be classified into two groups: background noise and interference noise. Background noise is present throughout the whole frequency spectrum. Interference noise represents a noise that is present in limited

parts of the frequency spectrum and which bandwidth overlaps with the bandwidth of the modulated signal. If interfering signal shares the same frequency spectrum, but uses different modulation its influence on the modulated signal can be treated the same as the background noise. If signals, which are interfering, are compliant, signal collision, known as co-channel interference, occurs. When compliant signals interfere, than they cause a collision, and their content may be damaged. If power of interfering signal is lower than the power of the originally received signal, there is a possibility that the original packet is received without any errors. This phenomenon, called capture effect, is in greater detail presented in this paper [11]. The amount of background noise presented in the received signal, is quantitatively represented in a form of Signal-to-Noise Ratio (SNR), which represents the ratio between the power of the received signal P_s and the power of the background noise P_N . Signal-to-Interference Ratio (SIR) represents the ratio between the power of the received signal P_s and the power of the interfering signal P_I . Signal-to-Noise-Interference Ratio (SNIR) represents the ratio between the power of the received signal P_s and the sum of powers of background P_N and interference noise P_I .

Since these two noise sources have a completely different effect on the constellation diagram [12], their real influence on the BER is investigated with the use of MATLAB experiment. Developed simulation model (Figure 2.), consists of the two transmitters and one receiver. Transmitter is composed of the Bernoulli Binary Generator, Symbol-to-Chip mapping block and baseband O-QPSK modulator. Transmitters send a modulated signal, with a normalized power level, through AWGN (Additive White Gaussian Noise) channel, where background noise is added to the modulated signal. Power level of the background noise added to the signal is determined by SNR. Power of the interfering signal is determined by SIR.

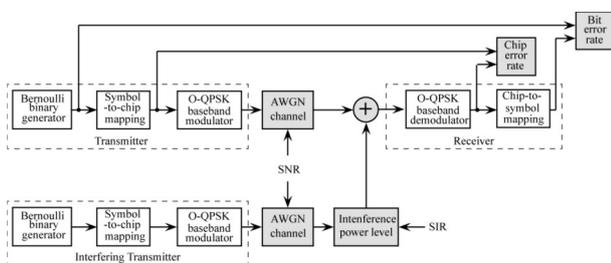


Figure 2: Matlab simulation model

Signals from both transmitters are added at the receiver side, where they are firstly demodulated by the O-QPSK demodulator. Received chip sequence is cross correlated to 16 known chip sequences and the most familiar is chosen as the output binary sequence. The

difference between transmitted and received chip and binary sequences are determined by error rate calculation blocks. In preformed simulations, the SNR and SIR values are changed, which results in changes in power levels of the interfering signal and background noise, relative to power of the modulated signal. Received chip and bit sequences are compared to transmitted sequences in order to determine Chip Error Rate (CER) and Bit Error Rate (BER).

The first part of the simulation is performed under the presence of just background noise without an interfering signal, where SNR changes in range of [+10 dB,-10 dB].

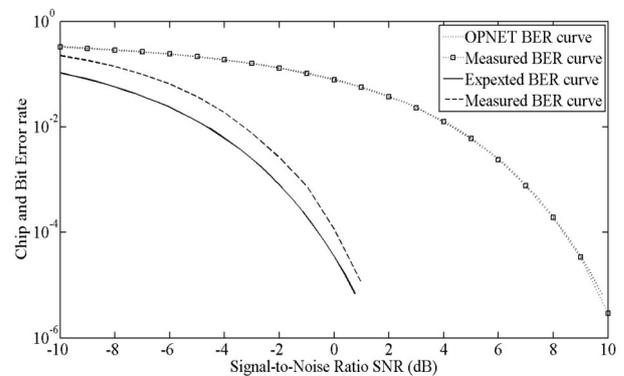


Figure 3: Error probability with just background noise

The results from Figure 3. show that the measured CER is in close match with theoretical results [2]. Results for measured BER curve show due to the use of signal spreading, an existence of the processing gain, although they do not reach the expected theoretical value of 9 dB [2]. This is probably because of use of quasi-orthogonal codes.

