

# Simulation Analysis of IEEE 802.15.4 for Wireless Networked Control Systems

Pedro Macedo and José A. Afonso  
Department of Industrial Electronics, University of Minho, Guimarães, Portugal  
jose.afonso@dei.uminho.pt

*Abstract—The deployment of wireless networks in industrial environments can bring several advantages over their wired counterparts; however, the characteristics of the wireless channels pose challenges to the provisioning of quality of service (QoS) that are not seen in wired networks. This paper provides an analysis of how important QoS parameters, such as message delivery ratio, delay and energy consumption, vary as a function of the number of sensor nodes injecting traffic in IEEE 802.15.4 networks operating in unbeaconed mode. Results show that the peer-to-peer topology enables better performance than the star topology, under the same conditions, indicating that the former is a better option if centralized control is not required. The use of retransmissions increases significantly the reliability of the network; however, even a high number of retransmissions are not enough to provide full reliability when the channel is highly affected by errors. Results also show that presence of hidden nodes can severely degrade the performance of the network, while the reduction of the turnaround time can improve the performance.*

## I. INTRODUCTION

The interest in the use of standard wireless network technologies to support monitoring, diagnosis and control applications in industrial environments has been steadily increasing in the last years. Wireless networks provide the capability of mobility and easy deployment of sensor nodes in inaccessible or hazardous environments, unlike wired systems which are restrained due to the use of cables. Ease of installation and maintenance due to lack of cabling also leads to the elimination of the time and cost incurred with the installation of a large number of cables.

Although industrial applications can benefit with wireless technology, many issues have to be addressed. Industrial environments are error-prone and the reliability of wireless channels is lower than the wired ones. The reliability in industry facilities may suffer due to attenuation, path loss, shadowing, multipath fading, interference from others wireless systems working in the same Industrial, Scientific and Medical (ISM) band, as well as noise generated by other sources, e.g. heavy machinery. Moreover, wireless sensor nodes normally are energy constrained and have limited computing power. Due to these factors, it is difficult to provide the reliable real-time communications typically required by industrial applications.

Most of the currently available wireless network products operate in the license free 2.4 GHz band. Some examples are wireless personal area networks (WPAN) such as Bluetooth and IEEE 802.15.4/ZigBee, as well as wireless local area networks (WLAN) such as IEEE 802.11 [1].

The purpose of this paper is to evaluate the performance of wireless networked control systems based on the IEEE 802.15.4 network technology using unslotted CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), through the use of simulation. A Networked Control System (NCS) is a control system where the control loops are closed through a real-time network. A NCS normally integrates four basic elements: sensors, to acquire information; controllers, to provide decision and commands; actuators, to perform the control commands; and a communication network, to enable the exchange of information. Two network topologies are evaluated and compared: star and peer-to-peer. Results are provided both for error free and burst errors wireless channel scenarios, as well as for different number of allowed retransmission attempts. For the peer-to-peer topology, simulation results of the impact of hidden nodes in the network performance are also presented.

This paper is organized as follows. The next section presents the related work and section III presents an overview of the IEEE 802.15.4 standard. In the fourth section, the simulation analysis and results are presented and discussed. Finally, section V presents the conclusions.

## II. RELATED WORK

Wireless Sensor Networks (WSN) are capable to collect data from the physical world, process them and make decisions based on the gathered data, so they present particular relevance in the context of industrial environments. In the WSNs, sensor nodes tend to be small and have limited energy, processing, and communication capacity, while the actuator nodes tend to have higher energy and processing capacity. In a WSN, the number of sensors nodes can be in the order of hundreds, but such dense deployment of larger number of actuators is usually not necessary.

The authors in [2] provide an overview of recent advances in wireless communication technologies, such as ad-hoc networks and wireless sensor/actuator networks applied to industrial automation. Three existing standards are discussed and compared: IEEE 802.15.1/Bluetooth, IEEE 802.11 and IEEE 802.15.4/ZigBee. From the results presented, the authors conclude that IEEE 802.15.4/ZigBee standards present better range (though the use of multihop communication), longer battery life, large capacity of sensor nodes in the network and low cost in comparison with the other standards. However, it presents lower network data rate,

which can be a limiting factor for some industrial applications.

