Effect of hidden nodes in IEEE 802.15.4/ZigBee Wireless Sensor Networks

Uroš Pešović, Jože Mohorko, Karl Benkič, Žarko Čučej

Abstract — **IEEE 802.15.4/ZigBee is the standard for short range, low data rate Wireless Sensor Networks (WSN). It is targeted for battery powered applications where a long battery life is main requirement. Packet collision caused due to hidden node problem is one of the main sources of unnecessary energy waste. Because of a hidden node problem which is not treated by standard our goal was to find its influences on the overall network performances.**

Keywords — **cluster-tree, hidden node, wireless personal area networks.**

I. Introduction

PACKET collision is a situation when two nodes simultaneously start transmission, and their packets will collide at recipient node which wouldn't be able to successfully receive any of these packets. Packets will need to be retransmitted again which would cause unnecessary energy waste. It will be also increased packet delivery time. In wired networks this problem was solved using collision detection mechanism where each node listen the transmission medium while sending the packet. If collision occurs, the transmission is aborted immediately. In wireless networks, transmitter and receiver share much of the radio components including antenna, so node could not use them at the same time. Even if we had separate pair of transmitter and receiver, power of radio transmission, would completely overshadow any received signal, since ratio between power of transmitted and received signal is as much as million to one. Common practice is that node listen the medium before any transmission. After ensures that medium is not occupied by other nodes, it can start radio transmission. This kind of medium access operates smoothly only if node is capable to hear all nodes which participate in network. Since this is the rare case, it is possible that two nodes, which don't hear each other, start simultaneous transmission.

If nodes A, B and C are located in that manner that nodes A and C are so far away that they are unable to hear each other, Figure 1. Node B is located between these nodes and it's capable to communicate with both of them. Simultaneous transmission from nodes A and C will cause packet collision on node B, and these nodes wouldn't be aware of collision they created until the end of the transmission. In this case, the station B wouldn't be able to receive any of the transmitted packets, and both packets need to be retransmitted again, which causes unnecessary energy consumption. According to papers [1] and [2] probability that two randomly distributed nodes in radio range of central node cannot hear each other is high as 41%.

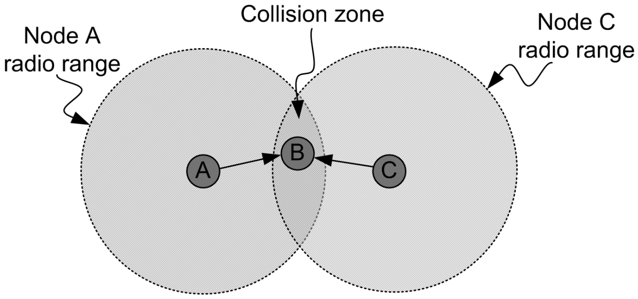

Fig.1 Explanation of hidden node problem

Common practice to avoid this phenomenon is to use the RTS/CTS handshake mechanism, which is used also in the IEEE 802.11 networks. The IEEE 802.15.4 standard [3] originally doesn't provide any mechanism to prevent occurrence of hidden node collisions. Our task, in this research, was to evaluate influence of the hidden node problem on the network performances.

II. IEEE 802.15.4/ZigBee standard

Medium access mechanism used in IEEE 802.15.4 employees *blind backoff* channel access. In this modification, of the classical CSMA/CA, node turns off its radio receiver during random backoff period in order to preserve energy. When the backoff period has expired a device performs *Clear Channel Assessment* (CCA) and if determine that channel is idle, it can begin with message transmission. The End devices, which are usually battery powered, should spend rest of the time with their receiver turned off, while devices such as routers and PAN coordinator keeps their receivers continuously turned on. The End devices use indirect addressing to find out that some data is waiting for them at PAN coordinator. This information is usually sent to them with beacon frames or by acknowledgment frames. Using this technique they don't need to continuously listen the medium thus significant energy savings can be achieved. This approach to the medium access is effective only when amount of traffic in network is relative low, for example only few percents of channel utilization.

U. Pešović is from Technical faculty Čačak, University of Kragujevac, (phone: +38132302721, fax:+38132342101, e-mail: pesovic@yahoo.com) and its PhD student at Faculty of Electrical Engineering and Computer Science, University of Maribor, Slovenia.

J. Mohorko, K. Benkič and Ž. Čučej are from Faculty of Electrical Engineering and Computer Science, University of Maribor, Slovenia (phone: +38622207184, e-mail: mohorko@uni-mb.si, k.benkic@uni-mb.si, zarko.cucej@uni-mb.si).

There are two types of collisions which can occur: contention collision and hidden node collision. The contention collisions occur when two devices simultaneously start a transmission. This kind of collision is much less frequent then the hidden node collision, because of the random backoff algorithm which is used in the CSMA/CA.