In the second part of the simulation collisions are modeled between the modulated and the interfering signal. The power of the interfering signal, relative to the power of the modulated signal is determined through the use of SIR value. Power level of the background noise, relative to the power of the modulated signal is determined by SNR parameter. The received chip and bit sequences are compared to the transmitted sequences in order to determine the Chip Error Rate (CER) and Bit Error Rate (BER). Since CER and BER are functions that depend on two variables, SNR and SIR, several simulations are performed for various fixed values of the SNR while during simulation, the SIR value is changed. These two parameters are transformed into SNIR, which give the ratio between the power of the modulated signal and all noise sources, including background noise and interference noise.

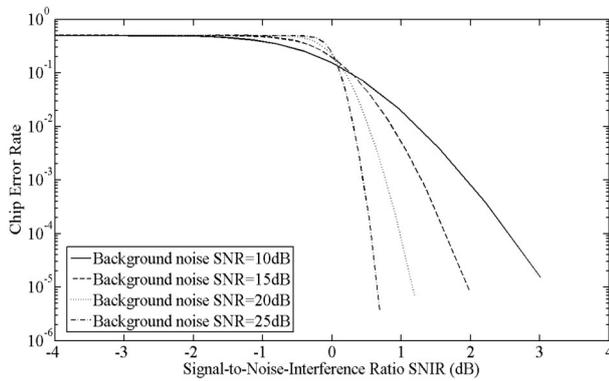


Figure 4: Error probability with both interference and background noise

Results obtained from simulations show significant differences between the effect of the background noise and interfering noise on the CER and BER. This indicates that these two noise sources need to be separated one from another. Based on the MATLAB simulation results, the appropriate model is created, which precisely models effects of these two noise sources on the chip and bit error probability.

3. IEEE 802.15.4 Simulation model

Effects that hidden nodes have on IEEE 802.15.4 WSN are examined by the developed simulation model in OPNET Modeler. The OPNET Modeler represents an environment for modeling, simulation and performance analysis of communication networks, devices and protocols. It is based on discrete event simulation, where simulation is executed as a chronological sequence of events. Each event occurs at an instant in time and marks a change of state in the system. OPNET Modeler provides hierarchical structure to modeling, where each level of the hierarchy describes different aspects of the complete model being simulated. Hierarchical model is composed from three levels: network model, node model and process model.

The starting point for a model presented in this paper is Open-ZB model of IEEE 802.15.4 network, developed by IPP-HURRAY! Group [13]. This model supports only star topology, where communication is established between a single PAN coordinator and arbitrary number of End Devices. Nodes in this model support Beacon Enabled mode with an unlimited radio range of all nodes participating in the network. Original Open-ZB model is modified in order to simulate effects of hidden nodes, and it is an upgraded structure that is presented in Figure 5.

