Computer Networks 167 (2020) 106986

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Experimental evaluation of the impact of packet length on wireless sensor networks subject to interference

Emanuele Lattanzi [a,*], Paolo Capellacci [a], Valerio Freschi [a]

Department of Pure and Applied Sciences, University of Urbino, Piazza della Repubblica 13, Urbino 61029, Italy

ARTICLE INFO

Article history:
Received 3 April 2019
Revised 22 August 2019
Accepted 7 November 2019
Available online 16 November 2019

Keywords:
Experimental study
Wireless sensor networks
Communication performance
Interference

ABSTRACT

Wireless sensor networks are nowadays considered an enabling technology for a wide spectrum of cyber-physical systems applications. However, in order to cope with stringent dependability and energy efficiency requirements, several research challenges have to be solved. Electromagnetic interference, for instance, adversely affects wireless communication, resulting into increased packet collisions and network congestion, and also increasing the energy consumption of devices. Highlighting the complex interplay between communication under interference and parameters of sensor networks is therefore mandatory for driving design choices and improving system performance. In this work we propose an experimental study of the reliability and energy efficiency of IEEE 802.15.4 compliant sensor networks under controlled interference, as a function of the packets length. The results of an extensive set of experiments on an ample range of low-power asynchronous, medium access protocols point out the trade-off between energy consumption and robustness to interference and also provide a comparative view of the protocols, thus indicating useful guidelines in the choice and in the design of several critical components.

1. Introduction

The widespread diffusion of wireless sensor networks (WSN) as enabling technology for planning sophisticated, ubiquitous cyber-physical systems motivates research efforts towards the design of reliable and energy efficient solutions [1].

However this endeavor is hampered by several factors, such for instance operativeness in environments subject to interference. Indeed, transmissions over a wireless medium could interfere with simultaneous transmissions from other nodes of the network or with other radio frequency devices operating within the same frequency range, often resulting in the impossibility of correct decoding at the receiver. The former type of interference is classified as *internal* while the latter is usually referred to as *external*. Specifically, dense WSN deployments are particularly prone to internal interference, while external interference is basically due to partial or complete overlapping of radio communication with that of other devices operating within the 2.4 GHz ISM band (e.g. Wi-Fi 802.11b/g/n or Bluetooth transceivers). Consumer electronics appliances (e.g. microwave ovens) could also generate interference within the 2.4 GHz ISM band because of electromagnetic compatibility issues [2].

Regardless of the type, interference impacts both the reliability of communication, thus determining dependability issues, and the energy consumption of sensor nodes, potentially impairing energy-aware communication protocols and power management techniques. As a consequence, detailed analysis of the interplay between interference and system-level design parameters is crucial for predicting the performance of low-power networked embedded systems [3,4].

In this article we introduce an extensive experimental study aimed at evaluating the effect of the packet length on the performance of communication links between pairs of low-power sensor nodes under interference. Interference signals are generated in a controllable manner according to pre-defined patterns, following the approaches proposed in recent scientific literature. The effect of the payload size is examined by evaluating different metrics and in a variety of possible configuration settings. Regarding the metrics, we propose an experimental set-up for: *i)* estimating the reliability of communication (e.g. in terms of packet reception rate); *ii)* measuring energy consumption at the receiver side. For what concerns the configurations, we analyse several state of the art low-power, medium access control (MAC) protocols based on the duty-cycling approach, together with an always active receiver used as baseline; for each of the studied low-power MAC layer we also provide a comprehensive summary to review its main features. The above described methodology enables a thorough exploration of the effects of interference on the system under

* Corresponding author.
E-mail address: emanuele.lattanzi@uniurb.it (E. Lattanzi).

https://doi.org/10.1016/j.comnet.2019.106986
1389-1286/

study, thus providing useful information to be exploited at design level.

The remainder of the article is organized as follows: in Section 2 we introduce some contributions in recent scientific literature and discuss their relationships with our approach; in Section 3 we recall some basic concepts regarding standard low power communication stack (namely the IEEE 802.15.4 standard) and interference in wireless communication (with a focus on reproducibility issues); in Section 4 we review the basics of the adopted radio duty-cycling protocols; in Section 5 we illustrate the set-up used for the experiments; in Section 6 we present the results and discuss their significance; in Section 7 we conclude with a brief summary of the contributions and with final considerations.

2. Related work

There is a significant amount of research contributions in scientific literature regarding the relation between interference and communication performance considering packet length in WSN. In this section we will outline what are the most relevant with respect to our work in a comparative perspective.