Several authors have presented performance analysis of IEEE 802.15.4 for monitoring purposes [3] [4]. On the other hand, this paper concerns the analysis of IEEE 802.15.4 not only for monitoring purposes, but also for control. That means that in a star network, for example, besides the traffic from sensor nodes to the coordinator, there is also traffic from the coordinator to the actuator nodes, and what matters is the end-to-end delay and reliability performance.

Some authors have studied the application of IEEE 802.15.4 protocol in industrial environments [5] [6]. In [5] the authors discuss how the developments in WSN applications depend of the fulfillment of constraints imposed by the applications, present a characterization of WSN applications, and enumerate several applications where WSNs can be applied, such as the medical, environmental, agricultural and industrial sectors, summarizing the technological challenges in WSN development to guarantee the those fulfillments, such as energy consumption, limited computing power, coverage of large areas and real-time deadlines.

In [6] the authors study the performance of the IEEE 802.15.4 standard in control applications for the industry using simulations. The authors considered a 1-byte payload and evaluated the energy consumption per byte, packet loss, delay and throughput. The simulations used an ideal channel where losses only occur due to collisions or buffer overflow. The hidden nodes problem was address, but only two nodes hidden from each other were considered. All the simulations were conducted using a star topology with the IEEE 802.15.4 operating in the beacon enable mode. This paper, on the other hand, considers the operation in the unbeaconed mode for both peer-to-peer and star networks, evaluates the performance with and without channel errors, and assesses the impact of hidden nodes with a larger number of nodes.

### III. IEEE 802.15.4 OVERVIEW

The IEEE 802.15.4 standard [7] specifies both physical (PHY) and medium access control (MAC) of a network. This standard aims for low power, low rate and low cost for sensors and control devices. The PHY layer is based on direct sequence spread spectrum (DSSS) to comply with the sharing rules of each band. It can operate in three different bands, for 868/915 bands we have 20/40 kbps and for 2.4 GHz we have 250 kbps. The MAC layer uses a contention based CSMA/CA mechanism. There are two different modes of operation, the unbeaconed mode, that uses an unslotted CSMA/CA variant, and the beaoned mode, where the network coordinator imposes a superframe structure and it is used a slotted CSMA/CA variant. The MAC layer also provides a TDMA (Time Division Multiple Access) scheme called guaranteed time slot (GTS); however, only seven GTS allocations per superframe are allowed at most, which limits significantly the number of supported devices.

The unslotted CSMA/CA algorithm is represented in Fig. 1 [7]. Before accessing the channel, the device must wait for a

random backoff interval defined in the interval from 0 to  $(2^{BE} - 1)$  backoff periods, where BE, the backoff exponent, initially takes the value *macMinBE* and one backoff period is equal to *aUnitBackoffPeriod* symbols. After that, if the clear channel assessment (CCA) function indicates that the channel is idle, the device starts its transmission after a turnaround time delay, which is the time necessary to for the radio transceiver to switch from receive state to the transmit state. If the channel is busy, the device defers its transmission and increments NB, the number of transmission attempts for the current packet. BE is also incremented if it has not reached its maximum value, *aMaxBE*. If the maximum number of transmission attempts, *macMaxCSMABackoffs*, was not reached, a new backoff interval is determined; otherwise, the algorithm declares a channel access failure. The values of the unslotted CSMA/CA parameters are specified in Table 1.

