Traffic Prioritisation in 802.15.6 MAC – Analysis of its CSMA/CA Algorithm and Proposals for Improvement

Mara Bukvić and Jelena Mišić, *Senior Member, IEEE*

***Abstract* — This paper focuses on the treatment of uplink traffic of the highest data priority, i.e. Emergency traffic in the 802.15.6 standard for a wireless body area network (WBAN). This standard is one of the choices available for the so-called wearable Internet or wireless connection between electronic devices worn on or implanted in the human body. The features for positive discrimination of emergency traffic are identified at three different components in the 802.15.6 standard in order to emphasize the importance of its prioritized delivery that must be always preserved due to potential applications in the field of monitoring of health variables. However, prioritization could be compromised by the anomaly in the medium access under contention algorithms in standard 802.15.6. That is the reason that we find it appropriate to address the anomaly, i.e. to describe a sequence of packets that can bring a station into the state in which it sends highest-priority data frames with the parameters of the back-off algorithm used for traffic with a significantly lower priority and thus reduces the station's chances to access the medium. The main contribution of this work is to identify the set of five conditions that must be met at the same time in order to make the anomaly to appear, and explain that the scene for anomaly manifestation would be set up periodically in secured communication. We provide a simulation study and discussion on the available solutions for preventing this anomaly including a minor change to the algorithm at the level of the standard.**

***Keywords* — body area network, CSMA/CA, IEEE 802.15.6, QoS, WBAN**

I. Introduction

ALTHOUGH there is a profound progress in connecting things and huge benefits from their internet connectivity in various areas of life, there are areas like wearable internet with significant room for improvement.

There is a wide variety of requirements imposed by the communication between small and portable electronic devices on/inside/in the vicinity of the human body with remote destinations. On the other hand, few candidate standards could be able to fulfil some of these requirements until the standard for the wireless networking of sensors and other devices located in the immediate vicinity of the human body, on the skin or inside it – the so-called 802.15.6 standard, was adopted in 2012 ([1]). It includes the selection of the frequency range and the characteristics of the antennas that have to emit a signal with very low power in order to minimise its specific absorption rate (SAR) in the body, thus increasing the user's safety and at the same time prolonging the device's battery life. Then, to mention some of the most important requirements, there are needs for relatively fast connectivity, whether it includes quality of service (QoS) or not. Also, the communication at a speed of up to 10Mbps could be secured through authentication with or without traffic encryption.

The standard IEEE 802.15.6 is designed for a wide range of applications [2], many of which are related to Health Care Services, medical monitoring, physical rehabilitation, physiological status monitoring, and assistance to people with special needs (visual impairment, speech problems, etc.). Also, the use of this standard for entertainment has also been recognized. Bearing in mind the various requirements of this wide range of applications, from life-critical to non-life-critical, from low-duty cycle and low data rate to high data rate multimedia applications, the QoS functionality is necessary and has been given an important place.

Mechanisms to achieve QoS in a wireless body area network (WBAN) with 802.15.6 include backoff window, period between frame transmissions and transmission duration that have been already proposed in other protocols [3]. The attention paid to QoS in the WBAN standard is significant and is best illustrated through a brief comparison between the short-range wireless protocols WLAN 802.11 and WPAN 802.15.4. ([4], [5]). Reference [6] provides a short overview of the traffic differentiation in IEEE 802.15.6, 802.11 and 802.15.4 standards, and draws parallels with respect to medium access control (MAC) mechanisms – contention and contention-free.

This paper focuses on the treatment of uplink traffic of the highest data priority, so-called Emergency traffic. In order to recognize the problem, it is important to understand features built in IEEE 802.15.6 standard for

Paper received April 4, 2015; revised Jun 9, 2015; accepted Jun 11, 2015. Date of publication July 15, 2015. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Grozdan Petrović.

This paper is a revised and expanded version of the paper presented at the 22th Telecommunications Forum TELFOR 2014.

Mara Bukvić, Network Engineer, is with the University of Belgrade Computer Centre, Kumanovska 7, 126119 Belgrade, Serbia (phone: 381-11-3031-257; e-mail: mara@rcub.bg.ac.rs).

