



**HAL**  
open science

## Wireless networked control system using ZigBee/IEEE 802.15.4

Najet Boughanmi, Ye-Qiong Song, Eric Rondeau

► **To cite this version:**

Najet Boughanmi, Ye-Qiong Song, Eric Rondeau. Wireless networked control system using ZigBee/IEEE 802.15.4. 13th IFAC Symposium on Information Control Problems in Manufacturing, INCOM'2009, Jun 2009, Moscou, Russia. pp.CDROM. inria-00430974

**HAL Id: inria-00430974**

**<https://inria.hal.science/inria-00430974v1>**

Submitted on 10 Nov 2009

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Wireless Networked Control System using ZigBee/IEEE 802.15.4<sup>\*</sup>

N. Boughanmi<sup>\*</sup> YQ. Song<sup>\*\*</sup> E. Rondeau<sup>\*\*\*</sup>

<sup>\*</sup> *LORIA-CRAN-INPL boughanm@loria.fr*

<sup>\*\*</sup> *LORIA-INPL 615 rue du Jardin botanique-CS 20101  
54603 Villers-lès-Nancy Cedex France song@loria.fr.*

<sup>\*\*\*</sup> *CRAN Université Henri Poincaré*

*Vandoeuvre-lès-Nancy Cedex France eric.rondeau@cran.uhp-nancy.fr*

---

**Abstract:** In this paper, the use of wireless sensor networks for networked control loop is analyzed. As the non beacon-enabled mode of IEEE 802.15.4/ZigBee does not ensure the stability for the control loop since non mechanism can prevent the perturbation coming from other applications sharing the same network, the quality of control has to be guaranteed for the control loop. Several possible solutions are investigated. The first one is the CSMA/CA with probabilistic priority by adjusting the minimum waiting time. The second one consists on a deterministic priority black burst mechanism in IEEE 802.15.4/ZigBee. The third one is the beacon-enabled mode using the Guaranteed Time Slot (GTS) mechanism.

---

## 1. INTRODUCTION

Networked Control Systems (NCS) [11] are getting an increasing interest from both industrials and researchers. However, they suffer from limitations in mobility and flexibility because of the network wires. Wireless Networked Control Systems (WNCS) are an alternative to overcome this problem since they offer easier configuration and maintenance especially in case of several networked control loops and in shared communication medium. As an example, RUNES project [RUN] has been interested in it and showed its importance.

The IEEE 802.15.4/ZigBee seems to be one of interesting wireless networks comparing to the others since it is a low-cost low-power Wireless Sensor Networks (WSN). Moreover, even an industrial standard as WirelessHART [1], which was designed to meet the requirements of wireless networks operating in industrial environments, uses IEEE 802.15.4-based Physical layer and MAC PDU.

However, IEEE 802.15.4/ZigBee with non beacon-enabled mode suffers from random delays because of CSMA/CA, frame losses and limited data rate. Moreover, the control traffic is perturbable by the other traffics sharing the communication medium.

First, a service's differentiation mechanism is proposed in order to improve the performances of the ZigBee for control loop in two senses. The first consist on making the medium access more deterministic. The second one aims to minimize the influence of the perturbation's traffics on the control one. Both issues are linked because minimizing the perturbation's influence on the control traffic reduces the access delay. The service differentiation will be ensured by providing a higher range of backoff exponents to the stations others than the control loop nodes to reduce

the probability of stations choosing the same number of backoff periods to sense the channel. Thus, the nodes are divide into two classes: high priority nodes and normal nodes. Probabilistic priority is assigned by changing the minimum backoff exponent (macMinBE) depending on the priority level of the node. In this paper, it is shown that this mechanism improves the QoS of the network offered to the control loop.

Second, the black burst mechanism [10] is used instead of CSMA/CA in IEEE 802.15.4/ZigBee to guarantee the quality of service for the higher priority nodes. When using this mechanism, high priority stations jam the medium for period of time ( black burst) proportional to their priority. After completing the black burst, the stations sense the medium to see if another station is sending a longer black burst. The station with the longest black burst will gain access to the medium.