Even in low level traffic conditions the hidden node problem can occur but its occurrence wouldn't much degrade network performance; it will just cause energy waste due packet collision and some packets will be delayed. If the network traffic amount increases beyond certain point, the hidden node problem starts serious degrading network performances. Frequent packet collisions will increase the channel utilization, increase message delivery time (end-to-end delay) and some packets can also be lost or dropped from transmission queues. This kind of scenario is also possible in the networks with lower amount of traffic, in places which represents the *traffic bottlenecks*. Occurrence of such events in some parts of the network can easily produce a chain reaction which could affect or even disrupt whole network's performances.

Such kind of scenarios is most possible to happen in cluster-tree networks where PAN coordinator represents a *traffic bottleneck*. In this topology PAN coordinator represent root of the tree which is extended by routers that forms branches in network. All traffic destined from tree branches are directed to the PAN coordinator. This topology is known as hierarchical topology because it is based on parent-child relations. Each router has only one parent and several child nodes. End devices can act only as children and represents network leafs.

The ZigBee standard [4] offers the mechanism, used to allocate unique network addresses to each node, known as the *default distributed address* [5]. When the PAN coordinator establishes network it provide a set of unique addresses to each potential parent which assign these addresses to its children. Parameters used in address allocation mechanism are presented in the Table 1. Depth d represent a minimum number of hops which are needed to send message from device to PAN coordinator which has depth 0, and default address 0.

Table 1. Parameters used for cluster-tree formation

Parameter	***Description***
C_m	Maximum number of children
R_m	Max. num. of routing capable children
L_m	Maximum network depth
d	Depth of device in network

The default address allocation scheme use these parameters to determine child address using $C_{skip}(d)$ function (1).

$$C_{skip}(d) = \begin{cases} 1 + C_m \cdot (L_m - d - 1) & ; R_m = 1 \\ \dfrac{C_m \cdot R_m^{L_m - d - 1} + R_m - C_m - 1}{R_m - 1} & ; R_m > 1 \end{cases} \quad (1)$$

Parent with address A assign address to its routing-capable child R which is equal to integer multiple value of $C_{skip}(d)$.

$$R = A + C_{skip}(d) \cdot i \quad ; \quad i \in [0, R_m - 1] \quad (2)$$

Address of End device E, which cannot be accepted as routing capable child, is assigned by (3)

$$E = A + C_{skip}(d) \cdot R_m + i \quad ; \quad i \in [0, C_m - R_m] \quad (3)$$

When the value of device depth d reaches the limit L_m, the value of $C_{skip}(d)$ function becomes zero for this device, and it cannot accept any additional children.

Besides address allocation, $C_{skip}(d)$ function is also useful when device needs to determine in which direction message should be forwarded, to relay message towards destination. If the device with address A, at depth d needs to forward message, it first checks if the destination device with address D is its descendant, using following relation (4).

$$A < D < A + C_{skip}(d - 1) \quad (4)$$

If a destination device is its descendant device, equation (5) can be used to calculate next hop address N:

$$N = A + 1 + \operatorname{int}\left(\frac{D - A - 1}{C_{skip}(d)} \right) \cdot C_{skip}(d) \quad (5)$$

If address of a destination device is not its descendant device, sends message towards its parent.

III. OPNET SIMULATION MODEL

OPNET Modeler represents environment for modeling, simulation and performance analysis of communication networks, devices and protocols. It's 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 [6]. 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.

Starting point for research work presented in this paper was Open-ZB model of IEEE 802.15.4.network, developed by IPP-HURRAY! Group [7], [8]. This model supports only star topology, where communication is established between single PAN coordinator and arbitrary number of End Devices. The original IEEE 802.15.4 sensor node, in this model, supports Beacon Enabled mode with unlimited radio range of all nodes, which participate in the network.

For our experiment purpose some modifications were introduced to the original model. The upgraded model consist of four protocol stack layers: physical, MAC layer, network layer and application layer. Beside protocol layers model has battery module which is used for computation of consumed energy. Structure can be seen on Figure 2. In order to simulate the hidden node effect, the radio ranges of transceivers need to be limited. This is done by changes introduced in the *link closure* stage of radio transceiver pipeline. In this modification, for a given transmit power and path loss between transmitter and receiver, the reception power of signal is calculated. If the signal power is lower than receiver's sensitivity threshold, a radio link would not be established. Additional statistical wires were introduced in the new model, which carry values of a received power and Bit Error Rate (BER). These values are used by a MAC Layer to distinguish between valid and collided packets.