The most representative studies can be coarsely divided into two main categories: analytical models/simulations and experimental studies. An analytical modeling of the effect of packet length on throughput, distance, and energy has been presented by Lettieri and Srivastava in [5]. The authors proposed to adapt the length of the data frames in order to better match wireless channels conditions and derived an analytical model for evaluating the effect of packet length on throughput, distance, and energy, validating their approach on devices equipped with WaveLAN radios. The problem of optimizing packet size in wireless sensor networks has been tackled by Vuran and Akyildiz with a focus on the effects of packet length on multi-hop WSN [6] under a general architecture (e.g. without any specification regarding MAC protocols), with validation provided in terms of numerical simulation. In [7], adaptation of transmission rate and payload size in response to interference variations has been proposed. The proposed approach has been validated by means of numerical simulations. In [8], a methodology for estimating the probability distribution function of idle period lengths of the interferer is presented. The probability distribution is then used to evaluate the interference level and the packet reception rate as a function of packet length. The main difference between our work and these studies is due to the fact that we present an experimental evaluation of the effect of packet size on the performance of systems implementing low-power protocols compliant with the IEEE 802.15.4 standard. In particular, we perform significant testing on real-world sensor nodes, subject to a controlled interference, by measuring reliability and energy efficiency in a wide range of possible configurations (i.e. with motes running different low-power MAC protocols).

Among the different works that have tackled the problem from the experimental point of view, Son et al. experimentally studied the effect of concurrent packet transmissions in low-power wireless networks and demonstrated the feasibility of successful packet reception with high probability even in the presence of concurrent transmissions if the signal-to-interference-plus-noise-ratio (SINR) exceeds a critical threshold [9]. In this case, the experiments were performed on a MAC protocol (namely, S-MAC [10]) configured without sleep cycles. Guo et al. studied the practical performance of Zigbee platforms when WiFi, Bluetooth and microwave oven interference sources are deployed in the same office environment [11]. In particular, they measured the received signal strength indicator, the link quality indicator, and the packet error rate as a function of distance, channel, and transmission power. Dong et al. introduced a strategy for adaptively deciding the size of payloads given the estimate of the quality of a link [12]. They evaluate its performances in a real testbed without any generated interference. King and co-authors proposed a method for estimating the energy consumption (hence the lifetime) of ContikiMAC-based motes, working in interference environment [13]. Naderi et al. presented an experimental study for quantifying (in terms of packet reception rate and RSSI) the effect of radio waves energy harvesting on data communication interference [14]. In [15] an experimental evaluation of the energy expenditure and packet reception rate of Contiki-driven WSN430 nodes (with X-MAC as medium access layer) is presented while Michel et al. analysed the ContikiMAC layer under interference, modeled and measured packet delivery rate and latency [4].

Differently from this second category of the works listed above, we experimentally investigate the impact of payload size in a single communication link where the pair of nodes is subject to interference, by performing measurements on state-of-the-art duty-cycling systems. In fact, we provide experimental measurements of the packet reception rate and of the energy consumption as a function of the payload size in a different interference setting (i.e. interference levels can be tuned according to specified patterns) and for different low-power duty cycling protocols (viz. X-MAC [16], LPP [17], and ContikiMAC [18]).

In summary, the above mentioned works focus on different aspects of the problem, but none of them investigates, as a whole, the following issues:

1. How packet size affects link communication reliability and energy consumption;
2. Experimental assessment of a range of specific, state-of-the-art, asynchronous duty cycling protocols for ultra-low-power applications;
3. Adoption of a set-up that enables to study the effect of precise and tunable interference levels.

In this work we aim at filling this gap by providing a thorough evaluation which attempts to encompass all these aspects.

3. Background information

3.1. The IEEE 802.15.4 Standard

The 802.15.4 standard was developed starting in 2000 from a joint work of the ZigBee and the IEEE 802 working groups. The main goal of this standard was to design a wireless communication protocol with ultra-low complexity and cost to be used in low-rate inexpensive fixed or portable devices operating in residential and industrial environments. Thanks to its low power requirements the 802.15.4 became very soon the main standard used for communicating in WSNs [19].

From the technical point of view, the standard defines both the physical layer (PHY) and medium access control (MAC) sublayer. The PHY layer can operate both in the unlicensed industrial scientific medical (ISM) 2.4 GHz band or in the ISM 868 MHz and 915 MHz bands available in Europe and North America respectively. The different communication bands involve different channel numbers with different transfer rates. In fact, the 2.4 GHz band provides 16 channels with a data rate of 250 kbits/s while the 915 MHz band has been divided into 10 channels with a data rate of 40 kbits/s. Finally, only one channel, with a data rate of 20 kbits/s, is provided in the 868 MHz band.

The MAC layer manages association and disassociation, frame acknowledgment, channel access, validation, and beacon creation. Compared to the MAC layer of 802.15.1 (Bluetooth™), which contains about 131 primitives, the 802.15.4 MAC layer, with its 26 primitives, shows a very low complexity making it suitable for low cost devices such as sensors nodes.

Furthermore, the MAC frame structure is very flexible and simple to manage the needs of different network sizes and topologies. For instance, the size of the address field may vary between 0 and 20 bytes in order to build networks containing up to 1 million devices. In addition, short 8-bit device addresses or 64-bit IEEE device addresses can also be used. This flexible structure helps to increase the efficiency of the protocol by keeping the packets short. Finally, the payload field may not exceed 127 bytes in length so that, to send larger data packet, an application level packetization is needed.

