A Comprehensive Analysis of the MAC Unreliability Problem in IEEE 802.15.4 Wireless Sensor Networks

Giuseppe Anastasi
Dept. of Information Engineering
University of Pisa, Italy
E-mail: giuseppe.anastasi@iet.unipi.it

Marco Conti
IIT-CNR
National Research Council, Italy
E-mail: marco.conti@iit.cnr.it

Mario Di Francesco
Dept. of Computer Science & Engineering
Univ. of Texas at Arlington, USA
E-mail: mariodf@uta.edu

Abstract – Wireless Sensor Networks (WSNs) represent a very promising solution in the field of wireless technologies for industrial applications. However, for a credible deployment of WSNs in an industrial environment, four main properties need to be fulfilled, i.e., *energy efficiency*, *scalability*, *reliability*, and *timeliness*. In this paper we focus on IEEE 802.15.4 WSNs and show that they can suffer from a serious *unreliability problem*. This problem arises whenever the power management mechanism is enabled for energy efficiency, and results in a very low packet delivery ratio, also when the number of sensor nodes in the network is very low (e.g., 5). We carried out an extensive analysis – based on both simulation and experiments on a real WSN – to investigate the fundamental reasons of this problem, and we found that it is caused by the contention-based MAC (Medium Access Control) protocol used for channel access and its default parameter values. We also found that, with a more appropriate MAC parameters setting, it is possible to mitigate the problem and achieve a delivery ratio up to 100%, at least in the scenarios considered in this paper. However, this improvement in communication reliability is achieved at the cost of an increased latency, which may not be acceptable for industrial applications with stringent timing requirements. In addition, in some cases this is possible only by choosing MAC parameter values formally not allowed by the standard.

Keywords – Wireless Sensor Networks, IEEE 802.15.4, MAC Protocol, Reliability, Timeliness, Energy Efficiency, Scalability

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are one of the most promising solutions in the field of industrial communications [1]. A WSN consists of a number of tiny sensor nodes deployed over a sensing field. Each node is a low power device capable of sensing physical information from the surrounding environment (e.g., temperature, pressure, vibrations), processing the acquired data locally, and sending them to one or more collection points, referred to as *sinks* or *base stations* [2]. Hence, a WSN can be regarded as a distributed sensing system that may be adequate for many monitoring and control applications [1]. Actually, WSNs have been already considered for many industrial applications including: factory automation [3], distributed and process control [4, 5, 6], real-time monitoring of machinery health, detection of liquid/gas leakage, radiation check, and so on [7]. And, based on recent studies [8], their exploitation for industrial applications is expected to increase significantly in the near future, especially in the fields of logistics, automation and control. This positive trend should also be favored by the adoption of two industrial standards, recently released by the IEEE and the ZigBee

Alliance, respectively. The IEEE 802.15.4 standard [9] defines the physical and MAC (Medium Access Control) layers of the protocol stack, while the ZigBee specification [10] covers the networking and application layers.

There are four key requirements that need to be fulfilled for a credible deployment of WSNs in industrial environments, i.e., *energy efficiency*, *scalability*, *reliability* and *timeliness* [1, 11]. *Energy efficiency* is extremely important as sensor nodes are typically powered by batteries – with a limited energy budget – which cannot be replaced nor recharged, due to environmental or cost constraints. Even when batteries can be replenished – e.g., by harvesting energy from the external environment [12] – efficient power management of sensor nodes is required to achieve an adequate network lifetime [13]. To this end, the 802.15.4 standard includes a power management mechanism, based on duty cycle, to minimize the activity of sensor nodes (see Section III). *Scalability* is another important factor to be considered because the number of deployed sensor nodes may be very high, especially when large geographical areas need to be monitored. Finally, *reliability* and *timeliness* are very critical issues in industrial environments. If a given percentage of the data packets is not delivered to the sink, correctly and within a pre-defined deadline, the correct behavior of the sensing system (e.g., the timely detection of an event) can be compromised. The maximum allowed latency depends on the specific application. Typical values are tens of milliseconds for discrete manufacturing, seconds for process control, and minutes for asset monitoring [11]. In the following, we will refer to the capability of meeting specific deadlines – or equivalently, of providing time-bounded latency – as *predictability*.

In an industrial scenario the reliability and/or the predictability can be hindered by a number of factors. First, sensor nodes may undergo failures due to the presence of dust, liquids, corrosive agents, etc. In addition, the quality of wireless communication may be severely affected by multi-path fading in signal propagation and external interferences produced by other devices and machinery operating in the same frequency band of sensor nodes [1, 14, 15, 16, 17]. Finally, data packets containing sensor readings may be dropped, or may experience an excessively long latency, due to congestion phenomena in the WSN. For instance, in WSNs where data transmissions are regulated by a contention-based MAC protocol, a fraction of packets could experience collisions and retransmissions, and could also be dropped by the MAC layer if the number of contending nodes is high. Since this may prevent the WSN from providing the required reliability and bounded latency, also when transmission errors do not occur and sensor nodes never fail, congestion phenomena should be avoided or controlled in an appropriate way.

In this paper we focus on IEEE 802.15.4 WSNs and show that they provide a very low reliability in terms of packet delivery ratio (i.e., the percentage of data packets correctly delivered to the sink node) when power management is enabled. We found that this behavior is caused by the 802.15.4 MAC protocol and therefore, throughout we will refer to it as the *802.15.4 MAC unreliability problem*. Specifically, we found that this problem – which is originated by the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) algorithm used for channel access – becomes critical when power management is enabled due to the default MAC parameters setting suggested by the standard.

Indeed, the IEEE 802.15.4 standard allows some flexibility in choosing CSMA/CA parameters, as it defines a range of allowed values for each of them. Our results show that, with an appropriate parameters setting, it is possible to mitigate the MAC unreliability problem and increase the delivery ratio, up to 100%, at least in the scenarios considered in this paper. However, this is achieved at the cost of a significantly higher latency, which might not be acceptable for industrial applications with stringent timing requirements. In addition, in some scenarios, a high delivery ratio can only be obtained by using CSMA/CA parameter values which are not compliant with the standard.

We validated our simulation results through an extended experimental analysis carried out on a real WSN. The experimental measurements confirm the simulation results and show that the solution envisaged to mitigate the MAC unreliability problem is viable, at least in some application scenarios. To the best of our knowledge, this is the first paper investigating the sensitiveness of the 802.15.4 performance to the CSMA/CA parameters setting, by using both simulation and measurements on a real WSN.

The rest of the paper is organized as follows. Section II discusses the related work. Section III introduces the 802.15.4 MAC protocol, while Section IV describes the simulation setup used for our analysis. Section V shows the effects of the 802.15.4 MAC unreliability problem. Section VI analyzes the impact of each single MAC parameter, while Section VII presents a possible solution to mitigate the problem. Section VIII discusses the results of the experimental analysis. Finally, conclusions are drawn in Section IX.

II. RELATED WORK

Many previous papers concerning WSNs focus on the 802.15.4 standard, which is considered the reference technology in the field, and is expected to have a significant impact also on industrial applications [1]. However, the suitability of the 802.15.4 MAC protocol for WSNs, with specific reference to industrial scenarios, has never been extensively analyzed. Actually, many papers are targeted to assess the performance of the 802.15.4 MAC protocol, mainly in terms of throughput and energy expenditure. But, in many cases they approach the problem analytically and, hence, introduce some assumptions to simplify the analysis. For example, [18] and [19] assume exponentially-distributed packet generation times, and do not consider the case of simultaneous transmission attempts by all – or many – sensor nodes (e.g., after an inactive period). Under these conditions, they do not observe any MAC unreliability problem (our simulation results also confirm that, under the same conditions, the delivery ratio is close to 100%). More realistic scenarios have been considered in [20, 21, 22, 23]. These papers investigate different aspects related to the performance of the 802.15.4 MAC. However, they too do not find out any severe limitation in the MAC protocol, especially in terms of reliability.

The limited scalability of the 802.15.4 MAC is pointed out by Yedavalli et al. [24] who analyze the performance in terms of throughput and energy consumption. They show that the 802.15.4 MAC performs very poorly when the number of contending nodes is high. However, they do not investigate the impact of the different MAC parameters. Instead, they propose an enhanced MAC protocol with better scalability properties.

Misic et al. [25] identify a number of potential issues that can degrade the performance of the MAC protocol, including possible congestions caused by the simultaneous attempts of several nodes to access the wireless medium after an inactive period. As in [24], they also propose some changes in the standard MAC protocol to overcome these issues, e.g., by introducing a random delay before the channel access to avoid possible congestions after an inactive period. We show here that this problem can be simply overcome with an appropriate setting of CSMA/CA parameters, without introducing any modification to the MAC protocol.

Issues related to the MAC unreliability, in terms of packet drop probability, have been addressed in [26, 27, 28, 29]. Shu et al. [26] consider a star network and assume that (**i**) all nodes attempt to transmit a packet at the beginning of the active period and, (**ii**) the acknowledgment mechanism is disabled. They show that the packet drop probability can be extremely high in this scenario, especially for large number of sensor nodes and packet sizes. However, they do not consider the effects of using acknowledgements and retransmissions. In addition, they miss to investigate the fundamental reasons for this behavior and, consequently, they do not propose any possible solution to fix or, at least, alleviate this problem.

Both [27] and [28] also consider a star network topology and analyze the MAC protocol performance under the assumption that each sensor node has an infinite backlog of packets to send (saturated traffic conditions). They both find out that, under these conditions, a large fraction of packets is dropped during the channel access, and the drop probability increases with the number of sensor nodes. Pollin et al. [28] suggest using a larger exponential backoff delay to alleviate the problem. Similarly, Singh et al. [27] show that using larger backoff parameter values can provide a significant decrease in the packet drop probability, at the cost of a decreased throughput when the number of nodes is low. In both cases, however, the focus of the analysis is on the maximum achievable throughput and energy consumption. Therefore, the high packet discard probability is not recognized as a major limitation, and is only marginally addressed by the authors.