Dr. Jelena Mišić, Professor, is with the Department of Computer Science Rm. Eng-261, George Vari Engineering and Computing Centre, Ryerson University, 245 Church Street, Toronto, Ontario, Canada, M5B 2K3 (phone: 416-979-5000 ext. 7404; fax: 416-979-5064, e-mail: jmisic@scs.ryerson.ca).

doi:10.5937/telfor1501008B

positive differentiation of Emergency traffic. Such features could be found in three elements of the standard.

The first type of traffic differentiation addresses the type of application that is supported by particular WBAN implementation. All of the applications are categorised into four groups of BAN services with different priorities. The lowest priority is given to non-medical services. The highest priority is given to medical services that detect and act upon emergency and medical implant event reports. i.e., Emergency traffic. The group of services supported by WBAN can be identified in MAC frames.

The second type of traffic differentiations could be recognized in superframe structure. The devices are organized in a star topology with one central controller (hub) that coordinates the activities of stations (nodes) and power consumption over time. The time is divided into superframes. A superframe starts with a management frame or the so-called beacon frame. The beacon frame is used to describe the structure of the superframe, i.e. the sequence of time intervals during which different medium access control mechanisms (such as, contention and contention-free) are required. The 802.15.6 standard is characterised by the possibility of having several phases (time intervals) within one superframe limited by a beacon interval, during which a succession of contention or contention-free services is ensured, as shown in Fig. 1. Each of these phases can be set to zero. The contention service is ensured in the EAP (exclusive access phase), RAP (random access phase), and CAP (contention access phase), while the contention-free mechanism is present in the managed access phases (MAP).

The contention between the controller and the stations for accessing a channel when their traffic is of the highest priority is isolated in a separate medium access control phase, i.e. EAP phase.

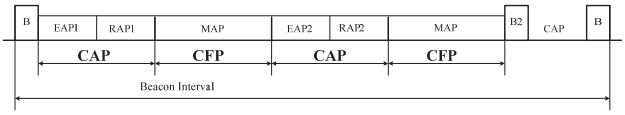


Fig. 1. The superframe structure in 802.15.6 protocols.

Finally, the most obvious type of traffic differentiation addresses prioritized access for traffic of different user priorities (UPs) can be achieved using, either Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) backoff algorithm or the slotted Aloha algorithm. Although the performance of Emergency data delivery could be affected by the anomaly in the medium access under both contention algorithms in standard 802.15.6, in this work we look into CSMA/CA access.

In terms of the treatment of prioritised traffic in CSMA/CA backoff algorithm, the 802.15.6 protocol is the most similar to IEEE 802.11 standard [4]. The MAC from IEEE 802.11 maps the UP into medium access categories (AC). The medium access for each category is controlled through a set of parameters: contention window size (CW) which doubles after every unsuccessful access attempt (defined by range CWmin, CWmax), inter frame space (AIF) and transmission opportunity limit (TXOP), i.e. the time interval during which the station is allowed to initiate transmission. The traffic differentiation in IEEE 802.11 is achieved by varying the following parameters depending on the UP value: a) the time interval during which the station listens to the medium before deciding whether it will enter the back-off procedure or frame sending (AIF), b) the value of the CW parameter in the back-off procedure, and c) the duration of the time interval during which the station can send the traffic after it has acquired the right to use the channel (TXOP).

A notable difference between contention access protocol in IEEE 802.15.6 and 802.11 standards is that the virtual collision between the AC access categories in IEEE 802.15.6 is not possible at the station itself, while this was allowed in 802.11. As a result the back-off algorithm in 802.15.16 is not initiated simultaneously for several packets of varying priority, but only for the highest priority packet regardless of the time of its arrival. Besides, the traffic differentiation in 802.15.6 is achieved by varying the value of contention window parameter in the back-off procedure (between CWmin and CWmax) and the duration of the time interval during which the station can send the traffic after it has acquired the channel. In 802.15.6, the time interval during which the station listens to the medium has a fixed value (SIFS) and does not depend on the user priority of the frame. All these differences come from the fact that IEEE 802.15.6 nodes are energy and computationally more limited than IEEE 802.11 nodes and require simplicity in contention procedure. However, these differences call for new modelling efforts for IEEE 802.15.6 since existing IEEE 802.11 models are not applicable.

Research studies about performance evaluation of IEEE 802.15.6 are still scarce. Anomalies of IEEE 802.15.6 standard have been addressed in [6] and [7], while more research is still needed due to the complexity of the standard.