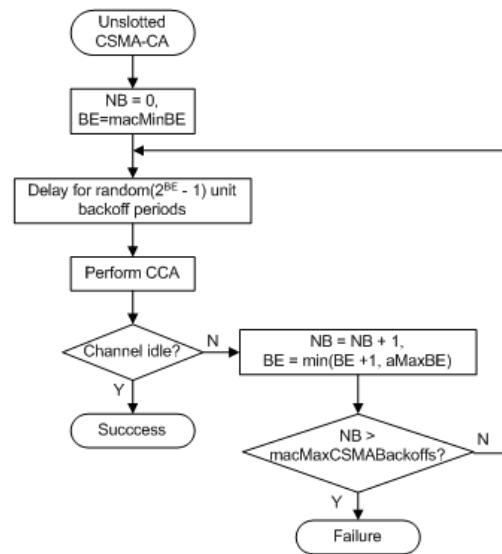


Fig. 1. Unslotted CSMA/CA algorithm.

TABLE I - Unslotted CSMA/CA parameters.

Parameter	Description	Value
<i>macMinBE</i>	The minimum value of the backoff exponent	[0-3], default = 3
<i>aUnitBackoffPeriod</i>	The length of the backoff period, where the symbol period (SP) is 16 $\mu$ s	20 SP
<i>aMaxBE</i>	The maximum value of the backoff exponent	5
<i>macMaxCSMABackoffs</i>	The maximum number of backoff periods	[0-5], default = 4

### IV. SIMULATION ANALYSIS

In order to produce the results presented in this section, a model of the IEEE 802.15.4 protocol was implemented using OMNeT++, a public-source, component-based, modular and open-architecture simulation environment [8].

The first part of the results provides a comparison of the performance of the network using two different network

topologies: star and peer-to-peer. Simulations comparing an ideal channel, to an error-prone channel are also presented. In the second part of the results, the peer-to-peer network topology is used to demonstrate the impact of the hidden nodes on the performance of the network. The effect of the turnaround time on the performance is analyzed in the third part.

The ideal channel is not affected by interference or fading, so the packet losses are due only to collisions or failure to access the channel. Regarding the error-prone channel, it is modeled using the Gilbert-Elliot model [9]. The channel alternates between a good state with low bit error rate (set to  $10^{-6}$ ) and a bad state, with very high bit error rate (set to  $10^{-2}$ ). The mean dwelling time was set to 10 ms for the bad state and 90 ms for the good state. This choice of parameters is intended to model fast fading, which typically occurs on timescales of milliseconds to tens of milliseconds [10] and can also represent interference from other sources such as Wi-Fi transmissions in the same band.

Each sensor node sends messages using an exponential traffic type, with a mean interarrival time of 100 ms. Data messages have a total of 27 bytes, being composed by 6 bytes of overhead from the physical layer, 11 bytes of overhead from the MAC layer and 10 bytes of data payload. The MAC layer overhead consists of 2 bytes for the Frame Control field, 1 byte for the Sequence Number, 6 Bytes for the Address field (2 bytes for the PAN identifier, 2 bytes for the source address and other 2 bytes for the destination address) and 2 bytes for the Frame Check Sequence (FCS). The overhead is significant when compared with the 10 bytes of the payload; nevertheless, this overhead is still substantially lower than the one imposed by networks such as the IEEE 802.11, where the overhead due to the MAC layer alone is 34 bytes.

When a message is not received, it can be retransmitted according to the number of retries previously set in the simulation. The acknowledgement (ACK) frame is 5 bytes long. The turnaround time is set to 192 ms, that is, 12 Symbol Periods (SP), which is the maximum value specified by the IEEE 802.15.4 standard. This is an important parameter because, the longer this time is, the higher is the vulnerability to collisions. The buffer of the MAC layer has a maximum size of 100 positions. Each simulation run ends when 50,000 messages are delivered to its final destination.

Results concerning the delivery ratio, maximum delay and energy consumption are presented in this section. The throughput, mean delay, collision ratio and percentage of failed transmission attempts were also measured, but are not presented due to lack of space. Concerning the energy consumption, it is assumed that the coordinator and the actuator nodes are always active, since they must be prepared to receive a new message at any time. In the specific case of the actuator nodes, measures to minimize the energy consumption are not taken into account because it is assumed that the power source that is used to drive the actuator does not have constraints to also power the node electronics.