Park et al. [29] also consider a star network topology and develop an accurate analytical model of the 802.15.4 MAC protocol in the beacon enabled mode. They explicitly consider the limited number of backoff stages and retransmissions, and derive the delivery ratio, average latency and power consumption as functions of the offered load and different MAC parameters. The authors show that, under saturated (or very high) traffic conditions and large number of nodes, the delivery ratio can be low. They also show its dependency on different MAC parameters. However, since the analysis mainly focuses on the unsaturated traffic regime, saturated traffic is considered an extreme scenario. In addition, the performance analysis is mainly targeted at validating the accuracy of the proposed model. Hence, as above, the authors do not emphasize any MAC unreliability problem and, consequently, they do not investigate its causes nor propose any solution to it. In this paper we investigate thoroughly the fundamental reasons for the MAC unreliability problem, and propose a solution for its mitigation. Unlike [24] and [25], we do not propose any modification to the standard MAC protocol. Instead, we show that the MAC unreliability problem can be mitigated by an appropriate setting of CSMA/CA parameters.

Strategies for tuning the 802.15.4 CSMA/CA algorithm are considered in [30] and [31]. Specifically, Nefzi et al. [30] introduce a service differentiation strategy, consisting in defining both CSMA/CA parameter sets (i.e., minimum and maximum backoff exponents, and the contention window size) and queuing policies so as to prioritize specific classes of traffic. However, since the focus is on message prioritization, little attention is devoted to reliability and energy expenditure. In addition, only a few CSMA/CA parameters are considered, and acknowledgements are not used. Youn et al. [31] propose a message prioritization mechanism exploiting a Gaussian distribution for the backoff procedure.

Although the proposed solution might be compatible to commercially-available transceivers, it is actually not compliant with the 802.15.4 standard, since the backoff procedure is different. On the other hand, our solution is fully compatible with the 802.15.4 standard, and can be used also in sensor nodes where the MAC protocol cannot be changed.

In the present paper we extend our previous analysis of the 802.15.4 MAC protocol where an ideal wireless channel was assumed [32]. In this paper we specifically refer to an industrial environment and, thus, we consider a more realistic scenario where wireless communication may be affected by (correlated) transmission errors due to fading and interference. In addition, while the analysis in [32] is almost completely based on simulation, in this paper we also reported experimental results derived from measurements on a real WSN. For the sake of space we only refer to a star network topology. Additional results for a cluster-tree (i.e., multi-hop) topology can be found in [33].

The effects of external interferences produced by other devices or machinery on the performance of an 802.15.4 WSN have been experimentally investigated by Bertocco el al. [17]. However, they consider an application-layer polling-based protocol for periodic data collection from sensor nodes and, hence, they do not specifically address issues related to the 802.15.4 MAC protocol. Using an application-layer protocol for data collection is a very common approach in industrial applications. Nevertheless, we think it is very important for industrial application developers to know the limits and capabilities of the underlying MAC protocol. To the best of our knowledge, this is the first paper investigating the sensitiveness of the 802.15.4 WSN performance to the MAC protocol parameters setting, by using both simulations and measurements on a real WSN.

III. IEEE 802.15.4 STANDARD

IEEE 802.15.4 [9] is a standard for low-rate, low-power, and low-cost Personal Area Networks (PANs). A PAN is formed by one PAN coordinator which is in charge of managing the whole network, and, optionally, by one or more coordinators which are responsible for a subset of nodes in the network. Ordinary nodes must associate with a (PAN) coordinator in order to communicate. The supported network topologies are *star* (single-hop), *cluster-tree* and *mesh* (multi-hop).

The standard defines two different channel access methods: a *beacon enabled* mode and a *non-beacon enabled* mode. The beacon enabled mode provides a power management mechanism based on a duty cycle. It uses a superframe structure (see Figure 1) which is bounded by *beacons*, i.e., special synchronization frames generated periodically by the coordinator node(s). The time between two consecutive beacons is called *Beacon Interval* (*BI*), and is defined through the *Beacon Order* (*BO*) parameter (BI=15.36·2^{BO} ms, with 0≤BO≤14)[1]. Each superframe consists of an active period and an inactive period. In the active period nodes communicate with the coordinator they associated with, while during the inactive period they enter a low power state to save energy. The active period is denoted as *Superframe Duration* (*SD*) and its size is defined by the *Superframe Order* (*SO*) parameter (SD=15.36·2^{SO} ms, with 0≤SO≤BO≤14). It can be further divided into a *Contention Access Period* (*CAP*) and a *Collision Free Period* (*CFP*). During the CAP a slotted CSMA/CA algorithm is used for channel access, while in the CFP communication occurs in a TDMA (Time Division Multiple Access) style by using a number of *Guaranteed Time Slots* (GTSs), pre-assigned to individual nodes. In the non-beacon enabled mode there is no superframe, nodes are always active (energy conservation is delegated to the layers above the MAC protocol) and use the unslotted CSMA/CA algorithm for channel access.

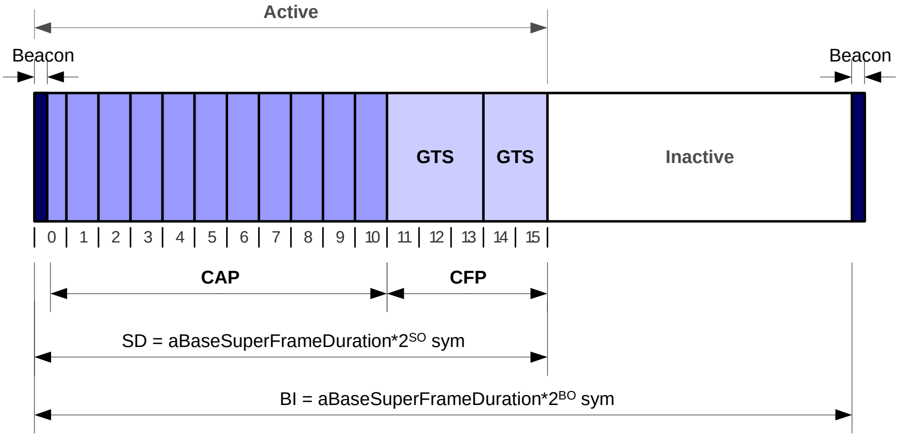

Active
Beacon
Beacon
GTS
GTS
Inactive
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
CAP
CFP
SD = aBaseSuperFrameDuration*2^SO sym
BI = aBaseSuperFrameDuration*2^BO sym

Figure 1. IEEE 802.15.4 Superframe Structure.

A. CSMA/CA algorithm

The CSMA/CA algorithm is used in both the *beacon enabled* mode (during the CAP portion of the active period) and the *non-beacon enabled* mode. In the beacon-enabled mode a slotted scheme is used – i.e., all operations are aligned to backoff period slots (whose duration is 320µs) – while in the non-beacon enabled mode there is no such alignment. For brevity, in the following we will refer to the slotted scheme, highlighting the differences in the unslotted variant, when necessary.

Upon receiving a data frame to be transmitted, the CSMA/CA algorithm performs the following steps.

[1] Throughout the paper we assume that the sensor network operates in the 2.4 GHz frequency band.

1. A set of state variables is initialized, i.e., the contention window size (*CW*=2, only for the slotted variant), the number of backoff stages carried out for the on-going transmission (*NB*=0), and the backoff exponent (*BE*=*macMinBE*).

2. A random backoff time, uniformly distributed in the range [0, $320\cdot(2^{BE}-1)$ μs], is generated and used to initialize a backoff timer. In the beacon-enabled mode, the starting time of the backoff timer is aligned with the beginning of the next backoff slot. In addition, if the backoff time is larger than the residual CAP duration, the backoff timer is stopped at the end of the CAP and resumed at the beginning of the next superframe. When the backoff timer expires, the algorithm proceeds to step 3.

3. A Clear Channel Assessment (CCA) is performed to check the state of the wireless medium.

   a) If the medium is busy, the state variables are updated as follows: *NB*=*NB*+1, *BE*=min(*BE*+1, *macMaxBE*) and *CW*=2 (only for the slotted variant). If the number of backoff stages has exceeded the maximum admissible value (i.e. *NB*>*macMaxCSMABackoffs*), the frame is dropped. Otherwise, the algorithm falls back to step 2.

   b) If the medium is free and the access mode is unslotted, the frame is immediately transmitted.

   c) If the medium is free and the access mode is slotted, then *CW*=*CW*-1. If *CW*=0 then the frame is transmitted[2]. Otherwise the algorithm falls back to step 3 to perform a second CCA.

It should be noted that, unlike the algorithm used in 802.11 WLANs, the 802.15.4 slotted CSMA/CA does not guarantee a transmission at the end of the backoff time after the channel is found clear. Instead, transmission occurs only if the wireless medium is found free for two consecutive CCAs.

The 802.15.4 CSMA/CA algorithm supports an optional retransmission scheme based on acknowledgements and timeouts. When the retransmission mechanism is enabled, destination nodes must send an acknowledgement just after receiving a correct data frame. The acknowledgement is not sent in case of collision and corrupted frame reception. On the sender side, if the acknowledgment is not (correctly) received within the pre-defined timeout, a retransmission is scheduled until the maximum number of retransmissions (*macMaxFrameRetries*) is reached. In the latter case the data frame is dropped.

[2] In the beacon-enabled mode, before starting the frame transmission, the algorithm calculates whether it is able to complete the operation within the current CAP. If there is not enough time, the transmission is deferred to the next superframe.

IV. SIMULATION ENVIRONMENT

To perform our simulation analysis we used the ns2 simulation tool [34], which includes the 802.15.4 module originally developed in [21] and the modifications in [35]. In all experiments we assumed that the 802.15.4 MAC protocol is operating on top of the 2.4 GHz physical layer, with a 250-Kbps maximum bit rate. The transmission range was set to 15 m (according to the settings in [21]), while the carrier sensing range was set to 30 m (according to the model in [36]).

In our experiments we considered a star network scenario where the sink node acts as the PAN coordinator and all other nodes operate with a duty cycle for power management. Sensor nodes are placed in a circle centered at the sink node, 10 m far from it. Due the considered radio model (the carrier sensing range is twice the transmission range), *all* nodes are in the carrier sensing range of each other. This minimizes the probability of collisions due to the hidden node problem [37]. The network uses the beacon-enabled mode. The duty cycle is set to about 1.5%, according to the typical values recommended by the ZigBee standard [10] which are in the range 0.1% - 2%. Specifically, the Beacon Interval is 125.8 s (BO=13), while the active period is 1.97 s (SO=7). Note that the active period is large enough to let every node send its data packets in all the analyzed scenarios, so that the enforced duty cycle does not harm the packet transmission process.