Third, the beacon enabled-mode in IEEE 802.15.4/ZigBee can offer medium access delay guarantees by means of the Guaranteed Time Slot (GTS) mechanism. A node can reserve a timeslot that it can use to transmit periodically its message. Hence, using the beacon enabled mode makes IEEE 802.15.4/ZigBee suitable for implementing closed-loop for real-time systems. In this paper, the capacity of IEEE 802.15.4/ZigBee to support closed control loops applications is investigated. The impact of network performance variations is evaluated in terms of Quality of Control (QoC). In particular, the limits of IEEE 802.15.4/ZigBee are shown: the lower bound of the sampling period of the control loop is 0.01536s, the number of control loops having the same sampling period is limited to two. A guideline is given to configure network parameters in order to meet QoC requirement of a control loop. Often, one needs to simulate the process, the control and the wireless network. There are several tools which allow the co-design of control loops and networks configurations. TrueTime [8], a Matlab/Simulink simulator, is

---

<sup>\*</sup> This work is partially supported by Safe-NECS project funded by ANR under ANR05SSIA001503.

used since it allows the simulation of the temporal aspects of multi-tasking real-time kernels and wireless networks within Simulink together with the continuous-time dynamics of the controlled plant. TrueTime does not implement the beacon-enabled mode of IEEE 802.15.4/ZigBee. So, this mode is added to TrueTime in order to study the effect of the GTS mechanism on wireless networked control systems. This package can be downloaded at <http://www.loria.fr/equipes/TRIO/packageGTS.zip>.

This paper is organized as follows. In Section 2 related works are discussed. Then, the considered NCS is described in Section 3. A brief overview of the IEEE 802.15.4/ZigBee is presented in Section 4. Section 5 presents analysis of the WNCS in CSMA/CA of the non beacon-enabled mode. In Section 6, the CSMA/CA with probabilistic priority is presented. The black burst mechanism is introduced and analyzed in Section 7. Section 8 deals with an analysis of GTS. Then, this paper concludes in Section 9.

## 2. RELATED WORK

Guaranteeing the network Quality of Service (QoS), especially for industrial process control architecture, is a common problem that has been addressed in several research work. In [7], the case of a dedicated network (CAN, WIFI, IEEE 802.15.4/ZigBee) to the process control application has been studied but the realistic case with other nodes than control loop nodes sharing the network has not been analyzed. In [2], the suitability of IEEE 802.11b for wireless networked control system has been analyzed and it has been shown that the network bandwidth is important for the performance of WNCS.

Koubâa et al. [5] proposed a simple differentiated service scheme for slotted CSMA/CA in IEEE 802.15.4 to improve the performance of time sensitive message. In [9], the authors have modified the initial value of backoff exponent in IEEE 802.15.4 MAC (slotted CSMA/CA) and proposed an adapted backoff exponent (ABE) algorithm. These works was restrained to the slotted CSMA/CA and was not analyzed in the case of wireless networked control systems.

The blackburst mechanism [10] was introduced in the IEEE 802.11 to minimize the delay for real time traffic. Blackburst requires that all high priority stations try to access the medium with constant interval, and the ability to jam the wireless medium for a period of time. This mechanism was not designated for IEEE 802.15.4. Moreover, the length of the black burst is determined by the time the station has been waiting to access the medium and not it's priority.

Some other works have dealt with the IEEE 802.15.4/ZigBee and especially the synchronization of the GTS mechanism. Francomme et al. [4] proposed a new synchronization method for beacons and GTSs in meshed networks using IEEE 802.15.4. Koubâa et al. [6] proposed a synchronization mechanism based on time division beacon scheduling to construct cluster-tree WSNs. Moreover, they proposed a methodology for an efficient duty-cycle management in each router to ensure the fairest use of bandwidth resources. Those works are centric over network Quality

of Service (QoS) and do not include any actual real-time applications.

These works show that the differentiation of service is a promising solution to guarantee the QoS required by the network and so the QoS needed by the control loop. Thus in this work we will analyze the WNCS using the probabilistic priority, the deterministic priority through the blackburst and the GTS mechanism in order to ensure the stability.