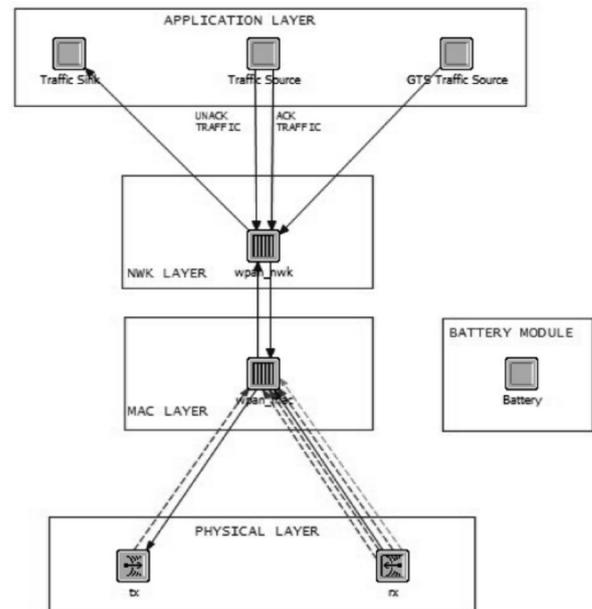


Figure 5: Upgraded OPEN-ZB simulation model

Crucial changes are introduced into the Physical Layer. In order to simulate the hidden node effect, radio range of transceivers needs to be limited. This is enabled through changes introduced in the Link Closure stage of the radio transceiver pipeline. For a given transmit power and path loss between the transmitter and receiver, power of the reception signal is calculated. If the signal power is lower than a receiver's sensitivity threshold, the radio link is not established. Path loss calculation is dependent on the distance between the transmitter and receiver and on terrain model, which is used in simulation. Value of the receiver's sensitivity threshold is chosen to be -85 dBm, according to the IEEE 802.15.4 standard specification. For standard transmit power level of 1mW (0dBm), transceiver radio range, with a free-space propagation model, is around 175m.

Further changes are introduced in Bit Error Rate Stage of the radio transceiver pipeline. Existing BER model used in OPNET network simulation tool is based on the claim that these two noise sources have the same influence on wireless transmission and that they can be treated as one common noise. Previous chapter shows that these noise sources need to be treated independently. If only a background noise is present in the communication channel, the appropriate BER curve from previous chapter is imported in the OPNET in the form of the table of the measured BER values. When both the background noise and the interference noise are present in communication channel, BER stage calculates a value of the bit error rate in accordance to parameters SIR and SNR. Data for such BER curve is imported in the OPNET in the form of a two-dimensional table of

the measured BER values. The obtained results for both cases are fed as output from Bit Error Rate Stage. In the Bit Error Allocation pipeline stage, the number of bit errors in a packet is determined. It is based on the values of the bit error rate and length of the packet in bits. Statistical wires, which connect Physical and Medium access layer, are used to carry values of the received power, SNIR, and bit errors for each packet. These values are used by MAC Layer to distinguish between valid and collided packets.

The MAC Layer is upgraded with Non-Beacon Enabled mode, which is missing in the original model. Now, the MAC layer is capable of operating in two modes, which is determined by the Beacon Order parameter. Implementation of the RTS/CTS Handshake mechanism starts with an introduction of two new types of frames into the MAC layer. Structure of the MAC header and MAC footer is similar to other MAC frames. RTS and CTS frames are distinguished from other frame types with their use of the 3 bit long Frame Type subfield. If data transfer requires acknowledgement of the successful reception, value of the Ack Request subfield is set to 1, both for RTS and CTS frames, in order to inform all other nodes that Acknowledgment frame transmits right after data transmission. MAC payload is composed from two fields: Data length and Power indication field. Data length field is used to provide information about the length of the data frame, which is further transferred. This information is first sent by RTS frame to the recipient, which returns it with CTS frame in order to inform all the hidden nodes about the following data transmission. Power indication field is optional, and it can be used in a process of adjusting the level of transmitting power during data and acknowledgment frame transmission. When a device wants to initiate a transmission sequence it sends information about the current level of the power transmission with RTS frame. When a destination node receives this frame, it calculates path-loss based on the power level of the transmitted and the received signal. It adjusts its transmit power if a packet needs acknowledgment and sends information with CTS frame about the power level, which is low enough that data frame is successfully received. After the reception of the CTS frame message the source node adjusts its power level and starts data transmission.

Channel access mechanism is modified a bit in comparison to the CSMA/CA use in IEEE 802.15.4. When a node wants to transmit, it firstly turns on its radio and listens for the specified amount of time for eventual RTS or CTS frame. If such frame appears, the node goes to low-power sleep until current data transmission is finished. Then it wakes up and listens for a random backoff time, and if none RTS or CTS frames are received, it sends its own RTS frame to destination node. When a desti-

nation receives this frame it immediately replies with CTS frame, after which the data frame is sent by source node. Transmission sequence is finished by sending an optional acknowledgment frame, after which a new contention for medium access can begin.

