A Study on the Impact of Packet Length on Communication in Low Power Wireless Sensor Networks under Interference

Valerio Freschi and Emanuele Lattanzi

***Abstract*—Reliability is nowadays considered a key requirement in wireless sensor networks for their increasing diffusion in various Internet of Things applications. However, radio interference from various sources may heavily affect the performance of wirelessly connected embedded devices, resulting into increased packet collisions and congestions. There is therefore a widely recognised need of both theoretical and practical investigations capable of shedding light on the factors affecting the operativeness of sensor networks subject to interference. In this article we investigate the role of packet length into the reliability and energy efficiency of low-power medium access protocols. Specifically, we propose a mathematical model to explore the functional dependence of the reliability of a pair of sensor nodes under interference from packet length. We also present a wide range of experimental evaluations aimed at validating the model and at providing novel insights on dependability issues. In particular, we assess the performance of Contiki's default MAC layer (together with that of an always listening receiver, as a baseline) in terms of packet loss rate and energy efficiency for varying payload lengths. Experimental results highlight the interplay between packet size and interference and in particular the trade-off between the robustness against interference and the overhead imposed to communication as a function of the length of data packets. The Pareto curve describing the energy efficiency as a function of the packet loss rate, demonstrates the existence of intermediate packet size representing an optimal choice for balancing energy consumption and communication reliability, enabling adequate system dimensioning at design-level.**

***Index Terms*—Wireless sensor networks, communication reliability, interference.**

I. Introduction

THE Internet of Things (IoT) technology is nowadays reaching a significant diffusion level. The integration of pervasively distributed objects equipped with sensing/actuation, communication and computation capabilities into a coherent ecosystem is indeed the key for achieving many goals in disparate application fields, ranging from industry to healthcare, from environmental monitoring to smart cities [1], [2], [3], [4], [5].

Within this framework, the increasing interest in the development of Wireless Sensor Networks (WSN) as building block of many IoT systems, prompts for the design of novel solutions capable of coping with stringent dependability and energy efficiency requirements [6], [7], [8], [9].

V. Freschi and E. Lattanzi are with the Department of Pure and Applied Sciences, University of Urbino, Piazza della Repubblica, 13, 61029 Urbino - Italy. e-mail: {emanuele.lattanzi,valerio.freschi}@uniurb.it.

Manuscript received XXXX XX, XXXX; revised XXXX XX, XXXX.

In low power WSNs, due to the intrinsically open nature of the wireless medium, the transmissions from a sender node can interfere with the transmission and reception capabilities of other nodes of the network (*internal interference*) or with some other neighboring radio frequency devices (*external interferences*). In particular, the internal interferences are clearly evident in crowded WSNs where they are mainly due to the heavy channel occupation which introduces packet jamming and increases both latency and packet collision probability.

On the other hand, external interferences essentially depend on a partial or complete overlapping of the communication band with an interfering device. For instance, the basic components of almost all current WSNs are working on the 2.4 GHz ISM band which is shared with other communication technologies such as Wi-Fi (802.11b/g/n) and Bluetooth. This frequency overlapping can cause unpredictable interferences which impairs the communication reliability and performance. Moreover, widespread electronic devices (e.g. microwave ovens) can also generate interferences on the 2.4 GHz ISM band without using it for communication [10].

Communication interference impacts not only on the reliability of the channel but also on the energy consumption of the nodes. In fact, in some cases, they can nullify the effort of energy aware communication protocols and of power management strategies implemented on the WSNs. For these reasons, understanding and modeling channel interference is an essential task in designing and developing low power WSNs.

Contribution: we present in this article a study on the impact of the length of packets payload on the performance of WSN in interference conditions, by investigating reliability and energy consumption of a communication link between low-power sensor nodes when the channel is subject to interference. The contributions provided in this article can be summarized as follows:

- we derive an analytical model of single link communication under interference for both an *always on* receiver and for a duty-cycled, low-power MAC protocol (e.g. *ContikiMAC*). The model provides a useful tool at design level to evaluate the impact of different parameters on the system performance, allowing for instance to predict how the payload length affects the expected number of received bytes under a given configuration.
- We validate the model within an experimental framework consistent with state-of-the art scientific literature.
- We provide extensive experimental results to investigate

the impact of packet length on either communication and energy metrics, under different settings (e.g. in presence or absence of a radio duty-cycling protocol). This exploration allows us to derive a Pareto curve describing the trade-off between energy and packet loss rate.

Outline: the remainder of the article is organized as follows: in Section II we discuss the relationship between our work and some representative, state-of-the-art contributions in recent scientific literature; in Section III we describe the features of the system we refer to and derive mathematical models to study the impact of packet size on its reliability; in Section IV we illustrate the experimental set-up that we adopted to study the problem in a real-world setting; in Section V we provide and comment the experimental results; in Section VI we conclude with some final considerations and remarks.

II. Related work

In the following we try to analyze what are, to the best of our knowledge, the most meaningful studies related to our work in scientific literature.

Lettieri and Srivastava proposed, among the first, to adapt the length of data packets to the changing conditions of wireless channels [11]. The aim of their work was to improve throughput, distance range, and energy consumption, for which they provided analytical modeling which was validated on PC running Linux OS. Experimental results were obtained for WaveLAN radios, hence not an IoT framework such, for instance, the IEEE 802.15.4 standard adopted in our work, where we analyze the impact of packet length on the reliability performance of systems running low-power protocols.

In [12], the authors studied a cross-layer solution for optimizing packet size in wireless sensor networks. Our work differs, with respect to this one, since: *i)* they propose a specific solution for packet length optimization in generic WSN architectures, while we aim at a detailed understanding of the effect of packet size on low-power communication protocols in interference environment; *ii)* in [12] the effects of multi-hop routing is taken into consideration, while we explore single link, pairwise communication under a definite model of interference; *iii)* they provide numerical simulation results of the optimization approach, while we complement our analysis with several experiments on real motes.

In [13], the authors presented a framework for measuring the interference levels through the characterization of the probability distribution function of idle period lengths. These estimates are used to evaluate the packet reception rate under interference as a function of packet length, without making any assumption on a particular MAC layer. Differently, in our work we either refer to MAC-*agnostic* systems and to specific, low-power protocol (i.e. ContikiMAC).

King *et al.* described in [14] a method for estimating the node energy consumption of a sensor node in environments subject to interference. The focus of their article was to gauge the lifetime of motes, however without any evaluation on the impact of packet size.

Dong *et al.* presented in [15] a method for dynamic control of packet length in WSN based on link quality estimation. Our proposal yields a complementary view of the problem through analytical and extensive experimental evaluation of the pairwise communication under interference, which further motivates adaptive implementations such the one proposed in [15].

Han and Lee introduced a technique for adapting the transmission rate and the payload size in response to interference variations [16]. They derived analytical results regarding packet collision probabilities under interference and validated their approach by means of numerical simulations. In our work, we apply the analytical evaluation to encompass specific low-power MAC protocols and perform significant testing on real-world sensor nodes.

Michel *et al.* analyzed the functioning of the ContikiMAC layer under interference, and derived a model for worst-case evaluations of packet delivery rate and latency [17]. However, their methodology doesn't target the impact of packet size on the performance of the system. In fact they fixed the packet size to 127 bytes (i.e. the maximum transmission unit in IEEE 802.15.4) as a worst case condition for IEEE 802.15.4-compliant communications, starting from the assumption that long packets are more likely to be corrupted than short ones.