## 3. THE CONSIDERED NETWORKED CONTROL SYSTEM

The considered system consists on a cart whose movement is guided along a rail [3]. We aim to control the cart's position. The variable characterizing the system's state ( $x^T = [d \dot{d}]$ ) are:  $d$ , the cart position along the rail measured from a reference point, and,  $\dot{d}$  its velocity. The simplified model of the system is described by the following differential equation where  $u$  is the input and  $k_1, k_2$  two parameters :

$$\ddot{d} = -k_1\dot{d} + k_2u \quad (1)$$

where  $k_1 = 12.6559$  and  $k_2 = 1.9243$ . A wireless sensor network containing the sensor (S), the controller (C) and the actuator (A) is introduced as shown in Figure 1. The network add new delays:  $\tau^{sc}$  is the delay between the sensor and the controller, and  $\tau^{ca}$  is the delay between the controller and the actuator ( Figure 2). The controller behaviour is characterised by the transfer function  $G_C(s)$  and the process (the cart here) by  $G_P(s)$ .  $U(s)$  is the command,  $E(s)$  the error,  $Y(s)$  the system response, and  $R(s)$  is the reference.

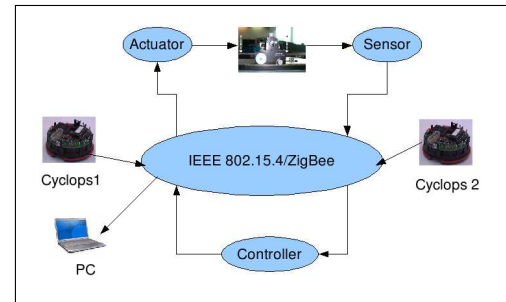


Fig. 1. IEEE 802.15.4/Zigbee using CSMA/CA: shared network

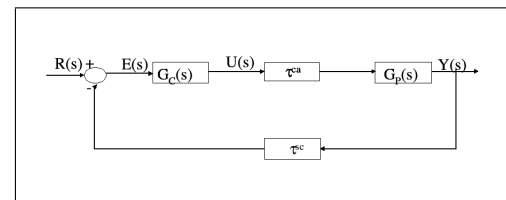


Fig. 2. The networked control system architecture

The sampling period should be higher than 0.010s [3]. In the rest of the paper, the impact of the network's performance on the controlled system is studied in both ideal and realistic cases. Besides, some solutions for some possible problems are presented.

#### 4. IEEE 802.15.4/ZIGBEE PROTOCOL OVERVIEW

The MAC protocol supports two operational modes that may be selected by the coordinator: beacon-enabled mode and non beacon-enabled mode.

- Non beacon-enabled mode : Medium access control is provided by an unslotted CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance) mechanism (using a random backoff time based on backoff period and Backoff Exponent (BE). There is no priority mechanism so no way to isolate a particular flow among all traffic.
- Beacon-enabled mode : Beacons are periodically sent by Zigbee coordinator to synchronize nodes that are associated with it, and to identify the Personal Area Network (PAN). Superframe is contained between two consecutive beacon frames. The superframe structure is used to manage communication between these devices. The superframe contains a Contention-Access Period and Contention-Free Period (CFP), and it may include an inactive period.

The inter frame space (IFS) defines the amount of time that separates the transmission of two consecutive frames. The MAC sublayer needs a finite amount of time to process data received by the physical layer. In an acknowledgment transmission, the IFS follows the acknowledgment frame, otherwise it follows the frame itself. The length of an IFS frame depends on the frame size. The transmission of short frames, which sizes are lower than  $aMaxSIFSFrameSize = 18Bytes$ , is followed by short IFS (SIFS). The transmission of long frames, whose size are greater than  $aMaxSIFSFrameSize$ , is followed by long IFS (LIFS).

#### 5. CSMA/CA

##### 5.1 Ideal case: dedicated WSN

The entire communication channel is dedicated to the control loop. The distances between sensor, actuator and controller are small enough so that they can receive the signals from each other.