Additional MAC commands for association are introduced and are used when new nodes join the network. Synchro module, used in the old model, is removed, since its role has been taken by a network layer, which controls the operation of the MAC layer through the use of service primitives. In the newly formed Network Layer, cluster-tree topology is supported. Star topology is implemented as a special case of cluster-tree topology, where network depth is set to the value of one. Mechanism of the network formation is implemented with default distributed address allocation to all nodes, which associate to the newly formed network.

4. Simulation results

Developed model of IEEE 802.15.4 wireless network, is used in simulations to demonstrate the effect of hidden node collisions of network performance. It is also used to analyze benefits of using the proposed RTS/CTS handshake mechanism to avoid hidden node collisions.

4.1 Influence of the hidden nodes on the network performance

Effect that hidden node collisions have on standard IEEE 802.15.4 CSMA/CA is demonstrated through two scenarios, with and without hidden nodes. Simulation scenarios are composed of eight End Devices, equidistant from PAN Coordinator, which create star topology. Medium Access layer operates in the Non-Beacon Enabled mode which uses un-slotted CSMA/CA medium access mechanism. Radio range of each device, under free-space propagation model is set to 175 m. In first simulation scenario, all End Devices that participate in the network can hear each other (distance between maximally separated End Devices is 160 m) and collisions due to the hidden node effect are avoided. In the second scenario, each End Device can hear four of the seven other End devices. This gives 42.9 % probability that each pair of the nodes is hidden from each other, which is close to the theoretical value of 41 % [4]. This scenario represents the near worst-case scenario because radio transmissions of the End Devices are received at PAN coordinator with the same power level, so each collision leads to a complete packet loss.

End Devices generate and transmit the acknowledged data frame whose destination is PAN coordinator. Data

frame has a constant application payload of 400 bits, which are extended with 216 bits of the packet overhead (64 bits added by the network layer, 104 bits added by the medium access layer and 48 bits added by the physical layer) and 88 bits long acknowledgment frame. Frames are generated with inter-arrival time according to Rayleigh probability density function. This distribution is chosen to simulate near-to-equidistant packets inter-arrival time, which simulates behavior of the real wireless sensor network.

In the first experiment, the amount of received application traffic (referred to as goodput) is monitored as a function of the generated application traffic for both simulation scenarios (with and without the hidden nodes). Application traffic represents an amount of application data per time unit (payload of the NWK frame), which is generated or received by a node:

$$\text{AppLoad} = M \lambda L \tag{1}$$

where M represents a number of nodes which generate application traffic, λ represents a number of generated packets in a unit of time (inversely proportional to packet inter-arrival time) and L represents the length of frame's data payload which is, in this case, equal to 400 bits.

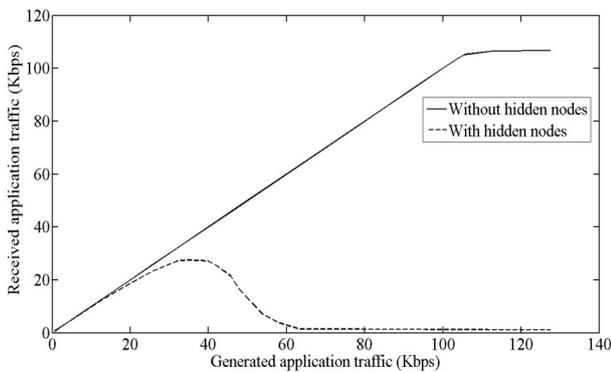


Figure 6: Received goodput as function of the generated application traffic

Presented results show that regular CSMA/CA without a presence of the hidden nodes performs very well, until it reaches its limits because of the channel saturation (Figure 6). In that situation, the amount of generated traffic is larger than what can be physically transmitted through channel; hence the unsent packet can overflow transmission buffers. When a small amount of application traffic is generated in a presence of the hidden nodes, the hidden node collisions are not that frequent and most of the generated application traffic is received. As application traffic increases, a number of collisions increases too, which leads to severe degradation of the network performance, where network goodput is reduced almost four times when compared

with the scenario without hidden nodes. The obtained results are similar to results presented in the paper [14].