III. System model and analysis

A. Reference System

In order to evaluate the communication performance over a low power wireless link, we refer to a minimal system (see Figure 1) composed of a sender node (*Sender*), which repeatedly sends packets, and a receiver node (*Receiver*) waiting for its. Then, an interference generator (*Interferer*) completes the set-up.

Depending on the positioning of the interferer with respect to the sender and the receiver, we might identify two configurations, represented in figures 1.(a) and 1.(b). In Figure 1.(a), the activity of the interferer influences both the sender and the receiver while, in Figure 1.(b), the sender node is positioned outside the interference area and it does not hear any interference. Distinguishing these two working conditions is particularly interesting because, usually, low power communication protocols make use of carrier sensing and collision avoidance (CSMA/CA) strategies which can differently alterate the dynamic of the system in the two cases.

In particular, the sender can decide to transmit a packet immediately or to postpone it depending on the SNR measured on the channel, while the receiver can sense the wireless medium to schedule a shutdown of the RF interface, and save power, if no packets are incoming. For these reasons, a sender node, in the first case (Figure 1.(a)), can interact with the interfering signals and totally or partially mitigate the effect of the interferences while, in case of Figure 1.(b), the sender perceives the communication channel always clear and it can not carry out any compensation mechanism.

B. Modeling the interference

From the physical point of view, decoding a wireless signal means to interpret a pattern which is radiated into space by the transmitter. This pattern incurs over distance to some

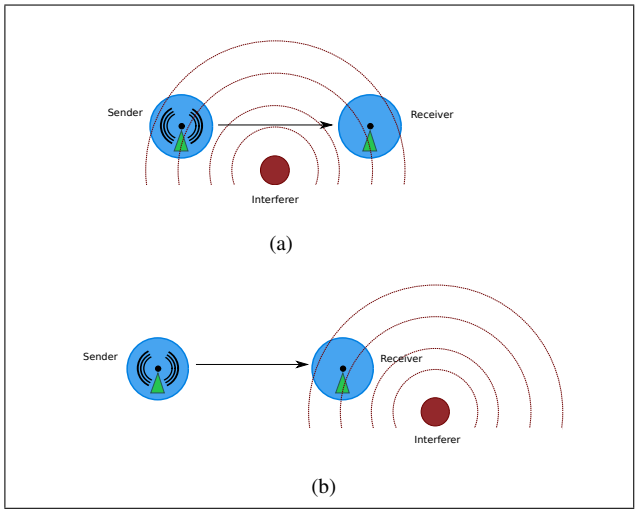


Fig. 1. Schematic of the reference system used to evaluate the communication performance of a low power wireless link under interference. In (a) the activity of the interferer influences both the sender and the receiver while in (b) only the receiver in positioned in the activity range of the interferer.

attenuation, distortion and interferences. Subsequently, the signal is decoded by treating the sum of all the other on-going signal transmissions as noise [18]. For instance, successfully decoding a symbol is an event whose probability depends upon several conditions such as the desired signal strength, the level of thermal noise, and the strength of interfering signals. The communication over wireless channels has been modeled, by networking scientists, at a variety of abstractions levels based on what the research focus was. Modeling the interference follows the same criterion and it strictly depends on the channel model. In general, the interference models have evolved in terms of complexity and sophistication over the time. Starting from one of the simplest models presented by G. Bianchi [19], which was based on the assumption of fixed communication and interference ranges, we move onto more complex approaches such as those attempting to model the *capture effect* of frequency modulation (e.g., the capture threshold model used in the network simulator ns2 [20]), or such as the physical model described by Gupta and Kumar [21]. In particular, the latter is an additive model based on a more realistic metric called *signal to interference plus noise ratio* (SINR) used to establish a the success of a signal transmission.

For the purpose of this work the concept of interference can be simplified by defining it as any signal, perceived at sender or receiver level, which lies above the *Clear Channel Assessment* (CCA, for short) threshold for a time long enough to prevent a symbol decoding. In particular we focus on the impact of packet length on the communication reliability with a given level of interference. The physical attenuation or composition of the interfering signals, which can lead to this given level, are beyond the scope of this study. According to this principle we can represent an interference as a binary signal, characterized only by the time in which its energy is below or above the CCA threshold.

From the experimental point of view, several authors have addressed the problem of creating predictable, reproducible and well-controlled interference patterns in a low power WSN testbed [22], [23]. Both the generation of internal and external interferences has been object of study in recent works.

Notably, the problem of generating realistic and repeatable external interferences is mostly addressed by recording interference patterns in a real environment and then playing it back by means of a dedicated wireless transceiver [23]. In this scenario, the greater the accuracy of the sampling and reproducing systems, and the greater will be its effectiveness. To this purpose, several Software Defined Radio (SDR) devices, such as the Universal Software Radio Peripherals (USRP) sold by National Instruments Corporation [24], are traditionally used. These devices are programmable radio transceivers which can be tuned to produce any desirable radio pattern with a high degree of stability and reproducibility.

On the other hand, generating internal interferences can be, to some extent, simpler, because of the exact frequency matching between the interfering and the interfered signals. For example, the most obvious and easy way to generate interferences is to program a node of the network to repeatedly send broadcast packets at a predefined transmission rate. This kind of interference leads to a heavy channel occupation which introduces packet jamming and increases the latency in other ongoing communications. Despite its simplicity, this method is hardly tunable and, above all, the dynamic of the generated interference suffers from a strong dependence on the software stack of the sending node [22].

Boano et al. in 2009 presented a practical approach to the problem of generating internal interferences [22]. This solution makes use of some RF transceivers available on sensor nodes, such as the Texas Instruments' CC2420, to generate a tunable frequency matching interference. In fact, this radio chip can be set into different transmit test modes through which it is possible to send a continuous unmodulated or randomly-modulated carrier without the need of any other hardware device.

The generation of an unmodulated and a modulated signal allows to produce two different kinds of interferences. In fact, the unmodulated carrier shows a concentrated power spectrum peaking at the center frequency, while the randomly-modulated signal has a power spectrum distributed across the channel bandwidth. From the practical point of view, a randomly-modulated signal can be used to emulate short bursts of interfering packets while an unmodulated carrier can generate an interference pattern similar to a background noise.

Boano et al. also suggest two strategies to obtain a tunable interference. The first one is to produce a continuous unmodulated carrier while varying the transmission power of the radio chip in order to manipulate the SNR of the wireless medium. The second strategy, on the contrary, involves configuring the transmission power of the interferer to the maximum level (so as to avoid any kind of communication in the channel) and then intermittently switching it on and off. In this way we obtain an interfering square wave characterized by two parameters, namely the mean time in which the transmitter is on (T_{busy}) and the time in which it is off (T_{idle}). By properly varying these two parameters different levels of interference can be achieved.

C. Modeling the system

Taking into consideration the wireless communication system illustrated in Figure 1, and given the definition of symbols adopted in the following of the article reported in Table I, we may proceed to the analytical derivation of some equations for modeling the system.