In [7], the lower bound for the sampling period  $T_e$  for IEEE 802.15.4 (non beacon-enabled mode) was evaluated as follows :

$$\begin{aligned}
 T_e \geq & \text{Random backoff duration (RBD)} \\
 & + \text{Data frame duration (DFD)} \\
 & + \text{time for acknowledgment (} t_{ack} \text{)} \\
 & + \text{ACK frame duration (AFD)} \\
 & + \text{Short Inter-Frame Space (SIFS)} \\
 & + \text{RBD} \\
 & + \text{DFD} \\
 & + t_{ack} + \text{AFD} + \text{SIFS}. \tag{2}
 \end{aligned}$$

The RBD is evaluated as  $RBD = Rand[0, 2^3 - 1] * BP$ . The backoff period (BP) is equal to  $320\mu s$ . The DFD is equal to  $352\mu s$ . As the  $aTurnaroundTime(TT) \leq t_{ack}$ ,

the  $t_{ack} = TT$  is considered equal to  $(192\mu s)$ . The AFD is set to  $160\mu s$ . As the SIFS must be greater than the TT and the minimal value of SIFS is  $aMinSIFSPeriod = 12symbols$ , then the SIFS value is equal to  $13symbols$  which is equivalent to  $208\mu s$  since  $1symbol = 16\mu s$ . Figure 3 shows flows in a sampling period. The limit of the sampling period was calculated equal to  $6304\mu s$ .

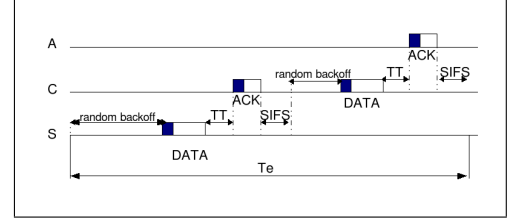


Fig. 3. Flows in a sampling period IEEE 802.15.4/Zigbee non beacon-enabled mode

Figure 4 shows the behavior of the plant Y (cart) and the reference R. The plant follows instantaneously the reference and it is stable.

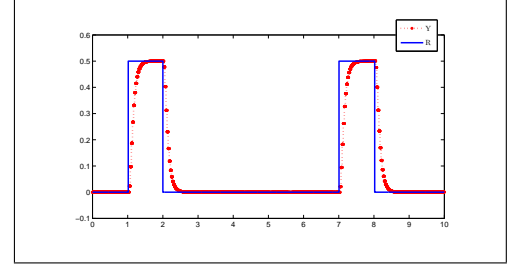


Fig. 4. IEEE 802.15.4/Zigbee using CSMA/CA in ideal case

##### 5.2 Realistic case: shared WSN

In practice, it is not reasonable to dedicate the entire communication channel to the control loop. In fact, the communication channel is shared by 2 cyclops (sensors equipped with camera) and a main control unit as shown in Figure 1. Hence, the wireless network is used to transmit image packets from cyclops to the main control unit. The image sensor has CIF resolution ( $352 \times 288$ ). Each cyclops sends, periodically,  $133octets$ . In the following, the plant behavior is studied for different perturbation load. The transmission period is modified in order to see the effect of the new additional network load on the NCS. Our NCS can stay stable if the additional network load is less than 44% of the total bandwidth. However, if this additional network load reaches 44% ( the transmission period of each cyclops =  $0.02s$ ), the cart becomes instable. Thus, the additional load of 44% of the total bandwidth is the upper limit for the stability of our WNCS. Hence, the unslotted CSMA/CA of the non beacon-enabled mode is not convenient for WNCSs.

#### 6. CSMA/CA WITH PROBABILISTIC PRIORITY

The CSMA/CA mechanism for IEEE 802.15.4 uses the random waiting delay for collision avoidance. It uses the backoff exponent (BE) which is related to how many backoff period (BP) a device must wait before attempting

to assess the channel activity. The algorithm attempts to avoid collision by waiting during a given delay randomly generated in the range of  $[0, 2^{BE} - 1] \times BP$ . If batterylife extension is activated then,  $BE = \min(2, macMinBE)$  else,  $BE = macMinBE$  where  $macMinBE$  attribute specifies the minimum of backoff exponent, which is set to 3 by default. This aspect is exploited in order to differentiate the services offered by the WSN. We propose to vary the randomly generated waiting delay depending on the priority of the packet. Thus, by choosing a higher  $macMinBE$  for the applications different from the control loop, the probability to have a longer delay is increased and the control loop nodes are allowed to send their data packets.