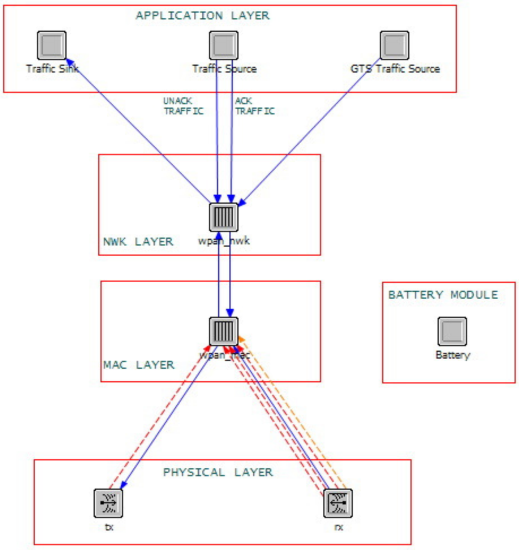

Figure 2. Upgraded OPEN-ZB simulation model

In the MAC layer we built missing Non-Beacon mode which uses un-slotted CSMA/CA mechanism. Also MAC commands for association/disassociation were introduced. In this newly model we built also new network layer, which support cluster-tree network topology. There the mechanism of network formation and routing algorithm is implemented.

IV. Simulation Results

Original network was composed from PAN Coordinator and 21 End Devices, which forming the cluster-tree network. There was also Analyzer node which used to capture all network traffic. Network was spanned in 1km x 1km area with radio range of single device of approximately 175m. Signal propagation between nodes is modeled by the free-space propagation model. Network was operated in Non-Beacon mode. The topology of self formed network is presented on figure 3. Network formation was performed according to cluster-tree formation parameters from table 2.

Table 1. Parameters used in simulation

Parameter	*Description*
C_m	3
R_m	3
L_m	3

In our simulation, traffic was generated by statistical modeled application traffic generators, where constant statistic was chosen for packet sizes and uniform for packet inter-arrival times. The destination of all application traffic was PAN coordinator. The overall traffic load *TL* is generated according to formula (6).

$$TL = M \cdot \lambda \cdot L \qquad (6)$$

There *M* is number of traffic sources (in our case 21 nodes that generate traffic), λ is number of packets in unit of time (inverse proportional to packet inter-arrival time which was ranged from 0.15s to 20s) and *L* is length of data payload (in our case 400 bits). This payload data was encapsulated in the frames which carry additional 216 bits for headers from physical, medium access and network layers.

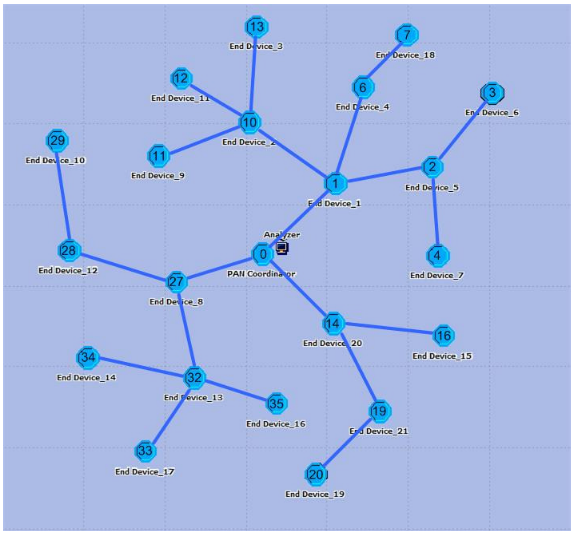

Figure 3. Cluster-tree topology of self formed network

In the first experiment we analyzed network goodput (amount of useful application traffic in bps) which is received by PAN coordinator as a function of traffic load. In same experiment we monitored goodput ratio as ratio between measured and expected goodput. Results are shown on Figure 4.

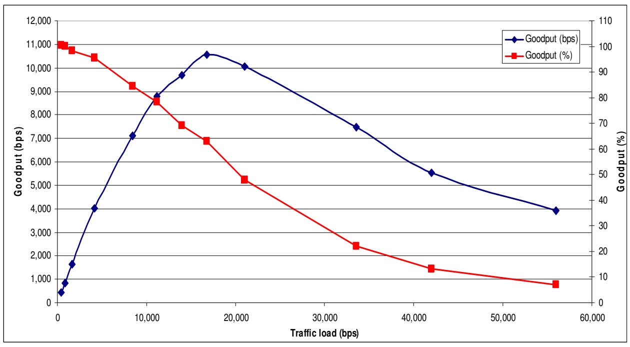

Figure 4. Network goodput

Goodput ratio is continuously declining function, because of increased number of collisions for bigger traffic load. That means that some amount of traffic was lost some were in the network before reaching the PAN coordinator. The mayor origin of this packet loss is in the collision caused by hidden node problem. Each time when collision happened, nodes starts retransmission, and they will probably cause collision again, because they don't know about existence of other hidden node. After several successive collisions packet is dropped from transmission queue and lost forever. The packet loss will be still grater if we use unacknowledged (broadcast) data transmission.