In terms of nomenclature used in this paper, a message with a unique sequence number can be characterized as information to be sent by the sensor nodes or the coordinator. On the other hand, a packet is an instance of a message, which means that in order to successfully deliver a message, the network may need to transmit several packets.

#### A. Topology Analysis

In the case of the star network topology, all the sensor nodes transmit to a coordinator (uplink) who redirects the message to the proper actuator (downlink). On the other hand, in the peer-to-peer topology, the sensor nodes transmit directly to the actuators. The topologies are depicted in Fig. 2, where  $S_i$  represents the sensor nodes,  $A_i$  are the actuator nodes and C is the Coordinator.

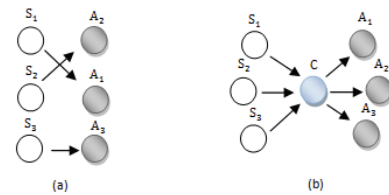


Fig. 2. Peer-to-Peer (a) and Star (b) network topologies.

The simulations consisted in increasing the number of sensor nodes in the network with the purpose to evaluate the scalability in terms of how many sensor nodes the networks can support while still providing a satisfying QoS level.

In these simulations, four modes of operation were considered: do not retransmit lost messages (Without ACK – 0 Ret); up to one retransmission attempt per message (1 Ret); up to three retransmissions attempts per message (3 Ret); and up to six retransmissions attempts per message (6 Ret). The goal for all these simulations is to compare the performance of the network for different values of retransmission attempts. Unless otherwise indicated, the graphs concern the channel with errors.

#### 1. Star Topology

Fig. 3 and Fig. 4 present the delivery ratio in the star network for the error free and error-prone channels, respectively. The delivery ratio for the error-prone channel is much worse than for the ideal channel, especially if the number of allowed retransmissions is low. It is also possible to observe that while the maximum delivery ratio achieved with the ideal channel is near 100%, for the error-prone channel the value is only slightly above 98%. This means that even though the use of up to six retransmissions enables a significant increase in the delivery ratio, it is not possible to recover from all errors in the scenario with channel errors. As the number of sensor nodes increase above a certain point, the delivery ratio tends to collapse. This happens because the increment in the network load increases the percentage of collided packets and failed transmissions attempts and reduces the bandwidth available for recovery from errors at the same time. In the case of the error-prone channel, with up

to six retransmissions the delivery ratio starts to drop when the number of nodes is higher than 13.

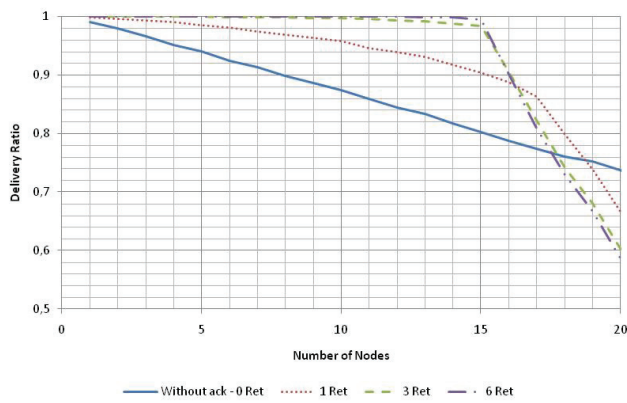


Fig. 3. Delivery ratio for the star network – error free channel.

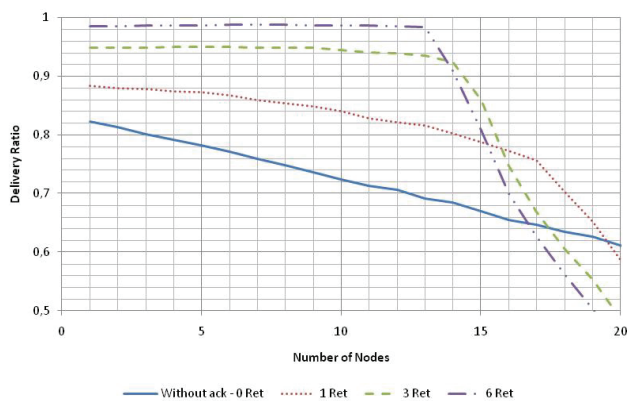


Fig. 4. Delivery ratio for the star network – channel with errors.