The nodes are divided into two classes: the first class contains the nodes of the WNCS (sensor, controller, and actuator), the second class is composed of the other nodes present in the WSN. The  $BE_{CL}$  represents the  $BE$  of the control loop nodes  $macMinBE_{CL}$  its  $macMinBE$ , and it is set to the default value 3. The  $macMinBE_{OA}$  and  $BE_{OA}$  are the  $macMinBE$  and the  $BE$  of the other applications sharing the WSN. When the batterylife extension is not activated, the control loop nodes have to wait  $random[0, 2^{BE_{CL}} - 1] \times BP$  ( $random[0, 7] \times BP$ ).

*Modifying macMinBE* The  $macMinBE_{OA}$  is increased for the applications with non critical real-time needs. Thus, their data packets wait during a delay randomly generated in a longer range ( $random[0, 2^{macMinBE_{OA}} - 1] \times BP$ ) than the one for the control loop. This is ensured via an assignment of a probabilistic priority to the nodes in the WSN. This probabilistic priority is ensured by modifying the range for the random delay. Hence, the higher priority nodes (the control loop nodes here) have more chance to send their data packets.

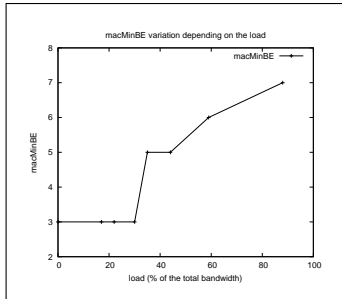


Fig. 5.  $macMinBE_{OA}$  variation depending on the perturbation load

Figure 5 shows the  $macMinBE_{OA}$ , obtained by simulations, which allows the control loop to be stable for different loads. For a small load (less than 35%), there is no need to increase the  $macMinBE$  since the default value 3 can afford the stability for the WNCS. When the disturbing load becomes important, the control loop becomes to be instable because of the long delay and the packets losses. Thus, increasing the  $macMinBE_{OA}$  allows the control loop to reach the stability in spite of the perturbing load. In fact, for the considered control loop, the value of 7 for  $macMinBE$  afford the stability for the control loop for a perturbation load of 90% of the total bandwidth.

Collisions still exist since the nodes of WSN can choose the same waiting delay.

*Modifying the minimum waiting time and the macMinBE*

We are interested in minimizing the collisions between nodes of the two classes (control loop and other applications). The lower-priority applications will wait during a delay randomly generated in the range of  $[variable, 2^{BE_{OA}} - 1]$  backoff periods. The question is how to choose the  $variable$ 's value. This variable is set to be equal to  $2^{BE_{CL}}$  so that there is no collision between the members of the two classes ( $variable = 8$ ).

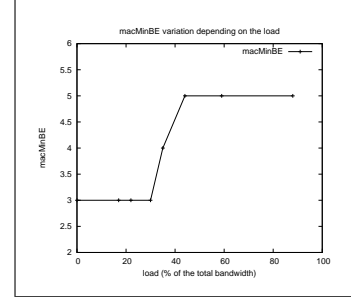


Fig. 6.  $macMinBE_{OA}$  variation depending on the perturbation load

Figure 6 presents the evolution of the  $macMinBE_{OA}$  which allow the WNCS to be stable for different perturbation loads. The value of  $macMinBE_{OA}$  using this method is less than the one found when only the  $macMinBE$  is modified. Thus, separating the ranges of random waiting value of the two classes improve the QoS offered to the WNCS.

*Discussion* This mechanism can lead to the under-use of the network resources due to the new waiting delay. Even when the communication medium is free and no one from the class of the control loop wants to send, the nodes of the other class have to choose their waiting period in a large range. This leads to under-use of the network resources. Moreover, this mechanism is not deterministic. Thus, the blackburst or the GTS mechanism can be used.