Symbol	Definition
SNR	Signal to Noise ratio
BER	Bit Error Rate
L	Payload length
H	Header length
p_f	Probability of transmission failure
p_c	Probability of transmission failure due to packet collision
p_s	Probability of transmission failure due to low Signal-to-Noise ratio
$p_{c\|busy}$	Probability of transmission failure given a packet transmission started in presence of interference
$p_{c\|idle}$	Probability of transmission failure given a packet transmission started in absence of interference
$p_{c\|data}$	Collision probability of data packets
$p_{c\|ack}$	Collision probability of ack packets
ρ	Channel occupancy rate of interference
τ_{idle}	mean duration of interferer idle state
R_{br}	Transmitter/receiver Radio bit-rate
T_{data}	Time needed to transmit(receive) a data packet
t_i	Time interval between two consecutive transmissions of the same packet (ContikiMAC)
t_m	Time threshold for additional frame probes transmission (ContikiMAC)
N_m	Additional number of frame probes (ContikiMAC)
R	Reliability
T	Expected received data per packet

TABLE I
SYMBOLS AND DEFINITIONS.

Specifically, assuming a given SNR at the receiver, if its value is lower than a given threshold or if the packet experiences a collision with the interference signal[1], the packet is lost. The probability of this transmission failure event, $p_f(L, SNR)$, can be written (see [16]) as:

$$p_f(L, SNR) = 1 - (1 - p_c(L)) \cdot (1 - p_s(L, SNR)) \quad (1)$$

with $p_c(L)$ defined as the probability of transmission failure due to packet collision and and $p_s(L, SNR)$ as the probability of transmission failure due to low SNR. In turn, p_s can be derived as in equation 2,

$$p_s(L, SNR) = 1 - (1 - BER(SNR))^{L_p + L_m + L} \quad (2)$$

where L is the payload length, L_p is the overhead of the physical layer and L_m that of the MAC layer.

In presence of interference, the channel can be modeled as a semi-Markov model [16] with two states (idle/busy), characterized by the respective probability density functions. In particular, given the mean duration length of the idle state τ_{idle} and the mean duration length of the busy state τ_{busy}, we can define by means of Equation 3 the channel occupancy rate of the interference signal ρ, which corresponds to the duty cycle in case of a square wave interference signal as the one adopted in this work:

$$\rho = \frac{\tau_{busy}}{\tau_{busy} + \tau_{idle}} \quad (3)$$

Indeed, p_c can be expressed as a function of the probability of failure given that the transmission started in presence ($p_{c|busy}$) or absence ($p_{c|idle}$) of interference as follows:

$$p_c = \rho \cdot p_{c|busy} + (1 - \rho) \cdot p_{c|idle} \quad (4)$$

As well, p_c can also be written as:

$$p_c = 1 - (1 - p_c^{data}) \cdot (1 - p_c^{ack}) \quad (5)$$

where p_c^{data} and p_c^{ack} identify the collision probability of data and ACK packets. In this article we focus on the single transmission of broadcast data packet, hence we do not need to investigate the impact of ACK packets, which reduces to neglecting the second term of equation 5 ($p_c^{ack} = 0$).

With this notation in hand, the collision probability of data packets can be calculated as:

$$p_c^{data} = \rho + (1 - \rho) \cdot p_{c|idle}^{data} \quad (6)$$

Let T_{idle} be a given idle state length, and T_{data} a given data packet transmission time. When the interferer enters the idle state, the system may incur a packet collision if a data packet is transmitted after an interval of $(T_{idle} - T_{data})$ seconds. We denote by T_d the time difference between the beginning of the idle state and the beginning of the reception of a new data packet ($0 \leq T_d \leq T_{idle}$), as depicted in Figure 2.

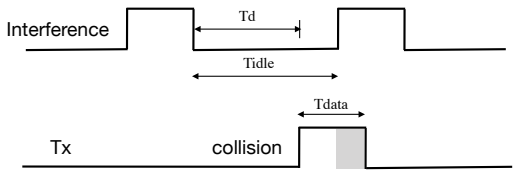


Fig. 2. Periodic interference square wave timing.

Under the assumption of a periodic square wave with duty cycle ρ representing the interference, the mean duration of the idle state is $\tau_{idle} = T_{idle}$, and that of the busy state is $\tau_{busy} = T_{busy}$. Hence we may write:

$$p_{c|idle}^{data} = Pr[T_{idle} < T_d + T_{pkt}^{data}] = \frac{T_{data}}{T_{idle}} = \frac{L}{R_{br} \cdot \tau_{idle}} \quad (7)$$

where R_{br} is the transmission bit rate. By plugging Equation 7 into Equation 6 we get:

$$p_c^{data} = \rho + (1 - \rho) \cdot \frac{L}{R_{br} \cdot \tau_{idle}} \quad (8)$$

It is worth noticing that taking into consideration different types of interference (e.g. a stochastic interference model) implies a derivation of formulas analogous to equations 7 and 8, making it possible to investigate several and different scenarios. For instance, it is possible to analytically derive

[1]For our purposes, collision is the overlapping of the interference signal with at least one bit of the transmitted signal in a way that makes it unintelligible to the receiver.

p_c^{data} in the case the idle state follows an exponential or a Pareto statistical distribution [16].

The analytical derivation conducted above represents the crux of the modeling for the system under study, which can be further specialized to take into account some features distinguishing the radio receiver operativeness.

D. Always on receiver

We now take into consideration the case of a receiver which continuously listens to the wireless channel for incoming packets (i.e. an *always on* receiver), when the transmitter doesn't perform any CSMA/CA strategy (i.e. it cannot hear the interference affecting the receiver). The value of p_c^{data} calculated by means of equation 8 can be straightforwardly used to obtain the probability of transmission failure caused by a packet collision (if the protocol doesn't make use of acknowledgment as for broadcast transmissions):

$$p_c = \rho + (1-\rho) \cdot \frac{L}{R_{br} \cdot \tau_{idle}} \tag{9}$$

Equation 9 highlights how the collision probability for a receiver always listening the channel depends on: *i)* the mean length of the idle state of the interference; *ii)* the channel occupancy rate of the interference; *iii)* the bit rate of the transmitter, and *iv)* the length of the packet payload.

The collision probability p_c might therefore be used as a proxy for estimating the reliability R of an *always on* receiver under the hypothesis that the interference only affects the receiver side of the communication system, according to the following:

$$R = 1 - p_c \tag{10}$$

E. The Contiki Radio Duty Cycling Protocol

Contiki provides an asynchronous duty-cycling protocol called ContikiMAC. A duty-cycling protocol switches the node radio transceiver between short listen periods and long sleep periods in order to reduce energy consumption. Moreover, the asynchronicity of the protocol entails that different nodes do not synchronize their listen periods but, when transmitting, they repeatedly send the same full data packet or a short preamble until either an ACK is received or the total transmission time exceeds the receiver wake-up interval. Data packets and preambles are commonly called strobes. In order to receive a packet, a node must wake up periodically for a short time to sense the wireless channel by means of the CCA mechanism. If the CCA succeeds (clear channel), there is no data packet to be received, and the node can go back to sleep to save power. If the CCA fails (busy channel), it stays awake to receive the incoming packet.

In the ContikiMAC protocol when a node wakes up it performs two successive CCA to determine whether there is an incoming transmission. When it receives a strobe, which in ContikiMAC is a data packet, it looks at the target node ID and, in case of mismatch, it immediately returns to sleep. Otherwise the packet is completely decoded, an ACK is sent to the sender, and the receiver is switched off until the next wake up interval [25].