For the same number of nodes, if more retransmission attempts are possible, the performance of the network in terms of delivery ratio increases; however, the channel gets busier, which tends to increase of the delay and energy consumption. Fig. 5 shows the maximum delay for the star network in the error-prone scenario. Due to a wide variation in range, the graphs are in logarithmic scale. It can be seen that the maximum delay for 13 nodes is higher than 0.8 s, which can be significant for real-time applications. In the case a maximum delay below 100 ms is required; the network would only be able to support 6 sensor nodes.

Fig. 6 presents the graph concerning the energy consumption per message for the sensor nodes. The energy per message is calculated taking in account only the consumption of the transceiver. For the energy consumption estimation, we have considered the parameters specified for JN5139 modules [11] from Jennic, as we are basing our implementation on these devices. When the module switches the transceiver on for the backoff process, the current is 22.79 mA and when the module starts to transmit, the current increases to 27.79 mA. After the transmission the transceiver is switched off. A 3 V voltage supply was considered.

The lifetime of the nodes can be estimated using these graphs. As an example, on a network consisting of 13 sensor nodes allowed to make up to six retransmission attempts, the

average energy spent by a node to transmit a message is 0.747 mJ. Since the mean interarrival time is 100 ms, the average number of messages transmitted by a node in one second is 10. Considering a module powered by a +3 V, 2400 mAh battery (25.92 kJ), each node would have a lifetime of approximately 40 days of continuous operation. This value does not take into account the consumption of other components of the node, such as the microcontroller (9.21 mA when active) or the sensors.

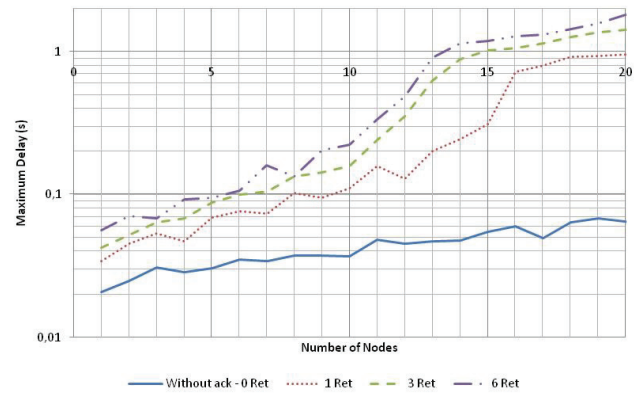


Fig. 5. Maximum delay for the star network.

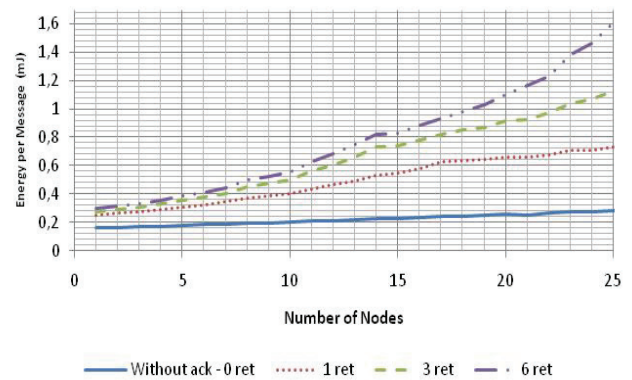


Fig. 6. Energy consumption for the sensor nodes in the star network.

## 2. Peer-to-Peer Topology

Fig. 7 and Fig. 8 present the delivery ratio in the peer-to-peer network for the error free and error-prone channels, respectively. In this topology, with channel errors and up to six allowed retransmission attempts, the network can support 26 nodes with delivery ratio above 98%, before the performance of the network starts to collapse. With this topology, the network supports a much higher number of sensor nodes than in the case of the star topology, either with or without errors in the channel. This happens because in the star topology every message has to be transmitted twice in the channel, by the node and by the coordinator, duplicating the network traffic load in relation to the peer-to-peer topology.