To simulate realistic packet errors/losses we used the Gilbert-Elliot model, which has been shown to provide a good approximation of fading in industrial environments [14, 15, 16]. In addition, this model has been used in a number of previous performance analysis of industrial wireless systems and networks (e.g., [38, 39, 40]). In our analysis we took an approach similar to [39] and [40], and used values inspired from real measurements [14]. Unless differently specified, we assumed a packet error rate (PER) of approximately 10%. Specifically, the PER in the bad and good state of the Gilbert-Elliot model is assumed to be 100% and 0%, respectively. Sojourn times in the two states are exponentially distributed and their average values are 5.7 and 46.2 ms, for bad and good state, respectively. To broaden our analysis, in some experiments we also considered different values of PER. These values were obtained by changing the average sojourn time in the bad state accordingly, while leaving all the other parameters unchanged.

We considered a reporting application where sensed data have to be reported to the sink periodically, which is a very common case in monitoring applications. However, for comparison purposes, we also considered a Poisson data generation process. Unless stated otherwise, acknowledgements are enabled and every sensor node generates one data packet per Beacon Interval (on average when the generation process is Poisson). The packet size – corresponding to the MAC frame payload – is 100 bytes, while the MAC frame header is 7 bytes[3].

A. Performance Indices

In our analysis we considered the following indices.

- *Delivery ratio*, defined as the ratio between the number of data packets correctly received by the sink and the total number of data packets generated by *all* sensor nodes. This index jointly represents the network *reliability* as well as the *scalability* of the data collection process.
- *Latency*, defined as the time from when the packet transmission is started at the source node to when the same packet is correctly received by the sink. We measured both its average value and its distribution. Latency characterizes the *timeliness* of the system.
- *On-time delivery ratio*, defined as the percentage of packets received correctly *and* within a certain pre-defined deadline. For delay-bounded applications the on-time delivery ratio (or, correspondingly, the *deadline miss ratio)*, provides the fraction of packets delivered on time (or missing the deadline). Hence, it combines both *reliability* and *predictability*.
- *Average energy per packet*, defined as the total energy consumed by each sensor node divided by the number of data packets correctly delivered to the sink. This index measures the *energy efficiency* of the WSN.

The energy consumed by a sensor node was calculated by using the model presented in [41], which is based on the Chipcon CC2420 radio transceiver [42]. Specifically, the model supports the following radio states: *transmit*, *receive*, *idle* (the transceiver is on, but it is not transmitting nor receiving, i.e., it is monitoring the channel) and *sleep* (the transceiver is off and can be switched back on quickly). In addition, the model accounts for the energy spent due to state transitions as well. Although the standard does not explicitly state when the transceiver should be sleeping – except for the inactive portion of the superframe when the beacon-enabled mode is used – to further improve the energy efficiency we put the transceiver into the sleep state when there is no packet to be transmitted, as proposed in [19].

In our experiments, for each simulated scenario, we performed 10 independent replicas, where each replica consists of 1000 Beacon Intervals. For each replica we discarded the initial transient period

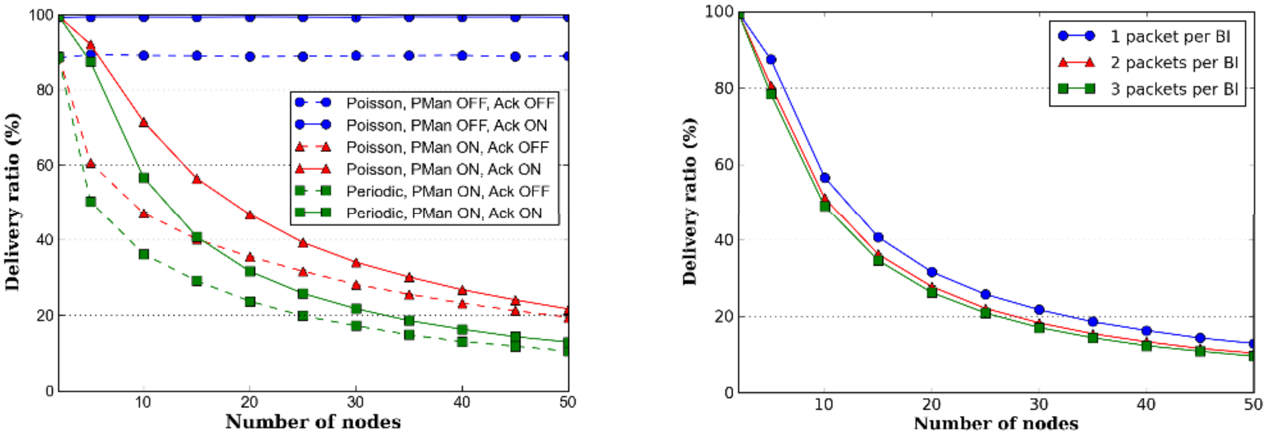
[3] In the following we assume that IEEE 802.15.4 short addresses are used, thus requiring 4 bytes in the MAC header.

(10% of the overall duration) during which nodes associate to the PAN coordinator and start generating data packets. The results shown below are averaged over all the different replicas. We also derived confidence intervals by using the independent replication method and a 95% confidence level. They are typically so small that they cannot be appreciated in the figures below.

V. THE MAC UNRELIABILITY PROBLEM

Many previous works [18, 19, 23, 27] have analyzed the performance of the 802.15.4 MAC protocol in a star network under the assumption that sensor nodes are *always* active (i.e., power management is disabled), and data packets are generated according to a *Poisson* process. Therefore, we start our analysis by comparing the MAC performance under Poisson and Periodic traffic patterns, when power management is enabled and disabled.

Figure 2-a shows the delivery ratio – as a function of the number of sensor nodes – for Periodic and Poisson packet arrivals, when the power management mechanism is enabled (PMan ON) and disabled (PMan OFF). The effects of packet retransmissions are also shown. Specifically, when packets are generated according to the Poisson distribution and power management is disabled (i.e., sensor nodes are always active), the delivery ratio is around 90% if acknowledgements and retransmissions are not used (Ack OFF). This is due to the effect of packet errors (PER is equal to 10%). The retransmission mechanism (Ack ON) allows to recover almost all corrupted packets, thus increasing the delivery ratio to approximately 100%.



(a) **(b)**

Figure 2. Delivery ratio in a star network with Poisson and Periodic traffic, when the power management is enabled and disabled (a). Impact of the packet generation rate on the delivery ratio (b).

When the arrival process is still Poisson but power management is enabled, the delivery ratio drops sharply with the number of nodes. The delivery ratio is even lower if the arrival process is Periodic instead of Poisson. As expected, in both cases retransmissions increase the communication reliability. However, when the number of nodes is high (e.g. 50), the delivery ratio is anyway very low, i.e., around 10% and 20% with Periodic and Poisson traffics, respectively.

For Poisson arrivals, the very different behavior – with and without power management – can be explained as follows. When nodes are always active, packets are transmitted immediately after their generation. Since generation times are spread along the Beacon Interval there is almost no contention among sensor nodes. Instead, when power management is enabled, the packets generated during the sleeping time are deferred to the beginning of the next Active Period, when all nodes wake up at the same time. Therefore, channel access attempts tend to become synchronized. If the data generation process is Periodic (instead of Poisson), packets are generated just before the beginning of the Active Period so as to minimize the latency. Hence, channel accesses are perfectly synchronized and this increases contention among nodes.

We also considered different values of the Beacon Interval while leaving the Active Period constant, i.e., we varied the duty cycle. We found that the delivery ratio does not depend on the Beacon Interval when the arrival process is Periodic. Instead, it is significantly affected when packets are generated according to Poisson. In the latter case, for a fixed number of nodes, the delivery ratio is close to 100% (90% if the retransmission mechanism is disabled) when the Beacon Interval is small – i.e., the duty cycle is high – and decreases progressively as the Beacon Interval increases. The different behavior can be easily explained. When packets are generated periodically, *all* nodes contend for channel access at the beginning of the Active Period. In case of Poisson traffic, since packet arrivals are spread along the Beacon Interval, *not all* nodes have to contend at the beginning of the Active Period. In detail, only nodes which generated packets during their sleeping time contend simultaneously at the beginning of the Active Period. This condition is more likely to happen when the relative duration of the Active Period with respect to the Beacon Interval is low.

The results in Figure 2-a clearly point out that the 802.15.4 MAC protocol is not able to manage contentions efficiently, even when a limited number of nodes try to access the wireless channel simultaneously, e.g., due to power management. Throughout, we will refer to this issue as the *802.15.4 MAC unreliability problem*. Its impact on performance is strongly affected by the data traffic pattern, i.e., for a given number of sensor nodes, the unreliability increases as the number of simultaneously contending nodes increases.

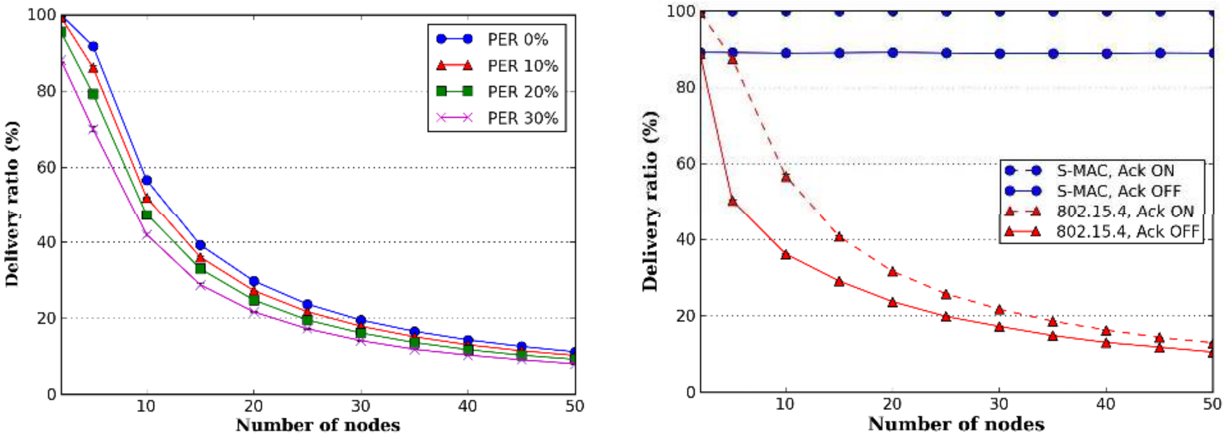
To broaden our analysis we investigated the impact on the MAC unreliability problem of a number of additional operating parameters such as packet generation rate, packet size, packet error rate. In all subsequent experiments we only considered the Periodic packet generation process – as this it more realistic than Poisson for (periodic) reporting applications – and assumed that the acknowledgement/retransmission mechanism is always enabled (unless differently specified).