In broadcast communication each packet must be received by all the nodes in the range and it is not foreseen the sending of any ACK by the receivers. In this case, a ContikiMAC sender keeps sending the same packet until the total transmission time exceeds the receiver wake-up interval. This results in a number of strobes decreasing as the size of the packet increases (larger packets take longer time to be sent).

An ad-hoc strategy (*fast sleep optimization*), based on the ContikiMAC timing constraints, helps a receiver node to determine if a negative CCA (channel busy) was caused by noise rather than an incoming packet and, consequently, allows the node to switch off the radio chip as soon as possible. In particular, this strategy tries to identify those radio patterns which are not related to a real transmission but which are the result of interfering signals [17]. From the practical point of view, the fast sleep optimization defines a so called *reception window*, following a negative CCA, which represents the time in which the node must recognize an incoming packet and decode it. Otherwise, if the radio pattern does not meet the MAC constraints or the incoming packet is undecodable or corrupted, the radio chip will be switched off. According to [25], this reception window rw can be computed as $rw = 2 \cdot L_{max}/R_{br} + t_i$, where t_i is the time interval between each strobe transmission, L_{max} is the maximum frame size provided by the protocol, and R_{br} is the radio bit rate.

The model describing the collision probability under interference for an *always on* receiver can be extended to take into account a duty-cycle receiver, such as the ContikiMAC protocol described above. In particular, we focus on the activity of the receiver when the MAC layer makes it enter into the *active* state. We also suppose that the interference only affects the receiver, so that the transmitter is not able to implement any mechanism for counteracting collisions.

Indeed, in ContikiMAC, the transmitter continues sending a data packet until one of these two conditions is met: *i)* the packet is acknowledged successfully; *ii)* a maximum number N_m of additional frame probes (determined by a specific time threshold t_m) is sent. Specifically, given the time threshold t_m and the time needed to send (or receive) a packet T_{data}, $N_m = \lfloor t_m/T_{data} - 1 \rfloor$ [17]. Hence, it is possible to estimate the probability of a successful transmission on the communication link (i.e. its reliability R) as:

$$R = (p_l \cdot p_a) + \sum_{k=1}^{N_m} (1-p_l)^k \cdot (p_l \cdot p_a) \tag{11}$$

where p_l represent the probability of a successful data packet transmission and p_a the probability of successful acknowledge.

We may modify the equation above by considering that we don't have any acknowledgment because of a broadcast transmission (hence $p_a = 1$) and that p_l can be derived from Equation 9 ($p_l = 1 - p_c$).

We can therefore derive the reliability R of the communication system under study as follows:

$$R = (1-p_c) + \sum_{k=1}^{N_m} p_c^k \cdot (1-p_c) \tag{12}$$

Hence, by taking the time threshold t_m (that limits the number of additional frame probes) equal to the reception window rw, we may use it in equation 12 to compute the reliability (equivalently, the collision probability) for the investigated communication system.

In Section V we will describe a set of experiments on real sensor nodes, aimed at validating the introduced mathematical models. Indeed, as it will be shown, the results highlight a rather accurate predictive power regarding the reliability of the two types of modeled receivers under interference. Consistently, the models might be used for the exploration of the design space at system level, thus providing a useful tool for this aim. An example of this type of analytical prediction is provided in the following subsection.

F. Expected received data per packet

The probability of a successful packet transmission (let it be P_{sp}) can be computed from Equations 1 and 2:

$$P_{sp} = 1 - p_f = (1-p_c)\cdot(1-p_s) = (1-p_c)\cdot(1-BER)^{(L+H)} \quad (13)$$

We remark here that we split P_{sp} into two terms: the first one, i.e. $(1-p_c)$, takes into account the probability of transmission failure due to packet collision events; the second one, i.e. $(1-BER)^{(L+H)}$, entails the probability of transmission failure due to low SNR imputable to other error sources (e.g. attenuation, fading, etc.). This is a convenient way to express P_{sp}, since it allows us to make use of the mathematical models derived in the previous sections for the failure probability referable to collisions.

P_{sp} can be used to compute the expected amount of data received per packet (hereafter denoted as T), for a given number of information bits contained in each packet [26].

From equation 13 we can obtain:

$$T = L \cdot P_{sp} = L \cdot (1-p_c) \cdot (1-BER)^{L+H} \quad (14)$$

where L the number of data bits per packet.

Transmission failure probabilities due to collisions can be derived from Equation 9 for an always on receiver, and from Equation 12 (as $1-R$) for a ContikiMAC-based receiver. Hence, Equation 14 is used to evaluate the expected amount of data that can be received for a given length of the packet payload, in a system subject to interference. A graphical representation of a numerical simulation is provided in Figure 3 where we plotted T as a function of the payload length for an *always on* and a *Contiki-based* receiver under two different noise level (i.e. $BER = 10^{-3}$ and $BER = 10^{-4}$, respectively).

Numerical experiments have been conducted assuming a 10B packet overhead, a transmission bit-rate of 250kbps, a maximum packet length of 127B, and (for the Contiki-based receiver) a time interval between two consecutive data packets (i.e. t_i) of 0.4ms. We modeled the interference as a square wave with $\tau_{idle} = 12ms$ and $\tau_{busy} = 4ms$, resulting into a duty cycle $\rho = 0.25$. Figure 3 shows a general tendency to a growth of T for increasing values of packet length. ContikiMAC results apparently advantageous because of a higher probability of successful packet sending due, in turn, to the policy of repeated transmissions within the reception window.

It is worth noticing that, on one hand, longer packets provide a better amortization of the overhead associated to headers, leading to higher values of T in the considered range of payload lengths. On the other hand, increasing the length of packets implies a lower robustness with respect to interference. In order to better evaluate this tension, we performed a second set of numerical experiments where we extended the possible packet lengths up to 510B, although the maximum payload length allowed by the IEEE 802.15.4 standard is 127B. We kept the remaining parameters unchanged, except for τ_{idle} that was set to 20ms to guarantee the time of flight of longer packets. Results are reported in Figure 4, where the trade-off between the higher amount of information carried on by longer packets and their reduced robustness against interference can be fully appreciated. For both types of considered receivers, the expected amount of received data increases with the packet length until a maximum value (25.6B for 100B payload length in the case of an always on receiver, 42.36B at 120B payload length in the case of a ContikiMAC receiver) and then starts to decrease for packet sizes higher than 100B and 120B.

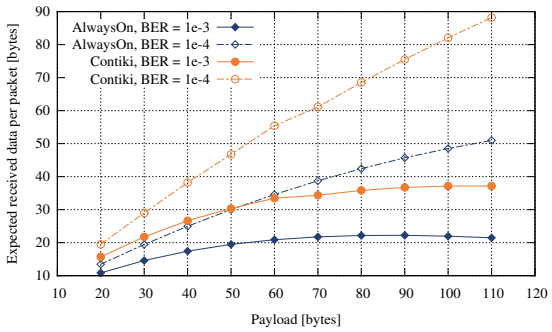


Fig. 3. Expected amount of data received per packet (T) as a function of payload length. Parameters: Header (overhead) = 10B, Bit-rate =250kbps, τ_{idle}=12ms, ρ=0.25, t_i = 0.4ms, max packet length = 127B)

IV. Experimental Setup

In this section we describe the experimental set-up used in extensive experiments aimed at investigating the impact of packet length on the communication performances achieved in a low power communication link under internal interferences.

First of all, we investigated the impact of the packet length on packet reception rate for simple always-on CSMA/CA communication protocol and for the ContikiMAC low power radio duty-cycling protocol [25]. Secondly, we measured how the packet length impacts the energy consumption of the nodes under interference.