Fig. 9 presents the maximum delay for the peer-to-peer topology with channel errors. In order to achieve a maximum delay below 100 ms in this case, the number of supported nodes has to drop to 19.

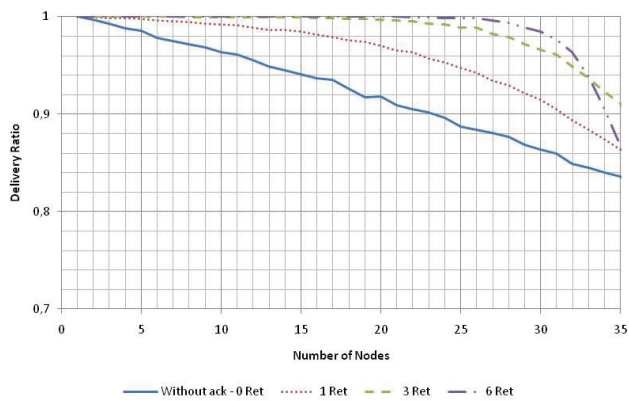


Fig. 7. Delivery ratio for the peer-to-peer network – error free channel.

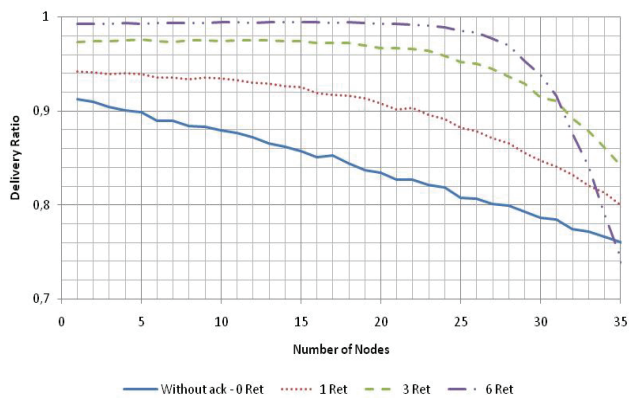


Fig. 8. Delivery ratio for the peer-to-peer network – channel with errors.

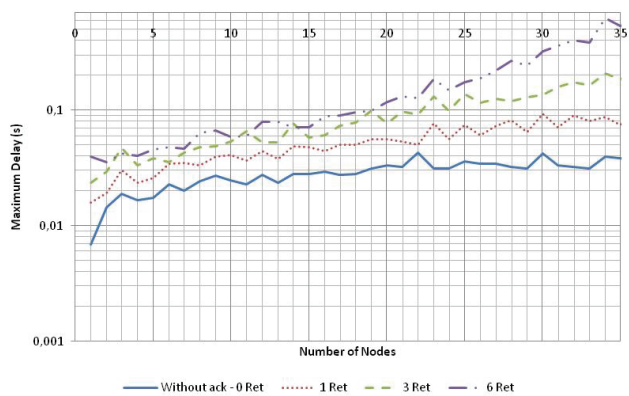


Fig. 9. Maximum delay for the peer-to-peer network.

The results of the energy consumption are depicted in the Fig. 10. Analyzing for the case of the star topology, with 13 sensor nodes and up to six retransmission attempts, the average energy consumption is 0.416 mJ. With the same battery, each node would have a lifetime of approximately 72 days, a improvement of 79.6% when compared with the star network.

### B. Impact of Hidden Nodes

In CSMA based networks the presence of hidden nodes can affect drastically the performance. One of the principles of a CSMA based network is that, before transmitting a message,

a node must first sense if the channel is idle. The problem occurs when a node starts transmitting, because it sensed the channel idle, but another node, hidden from it, had already started its transmission. In this case a collision will occur, and both packets will be lost.