Figure 2-b shows that, as expected, the MAC unreliability becomes more and more serious as the packet generation rate, i.e., the offered load, increases. It is worthwhile emphasizing that 50 nodes generating three 100-byte packets per Beacon Interval produce an aggregate offered load of approximately 70 Kbps[4]. On the other side, the network data rate is 250 Kbps and the maximum throughput that can be achieved with the 802.15.4 MAC protocol is about 140 Kbps [43]. Also, the overall number of packets generated by all sensor nodes during each Active Period (150 in the case of 3 packets per Beacon Interval) is much lower than the total number of packets that could be transmitted during an Active Period using an ideal transmission schedule. In the latter case packets are transmitted back-to-back, and the total time required for transmitting a single packet is $D_{tot} = D_{frame} + aTurnaroundTime + D_{ack} + LIFS$, where D_{frame} (D_{ack}) is the data (ack) frame transmission time, *aTurnaroundTime* is the delay for switching the transceiver from transmit to receive mode, and *LIFS* is the duration of a Long Inter Frame Space [9]. In our scenario[5] it turns out D_{tot} = 4.864 ms (4.320 ms if acknowledgements are disabled) and, consequently, the total number of packets that could be accommodated within an Active Period (1.966s) is approximately 404 (455 without acknowledgements). Hence, assuming a packet generation of 3 packets per Beacon Interval, up to 134 or 151 sensor nodes (with and without acknowledgements, respectively) could be theoretically supported by an ideal transmission schedule.

We also investigated the effect of varying the packet size, while leaving the packet generation rate unchanged. The trend is similar to that shown in Figure 2-b (the results are not shown here for the sake of space). This is because the offered load tends to increase in both cases.

[4] We considered an overall packet size of 115 bytes (6-byte PHY header + 7-byte MAC header + 100-byte payload + 2-byte MAC trailer). The Active Period is 1.966s.

[5] We considered D_{frame} = 3.68 ms (6-byte PHY header + 7-byte MAC header + 100-byte payload + 2-byte MAC trailer), D_{ack} = 0.352 ms (6-byte PHY header + 5-byte MAC header and trailer), *aTurnaroundTime* = 0.192 ms, *LIFS* = 0.640 ms. We used the Long Inter Frame Space as the frame size is more than 18 bytes [9].



(a) **(b)**

Figure 3. Impact of Packet Error Rate on the delivery ratio (a) and comparison with S-MAC (b).

Finally, we varied the PER in the range [0-30] % to analyze the effects of (correlated) transmission errors on the MAC performance. As expected, Figure 3-a shows that the MAC unreliability increases as the PER increases, since the source sensor nodes have to retransmit more frames. We can also observe that the impact of transmission errors is much more apparent when the number of sensor nodes is low. This is because, when the number of nodes is large and for a given PER value, the effects of congestion predominate over those originated by transmission errors.

The results presented above show that the 802.15.4 MAC has a very poor performance, in terms of delivery ratio, in the considered scenario. In our analysis we referred to a star network topology. However, similar conclusions are also drawn in [33] where a cluster-tree (i.e., multi-hop) topology is considered. It is well known that CSMA-based MAC protocols do not perform well when a large number of sensor nodes start transmitting simultaneously [44]. However, this well-known problem is much more severe in the 802.15.4 MAC than in other similar MAC protocols, as highlighted in Figure 3-b. There, we compare the performance of the 802.15.4 MAC with that of S-MAC [45], another very popular contention-based MAC protocol for WSNs. S-MAC is based on the well-known 802.11 CSMA/CA algorithm [46] for regulating channel access. As above, all sensor nodes start transmitting simultaneously. We can see that, in the same operating conditions, S-MAC is able to provide a 100% delivery ratio, irrespective of the number of nodes, if the retransmission mechanism is enabled.

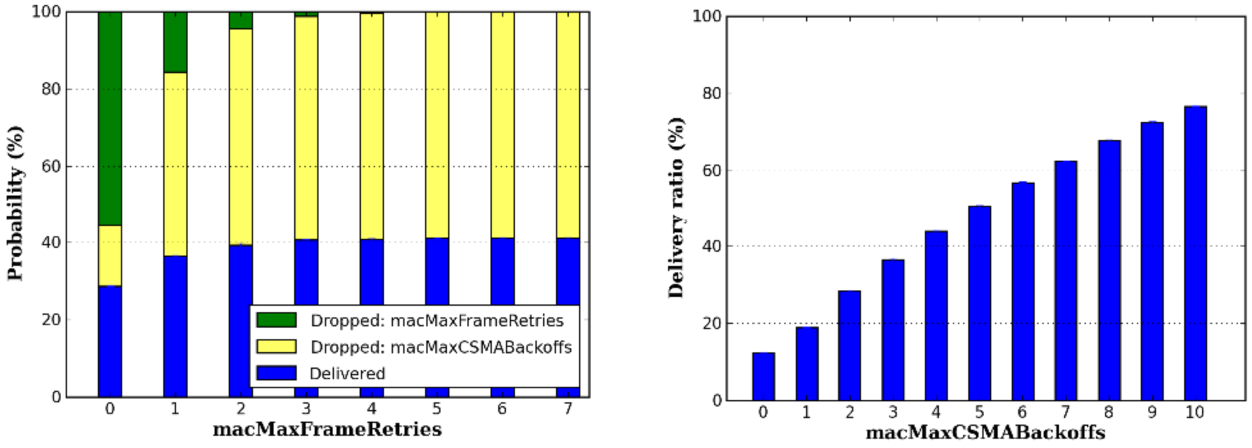
VI. IMPACT OF CSMA/CA PARAMETERS

The results presented in the previous section showed that the MAC unreliability problem in 802.15.4 WSNs is much more severe than in other contention-based WSNs, and it can seriously degrade the performance of the data collection process. Thus, it is very important to properly understand the fundamental reasons of this behavior so as to mitigate its negative effects. To this end, we performed a thorough simulation analysis to investigate the impact of each single CSMA/CA parameter. Table 1 summarizes the parameters introduced in Section III and the related ranges and default values defined in the standard. For completeness, Table 1 refers to both the 2003 and 2006 standard releases but in our analysis we only referred to the most recent release.

TABLE 1. 802.15.4 CSMA PROTOCOL PARAMETERS

Parameter	Allowed Values		Description
	2003 Release [47]	2006 Release [9]	
macMaxFrameRetries	Constant: 3 (*aMaxFrameRetries*)	Range: 0-7 **Default: 3**	Maximum number of retransmissions
macMaxCSMABackoffs	Range: 0-5 Default: 4	Range: 0-5 **Default: 4**	Maximum number of backoff stages
macMaxBE	Constant: 5 (*aMaxBE*)	Range: 3-8 **Default: 5**	Maximum backoff window exponent
macMinBE	Range: 0-3 Default: 3	Range: 0-7 **Default: 3**	Minimum backoff window exponent

We focused on a star network with 15 sensor nodes and PER=10%, and evaluated the impact of each single MAC parameter, not only in terms of delivery ratio, but also in terms of energy efficiency and latency experienced by data packets. For the sake of space, we only show the delivery ratio below. Since the general trend is similar to that observed in ideal channel conditions, the reader can refer to [32] for a more detailed analysis of the impact of each single parameter on the 802.15.4 MAC performance.

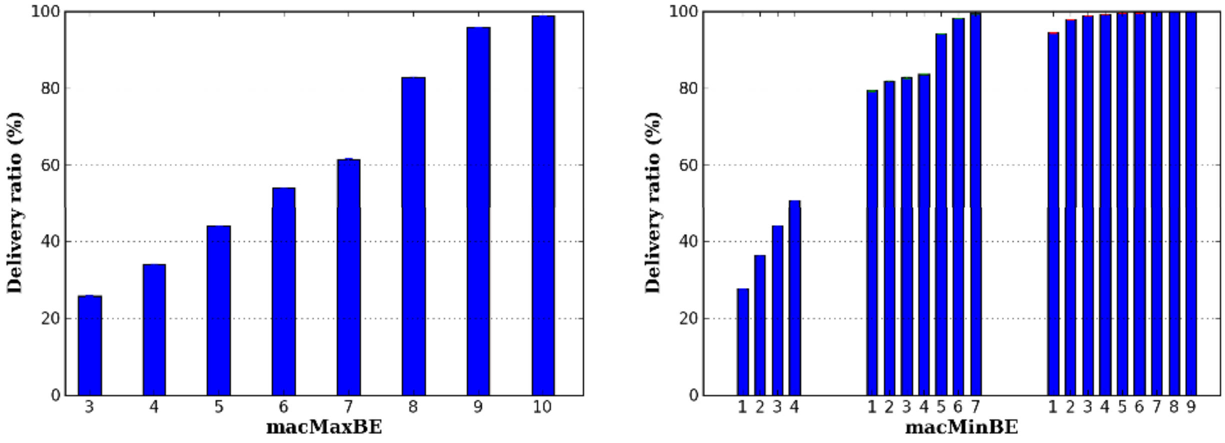


(a) **(b)**

Figure 4. Delivery ratio and packet dropping probability vs. maximum number of retransmissions (a). Impact of macMaxCSMABackoff on the delivery ratio (b).