A. System Set-Up

Our reference system has been implemented by means of two sensor nodes plus an interference generator that we placed in an office environment close to each other ($< 1m$). Each experiment lasts for 30 minutes and was conducted on the IEEE 802.15.4 channel 26 in order to reduce uncontrolled

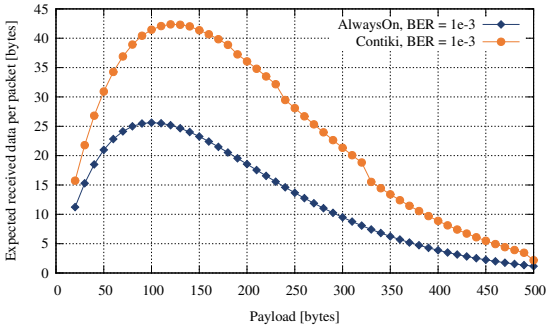


Fig. 4. Expected amount of data received per packet (T) as a function of payload length. Parameters: Header (overhead) = 10B, Bit-rate =250kbps, τ_{idle}=20ms, ρ=0.25, time guard = 0.4ms, max packet length = 510B)

interferences. In fact, channel 26 does not overlap with WiFi communication which is the major source of external interference in our office building. Each run is composed of about 1,000 repetitions (one every 1.8 seconds) of a broadcast packet transmission subject to a periodic generated internal interference.

For both the sender and the receiver we used a VirtualSense node, which is an open-hardware ultra low-power sensor module featuring a java-compatible virtual runtime environment [27]. From the hardware point of view, the last release of VirtualSense used in this work is built around the new Texas Instruments' CC2538 system-on-chip microcontroller designed for 2.4-GHz IEEE 802.15.4 applications [28]. The software stack has been created starting from the Contiki operating system [29] and the Darjeeling java compatible virtual machine [30]. Both of them have been suitably modified in order to allow a VirtualSense node to concurrently execute typical WSN tasks with an average power consumption of a few micro Watts [31].

Contiki is an open source operating system built for the Internet of Things. It currently supports a wide range of IoT hardware platforms (particularly tiny low-cost and low-power devices), ranging from the old 8-bit MOS 6502, to the modern Atmel, Freescale and Texas Instruments 32-bit microcontrollers; it also features fully certified IPv6 stack and low-power communication stacks for the IoT (included 6LoWPAN, RPL or CoAP) [32]. Contiki is developed and maintained by academic and industry communities worldwide, with contributions from Atmel, Cisco, ETH, Redwire LLC, SAP, Thingsquare, and many others [29]. These features make it an ideal choice as building block for our experimental evaluations.

Contiki provides three different network stacks, which are: IPv4, IPv6, and Rime. The two TCP/IP stacks are devoted to manage connection in IoT devices while the Rime stack is a set of custom lightweight networking protocols designed for low-power wireless networks. In this work we focus on the Rime stack which is composed of the following four software layers: *i)* Network; *ii)* MAC - Medium Access Control; *iii)* RDC - Radio Duty Cycling; *iv)* Radio. The *Network* layer consists of the application, the transport and the routing layers as described by a classical OSI structure while the *MAC* layer represents the IEEE 802 data link layer where Contiki provides a simple CSMA/CA protocol. The *RDC* and the *Radio* layers represent together the physical layer. The *Radio* layer manages the RF chip by providing appropriate software driver while the *RDC* layer implements X-MAC, ContikiMAC, and LPP radio duty cycling protocols [33], [25], [34].

In each experiment the broadcast communication has been obtained by means of the send and receive primitives provided by the Rime stack without any routing protocol. The stack has been configured with the default CSMA/CA (`csma_driver`) and with the RDC layer initialized with a null RDC (`nullrdc_driver`) for the AlwaysOn configuration and with the ContikiMAC RDC (`contikimac_driver`) for the homonymous configuration. The RF chip of the nodes was programmed to communicate using an output power of -3 dBm.

B. The Interferer

We built an internal frequency matching interferer starting from a VirtualSense node with a suitably modified radio layer. In particular, the interferer has been programmed with a Contiki task which initializes the RF chip to generate a randomly-modulated signal, at a constant output power of 7 dBm, and which repeatedly turns off and on the transmission according the T_{busy} and T_{idle} parameters. The value of these parameters have been tuned empirically in order to obtain an appreciable packet loss rate with the constraint that T_{idle} must not be lower than three times the duration of the transmission of the longer packet. This constraint has been imposed to largely ensure that for each packet length there is a time window, without interference, long enough to allow the complete transmission of the message. For each experiments, T_{busy} and T_{idle} have been set respectively to $4ms$ and $12ms$, respectively.

Building the reference systems described in Figure 1 entails modifying the position of the interferer with respect to the sender and to the receiver. While the configuration of Figure 1.(a) is simply obtained by positioning the sender, the receiver, and the interferer close to each other, building the set-up represented in Figure 1.(b) is more complicated due to the variability and uncertainty of the communication range of the nodes. For these reasons we chose to build this set-up synthetically by modifying the sender node radio layer so that, for any value of the SNR measured, the low level CCA function will always returns true (clear channel).

C. Power Measurement

The current consumption of the sensor nodes was measured by continuously sampling the voltage generated across a 49Ω sensing resistor in series with power supply. In particular, the digital waveforms were collected by means of a National Instruments NI-DAQmx PCI-6251 16-channel data acquisition board connected to a BNC-2120 shielded connector block [35], [36]. During the experiments, the monitored node was powered at 3.3V by a NGMO2 Rohde & Schwarz dual-channel power supply [37].

V. Results

A. Model validation

We firstly describe the set of experiments that have been performed in order to validate the mathematical models introduced in Section III, whose results are reported in Figure 5.

Given the experimental set-up described in Section IV we compared the packet reception rate of either an always on receiver and a ContikiMAC based receiver against the results obtained by means of numerical simulations. In the experiments, for both types of receiver configuration, the transmitter could not counteract the interference (so that no collision avoidance strategy could be implemented). Figure 5 clearly illustrates the good accordance between the reliability values achieved through modeling equations and the packet reception rates measured experimentally for different payload lengths.

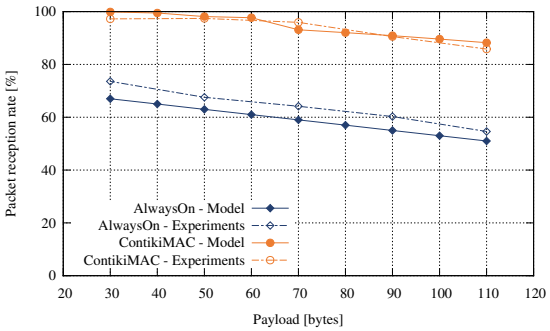


Fig. 5. Comparison of experimental results with models.

B. Packet Reception Rate

In order to get further insights, we extended to other receivers the measurement of the packet reception rate obtained while varying the length of the packet payload. Figure 6 shows the data obtained using different protocols for both configurations described in section III-A. The plots labeled with the suffix "-R" are related to the configuration in which the interference is perceived only by the receiver node, such as in Figure 1.(b). For this reason, the transmitter in this case cannot perform any collision avoidance strategy.