This paper is organised as follows. In Section II, we give a brief overview of the treatment of different priority traffic in the CSMA/CA algorithm of the IEEE 802.15.6 protocol specifications. Section III describes a potential anomaly occurring when sending packets with a different priority in the phase of contention for accessing the medium. Section IV further explains in more details the set of conditions necessary for the anomaly manifestation and describes in more detail the available solution to avoid this anomaly. In Section V, we offer a simulation study of the effect of anomaly and propose a solution to delivery of Emergency traffic.

II. Description of the CSMA/CA Algorithm in IEEE 802.15.6

As shown in Fig. 1., during EAP (exclusive access phase), RAP (random access phase) and CAP (contention access phase), the station can only get an opportunity to send data through contention, i.e. only when it wins a contended allocation; the access method is either CSMA/CA or slotted Aloha, depending on the frequency band.

The anomaly in the medium access control and its impact on the delivery of traffic with a different priority are explained by using the CSMA/CA method as an

example, which extends by analogy to slotted Aloha. There is a difference in the mapping of UP with predefined values of the algorithm parameters. In the case of CSMA/CA, the parameters used for the lower and upper CW limits are CWmin and CWmax (see Table 1), while the slotted Aloha method uses CPmin and CPmax values for contention probability (CP) thresholds.

Each station (node) stores the values of the following two parameters: the back-off counter (BC) and the contention window (CW).

Each packet of the UP priority can start competing for access to the medium whenever BC=0, by setting BC to a randomly selected whole number uniformly distributed within the range [1, CW].

The CW value is determined in the following way:

- CW = CWmin[UP], if the station has never had an opportunity to transmit, and also when it has completed its last frame transmission with success i.e. it has requested and received the acknowledgement (Ack) in the last contented allocation (Node Succeeded).
- The CW remains unchanged if the station has not requested acknowledgement for the last frame sent at the end of the last contended allocation, and if the station has failed to complete the transmission, i.e. when it has requested acknowledgement of the successful receipt of the last transmitted frame during the contended allocation and has not received such an acknowledgement (Node Fail) in m number of consecutive attempts, where m is an odd number.
- CW= 2*CW, if the station has failed to complete the transmission in n number of consecutive attempts, where n is an even number.
- CW=CWmax[UP], if the CW value, obtained by doubling the CW, exceeds CWmax [UP].

TABLE 1: USER PRIORITIES.

UP	***Traffic designation***	FT	CSMA/CA	
			CWmin	CWmax
0	Background (BK)	D	16	64
1	Best effort (BE)	D	16	32
2	Excellent effort (EE)	D	8	32
3	Video (VI)	D	8	16
4	Voice (VO)	D	4	16
5	Medical data	D/M	4	8
6	High-priority medical data	D/M	2	8
7	Emergency	D	1	4

*) FT: Frame Type - D: Data; M: Management

BC indicates the number of slots of a fixed duration, the so-called CSMA slots, during which the medium is supposed to be idle so that the station would get an opportunity to transmit (i.e. the contended allocation), by counting down to zero. The back-off counter is initialized at zero, and once decremented it resets to the new value and locks. The station can only count down free slots when the back-off counter is unlocked. The station can unlock the back-off counter if both of the following conditions are met: the medium is available for no less than SIFS in the RAP or CAP phases where UP<7, or in the EAP, RAP or CAP phases where UP=7, and the time interval from the start of the CSMA slot to the end of the EAP, RAP or CAP phase is sufficient for completing the frame transmission.

The station must lock the back-off counter in the following cases: if the BC value is set to a new value after it has previously reached zero; if the medium is busy; if the RAP or CAP time phases are not active where UP<7, or the EAP, RAP or CAP phases where UP=7; if the time interval from the start to the end of the EAP, RAP or CAP phase is insufficient for completing the frame transmission.

At the end of an idle CSMA slot in which the BC is decremented to zero, the station gets the opportunity to transmit a frame of UP priority. As long as the station receives the message that the frame has been successfully transmitted, it can continue sending, within the current allocation, frames of the same or higher priority than the one that won the right to access the medium. When the transmission fails, the station loses the contended allocation.

Once it has a contended allocation, the station can send up to two frames where UP<=5, or up to four frames where UP>=6.