Figure 4-a shows that increasing the maximum allowed number of retransmissions – i.e., the *macMaxFrameRetries* parameter (while leaving all other parameters to their default values) – does not provide any significant effect on the delivery ratio for values larger than one. This is because almost all undelivered packets are dropped by the MAC protocol because of the exceeded number of backoff stages (the maximum allowed values is specified by the *macMaxCSMABackoffs* parameter, set to 4 by default). As clearly shown in Figure 4-a, the percentage of packets discarded for exceeded number of retransmissions is negligible when *macMaxFrameRetries* ≥ 2. We found that a higher number of retransmissions can be beneficial only when the PER is very high (e.g., 30% and beyond) and the number of sensor nodes large (e.g., 30 or more).

Based on the results in Figure 4-a, we would expect that an increase in the maximum number of allowed backoff stages produce a significant impact on the MAC reliability. Actually, increasing the *macMaxCSMABackoffs* parameter – while leaving all other parameters to their default values – results in an almost linear increase in the delivery ratio (see Figure 4-b). Furthermore, in these experiments we also observed a better energy efficiency, at the cost of an increased latency experienced by packets. The latency increases because a larger number of packets is successfully transmitted, which takes more time. At the same time, the average energy consumption per packet decreases (significantly) because this larger number of successful transmissions only requires a limited amount of additional energy. The results presented in Figure 4-b show that increasing the *macMaxCSMABackoffs* parameter produces a significant increase of the delivery ratio but, also for large *macMaxCSMABackoffs* values, it remains well below 100%.



(a) **(b)**

Figure 5. Inpact on the delivery ratio of macMaxBE (a) and macMinBE (b).

Figure 5-a shows the effects of increasing the maximum backoff-window size (through the *macMaxBE* parameter), while leaving the maximum number of retransmissions and the minimum window size (i.e., the *macMinBE* parameter) to their default values. Now the delivery ratio increases up to values very close to 100%. This is due to the combined effect of a larger backoff window size and a higher number of backoff stages, which are bounded by the following constraint[6]:

$$macMaxCSMABackoffs \geq macMaxBE - macMinBE \qquad (1)$$

Due to motivations similar to the ones we have already discussed, the packet latency increases accordingly, while the energy consumption per packet decreases significantly.

Finally, we fixed *macMaxBE* and varied *macMinBE* in the range [1, *macMaxBE*-1], while leaving *macMaxFrameRetries* to its default value. Figure 5-b, which refers to three different values of *macMaxBE* (i.e., 5, 8, and 10), shows that increasing the minimum backoff-window size further increases the delivery ratio, up to 100%. This is because a larger initial backoff window reduces the collision probability in the first backoff stages. As above, the latency experienced by packets increases while the average energy consumed per packet correctly delivered to the sink node decreases.

Based on the above-mentioned results, the following conclusions can be drawn. The MAC reliability can be improved – up to a 100% delivery ratio – by increasing one or more MAC parameters, as this spreads the transmission attempts of different sensor nodes over a longer time interval, thus reducing the number of simultaneously contending nodes, and increases the number of allowed trials per packet. The cost to be paid is an increase in the latency experienced by packets while the average energy per packet reduces, even significantly. An increased latency may be a problem in many delay-bounded industrial applications, where packets must be delivered within a predefined deadline. These conclusions suggest that the MAC unreliability problem, which is originated by the CSMA/CA algorithm, is made worse by the default parameters setting, which appears to be not appropriate for WSNs with power management enabled. The key question to answer is, thus, whether a more appropriate parameters setting can mitigate the problem without introducing unacceptable side effects (e.g., excessive latency). This will be investigated in the next section.

[6] In order to satisfy Constraint (1) for all evaluated values of *macMaxBe* and *macMaxBE*, in the simulation we set *macMaxCSMABackoffs* to 10.

VII. PROBLEM MITIGATION

To answer the previous question we considered three different sets of CSMA/CA parameter values, summarized in Table 2, and defined as follows.

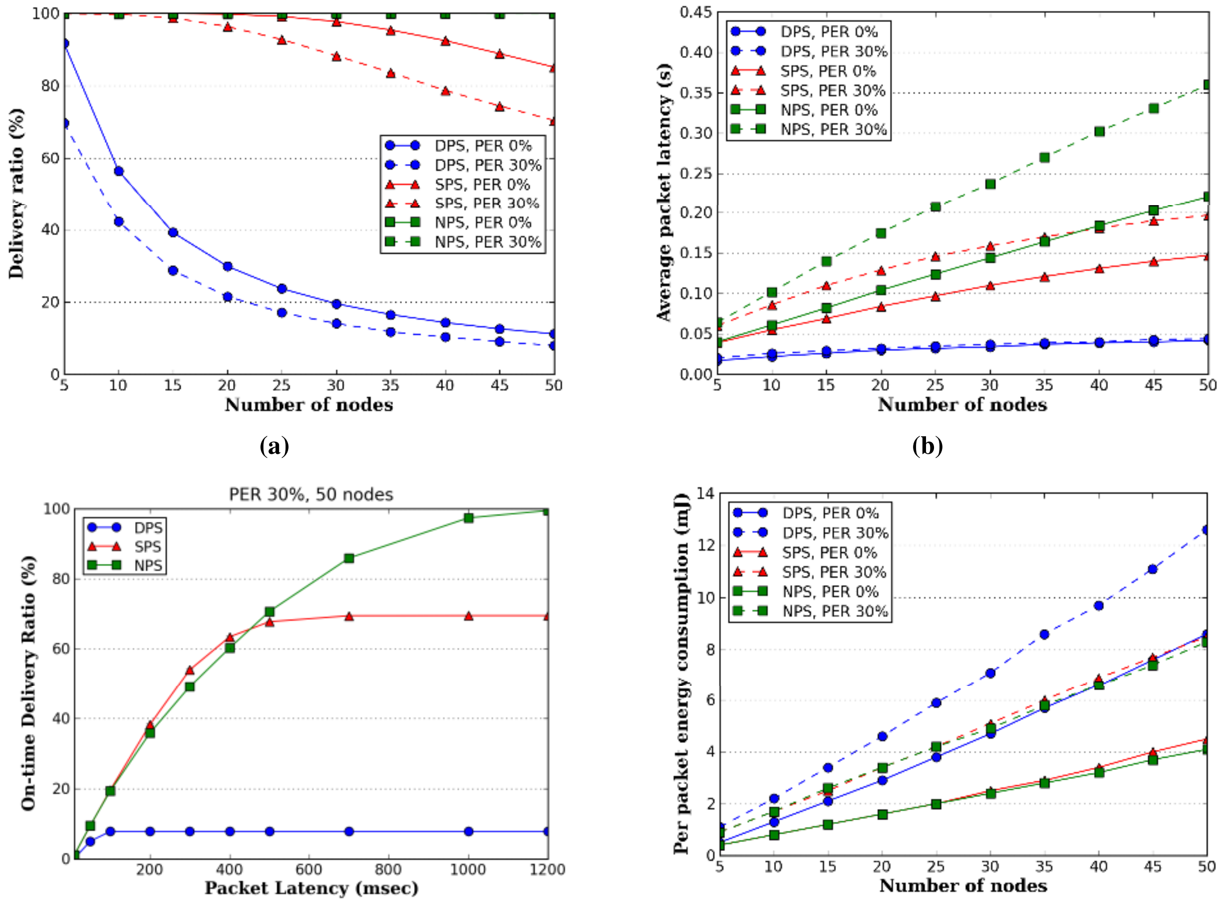
- *Default Parameters Set (DPS).* This set consists of the default values specified by the standard.
- *Standard Parameters Set (SPS).* This set consists of parameter values still compliant with the 802.15.4 standard (2006 release). Specifically, all parameters are set to the corresponding maximum value allowed by the standard (see Table 2).
- *Non-standard Parameters Set (NPS).* This set of parameter values is not compliant with the 802.15.4 standard. In particular, all parameters are set to values beyond the maximum ones allowed by the standard (see Table 2).

TABLE 2. CSMA/CA PARAMETER SETS

Parameter set	*macMinBE*	*macMaxBE*	*macMaxCSMABackoffs*	*macMaxFrameRetries*
DPS	3	5	4	3
SPS	7	8	5	7
NPS	8	10	10	10

Below, we will consider again the star network scenario analyzed in Section V, and will re-derive the performance, under the three CSMA/CA parameter sets defined above, for two different PER values (0% and 30%). The four plots in Figure 6 show how the different performance indices change when passing from one parameter set to another. In terms of delivery ratio (Figure 6-a), there is a dramatic increase when moving from DPS to SPS. However, the delivery ratio remains significantly below 100% when the number of sensor nodes is large and/or the channel is very unreliable. Instead, when using the non-standard parameter set (i.e., NPS) the delivery ratio is approximately 100% even in such extreme conditions. Obviously, this increase in the delivery ratio comes at the cost of a larger packet latency.

Figure 6-b shows that, with 50 nodes and PER=30%, the average latency increases from 50 ms (DPS) to 200 ms (SPS) and more than 350 ms (NPS). We also found that the 99-th percentile of the latency distribution with SPS and NSP, is approximately 0.7s and 1.2s, respectively. These values are clearly unacceptable for many industrial applications, where packets must be delivered within a certain deadline. Therefore, for this specific scenario, we measured the fraction of packets delivered on time, as a function of the maximum latency tolerated by the application. Figure 6-c shows that, while it is always convenient using parameter values larger than the default ones, using very large values might not be so convenient, depending on the type of industrial application [11]. For example, when the deadline is less than or equal to 100 ms, the fraction of packets delivered on time is below 20%, irrespective of the parameter set.



(a)

(b)

(c)

(d)

Figure 6. Delivery ratio (a), average latency (b), on-time delivery ratio (c), and energy efficiency (d) with DPS, SPS and NPS sets.

Passing from DPS to SPS and NPS also increases the total energy consumption as a larger number of packets are transmitted by sensor nodes. However, if we look at the average energy consumption per packet (Figure 6-d), instead of the total energy consumption, there is a significant decrease when passing from DPS to SPS (from 12.6 mJ/packet to approximately 8 mJ/packet, with 50 nodes and PER=30%). This is because the additional energy consumption is largely compensated by the significant increase in the number of (correctly) delivered packets. We can observe a slight decrease also when passing from SPS to NPS. However, the results in Figure 6-d do not consider any constraints in the maximum latency tolerated by the application. This is not the case for time-bounded applications. For instance, assuming a maximum latency of 100 ms, both SPS and NPS deliver approximately 20%

of packets on time. However, the energy cost for each packet delivered on time is, on average, 30.1 mJ with SPS and 41.9 mJ with NPS.