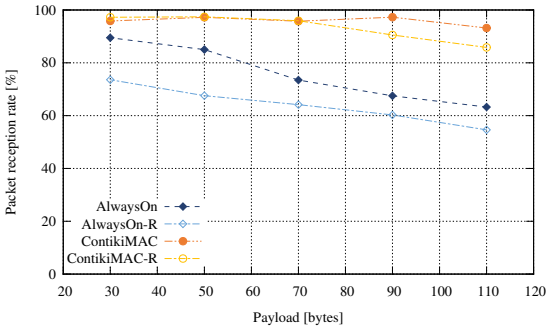


Fig. 6. Packet reception rate as a function of the payload length in different communication protocols.

The CSMA/CA without radio duty cycling protocol (AlwaysOn in Figure 6) shows a strong dependency of the packet reception rate from the length of the packet payload with respect to the ContikiMAC. In particular, when no collision avoidance strategies were performed on the sender node (AlwaysOn-R), we measured the stronger dependency which implies, in the case of the largest payload, the delivery of only about 55% of the total packets. It is interesting to point out how the use of the data packet as a wake up strobe, performed by the low-power radio duty cycling protocol, partially mitigates the effect of the increased collision probability due to the a longer payload. This strategy, together with the collision avoidance mechanism, strongly increases the packet reception rate obtained by ContikiMAC which, in the worst case, does not fall below about 93%.

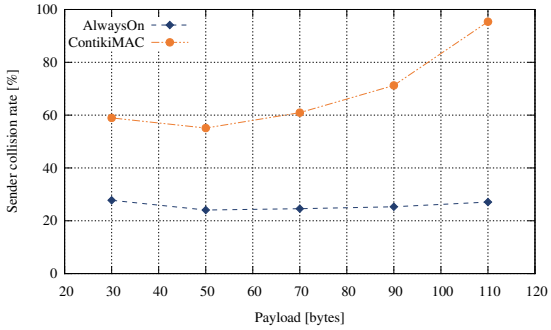


Fig. 7. Collision rate detected by the sender versus payload length in different communication protocols.

The strong reliability shown by ContikiMAC is largely due to the design choice of sending several replies of the data packet as wake up strobes. This great workload, sustained by the transmitting node, if on the one hand increases the communication reliability, on the other, unavoidably, leads to a rising of energy consumption of the transmitter. Moreover, the Contiki transmitter also implements several dedicated collision detection and avoidance strategies which allow it to achieve better performance than normal CSMA/CA mechanisms. In particular, if a collision is detected when sending a single strobe, the transmission of the following strobes is suspended and postponed for a while. This reiterated channel sensing, carried out for each strobe, facilitates the adaptation of the train of strobes to a possible interference pattern.

In order to quantify the effort made by the transmitter, during each run, we counted the number of collisions detected by the sender when it is subject to the interferer signal. Figure 7 plots the sender collision rate versus the payload length for ContikiMAC and for the simple always-on CSMA/CA protocol. Interestingly, for the traditional CSMA/CA protocol the number of collisions detected does not show a dependency on the size of the packet. In fact, the CCA is performed only once before starting the transmission. On the contrary, ContikiMAC always shows a higher value of collisions which, moreover, strongly increases with the length of the packet sent. For instance, with a payload of 110 bytes the collision rate, and consequently the number of retransmissions, grows up to about 95%. This ensures a higher reliability at a strong energy

cost.

To clearly point out how the ContikiMAC sender strategies impact on the communication reliability we introduce Figures 8(a) and (b). These figures report the ContikiMAC behavior by plotting the instantaneous current draw of the sender (blue curve) and of the interferer (red curve). In particular, these plots have been obtained by sampling, at the same time, the current draw by the sender and by the interferer by means of two parallel data acquisition channel to have two synchronized tracks. Figure 8.(a) shows the current peaks corresponding to the strobes burst made by the sender while the interferer was emitting on its range. From the plot it is clear how the ContikiMAC CSMA/CA strategies increase the communication reliability. In fact, we note that the sender, after a first period in which the strobes collide with the interfering signal, starts sending packets exactly on its *idle period* thus resulting in a strong adaptation and a high delivery probability of the last strobes. On the contrary, in the case of a transmitter that can not perceive the interference no adaptations can be done (Figure 8.(b)), and the communication reliability decreases.

C. Packet Corruption Rate

In order to evaluate the effectiveness of the interferer we measured the packet corruption rate at the receiver level. This has been simply defined as the ratio between the number of corrupted packets received at the radio layer (a statistics enabled through the *badcrc* variable in Contiki operating system) and the total number of received packets (counted by means of the *llrx* variable). We use this metric to discover if there is an appreciable dependence of the impact of the interferer from the communication protocols. If true indeed, we must conclude that there is a coupling phenomenon between the interferer and a certain communication mechanism, which implies a non-homogeneous behavior of the interferer.

Figure 9 shows the packet corruption rate when the payload length is varied, for ContikiMAC and always-on CSMA/CA protocols. All the plots show a sizeable dependence of the corruption rate from the packet length but no appreciable correlation with the communication mechanism can be shown. This allows us to state that the generated interference can be considered homogeneous with respect to the tested protocols.

Figure 10 has been obtained by dividing the packet corruption rate, shown in Figure 9, by the bit length of the payload to obtain the Estimated Bit Error Rate (EBER). The data have also been fitted by means of a linear interpolation function and the measured parameters have been reported to the graph. Interestingly, the dependence of the EBER from the payload length is about $1.71 * 10^{-6}$ which is almost two order of magnitude lower than the average value (about $4.46 * 10^{-4}$). For this reason we can consider the probability of corrupting a bit not related to the length of the packet as assumed in the modeling section III.

D. Energy Consumption

The last set of experiments has been carried out to investigate the impact of interference on the energy consumed by the receiver node. In particular, for the entire duration of the test, the current drawn by the receiver node has been sampled and waveforms have been processed to calculate the average energy consumed per delivered bit. It is worth noticing that the energy consumed to receive a corrupted packet is attributed to the packets actually delivered so that the greater the number of corrupted packets received and the greater will be the resulting average energy per bit.

Figure 11 shows the average energy spent for a delivered bit when the payload length increases. As expected, for both communication protocols the energy consumed per bit decreases while the packet size increases, reflecting the fact that, from an energy point of view, it is always convenient to send longer packets despite their greater probability of collision. Moreover, the always-on CSMA/CA protocol, since it never turns off the radio chip, shows an energy consumption of about one order of magnitude greater than the ContikiMAC. It is interesting to note that, for both protocols, the configuration in which the interference is perceived only by the receiver ("-R" plots) entails a greater energy consumption with respect to the corresponding not "-R" configuration. This must be clearly attributed to the increased number of corrupted packets received which are due to the impossibility, for the sender node, of implementing any collision avoidance strategies.

To better highlight the interplay between packet length, energy efficiency, and packet loss we finally introduce Figure 12, which shows a Pareto curve illustrating the trade-off between packet loss rate and energy consumption per bit.