III. ANOMALIES IN THE MEDIUM ACCESS CONTROL AND THEIR IMPACT ON THE DELIVERY OF THE HIGHEST PRIORITY TRAFFIC

In analysing the characteristics of the 802.15.6 CSMA/CA method of accessing medium in the OPNET simulation model, we have observed that a certain packet sequence may cause the station to transmit the highest priority (emergency) frames using the back-off algorithm parameters envisaged for traffic of much lower priority. This decreases the station's chances to access the medium with the highest priority packet. According to the published results of the simulation and analytical model [8], in congested environments the stations that do not transmit with the highest priority may starve.

Fig. 2 shows the conditions in which this anomaly occurs. It occurs when a station competing for the medium with a UP<7 frame (UP=3 is used in the example shown in the image) gets a contended allocation after one or more unsuccessful attempts, which increases its CW under the given algorithm with each even number of unsuccessful attempts to access the medium. Once it has obtained the right to transmit, after it executed the F1 transaction in this example, the station keeps the medium and it has the right to perform, without further competition, another transaction (F2) involving a frame of the same or higher priority. If the station does not seek acknowledgment of receipt for the frame in F2, the CW remains unchanged at the end of the current contended allocation. Thus, each subsequent frame for which no acknowledgment is requested, even if it is a frame of the highest UP, can enter the competition for the medium with a CW value several

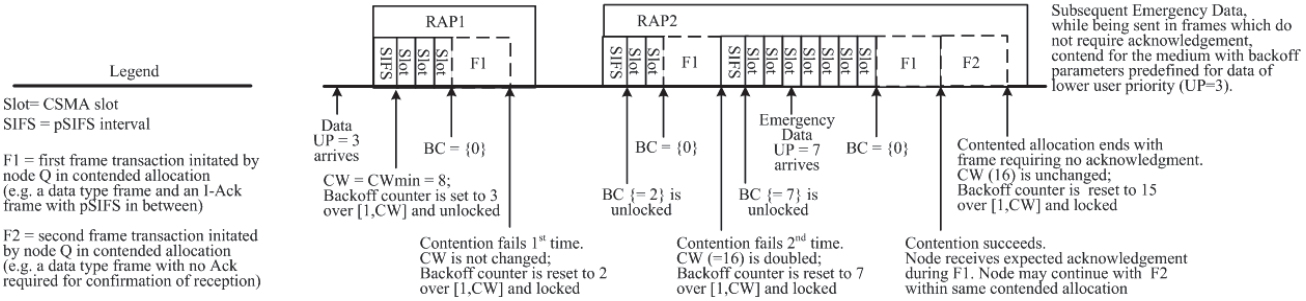


Fig. 2. Conditions in an anomaly may occur in the functioning of 802.15.6 CSMA/CA.

TABLE 2: THE COMBINATION (STATUS SINCE THE LAST TRANSACTION, CONSECUTIVE FRAMES OF VARIOUS USER PRIORITIES) INDICATIVE OF AN ANOMALY.

	CW^{old}		$CW_{current}$	CW^{new}		Status of last frame TX in contended allocation		
	min	max		min	max	Success (Req. Ack)	Failed (Req. Ack)	No Ack Req.
$UP_{old} = UP_{new}$						CW^{new}_{min}	$CW^{new}_{min} = CW^{old}_{min}$	$CW^{new}_{min} = CW^{old}_{min}$ $CW^{new}_{max} = CW^{old}_{max}$
$UP_{old} < UP_{new}$						CW^{new}_{min}		$CW_{current} > CW_{max}$
3 7	8	16	16	1	4		Exception – retry number odd (A)	Anomaly (B)
0 3	16	64	32	8	16			
$UP_{old} > UP_{new}$						CW^{new}_{min}	Algorithm will continue backoff procedure with old frames, ie. enter the retransmission	
5 0	4	8	8	16	64			
3 0	8	16	8	16	64			

times higher than CWmax for the given UP, which prolongs the delay in the delivery of packets.

This explanation is supplemented by the analysis provided in Table 2. The station enters the competition for the medium with a frame whose priority equals 3.