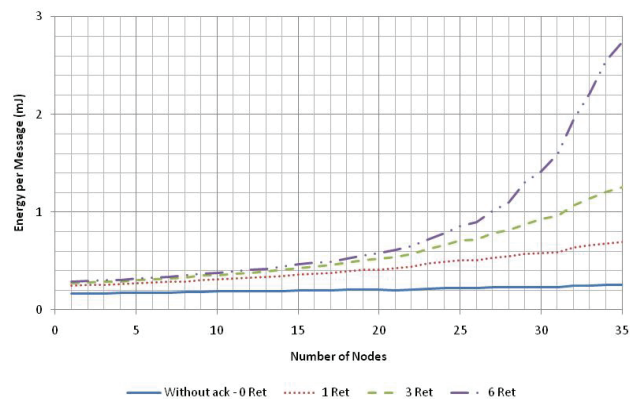


Fig. 10. Energy consumption for the sensors in the peer-to-peer network.

This simulation consisted in increasing the percentage of hidden nodes in a peer-to-peer network from 0% to 20%, in 5% increments. Fig. 11 presents the delivery ratio considering channel errors and up to six allowed retransmission attempts; the impact of hidden nodes for the other scenarios is similar. The negative impact of hidden nodes in the performance of the network is easily observed. For example, for a network with 25 sensor nodes, the delivery ratio decreases from 98.5% without hidden nodes to 74% with 20% of hidden nodes.

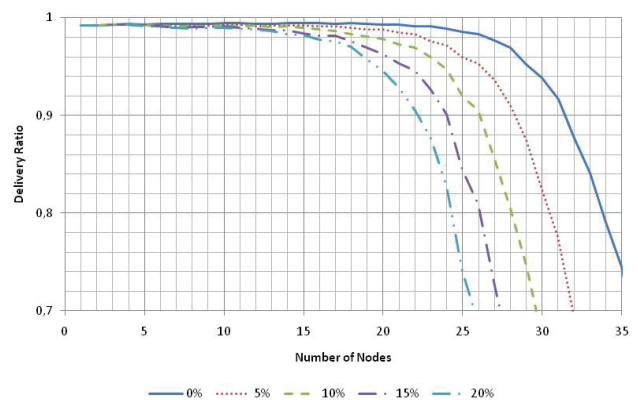


Fig. 11. Delivery ratio with different percentages of hidden nodes.

### C. Turnaround Time Analysis

The turnaround time is an important parameter in CSMA based networks. Ideally, after a node senses the channel, detects that it is free and takes the decision to transmit, it would be able to start transmitting immediately; however, the transceiver must first switch from the receiver state to the transmitter state. During this turnaround time, other nodes may sense the channel and, since the first node has not started transmitting yet, they will detect a free channel and take the

decision to transmit as well. Therefore, the longer is the turnaround time, the higher is the probability of collisions.

Three different times of turnaround time were evaluated, 8 SP (128  $\mu$ s), 12 SP (192  $\mu$ s) and 16 SP (256  $\mu$ s). The simulation scenario consisted of the peer-to-peer topology with the error-prone channel and up to six retransmission attempts. As Fig. 12 shows, the delivery ratio decreases earlier for higher values of the turnaround time, since the collisions become more frequent. Taking the example of a network with 29 sensor nodes, with a turnaround time of 128  $\mu$ s, the system presents a delivery ratio of 99%, while with a turnaround time of 256  $\mu$ s the delivery ratio drops to 81%.

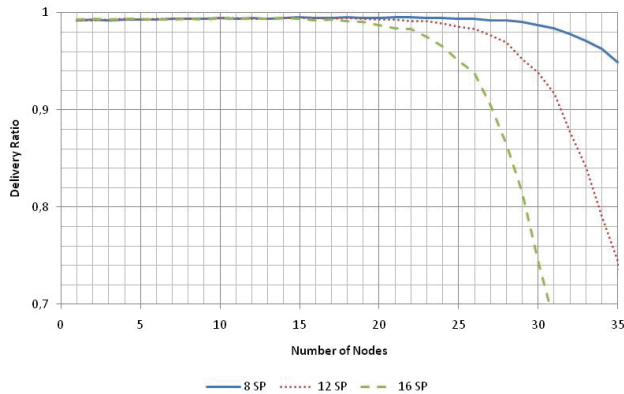


Fig. 12. Delivery ratio with different values of turnaround time.