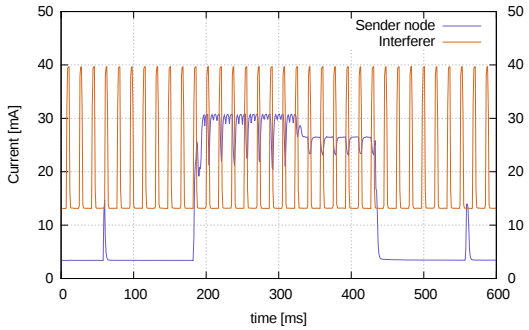
The figure plots (for a given value of the payload size) the average energy consumed for receiving a single bit as a function of the corresponding packet loss rate. Results clearly point out that longer packets, corresponding to lower energy per bit, are not the optimal design choice because of their higher loss rates when subject to interference . On the other hand, shorter packets provide a lower loss rate at the cost of a rapid increase in energy consumption. According to the classic Pareto front of a multiobjective optimization, the optimal choice can be found in a trade-off between energy consumption and packet loss rate using intermediate packet lengths.

VI. Conclusions

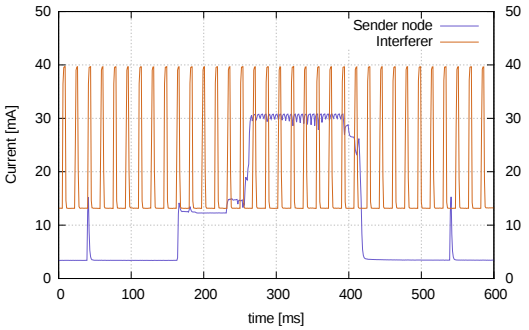
Wireless sensor networks are increasingly considered a cornerstone of sophisticated, distributed cyber-physical systems for a variety of tasks. However, the capability of designing dependable solutions is crucial for successful deployments in realistic scenarios. Electromagnetic interference could severely impact the performance of a WSN, thus prompting for either accurate modeling and detailed experimental evaluation in realistic settings.

To this aim, we presented in this work two contributions: first, we derived an analytical evaluation of the reliability of a communication link subject to interference; second, we performed extensive experiments on real-world low-power sensor nodes to characterize the reliability and energy expenditure of such a system.

We confirmed the impact of packet lengths on reliability under interference: on one side, longer packets have reduced



(a)



(b)

Fig. 8. Instantaneous currents draw of the sender node (blue curve), running the ContikiMAC radio duty cycling, and of the interferer (red curve) while the sender node was inside the activity range (a) and outside of the activity range (b) of the interferer as defined in Figure 1.

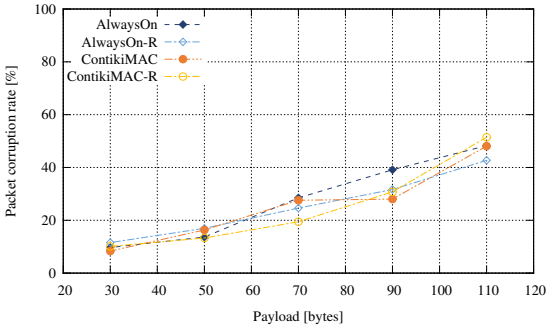


Fig. 9. Comparison of the packet corruption rate Vs payload length in different communication protocols.

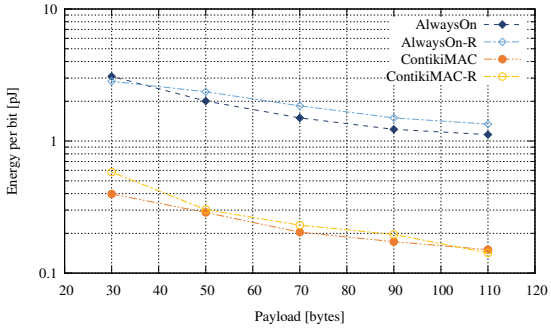


Fig. 11. Average energy spent by the receiver node for a delivered bit versus payload length in different communication protocols.

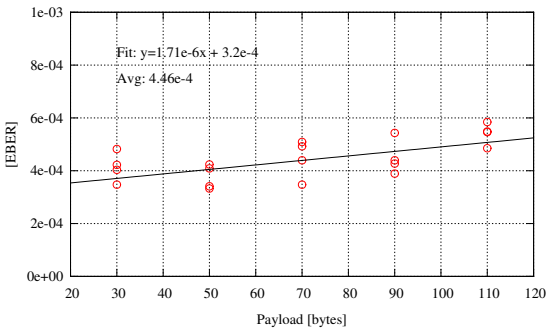


Fig. 10. Estimated Bit Error Rate (EBER) Vs payload length.

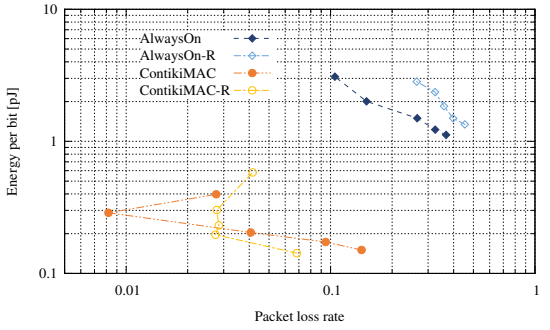


Fig. 12. Pareto curve showing the trade-off between energy spent per delivered bit and packet loss rate in different communication protocols.

impact on data overhead; on the other side they are exposed to higher collision probabilities. We evaluated the performance of ContikiMAC with respect to the dependence of the packet loss ratio from the payload lengths and we characterized the energy efficiency of the system under study by accurately measuring the spent energy with different payload sizes, under different configurations. Experimental results clearly illustrate the trade-off between packet lengths, reliability and energy consumption, summarized by Pareto plots that can provide useful insights for system dimensioning at design-level.

Regarding the possibility of future works we may envision to extend the investigation to other directions. In particular, it would be interesting to analyze the combined effect of interference and packet length on other low-power MAC layers either in an asynchronous context (e.g. X-MAC [33] or LPP [34]) and in synchronous systems (e.g. Orchestra [38]).

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, Feb 2014.

[3] C. Stergiou and K. E. Psannis, "Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey," *International Journal of Network Management*, vol. 27, no. 3, p. e1930, 2017.

[4] A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, and B. B. Gupta, "Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings," *Future Generation Computer Systems*, vol. 82, pp. 349–357, 2018.

[5] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Generation Computer Systems*, vol. 78, pp. 964–975, 2018.

[6] M. Dong, K. Ota, and A. Liu, "RMER: Reliable and Energy-Efficient Data Collection for Large-Scale Wireless Sensor Networks," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 511–519, 2016.

[7] M. Zhao, I. W. H. Ho, and P. H. J. Chong, "An energy-efficient region-based rpl routing protocol for low-power and lossy networks," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1319–1333, 2016.

[8] U. Raza, A. Bogliolo, V. Freschi, E. Lattanzi, and A. L. Murphy, "A Two-Prong Approach to Energy-Efficient WSNs: Wake-Up Receivers plus Dedicated, Model-Based Sensing," *Ad Hoc Networks*, vol. 45, pp. 1–12, 2016.

[9] A. Bogliolo, E. Lattanzi, and V. Freschi, "Idleness as a Resource in Energy-Neutral WSNs," in *ENSSys '13: Proceedings of the 1st International Workshop on Energy Neutral Sensing Systems*. New York, NY, USA: ACM, 2013, pp. 1–6.

[10] A. Sikora and V. Groza, "Coexistence of ieee802. 15.4 with other systems in the 2.4 ghz-ism-band," in *IEEE Instrumentation and Measurement Technology Conference Proceedings*, vol. 22, no. 2. IEEE; 1999, 2005, p. 1786.