This means that if the station has the opportunity to send a frame with priority UP=3, its CWcurrent will be at least 8, and after two failed attempts to send the packet CWcurrent=16. If during the back-off procedure, the station prepares several frames of the highest priority (UP=7) for transmission, it will be able to send one frame of the highest priority during the same contended allocation. The transmission of the next frame of the highest priority will not be allowed during the current allocation. It will be necessary for the station to compete in order to transmit that frame. What is important here is the parameters with which the competition is entered, i.e. the CWcurrent over which the value of the back-off counter is uniformly distributed. If no acknowledgment (no Ack) is requested for the highest-priority frame, the CW value remains unchanged. The anomaly is reflected in the fact that the value of CW in the given conditions is at least two times higher than the maximum value envisaged for the highest-priority frames (CWmax=4).

As long as the station is transmitting frames without requesting acknowledgment, it will compete for the medium with lower-priority traffic characteristics, which decreases its chances of accessing the medium during the contention phases.

The management frames of UP=5 or UP=6 priorities are not susceptible to this anomaly because they have to request acknowledgment according to the protocol, so the result at the end of the current contended allocation can either be success or failure. In Table 2, the success and fail columns show the results of the last transaction within the contended allocation, while the corresponding CW values are presented in the relevant fields. Field B shows that the anomaly affects the frames that do not include acknowledgment of receipt. Field A shows that, according to the algorithm, the doubled CW values of the frames that include acknowledgement will be reduced to CWmax [UPnew] upon each even number of unsuccessful outcomes.

IV. AVAILABLE SOLUTIONS AGAINST ANOMALY

The anomaly can be observed only if all of the following five conditions are met:

1. the option of sending more than one frame within the same contention based allocation takes place. The protocol allows the station to send up to four frames of priority 6 or 7, or two frames for all priorities less than 6 within the same allocation.

2. the frame that won the contention and the frame that ends the allocation are of different priorities. The protocol states that the station can continue sending, within current allocation, frames of the same or higher priority than UP of the frame that won the contented allocation.

3. the frame with Ack. Request won the allocation, but the allocation ended with the unacknowledged frame.

4. the node had run backoff procedure in a few consecutive attempts and has failed to complete the transmission, such that before the frame finally won the allocation that current CW value has been increased significantly over the maximum value of the next frame

that is sent with unAck reqest. The protocol stated that upon transmission of unAck frame, the CW remains the same at the next run of backoff procedure.

5. New backoff procedure is initiated by a frame with priority higher than the priority of the frame that had won previous backoff procedure and all subsequent frames are sent without Ack request as well.

The potential and realistic scenario with all these conditions fulfilled can be described as follows: Once the station is associated with the hub (i.e it is connected and holds an assigned Connected_NID), it could arrange scheduled access to medium, desired wakeup period or secured communication. Occasionally, nodes need to update some parameters of their connection to the hub. This also applies to a node that sends most emergent information toward the hub, as it can be expected that such communication be secured by usage of Pairwise Temporal Key (PTK). PTK shall be retired no later than the limited number of frames secured by it in a sequence has been reached. Once one of parties starts using a new PTK, both parties shall no longer use any old PTK. Therefore, the node must notify the hub about PTK retirement by running a PTK creation procedure to generate a new PTK. In other words, a node periodically initiates new negotiation with the hub that starts with a Connection Request frame. A Connection Request may be of priority five or six (as management frame class). This is lower than the high possible priority of Emergency frames. In addition, all management frames must be sent with ACK required, while Emergency frames do not require acknowledgements. If an Emergency frame is indeed sent without requiring the acknowledgement, the conditions for anomaly appearance have been achieved periodically. Therefore, the remedy for the anomaly, in the first place, will be to send Emergency frames with the Ack request.

This anomaly is not only related to secure communications but also to other scenarios. When nodes need to update any parameters of their connection to the hub, e.g. arrange a scheduled allocation during the MAP phase, new arrangements are negotiated through exchange of sequence of management frames. For simplicity in our simulation analysis we considered unsecured communication.

By sending Emergency frames with Ack Request, the third condition from the list is prevented to fulfil and consequently the anomaly to appear. Further the anomaly would not appear if any of the conditions from the list could be prevented. For example, it could not appear when a node transmits just one frame in a contention based allocation. The occurrence of anomaly is related to all combinations of frames of different priorities. Although we can question the reality of scenario that the same node marks the data with user priority for Video and Emergency, this can be used as a basis for launching denial of service attack. However, under normal conditions, the anomaly cannot occur if a node transmits frames of the same priorities in a contention based allocation. As the modification of the standard which could eliminate the first and second conditions from the list would require major change of the access algorithm, we do not consider it in this work.