## V. CONCLUSION

A simulation analysis of the performance of a wireless networked control system based on the IEEE 802.15.4 network technology using the unslotted CSMA/CA mode was presented in this paper. Two sets of topologies were analyzed and compared: star and peer-to-peer. Simulation results with an increasing number of sensor nodes were provided, for different number of allowed retransmission attempts and for error free and burst errors channels. The model of channel with errors provides a more realistic scenario for industrial environments. The impact of hidden nodes and different values of turnaround time on the performance of the network was also evaluated.

If more retransmissions attempts are allowed, the delivery ratio increases, but the delay also increases, because the medium becomes busier. Analyzing the results for a system that allows up to six retransmission attempts which is subject to an error-prone channel with the parameters defined in section IV; if a maximum delay below 100 ms is required, the peer-to-peer topology can support 19 sensor nodes with a delivery ratio of 99.3%, while the star topology can support only 6 sensor nodes with 98.6% of delivery ratio. Even with a high number of allowed retransmissions, it was not possible to achieve a reliability of 100% under the error-prone channel conditions, so the system is not suitable for hard real-time applications. The performance for the peer-to-peer topology is better because the sensor nodes transmit directly to the

actuator nodes, while in the star topology the messages have to pass through the coordinator, duplicating the load in the medium. Therefore, the peer-to-peer topology is a better option if centralized control is not required.

The performance of the network is significantly affected by hidden nodes, but the IEEE 802.15.4 does not provide a mechanism to deal with this problem. On the other hand, the performance can be improved through the reduction of the turnaround time.

## ACKNOWLEDGMENT

This work is supported by FCT project PTDC/EEA-TEL/68625/2006, Portugal.

## REFERENCES

- [1] A. Willig, K. Matheus and A. Wolisz, "Wireless Technology in Industrial Networks", Proceedings of the IEEE, vol. 93, no. 6, pp. 1130-1151, June 2005.
- [2] M.Mathiesen, G. Thonet and N. Aakvaag, "Wireless Ad-Hoc Networks for Industrial Automation: Current Trends and Future Prospects", ABB Corporate Research, 2005.
- [3] B. Latre et al, "Throughput and Delay Analysis of Unslotted IEEE 802.15.4", J. Networks 1(1), pp. 20-28, 2006.
- [4] H. F. López, P. Macedo, J. A. Afonso, J. H. Correia and R. Simões, "Performance Evaluation of a ZigBee-based Medical Sensor Network", In *International Workshop on Wireless Pervasive Healthcare (WiPH 2009)*, London, UK, March 2009.
- [5] D. Martínez, F. Blanes, J. Simo and A. Crespo, "Wireless Sensor and Actuator Networks: Characterization and Case Study for Confined Spaces Healthcare Applications", Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 687-693, 2008.
- [6] F. Chen, N. Wang, R. German and F. Dressler, "Simulation study of IEEE 802.15.4 LR-WPAN for industrial applications", *Wireless Communication and Mobile Computing*, 2009.
- [7] IEEE Std 802.15.4-2006 — Part 15.4: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), September 2006.
- [8] A. Varga, "The OMNeT++ Discrete Event Simulation System" In *European Simulation Multiconference (ESM 2001)*, Prague, Czech Republic, June 2001.
- [9] J. Ebert, A. Willig, "A Gilbert-Elliot Bit Error Model and the Efficient Use in Packet Level Simulation", TKN Technical Report TKN-99-002, March 1999.
- [10] A. Willig, "Recent and Emerging Topics in Wireless Industrial Communications: A Selection", *IEEE Transactions in Industrial Informatics*, vol. 4, no. 2, May 2008.
- [11] Jennic Wireless Microcontrollers. <http://www.jennic.com/>