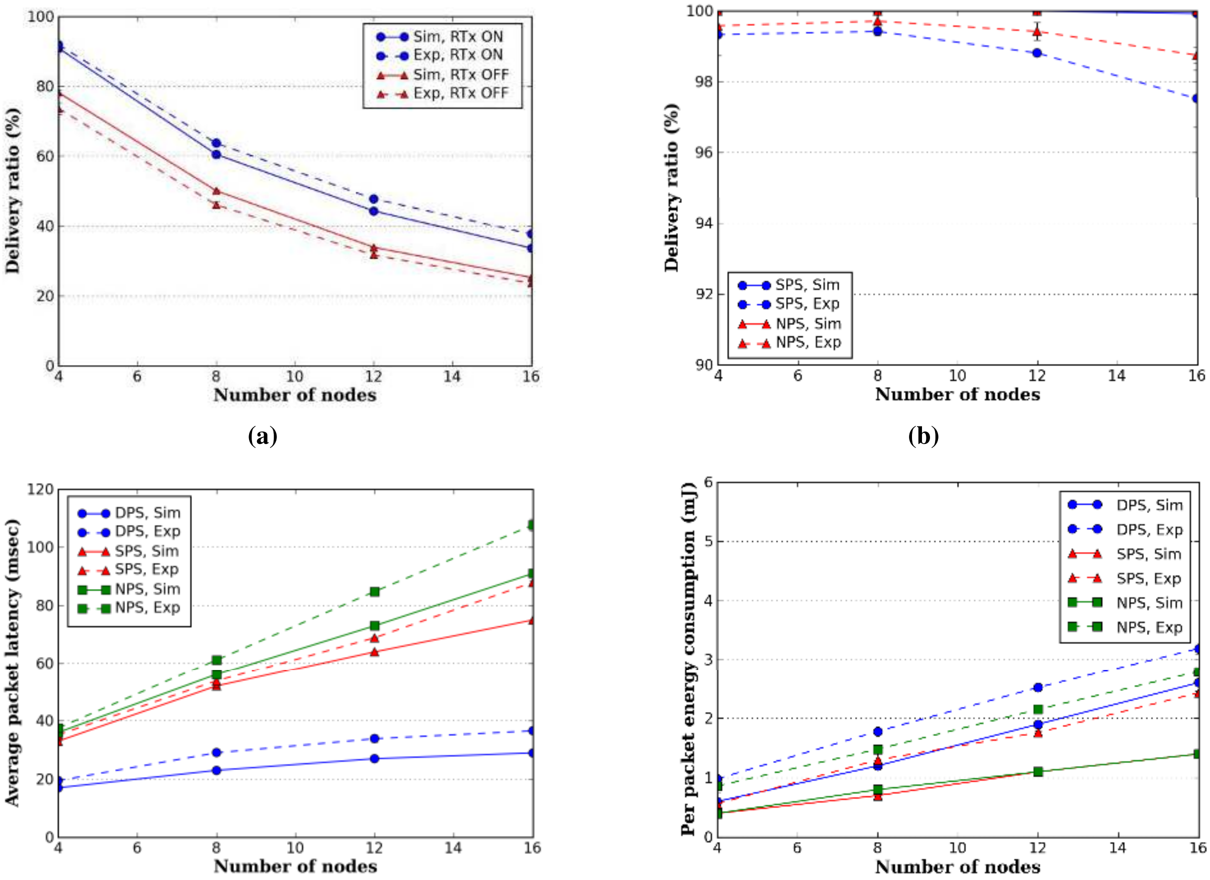
To conclude our simulation analysis, we also performed experiments where we varied the offered load (i.e., 1, 2, 3 packets per Beacon Interval), while leaving the PER value constant at 10%. The obtained results are aligned with those shown in Figure 6, and are thus omitted for the sake of space.

The results presented in this section confirm that in 802.15.4 WSNs the MAC unreliability problem is made more severe than in other similar WSNs by the default parameter values suggested by the standard. They also show that, in the considered scenario, a delivery ratio of 100% (or very close to 100%) can be achieved by just setting the MAC parameters to more appropriate values. However, since the increase in the delivery ratio is achieved at the cost of a higher latency, and due to the random nature of the CSMA/CA algorithm, an appropriate parameters setting that guarantees both reliability and bounded latency for time-sensitive applications does not exist. Figure 6-c shows that when the maximum latency tolerated by the application is less than 100 ms the fraction of packets delivered *on time* is below 20%, for any MAC parameters setting.

VIII. EXPERIMENTAL ANALYSYS

Since simulation experiments might not take into account all factors that can occur in a real environment, we also performed a set of measurements on a real WSN. The purpose of these experiments is twofold: (**i**) to validate the simulation results, thus confirming that the MAC unreliability problem also occurs in real WSNs, and (**ii**) to show that the solution envisaged in Section VII is viable in a practical scenario. Our testbed consists of Tmote Sky sensor nodes [48] with TinyOS 2.x operating system [49]. Tmote Sky sensor nodes use the Chipcon CC2420 radio transceiver [42] that is compliant to the 802.15.4 physical layer and supports a 250 Kbps bit rate over the unlicensed 2.4 GHz ISM band. Instead of using the default MAC protocol shipped with the TinyOS software, we used TKN15.4 [50], an implementation of the 802.15.4 MAC protocol for TinyOS 2.x, developed by the TKN group at TU Berlin. Since the TKN15.4 source code is freely available it is possible to change the MAC parameters even beyond the maximum values allowed by the standard.

In our experimental analysis we referred to the same star network scenario and common parameters setting considered in the simulation analysis. Although we did not deploy the WSN in a real industrial environment, nevertheless we ran our experiments in a working place with several sources of interfering signals, including many WiFi networks. Since we are using the beacon enabled mode – and beacon transmission is performed by the coordinator/sink node without contention with other nodes – we used the beacon loss rate (as perceived at sensor nodes) as an estimate of PER, and used the estimated value in the corresponding simulation experiment. Clearly, the channel conditions vary over time, while in simulations we used the average value measured during the entire experiment. To increase the accuracy of our results, we performed 5 different replicas for each experiment. The results presented below are averaged over the 5 replicas (in the figures we also report the standard deviations).



(a)

(b)

(c)

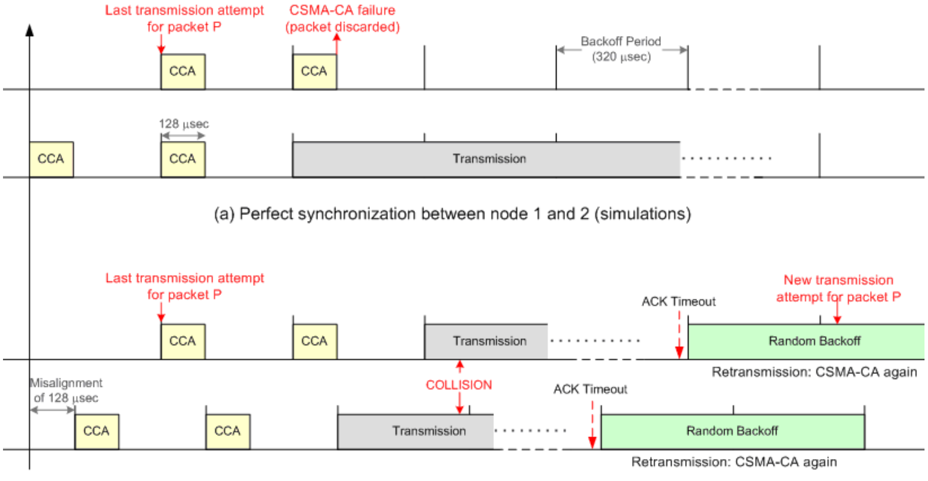
(d)

Figure 7. Comparison between simulation and experimental results.

Figure 7-a compares the delivery ratio, obtained with simulation (continuous line) and real experiments (dashed line), when using the default parameters setting (i.e., DPS). We measured the delivery ratio with the retransmission mechanism enabled (RTx ON) and disabled (RTx OFF). In both cases, the simulation and experimental curves exhibit the same trend and are very close to each other.

When the retransmission mechanism is enabled the experimental results are better than the corresponding simulation results, which may appear odd. Actually, this is due to misalignments in clocks of different sensor nodes which occur in real WSNs (while in simulations the clocks of all nodes are perfectly synchronized). As shown in [50], if the clock misalignment of two different nodes is larger than the duration of a CCA, it may result in an increased number of collisions with respect to the case of perfectly synchronized clocks.

In our scenario the effect of clock misalignments provides a higher delivery ratio, but at the cost of increased latency. We show this by means of the example depicted in Figure 8, where Node 1 is trying to transmit a packet to the sink node. It has already sensed the wireless medium and found it busy for *macMaxCSMABackoffs*-1 consecutive times. Thus, it has only one more chance before dropping the packet due to exceeded number of backoff stages. In Figure 8-a, where clocks of different sensor nodes are perfectly synchronized, as in simulation, Node 1 founds the channel busy again and drops the packet. In Figure 8-b, due to the clock misalignment between Node 1 and Node 2, Node 1 experiences a collision, and, according to the CSMA/CA algorithm, resets the number of backoff stages and starts a new access cycle. Hence, the packet has more chances to be transmitted in the latter case. This is also confirmed by the set of experiments where we disabled the retransmission mechanism (the results are also shown in Figure 7-a). Of course, disabling retransmissions reduces the probability of successful transmission and, hence, the delivery ratio. However, it also nullifies the effect of clock misalignments as collided packets cannot be retransmitted. Hence, the experimental results tend to be slightly worse than the corresponding simulation results.