The maximum goodput which we achieved, for acknowledged data transmission, was 10,500 bps but with loss of 35% of generated packets. Further increase of traffic load congests channel and effective goodput starts to fall. Also the effect of collisions on the packet delivery time (end-to-end delay) is analyzed as shown on the Figure 5. Packet delivery time represents time which passed form packet generation to successful packet delivery to its destination. As collisions happen, packet will need to be retransmitted and its delivery time will be increased.

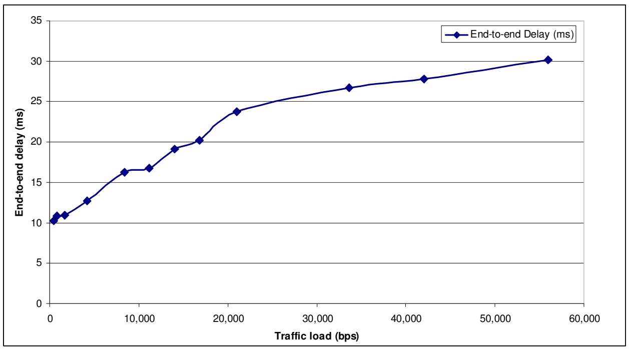

Figure 5. End-to-end delay of received packets

We estimated power consumption of network. This estimation was based on power consumption of MICAz sensor node [9]. Power consumption for various operating modes used with MICAz nodes is presented in table 3.

Table 3. Power consumption of MICAz sensor node

Operating mode	*Power consumption (mW)*
Transmission	52.2
Reception	83.1
Idle	0.105
Sleep	0.048

Based on the measured energy consumption we calculated energy cost per one successfully received bit. Results are shown on Figure 6. As we can see, energy cost is low up to the point, where we reached maximum goodput. After that point, energy cost increasing because a lot of energy was spent on retransmissions and also amount of success received application traffic falls.

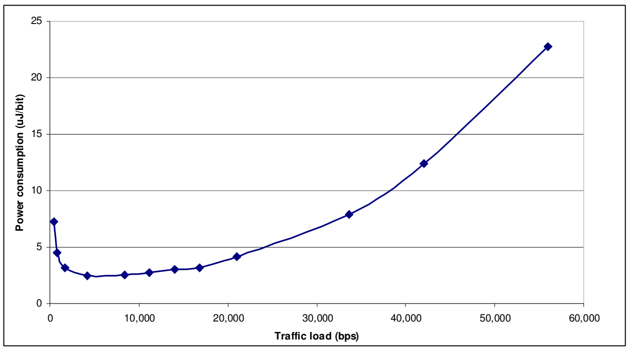

Figure 6. Energy consumption per transferred bit

V. Conclusion

Hidden node problem is one of the biggest unsolved problems in IEEE 802.15.4/ZigBee networks. It degrades network performances and causes unnecessary energy waste. One of the biggest consequences of hidden node problem is in huge packet loss, both for acknowledged and especially for unacknowledged packets, which is not acceptable for most kind of applications.

Our further work will be focused in finding solution for this hidden node problem for IEEE 802.15.4/ZigBee networks, by implementation of RTS/CTS handshake mechanism similarly as in IEEE 802.11 networks.

References

[1] S.T. Sheu, Y.Y. Shih W.T. Lee "CSMA/CF Protocol for IEEE 802.15.4 WPANs," IEEE Transactions on vehicular technology, Vol. 58, No. 3, March 2009.

[2] Y.C. Tseng, S.Y. NI, E.Y. Shih, "Adaptive approaches to relieving broadcast storms in a wireless multihop mobile ad hoc network", IEEE Transactions on Computing, Vol. 52, No 5, oo. 545-556, May 2003.

[3] IEEE 802.15.4 Standard-2006, "Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications *for Low-Rate Wireless Personal Area Networks (LR-WPANs)*" , IEEE-SA Standards Board 2006

[4] ZigBee Alliance, "*ZigBee Specification*", http://www.zigbee.org

[5] S. Farahani, "ZigBee wireless networks and transceivers", ISBN: 978-0-7506-8393-7, Newnes publications 2008

[6] Stewart Robinson, Simulation: The Practice of Model Development and Use, John Wiley & Sons, 2004

[7] "OpenSource Toolset for IEEE 802.15.4 and ZigBee" http://www.open-zb.net/

[8] P.Jurcik, A. Koubaa, "The IEEE 802.15.4 OPNET Simulation Model: Reference Guide v2", Technical report HURRAY-TR-070509

[9] Crossbow, Inc. http://www.xbow.com/