One of the consequences of the hidden node problem is the loss of transmitted packets, due to collisions, which destroy their content, so they cannot be received. Ratio of the successful packet delivery is used to express the ratio between a number of the received and number of the generated data frames. Results for the ratio of the successful packet delivery (Figure 7), show that CSMA/CA, without a presence of the hidden stations, has 100% success probability of the delivered packets. When it reaches its channel capacity limit, the number of generated packets is higher than the number of packets which can be transmitted. Packets, which cannot be transmitted, are dropped. In the presence of the hidden nodes, packets are lost for every hidden node collision and as traffic increases so does the number of collisions, which results in a higher number of lost packets.

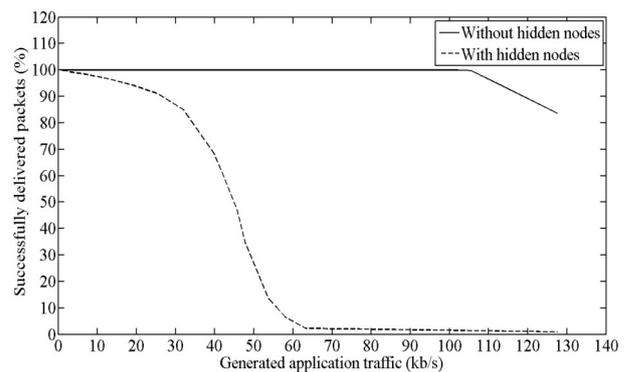


Figure 7: Ratio of the successfully delivered packets

Packet delivery time represents the time, which elapsed from its creation to the time when a packet is successfully received by destination node. This time is often called End-to-End delay. The measured results of the End-to-End Delay, for both scenarios, are presented in the Figure 8.

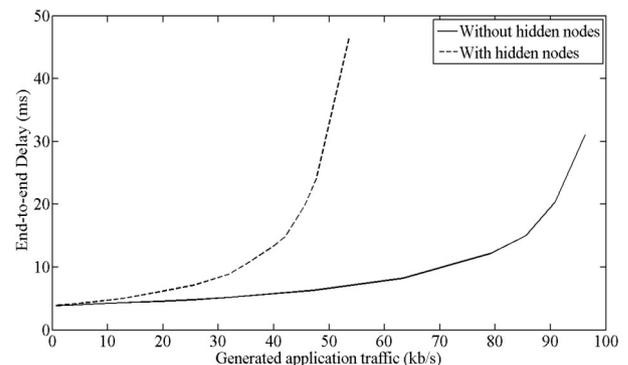


Figure 8: End-to-end delay of the transmitted packets

In regular CSMA/CA without a presence of the hidden stations, Packet delivery time gradually increases, because nodes need to wait until the end of the current transmission, to start their own transmission. As the amount of traffic increases, the average time also increases. In that case the node needs to wait until the channel is free. Packet collisions, caused by the hidden stations, require packet retransmissions, which additionally increases packet delivery time.

In both scenarios, when channel becomes saturated with traffic, packets cannot be transmitted and they are stored in queues or even dropped if the queues are full. This event dramatically increases end-to-end delay.