## 7. BLACKBURST MECHANISM TO ACHIEVE DETERMINISTIC PRIORITY

The goal of black burst [10] is to minimize the delay for the real-time traffic. The black burst mechanism requires that:(i) all stations try to access the medium with equal, constant interval, blackburst period as shown in Figure 8; (ii) the ability to jam the medium for a period of time. When a new cycle starts, each station who wants to send a frame, sends a blackburst to jam the channel. The length of the blackburst is determined by the priority of the application, and is calculated as a number of black slots. The duration of a black slot  $t_{bslot}$  is at least equal to the turn around time (TT) ( $t_{bslot} \geq TT$ ). After transmitting the blackburst, the station listens to the medium for an observation time  $t_{obs}$  ( $t_{obs} < t_{bslot}$ ) to see if another station is sending a longer blackburst. This would imply that this station has higher priority, so it should access the medium first. If the medium is idle, the station will then send its frame, otherwise it will wait until the medium becomes idle again and enter another black burst period. As it is supposed that there is different priority for each station, the black burst mechanism will yield to a unique winner.

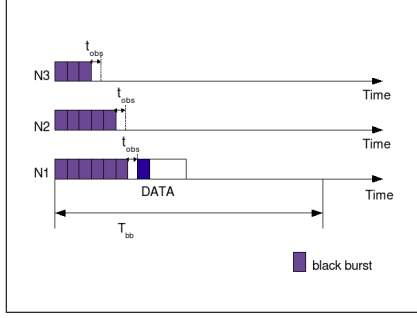


Fig. 7. Competition to access to the communication medium

Figure 7 shows three nodes competing to access to the communication medium. Node  $N3$  has the lowest priority, thus it is the first one to finish the transmission of black burst. Then, it listens to the medium during a  $t_{obs}$  and it finds that there is someone else sending. Hence,  $N3$  quits. The same thing for node  $N2$ . When node  $N1$  (with the highest priority) transmits its black bursts and then listens to the medium, it finds it free. Thus,  $N1$  is the winner and start to send its data packet.

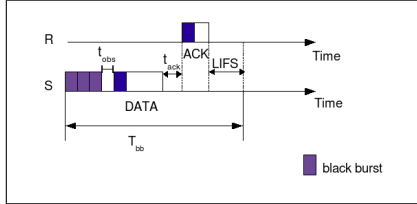


Fig. 8. Flows in a black burst period

Figure 8 shows flows in a black burst period  $T_{bb}$ . The black burst period is evaluated as

$$\begin{aligned}
 T_{bb} = & \maxPrio \times t_{bslot} + t_{obs} \\
 & + \text{Maximum Data Frame Duration} \\
 & + t_{ack} + \text{ACK frame duration} \\
 & + \text{Long Inter-Frame Space (LIFS)} \quad (3)
 \end{aligned}$$

where

$$\begin{aligned}
 aTurnaroundTime \leq t_{ack} \leq & (aTurnaroundTime \\
 & + aUnitBackoffPeriod)
 \end{aligned}$$

(12 symbols  $\leq t_{ack} \leq$  32 symbols). The length of the Maximum Data Frame Duration, in the IEEE 802.15.4, is fixed to 133 octets, so the transmission duration is equal to  $4256\mu s$ . The same value, as used in the CSMA/CA, is maintained for ACK Frame Duration ( $160\mu s$ ), the  $t_{ack}$  (32 symbols,  $512\mu s$ ) and the LIFS (40 symbols,  $640\mu s$ ). The duration of the black slot is set to TT, so  $t_{bslot} = 192\mu s$ . Besides, the observation time  $t_{obs}$  is fixed to  $180\mu s$ .

$$T_{bb} = \maxPrio \times t_{bslot} + cste \quad (4)$$

For the studied system, the maximum priority value is fixed to five (since we have five nodes in the network). Thus, the black burst period is equal to  $6708\mu s$ . Using static priority in this part and ensuring that messages have different priorities, we guarantee that each black burst contention period will yield a unique winner.

**Implementation and results** The black burst mechanism is implemented and added to the TrueTime package. The used configuration is shown in Figure 1. Higher priority is assigned to the control loop nodes, so that, whenever one of them has a data packet, he can send it no later than a  $T_{bb}$ . For important perturbation loads (more than 90% of the total bandwidth), the simulation results show that the cart answer follows the reference. Thus, the black burst mechanism ensures that our wireless networked control system remains stable.