Therefore, for our further analysis two possible solutions and their impact on the protocol performance are considered. The first solution would be to ensure that all the Emergency frames are transmitted together with the request for acknowledgment (Ack) and thus prevent fulfilment of the third and fifth conditions from the list. If one intends to send unacknowledged Emergency frames or provide a solution for all cases of different user priorities, in order to escape anomaly it is necessary to make a change to the algorithm at the level of the standard, so that the check whether CW exceeds CWmax[UP] is performed upon the entry of the UP packet in the medium access contention procedure, rather than only upon doubling the CW value. In simulation studies we examined the effect of this minor change to the algorithm on its performance. We provide a discussion of the basic results in the next chapter.

V. Simulation Study for Evaluation the Impact of Anomaly and Proposed Solutions

In this section, we focus on two experiments that demonstrate the impact of anomaly on the node. We develop simulation models for the WBAN CSMA/CA access protocols using the OPNET network simulator.

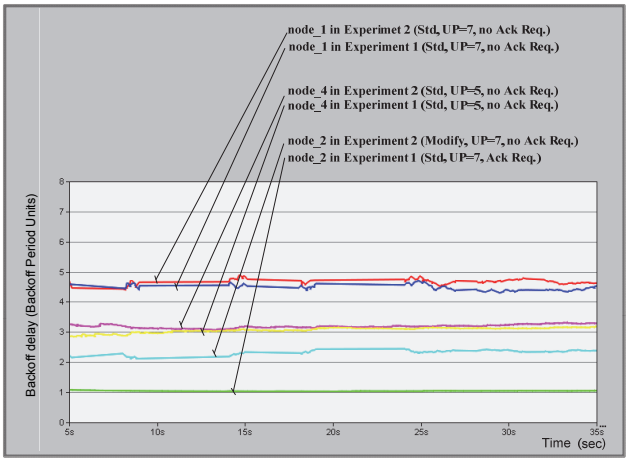
In our analysis, we used simulation parameters as shown in Table 3. As we must be able to identify the impact of anomaly that is manifested at MAC layer, we do not accurately match a real condition on Physical layer, like impact of BER or channel fading. Hence, retransmissions are only a consequence of collisions on the medium and we are able to test our hypothesis in the condition of heavy network load.

Table 3: Simulation Parameters.

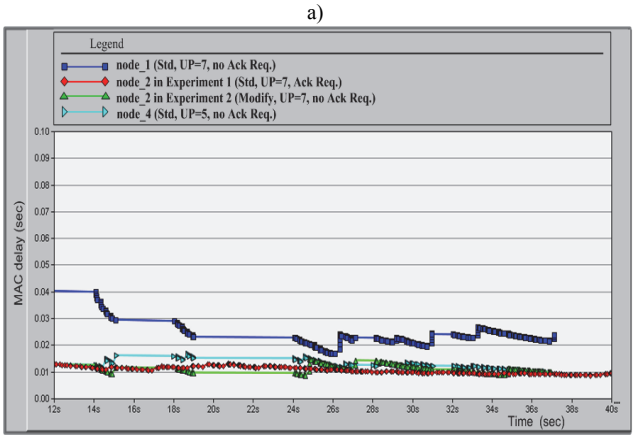
WBAN parameters		
Frequency band	2360-2500 MHz	
Data transmission rate	485.7 Kbps	
Length of phases enabled in beacon enabled mode	EAP1: 20 msec RAP1: 96 msec MAP1: 140msec	
Traffic pattern of four Observed Nodes	node_x, (x=1,2,4)	node_3
Constant payload size	100	200
Data Stream of frames UP=7 (no Ack Req.)		
mean data rate	5.5Kb/s	5.5Kb/s
inter-arrival times	Uniformly distributed	
Data stream of frames UP≠7 with Ack Req.		
mean data rate	10Kb/s	10Kb/s
inter-arrival times	Poisson	
Traffic pattern of three Background Nodes	Min	max
mean data rate	1Kb/s	10Kb/s

The WBAN network consists of a hub and seven nodes. Nodes are considered connected to WBAN, i.e. the phase of association the node to BAN has been completed. We decide to enable a node with feasibility to associate user priority to two, each independent of another, data streams, instead to model the management frames for (re)negotiate the parameters of communication with the hub in

connection setup procedure. One data stream is to generate frames with Ack. request and the other is to generate frames without requesting an acknowledgement. These data streams are switched alternatively and randomly. All traffic in the network is uplink traffic.



a)



b)

Fig. 3 Two solutions, one sending frames with acknowledgement request, the other implementing minor changes on algorithm are considered. Their impact on node behavior with and without manifested anomaly compared to the node which transmits with lower priority traffic are measured in terms of: a) mean backoff time, b) access delay.