4.2 Network performances with hidden node avoidance mechanism

Hidden node avoidance mechanism presented in this paper, based on RTS/CTS handshake mechanism, is compared to a standard CSMA/CA medium access in the presence of hidden nodes. RTS/CTS handshake mechanism is added to CSMA/CA MAC, which is originally used in the IEEE 802.15.4. Unit backoff period of the modified medium access mechanism is increased from 20 to 92 symbols (from 80 to 368 bits) in order to accept one complete RTS/CTS sequence. This sequence is composed of one RTS and CTS frame, each 160 bit long, which are separated by a turn-around time, which is 12 symbols (48 bits) long. This modification prevents collisions during a contention phase.

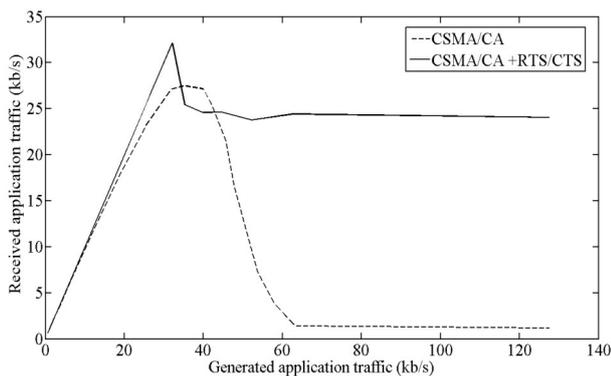


Figure 9: Application goodput with and without RTS/CTS mechanism

In the first experiment, the amount of the received application goodput is monitored, both for regular and CSMA/CA with the hidden node avoidance mechanism. Results presented in Figures 9 and 10 show that the hidden node avoidance mechanism works as expected and that all the hidden node collisions are avoided and that there is not any packet loss. The proposed hidden node problem avoidance mechanism reaches its maximum output, which is three times lower than the

standard CSMA/CA, without an influence of the hidden stations. The main reason for this reduced capacity is in high packet overhead, which increases by RTS and CTS frames, when compared to the standard transmission sequence.

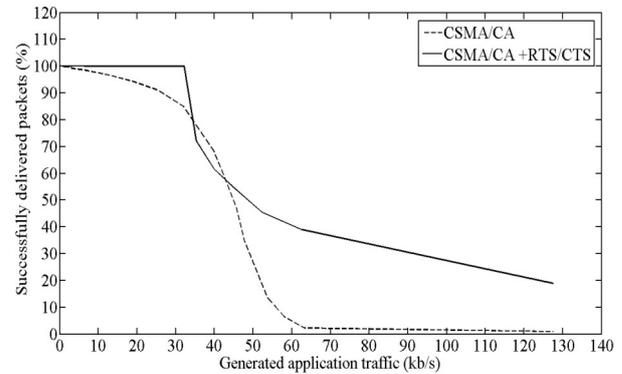


Figure 10: Ratio of the successfully delivered packets with and without RTS/CTS mechanism

In the last experiment, the end-to-end delay of the standard and modified CSMA/CA is compared. The proposed hidden node avoidance mechanism almost has twice the longer end-to-end delay, in comparison to the original CSMA/CA used in the IEEE 802.15.4 (Figure 11). The reason for a longer end-to-end delay is in much longer transmission sequence, which requires transmission of the additional RTS and CTS frames, prior to data transmission. Furthermore, unit of the backoff period increases 4.5 times, which additionally increases the overall packet delay.

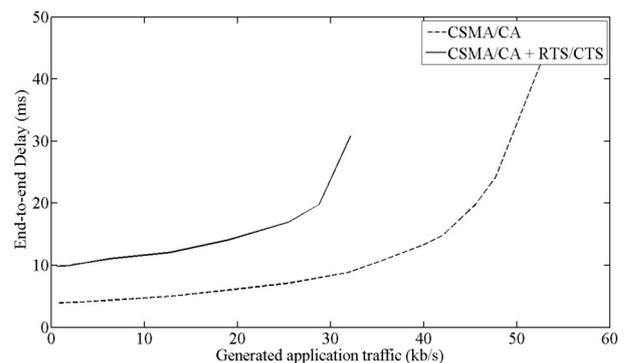


Figure 11: End-to-end delay with and without RTS/CTS mechanism

5. Conclusion

The hidden node problem represents a real threat to any type of wireless communication. This paper presents an effect that hidden node collisions have on IEEE 802.15.4 networks, which originally do not offer any kind of protection against this problem. The results show a severe degradation of the network performance