Last transmission attempt for packet P
CSMA-CA failure (packet discarded)
Backoff Period (320 µsec)
CCA
CCA
128 µsec
CCA
CCA
Transmission
Last transmission attempt for packet P
New transmission attempt for packet P
ACK Timeout
CCA
CCA
Transmission
Random Backoff
Retransmission: CSMA-CA again
Misalignment of 128 µsec
COLLISION
ACK Timeout
CCA
CCA
Transmission
Random Backoff
Retransmission: CSMA-CA again

(a) Perfect synchronization between node 1 and 2 (simulations)

(b) Misalignment between node 1 and 2 (experiments)

Figure 8. Effects of clock misalignment on packet transmissions.

The experimental measurements shown in Figure 7-a validate our previous simulation results, and confirm that the MAC unreliability problem occurs in real WSNs too. We performed further experiments to check whether our envisaged solution, i.e., using higher MAC parameter values, may be effective in a real environment. Figure 7-b shows the delivery ratio when using the SPS and NPS sets defined above. Actually, both sets provide a delivery ratio very close to 100% (we zoomed on the 90-100% range in the figure). NPS and SPS show about the same delivery ratio as in the experimental study we analyzed only small/medium size WSNs (up to 16 nodes).

In addition to delivery ratio, we also measured the average latency experienced by packets (Figure 7-c) and the average energy consumption per delivered packet (Figure 7-d). The experimental measurements for latency confirm the trend observed in simulation experiments. However, Figure 7-c shows that the average latency in the testbed is larger than that measured in simulation experiments. This is also due to the effect of clock misalignments described above. Clearly, the latter becomes more and more relevant as the number of nodes increases (since the collision probability increases accordingly), and this justifies the increasing discrepancy between simulation and experimental results, as the number of sensor nodes increases.

Finally, Figure 7-d compares the energy efficiency in the real experiments and simulations. As expected, the average energy consumption per (delivered) packet in the real WSN is larger than that in the simulation experiments. This is because packets take more time to be transmitted, as shown in Figure 7-c. The experimental results confirm that the WSN becomes more energy efficient (i.e., the energy per message decreases) when using SPS or NPS, instead of DPS. The only difference, with respect to simulations, is that curves for SPS and NPS are no more overlapped. This is because, when using NPS, instead of SPS, the average latency – and, correspondingly, the total energy consumption – increases more than in the corresponding simulation experiments, while the delivery ratio remains approximately the same (see Figure 7-c and Figure 7-b). We expect that the energy efficiency of NPS solution with respect to SPS increases while increasing the number of sensor nodes and/or the PER. In fact, as shown in Figure 6-a, for large networks (e.g., > 40 nodes) and/or large PER, the NPS delivery ratio is considerably higher than that of SPS.

To summarize, our results confirm that using a CSMA/CA parameters setting different from the default one significantly improves the 802.15.4 performance, in terms of delivery ratio. However, the selection of the optimal parameter setting depends on dynamic network conditions and, hence, an adaptive mechanism is required for tuning the 802.15.4 parameters

IX. CONCLUSIONS

In this paper we have investigated, through both simulation and experiments on a real testbed, the performance of IEEE 802.15.4 WSNs when power management is enabled for energy conservation. We have observed that sensor nodes experience a low communication reliability in terms of delivery ratio which may prevent the distributed sensing system from operating properly (e.g., as for a timely detection of events). We have referred to this issue as the *MAC unreliability problem* as it is originated by the contention-based 802.15.4 MAC protocol.

To understand the fundamental reasons of this problem, we have performed a thorough simulation analysis. We have found that the problem is essentially due to the CSMA/CA algorithm used by the 802.15.4 MAC for channel access, which is not able to efficiently handle contention when the number of simultaneously contending nodes is relatively high (a similar problem does not occur when using a Time Division or polling scheme for channel access). Although this is a problem common to all contention-based MAC protocols, nevertheless in the 802.15.4 MAC it is made more severe than in other similar cases (e.g., S-MAC) due to the MAC parameters setting suggested by the standard. Specifically, we have shown that the default CSMA/CA parameter values specified by the standard are not appropriate for WSNs exploiting power management. Furthermore, we have also shown that, with appropriate parameter settings we can achieve a 100% delivery ratio, at least in the scenarios considered in this paper. However, our simulation results have shown that, in WSNs with large number of nodes and/or high traffic conditions, the desired delivery ratio can be achieved only by using MAC parameter values not compliant with the 802.15.4 standard. More important, the increase in the delivery ratio is obtained at the cost of a significant higher latency, which may not be acceptable for delay-bounded applications. In fact, we have shown that, in its current form, the 802.15.4 MAC is not appropriate for industrial applications with very stringent latency requirements, as it is not able to guarantee an acceptable reliability level subject to the required timeliness, especially if the number of sensor nodes is large and/or the offered load is high. Experimental measurements on a real testbed have confirmed all the conclusions drawn from the simulation analysis. The cost to be paid, in terms of additional latency and energy consumption, appears to be even higher in a real environment.

The above analysis paves the way for further research. Since the most appropriate MAC parameters setting depends on the network operating conditions (e.g., number of nodes, offered load, packet loss rate) as well as on the Quality of Service (QoS) required by the applications (e.g., delivery ratio, latency, etc.) we are currently investigating an adaptive scheme which can dynamically tune the MAC parameters setting to meet the applications requirements, at least for (industrial) applications without stringent latency requirements. Ideally, this algorithm should dynamically select the most appropriate parameters setting to provide the required QoS with the minimum energy expenditure, under varying operating conditions.

ACKNOWLEDGEMENTS

This work has been carried out while Mario Di Francesco was at the Department of Information Engineering, University of Pisa (Italy). This work has been partially supported by the European Commission under the FP6-2005-NEST-PATH MEMORY project, and by the Italian Ministry for Education and Scientific Research (MIUR) under the PRIN WiSe DeMon project. The authors would like to thank Vincenzo Neri for the fundamental help in the evaluation.

REFERENCES

[1] A. Willig, "Recent and Emerging Topics in Wireless Industrial Communications: a Selection", *IEEE Transactions on Industrial Informatics*, Vol. 4, N. 2, May 2008.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: a Survey", *Computer Networks*, Vol.38, N. 4, March 2002.

[3] D. Miorandi, E. Uhlemann, S. Vitturi and A. Willig, "Guest Editorial: Special Section on Wireless Technologies in Factory and Industrial Automation, Part I", *IEEE Transactions on Industrial Informatics*, Vol. 3 (2), pp. 95-98, May 2007.

[4] M. D. Lemmon, Q. Ling, and Y. Sun, "Overload management in sensor-actuator networks used for spatially-distributed control systems," *Proc. ACM International Conference on Embedded Networked Sensor Systems (SenSys)*, Los Angeles, CA, Nov. 2003, pp. 162–170.

[5] B. Sinopoli, C. Sharp, L. Schenato, S. Schaffert, and S. S. Sastry, "Distributed Control Applications within Sensor Networks," *Proc. of the IEEE*, vol. 91, no. 8, pp. 1235–1246, Aug. 2003.

[6] G. Platt, M. Blyde, S. Curtin, J. Ward, "Distributed Wireless Sensor Networks and Industrial Control Systems - a New Partnership**",** *Proc. IEEE Workshop on Embedded Networked Sensors (EmNetS-II)*, April 30 - May 01, 2005.

[7] K. S. Low, W. N. N. Win, and M. J. Er, "Wireless Sensor Networks for Industrial Environments," *Proc. International Conference on Computational Intelligence for Modeling, Control and Automation (CIMCA 2005)*, Nov. 2005.

[8] Embedded WiSeNTs Consortium, "Embedded WiSeNts Research Roadmap (Deliverable 3.3)", available at `http://www.embedded-wisents.org`.

[9] IEEE Standard for Information technology, Part 15.4; Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Computer Society, 2006.

[10] ZigBee Alliance, The ZigBee Specification version 1.0 (Q4/2007)

[11] R. Zurawski, "Networked Embedded Systems: An Overview" Chapter 1 in Networked Embedded Systems (R. Zurawski, Editor), pp. 1.11-1.16, CRC Press, 2009

[12] IEEE Pervasive Computing, "Energy Harvesting and Conservation", Vol. 4, Issue 1, Jan-Mar. 2005.

[13] G. Anastasi, M. Conti, M. Di Francesco, A. Passarella, "Energy Conservation in Wireless Sensor Networks: a Survey", *Ad Hoc Networks*, Vol. 7, N.3, May 2009.

[14] A. Willig, M. Kubisch, C. Hoene, and A. Wolisz, "Measurements of a Wireless link in an Industrial Environment using an IEEE 802.11-compliant Physical Layer," *IEEE Trans. on Ind. Electronics*, Vol. 49, no. 6, pp. 1265–1282, December 2002.

[15] D. Brevi, D. Mazzocchi, R. Scopigno, A. Bonivento, R. Calcagno, and F. Rusina, “A Methodology for the Analysis of 802.11a Links in Industrial Environments,” *Proc. IEEE International Workshop on Factory Communication Systems (WFCS 2006)*, Turin, Italy, June 27-30, 2006, pp. 165–174.

[16] E. Tanghe, W. Joseph, L. Verloock, L. Martens, H. Capoen, K. V. Herwegen, and W. Vantomme, “The Industrial Indoor Channel: Large–scale and Temporal Fading at 900, 2400 and 5200 MHz,” *IEEE Transactions on Wireless Communications*, Vol. 7, No. 7, July 2008.

[17] M. Bertocco, G. Gamba, A. Sona, S. Vitturi, “Experimental Characterization of Wireless Sensor Networks for Industrial Applications”, *IEEE Transactions on Instrumentation and Measurements*, Vol. 57, N. 8, August 2008.

[18] J. Mišic, S. Shafi, and V. B. Mišic, “The Impact of MAC Parameters on the Performance of 802.15.4 PAN”, *Ad Hoc Networks* Vol. 3, N. 5, pp. 509–528, 2005.

[19] I. Ramachandran, A. K. Das, S. Roy, “Analysis of the Contention Access Period of IEEE 802.15.4 MAC”, *ACM Transactions on Sensor Networks (TOSN),* Vol. 3(1), March 2007.

[20] G. Lu, B. Krishnamachari, C. Raghavendra, “Performance Evaluation of the IEEE 802.15.4 MAC for Low-rate Low-power Wireless Networks”, *Proc. Energy-Efficient Wireless Communications and Networks Conference (EWCN’04),* 2004.