In experiments, we tracked two target nodes that generate Emergency traffic in a stream of highest priority frames. One node, namely node_1, implemented CSMA/CA algorithm from the standard, and the other one implemented proposed solutions (node_2). We expected that anomaly would be manifested in the behaviour of a target node in a way that its performance would approach the performance of nodes with a lower user priority. Thus, the performance of node_4 has been included in the graphs for comparison.

The first experiment focuses on a solution that recommends sending Emergency traffic in frames with Ack enabled. The node_0 sends frames with UP=7 requesting no Ack, while node_1 follows the recommendation. Nodes are observed starting at the point at which the current value of CW is set to CWmax of frames with UP=5, and continue to send frames according to the algorithm from standards. In the second experiment, the same pattern is repeated, but this time node_1 used a modified algorithm to send a frame with noAck request. Results from those experiments have been jointly shown on the same graphs for each observed network performance. Network performance is measured in terms of backoff units and medium assess delay (MAC Delay).

Fig. 3.a. shows the mean number of backoff slots encountered in the observed nodes node_0, node_1 and node_4 on a time scale. The solution based on sending frames with Ack request enabled shows the best results (~1), because each successful transmission will reset CW to CWmin. Solution based on a modified algorithm will decrease CW for unacknowledged frames, but CW will remain on its maximum value for frames with UP=7.

The mean number of backoff slots affects the mean back-off time. However, the back-off time is not necessarily continuous because the station has the opportunity to decrement the value of the back-off counter for each available CSMA slot only when the back-off counter is unlocked. We also measured the mean medium access delay (MAC Delay) computed as the interval from the time the packet was inserted into the transmission queue until the time the packet was sent to the physical layer for the first time. Fig. 3.b shows the results from two experiments on a time scale. Sending the frame with Ack request will preserve the mean MAC Delay value.

VI. Conclusion

In this paper, we define the set of five conditions that must be simultaneously fulfilled for the anomaly to appear in CSMA/CA of IEEE 802.15.6. Two possible solutions and their impact on the protocol performance are considered. The initial simulation study provides the results under a heavy network load. This work will continue in the form of preparing a more accurate simulation model in order to gain a more detailed insight into the abilities of the 802.15.6 standard in terms of delivery of Emergency traffic in WBAN under a light network load.

References

[1] IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks, IEEE Std 802.15.6, 2012.

[2] A. W. Astrin, H.-B Li, and R. Kohno, "Standardization for Body Area Networks," *IEICE Trans. Commun*. E92-B(2): 366–372, Feb. 2009.

[3] Reddy, T. Bheemarjuna, I. Karthigeyan, B. S. Manoj, and C. Murthy., "Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions," *Ad Hoc Networks 4*, no. 1: 83-124, 2006.

[4] IEEE Standard for Local and metropolitan area networks—Specific requirements Part 11, IEEE Standard 802.11, 2007.

[5] IEEE Standard for Local and metropolitan area networks - Part 15.4, IEEE Standard 802.15.4, 2006.

[6] M. Bukvic, and J. Misic, "Traffic Prioritisation in 802.15.6 MAC – Similarities and Differences with 802.11 and 802.15.4," (In Serbian), Proceedings of *Telfor Conference*, November 2014, pp 135 – 138.

[7] M. Bukvic, and J. Misic, "Access Anomaly of Emergency Traffic in CSMA/CA of IEEE 802.15.6," accepted to be presented at *Conference IWCMC 2015*, August 2015.

[8] S. Rashwand, J. Misic and H. Khazaei, "Performance Analysis of IEEE 802.15.6 Under Saturation Condition and Error-Prone Channel," *Proceedings of IEEE Networking Conference WCNC'11*, March 2011, pp. 1167 – 1172.