caused by the hidden node collisions, which drastically reduces useful application's goodput and increases in number of lost packets and packet delivery time. The proposed RTS/CTS handshake mechanism for IEEE 802.15.4 networks enables avoidance of hidden node collisions. Network goodput is increased when compared to standard CSMA/CA, especially in high traffic conditions. Also, packet loss is much lower with the proposed hidden avoidance mechanism, compared to a standard CSMA/CA medium access in presence of hidden nodes. The main drawback of this mechanism is its high packet overhead, which is caused through addition of RTS and CTS frames to data transmission sequence, which increases end-to-end delay. Based on the results, it can be conclude that RTS/CTS handshake mechanism can be used as the hidden node problem avoidance mechanism in the IEEE 802.15.4 wireless networks.

6. References

1. U. Pesovic, A. Peulic, Z. Cucej, "MAC protocols for wireless sensor networks", *Elektrotehnicki vestnik*, Vol. pp.50-55, 2008.
2. IEEE 802.15 Task Group 4, "Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)", 2003.
- [3. S.T. Sheu, Y.Y. Shih W.T. Lee "CSMA/CF Protocol 0for IEEE 802.15.4 WPANs," *IEEE Transactions on vehicular technology*, Vol. 58, 2009.
4. Y.C. Tseng, S.Y. Ni, E.Y. Shih, "Adaptive approaches to relieving broadcast storms in a wireless multi-hop mobile ad hoc network", *IEEE Transactions on Computing*, Vol. 52, No 5, oo. 545-556, 2003.
5. F. Tobagi, L. Kleinrock, "Packet switching in radio channels: Part II-The hidden terminal problem in carrier sense multiple-access and the busy-tone solution *IEEE Transactions on Communications*", Vol. 23, pp. 1417-1433, 1975.
6. J. Deng, B. Liang, P. K. Varshney, "Tuning the carrier sensing range of IEEE 802.11 MAC", *Global Telecommunications Conference*, 2004.
7. L. Hwang, "Grouping strategy for solving hidden node problem in IEEE 802.15.4 LR-WPAN", *Proc. IEEE 1st Int. Conf. Wireless Internet*, 2005.
8. F. A. Tobagi, L. Kleinrock, "Improving Quality-of-Service in Wireless Sensor Networks by Mitigating Hidden-Node Collisions", *IEEE Trans. on Communications*, Vol 5. pp 299 - 313, 2009.
9. V. Bharghavan, A. Demers, S. Shenker, L. Zhang, "MACAW: A Media Access Protocol for Wireless LAN's", *SIGCOMM '94: Proceedings of the conference on Communications architectures, protocols and applications*, 1994.
10. S. Farahani, "ZigBee wireless networks and transceivers", *Newnes publications*, 2008.
11. K. Whitehouse, A. Woo, F. Jiang, J. Polastre, D. Culler, "Exploiting the Capture Effect for Collision Detection and Recovery", *The Second IEEE Workshop on Embedded Networked Sensors*, 2005.
12. U. Pesovic, "Hidden node avoidance mechanism for IEEE 802.15.4/ZIGBEE wireless sensor networks", *Master thesis, University of Maribor*, 2010.
13. "The IEEE 802.15.4 OPNET simulation model: reference guide v2.0.", *IPP-HURRAY Technical Report*, 2007.
14. D. Koscielnik, "Influence of the Hidden Stations and the Exposed Station for the Throughput of the LR-WPAN", *IEEE International Symposium on Industrial Electronics*, 2009.

Arrived: 16. 08. 2012

Accepted: 23. 01. 2013