[21] J. Zheng, M. J. Lee, “A Comprehensive Performance Study of IEEE 802.15.4”, *IEEE Press Book*, 2004.

[22] K. Leibnitz, N. Wakamiya, M. Murata, “Modeling of IEEE 802.15.4 in a Cluster of Synchronized Sensor Nodes”, Proc.19th *International Teletraffic Congress (ITC-19),* Beijing, China, August 2005.

[23] A. Koubaa, M. Alves, E. Tovar, “A Comprehensive Simulation Study of Slotted CSMA/CA for IEEE 802.15.4 Wireless Sensor Networks”, *Proc. IEEE International Workshop on Factory Communication Systems (WFCS’06)*, Torino, Italy, June 2006.

[24] K. Yedavalli, B. Krishnamachari, “Enhancement of the IEEE 802.15.4 MAC Protocol for Scalable Data Collection in Dense Sensor Networks”, *Proc. International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt08),* Berlin, Germany, March 31 - April 4, 2008.

[25] J. Mišic, S. Shafi, and V. B. Mišic, “Performance limitations of the MAC layer in 802.15.4 Low Rate WPAN”, *Computer Communications*, Volume 29, N. 13-14, August 2006, pp 2534-2541.

[26] F. Shu, T. Sakurai, M. Zukerman and H. L. Vu, “Packet Loss Analysis of the IEEE 802.15.4 MAC without Acknowledgment”, *IEEE Communication Letters*, vol. 11, N.1, January 2007.

[27] C. K. Singh, A. Kumar, P. M. Ameer, “Performance Evaluation of an IEEE 802.15.4 Sensor Network With a Star Topology”, *Wireless Networks*, Vol. 14, N. 4, August 2008.

[28] S. Pollin, M. Ergen, S. Ergen, B. Bougard, L. Van der Perre, I. Moerman, A. Bahai, F. Catthoor, “Performance Analysis of Slotted Carrier Sense IEEE 802.15.4 Medium Access”, *IEEE Trans. Wireless Communications*, Vol. 7, N. 9, September 2008.

[29] P. Park, P. Di Marco, P. Soldati, C. Fischione, K. H. Johansson, “A Generalized Markov Model for an Effective Analysis of Slotted IEEE 802.15.4”, Proc. *IEEE International Conference on Mobile Ad-hoc and Sensor Systems 2009 (IEEE MASS 09)*, Macau, China, October 2009.

[30] B. Nefzi, Y.-Q. Song, A. Koubaa, M. Alves, “Improving the IEEE 802.15.4 Slotted CSMA/CA MAC for Time-Critical Events in Wireless Sensor Networks”, *the 5th International Workshop on Real-Time Networks (RTN’06)*, Dresden, Germany, July 5-7, 2006.

[31] M.-J. Youn, Y.-Y. Oh, J. Lee, Y. Kim, “IEEE 802.15.4 Based QoS Support Slotted CSMA/CA MAC for Wireless Sensor Networks", *International Conference on Sensor Technologies and Applications 2007 (SensorComm07)*, pp.113-117, 14-20 Oct. 2007.

[32] G. Anastasi, M. Conti, M. Di Francesco, “The MAC Unreliability Problem in IEEE 802.15.4 Wireless Sensor Networks”, *Proceedings ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM 2009),* Tenerife, Spain, October 26-30, 2009.

[33] G. Anastasi, M. Conti, M. Di Francesco, V. Neri, “Reliability and Energy Efficiency in Multi-hop 802.15.4/ZigBee Wireless Sensor Networks”, Proceedings of the *IEEE Symposium on Computers and Communications (ISCC 2010),* Riccione, Italy, June 22-25, 2010.

[34] Network Simulator Ns2, `http://www.isu.edu/nsnam/ns`.

[35] I. Ramachandran, “Changes Made to the IEEE 802.15.4 NS-2 Implementation”, available at http://www.ee.washington.edu/research/funlab/802_15_4/ns2_changes.pdf.

[36] G. Anastasi, E. Borgia, M. Conti, E. Gregori and A. Passarella, “Understanding the Real Behavior of 802.11 and Mote Ad hoc Networks”, *Pervasive and Mobile Computing*, Vol. 1, N. 2, 2005.

[37] J. Kurose, K. Ross, “Wireless and Mobile Networks”, Chapter 6 in *Computer Networking. A Top-Down Approach*, IV Edition, Addison Wesley, 2007.

[38] A. Willig, “Polling-based MAC Protocols for Improving Real-Time Performance in a Wireless Profibus”, *IEEE Transactions on Industrial Electronics*, Vol. 50, No. 4, August 2003.

[39] F. De Pellegrini, D. Miorandi, S. Vitturi, A. Zanella, “On the Use of Wireless Networks at Low Level of Factory Automation”, *IEEE Transactions on Industrial Informatics*, Vol. 2, N. 2, May 2006.

[40] G. Anastasi, M. Conti, M. Di Francesco, “Extending the Lifetime of Wireless Sensor Networks through Adaptive Sleep”, *IEEE Transactions on Industrial Informatics*, Vol. 5, N. 3, pp. 351-365, August 2009.

[41] B. Bougard, F. Catthoor, D. C. Daly, A. Chandrakasan, and W. Dehaene, “Energy Efficiency of the IEEE 802.15.4 Standard in Dense Wireless Microsensor Networks: Modeling and Improvement Perspectives”, *Proc. Conference on Design, Automation and Test in Europe (DATE),* Volume 1, pp. 196-201, March 7-11, 2005.

[42] Chipcon CC2420 Website, http://focus.ti.com/docs/prod/folders/print/cc2420.html.

[43] B. Latré, P. De Mil, I. Moerman, N. Van Dierdonck, B. Dhoedt, and P. Demeester, “Maximum Throughput and Minimum Delay in IEEE 802.15.4”, *Lecture Notes in Computer Science*, Vol. 3794, pp. 866-876, 2005.

[44] Kleinrock, L. and F. Tobagi, “Packet Switching in Radio Channels: Part I--Carrier Sense Multiple-Access Modes and their Throughput-Delay Characteristics”, *IEEE Transactions on Communications*, Vol. COM-23, No. 12, pp. 1400-1416, December 1975.

[45] W. Ye, J. Heidemann and D. Estrin, “Medium Access Control With Coordinated Adaptive Sleeping for Wireless Sensor Networks”, *IEEE/ACM Transactions on Networking*, Vol.12, N. 3, pp. 493-506, June 2004.

[46] IEEE standard for Wireless LAN- Medium Access Control and Physical Layer Specification, 802.11, IEEE Computer Society November 1997.

[47] IEEE Standard for Information technology, Part 15.4; Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Computer Society, 2003.

[48] Tmote Sky Platform, MoteIV Corporation, http://www.moteiv.com/products/tmotesky.php.

[49] P. Levis, D. Gay, V. Handziski, J.-H. Hauer, B. Greenstein, M. Turon, J. Hui, K. Klues, C. Sharp, R. Szewczyk, J. Polastre, P. Buonadonna, L. Nachman, G. Tolle, D. Culler, and A. Wolisz, “T2: A Second Generation OS For Embedded Sensor Networks”, Technical Report TKN-05-007, Telecommunication Networks Group, Technical University Berlin, November 2005.

[50] J.-H. Hauer, “TKN15.4: an IEEE 802.15.4 MAC implementation for TinyOS 2”, Technical Report TKN-08-003, Telecommunication Networks Group, Technical University Berlin, March 2009.

Giuseppe Anastasi is an associate professor of Computer Engineering at the Department of Information Engineering of the University of Pisa, Italy. He received the MS degree in Electronics Engineering, and the PhD degree in Computer Engineering, both from the University of Pisa, in 1990 and 1995, respectively. His current research interests include pervasive computing, wirelss sensor networks, and sustainable computing. He is a co-editor of the book *Advanced Lectures in Networking* (LNCS 2497, Springer, 2002), and has published more than 90 research papers in the area of networking architectures and protocols. He is an area editor of *Computer Communications (ComCom), Pervasive and Mobile Computing (PMC)* and *Sustainable Computing (SusCom)*. He has served as Program Chair of IEEE PerCom 2010, Program Co-chair of IEEE WoWMoM 2008, Vice Program Chair of IEEE MASS 2007, General Co-chair of IEEE WoWMoM 2005, Workshops Chair of IEEE PerCom 2006, IEEE WoWMoM 2006, and IEEE ICCCN 2007. He is a member of the IEEE Computer Society.

Marco Conti is a research director at the Institute of Informatics and Telematics (IIT), an institute of the Italian National Research Council (CNR). He published in journals and conference proceedings more than 250 research papers related to design, modeling, and performance evaluation of computer-network architectures and protocols. He coauthored the book "Metropolitan Area Networks" (1997) and is co-editor of the books "Mobile Ad Hoc Networking" (2004) and "Mobile Ad Hoc Networks: From Theory to Reality" (2007). He is the chair of the IFIP WG 6.3 "Performance of Communication Systems". He is the Editor-in-chief of the Computer Communications Journal and Associate Editor-in-chief of Pervasive and Mobile Computing Journal; he is on the editorial board of IEEE Transactions on Mobile Computing, Ad Hoc Networks, Journal of Communications Systems, and Wireless Ad Hoc and Sensor Networks. He served as general chair of ACM REALMAN 2006 and IEEE MASS 2007, and as general Co-chair of IEEE WoWMoM 2006, ACM MobiOpp 2007, and IEEE PerCom 2010. He served as TPC chair of IEEE PerCom 2006, and of the IFIP-TC6 conferences Networking 2002 and PWC 2003, and as TPC Co-chair of ACM WoWMoM 2002, WiOpt 2004, IEEE WoWMoM 2005, ACM MobiHoc 2006 and ACM MobiOpp 2010.

Mario Di Francesco is a research associate at the Department of Computer Science and Engineering, University of Texas at Arlington. He received his Ph.D. degree from the Department of Information Engineering, University of Pisa, in 2009. He was also a research assistant at the Real-Time Systems (ReTIS) laboratory of the Scuola Superiore S. Anna in 2009. He was a TPC member of PerCom 2010, and has been TPC member of IEEE PerSeNS since 2009. He also served as publication co-chair of IEEE WoWMoM 2006. His current research interests include pervasive computing and wireless sensor networks.