[11] P. Lettieri and M. B. Srivastava, "Adaptive frame length control for improving wireless link throughput, range, and energy efficiency," in *INFOCOM'98. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 2. IEEE, 1998, pp. 564–571.

[12] M. C. Vuran and I. F. Akyildiz, "Cross-layer packet size optimization for wireless terrestrial, underwater, and underground sensor networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008, pp. 226–230.

[13] J. Brown, U. Roedig, C. A. Boano, and K. Römer, "Estimating packet reception rate in noisy environments," in *Local Computer Networks Workshops (LCN Workshops), 2014 IEEE 39th Conference on*. IEEE, 2014, pp. 583–591.

[14] A. King, J. Brown, J. Vidler, and U. Roedig, "Estimating node lifetime in interference environments," in *Local Computer Networks Conference Workshops (LCN Workshops), 2015 IEEE 40th*. IEEE, 2015, pp. 796–803.

[15] W. Dong, C. Chen, X. Liu, Y. He, Y. Liu, J. Bu, and X. Xu, "Dynamic packet length control in wireless sensor networks," *IEEE Transactions on wireless communications*, vol. 13, no. 3, pp. 1172–1181, 2014.

[16] J.-S. Han and Y.-H. Lee, "Interference-Robust Transmission in Wireless Sensor Networks," *Sensors*, vol. 16, no. 11, p. 1910, 2016.

[17] M. Michel, T. Voigt, L. Mottola, N. Tsiftes, and B. Quoitin, "Predictable MAC-level Performance in Low-power Wireless under Interference," *EWSN '16 Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks*, pp. 13–22, 2016. [Online]. Available: https://dl.acm.org/citation.cfm?id=2893714

[18] A. Iyer, C. Rosenberg, and A. Karnik, "What is the right model for wireless channel interference?" *IEEE Transactions on Wireless Communications*, vol. 8, no. 5, 2009.

[19] G. Bianchi, "IEEE 802.11-saturation throughput analysis," *IEEE Communications Letters*, vol. 2, no. 12, pp. 318–320, 1998.

[20] T. Issariyakul and E. Hossain, "Introduction to Network Simulator 2 (NS2)," in *Introduction to Network Simulator NS2*. Springer, 2012, pp. 21–40.

[21] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Transactions on information theory*, vol. 46, no. 2, pp. 388–404, 2000.

[22] C. A. Boano, Z. He, Y. Li, T. Voigt, M. Zúñiga, and A. Willig, "Controllable radio interference for experimental and testing purposes in Wireless Sensor Networks," *Proceedings - Conference on Local Computer Networks, LCN*, pp. 865–872, 2009.

[23] C. A. Boano, T. Voigt, C. Noda, K. Romer, and M. Zuniga, "JamLab: Augmenting sensornet testbeds with realistic and controlled interference generation," *Proceedings of the 10th ACM/IEEE International Conference on Information Processing in Sensor Networks*, pp. 175–186, 2011.

[24] Universal software radio peripheral (usrp). Ettus Research LLC. [Online]. Available: http://www.ettus.com

[25] A. Dunkels, "The ContikiMAC Radio Duty Cycling Protocol," *SICS Technical Report T2011:13 , ISSN 1100-3154*, pp. 1–11, 2011. [Online]. Available: http://dunkels.com/adam/dunkels11contikimac.pdf

[26] M. Holland, T. Wang, B. Tavli, A. Seyedi, and W. Heinzelman, "Optimizing Physical-Layer Parameters for Wireless Sensor Networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 7, no. 4, p. 28, 2011.

[27] E. Lattanzi, V. Freschi, and A. Bogliolo, "Supporting preemptive multitasking in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, pp. 1–10, 2014.

[28] CC2538 Powerful Wireless Microcontroller System-On-Chip for 2.4-GHz IEEE 802.15.4, 6LoWPAN, and ZigBee Applications. Texas Instruments. [Online]. Available: http://www.ti.com/lit/ds/symlink/cc2538.pdf

[29] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki - A Lightweight and Flexible Operating System for Tiny Networked Sensors," in *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks*, ser. LCN '04. Washington, DC, USA: IEEE Computer Society, 2004, pp. 455–462. [Online]. Available: http://dx.doi.org/10.1109/LCN.2004.38

[30] N. Brouwers, K. Langendoen, and P. Corke, "Darjeeling, a feature-rich VM for the resource poor," in *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*, ser. SenSys '09. New York, NY, USA: ACM, 2009, pp. 169–182. [Online]. Available: http://doi.acm.org/10.1145/1644038.1644056

[31] E. Lattanzi and A. Bogliolo, "Hardware filtering of non-intended frames for energy optimisation in wireless sensor networks," *International Journal of Sensor Networks*, vol. 15, no. 2, p. 10, 2014.

[32] T. Watteyne, V. Handziski, X. Vilajosana, S. Duquennoy, O. Hahm, E. Baccelli, and A. Wolisz, "Industrial Wireless IP-Based Cyber-Physical Systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1025–1038, 2016.

[33] M. Buettner, G. V. Yee, E. Anderson, and R. Han, "X-MAC: A Short Preamble MAC Protocol for Duty-cycled Wireless Sensor Networks," in *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems*, ser. SenSys '06. New York, NY, USA: ACM, 2006, pp. 307–320. [Online]. Available: http://doi.acm.org/10.1145/1182807.1182838

[34] R. Musaloiu-E., C.-J. M. Liang, and A. Terzis, "Koala: Ultra-Low Power Data Retrieval in Wireless Sensor Networks," in *2008 International Conference on Information Processing in Sensor Networks (ipsn 2008)*, 2008, pp. 421–432. [Online]. Available: http://ieeexplore.ieee.org/document/4505492/

[35] Pc-6251 datasheet. National Instruments. [Online]. Available: http://www.ni.com/pdf/manuals/375213c.pdf

[36] Installation guide bnc-2120. National Instruments. [Online]. Available: http://www.ni.com/pdf/manuals/372123d.pdf

[37] Ngmo2 datasheet. Rohde & Schwarz. [Online]. Available: https://www.rohde-schwarz.com/it/brochure-scheda-tecnica/ngmo2/

[38] S. Duquennoy, B. Al Nahas, O. Landsiedel, and T. Watteyne, "Orchestra: Robust Mesh Networks Through Autonomously Scheduled TSCH," in *Proceedings of the 13th ACM conference on embedded networked sensor systems*. ACM, 2015, pp. 337–350.

Valerio Freschi graduated in Electronic Engineering at University of Ancona, Italy, in 1999 and received the Ph.D. degree in Computer Science Engineering from University of Ferrara, Italy in 2006. He is currently Research fellow in Computer Engineering at the Department of Pure and Applied Sciences (DiSPeA) of the University of Urbino, Italy. His research interests include wireless sensor networks, energy-efficient algorithms, bioinformatics, mobile crowdsensing.

Emanuele Lattanzi received the Laurea degree (summa cum laude) in 2001 and the Ph.D. degree from the University of Urbino, Italy, in 2005. Since 2001, he has been with the Information Science and Technology Institute, University of Urbino. In 2003, he was with the Department of Computer Science and Engineering, Pennsylvania State University, as a Visiting Scholar with Prof. V. Narayanan. Since 2008, he has been Assistant Professor of Information Processing Systems with the University of Urbino, Italy. His research interests include wireless sensor networks, wireless embedded systems, energy-aware routing algorithms, dynamic power management, multimedia applications, and simulation.