**Discussion** This approach is interesting when the sampling period of the control loop is greater than the black burst period ( $T_e > T_{bb}$ ). Thus, if the control loop nodes have the highest priority then their data packets will be sent and the controlled system will reach the required QoC. The maximal priority value is given by

$$\maxPrio \leq \left\lfloor \frac{T_e - cste}{t_{bslot}} \right\rfloor. \quad (5)$$

If the highest priority in the WSN do not satisfy the inequation (5) the black burst mechanism will not guarantee anymore the stability for the WNCs. Thus, the GTS mechanism is an interesting alternative to resolve this problem.

## 8. GTS MECHANISM

To ensure the stability of the WNCs, we are interested in the beacon-enabled mode of the IEEE 802.15.4. Indeed, network resources are reserved using the GTS mechanism. The superframe duration (SD) is given by  $SD = aBaseSuperframeDuration \cdot 2^{SO}$  for  $0 \leq SO \leq BO \leq 14$  where SO is the Superframe Order. SD is divided into 16 equally-sized time slots, during which frame transmissions are allowed. GTSs are allocated by the PAN coordinator. The PAN coordinator can allocate at most seven GTSs and each GTS may occupy more than one time slot.

Each node in the control loop will have a reserved GTS whose size will be 1 slot since the control data is not big (small frame). Figure 9 shows that 3 GTSs (3 slots) are needed, but as the superframe has at least 16 slots (if the inactive part is omitted), the WNCs sampling period  $T_e$  has to be at least equal to the superframe duration. Indeed,  $T_e$  must be greater than  $SD$ . As the smallest superframe duration (for  $SO = 0$ ) is equal to  $0.01536s$ , then the WNCs sampling period  $T_e$  is greater than  $T_{e_{min}} = 0.01536s$ . Besides, since the number of GTS is restricted to 7, the GTS mechanism cannot afford QoS guarantees to more than two control loops with the same sampling period. Otherwise, one should use the scheduling policy in [4].

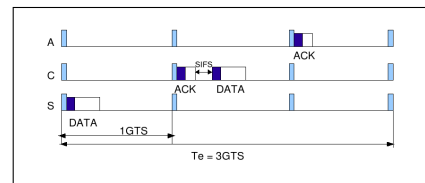


Fig. 9. Used GTSs by the WNCs



Moreover, the sensor and the controller use only CFP to send sensing and control data so that they do not use the CAP part. The CAP part is used by other nodes using the WSN.

The beacon-enabled mode of the IEEE 802.15.4/ZigBee is developed and added to TrueTime. Figure 10 shows its network parameterization.

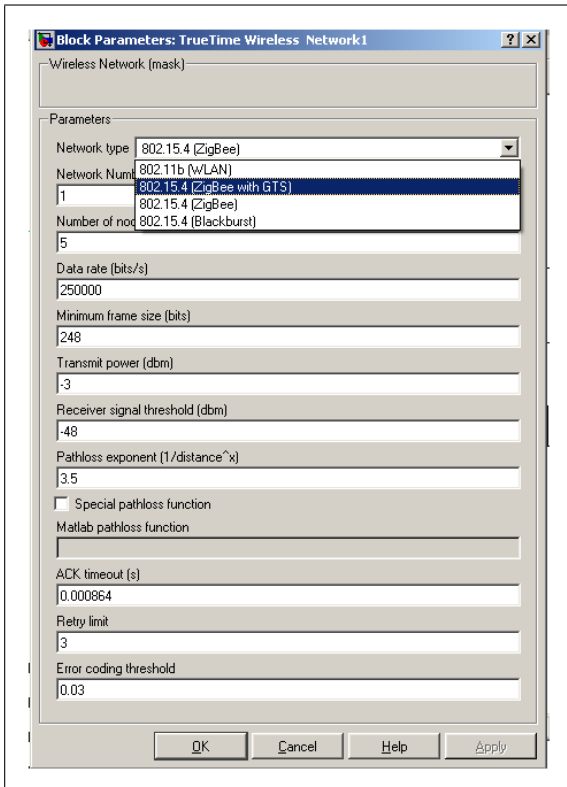


Fig. 10. The IEEE 802.15.4/ZigBee with beacon enabled mode in TrueTime

### 8.1 Simulation and results

The considered system is shown in Figure 1. This system is simulated using the IEEE 802.15.4/ZigBee beacon-enabled mode. Moreover, in these simulations the mechanism of signal adaptation is disabled since it creates messages and disturbs the GTS mechanism (more than one GTS are needed for each node). Besides, only two GTS are used, one for the controller and another for the sensor because, in TrueTime the acknowledgement is fictive.

It is assumed that there is no energy problem for the nodes (infinite amount of energy). Moreover, the controller is considered as the PAN coordinator. The mobility problem (nodes are static) is not addressed for the moment. Besides, in the simulation example, the acknowledgement is not taken into account. So, only two GTSs are needed. The nodes send only in their reserved GTS and without packet loss.

Several perturbation's loads higher than 44% are tested. The plant behavior follows almost exactly the reference. Thus, using the GTS mechanism guarantees the network QoS and the required QoC for the control loop.

## 9. CONCLUSIONS

In this paper, three mechanisms of service differentiation are presented: the CSMA/CA using the probabilistic priority, the IEEE 802.15.4 using the blackburst mechanism, and the GTS mechanism of the beacon-enabled mode of the IEEE 802.15.4. These mechanisms are implemented and tested on the considered networked control system using TrueTime. From this study, we show that IEEE 802.15.4 can be used for the WNCS with the proposed mechanisms. As future work, we aim to manage the QoS offered to the WNCS depending on the state of the controlled system.

## REFERENCES

- [RUN] RUNES project. <http://www.ist-runes.org/>.
- [1] HART, 2007. <http://hartcomm2.org/>.
- [2] J. Colandairaj, G.W. Irwin, and W. Scanlon. Analysis of an IEEE 802.11b wireless networked control system. In *Proc. 1st NeCST Workshop on Networked Control Systems and Fault Tolerant Control*, pages 19–25, Ajaccio, France, October 2005. Invited Guest Lecture.
- [3] F. Felicioni, N. Jia, Y. Song, and F. Simonot-Lion. Impact of a (m,k)-firm data dropouts policy on the quality of control. In *6th IEEE International Workshop on Factory Communication Systems*, volume Factory Communication Systems, 2006 IEEE International Workshop on, pages 353–359, Torino, Italy, 28/06/2006. <http://ieeexplore.ieee.org>.
- [4] J. Francomme, G. Mercier, and T. Val. Beacon synchronization for GTS collision avoidance in an IEEE 802.15.4 meshed network. In *FET'07*, 7-9 November 2007.
- [5] A. Koubâa, M. Alves, and Y. Song B. Nefzi. Improving the ieee 802.15.4 slotted csma/ca for time-critical events in wireless sensor networks. In *Workshop of Real-Time Networks (RTN 2006), Satellite Workshop to ECRTS 2006*, Dresden, Germany, July 2006.
- [6] A. Koubâa, A. Cunha, and M. Alves. A time division beacon scheduling mechanism for IEEE 802.15.4/ZigBee cluster-tree wireless sensor networks. In *19th ECRTS*, July 2007.
- [7] G. Mouney, G. Juanole, and C. Calmettes. On the implementation of one process control application type through a network. considering three LANs: CAN, WiFi, ZigBee. In *17th IFAC World Congress*, July 6-11 2008.
- [8] M. Ohlin, D. Henriksson, and A. Cervin. *TrueTime1.5-Reference Manual*. Department of Automatic Control Lund University, 2007.
- [9] V.P. Rao and D. Marandin. Adaptive backoff exponent algorithm for zigbee (IEEE 802.15.4). *Next Generation Teletraffic and Wired/Wireless Advanced Networking*, 4003/2006:501–516, september 2006.
- [10] J.L. Sobrino and A.S. Krishnakumar. Quality of service in ad hoc carrier sense multiple access networks. *Selected Areas in Communications, IEEE Journal on*, 17(8):1353–1368, Aug 1999.
- [11] S. Zampieri. Trends in networked control systems. In *17th IFAC World Congress*, July 6-11 2008.