Other important features of the 802.15.4 standard are: real-time suitability, channel sensing multiple access with collision avoidance (CSMA/CA), support to encrypted communications and to link quality and energy detection.

3.2. Wireless interference

In wireless communication, symbols decoding can be viewed as a stochastic process whose probability depends upon several physical conditions which alterate the electromagnetic signal. For instance, the desired signal is normally compounded with thermal noise, several interfering signals, and, moreover, it is attenuated and distorted over the distance. In this scenario, successfully decoding a wireless bit is strictly related with the capability of the receiver to recognize the signal pattern transmitted by the sender by treating the sum of all the other on-going signal transmissions as noise [20]. In order to increase the communication reliability several strategies such as error detecting codes, for instance the cyclic redundancy check (CRC), or such as the error correcting code (ECC) have been implemented which can mitigate the dangerous effect of spurious interferences.

The concept of interference can be treated at various levels of abstraction and at different levels of depth but, for our purpose, we can assume that an interference can be represented by any signal, perceived at sender or receiver level, which results above the Clear Channel Assessment (CCA) threshold for a time long enough to prevent a symbol decoding. According to this definition each interfering signal can be represented as a binary value changing over the time. In particular, as represented in Fig. 1, the interference can be characterized by the time in which its energy is below (T_{idle}) or above (T_{busy}) the CCA threshold.

Given an idle interval of length T_{idle} and given a data packet transmission time T_{data} a collision may occur if a data packet is transmitted after a time interval T_d for which ($T_{data} + T_d > T_{idle}$). Notice that, this definition assumes, for sake of simplicity, no ECC strategies at the receiver, so that each colliding bit leads to the whole packet corruption which will be discarded at physical level.

Creating reproducible and well-controlled interference patterns has been a research goal of several authors. In particular, generating a realistic and repeatable external interference have been mostly addressed by recording a real interference pattern and then playing it back using a dedicated wireless transceiver [3]. In order to improve the accuracy while reproducing the interference, several dedicated devices, such as the Universal Software Radio Peripherals (USRP)can be used [21]. Thanks to these devices, it is possible to produce any desirable radio pattern by easily programming its radio transceiver. The main feature of these professional devices is their high degree of stability and reproducibility which allow a faithful replaying of previously collected interference traces.

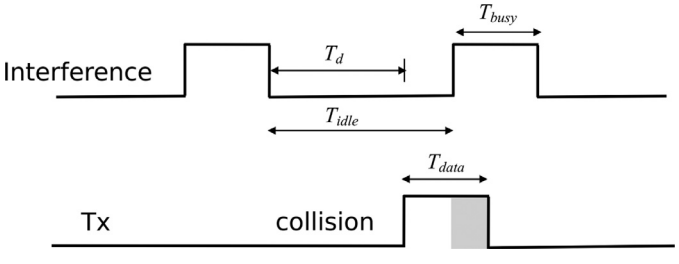

Fig. 1. Periodic interference square wave timing.

From a technical point of view, generating internal interferences is simpler with respect to the external interference thanks to the exact frequency matching between the interfering and the interfered signals. In fact, the most obvious and easy way is to program a node of the network to continuously send broadcast packets at a predefined transmission rate. The interference generated in this way leads to a heavy channel occupation which increases communication latency, collision probability, and packet jamming but its major drawback, despite its simplicity, is due to its low tuning capability and to the strong dependency of the generated interference from the software stack of the sending node [3]. As described by Boano et al. in 2009, a more suitable and practical way to generate internal interference can be smoothly implemented by means of some RF transceivers available on sensor nodes, such as the Texas Instruments' CC2420 [22]. In particular, the proposed solution is based on different transmit test modes, available on these transceivers, through which it is possible to send a continuous unmodulated or randomly-modulated carrier without the need of any other hardware device. For instance, the unmodulated carrier, which shows a concentrated power spectrum peaking at the center frequency, can generate an interference pattern which is similar to a background noise while, the randomly-modulated signal, showing a power spectrum distributed across the channel bandwidth, can be used to emulate short bursts of interfering packets. In order to obtain a tunable and reproducible interference Boano et al. suggest two alternative strategies. The first one is aimed at manipulating the SNR of the wireless medium by means of a radio chip producing a continuous unmodulated carrier. The SNR tuning is obtained by varying the transmission power of the radio chip at a desired level. The second strategy, on the other hand, is intended to emulate repeated bursts of interfering packets by configuring the transmission power of the interferer to its maximum level (so as to avoid any kind of communication) and then intermittently switching it on and off. This results is an interfering square wave characterized by two parameter which are: the time in which the transmitter is on (T_{busy}) and the time in which it is off (T_{idle}).

According to this assumptions we can define the channel occupancy rate of the interference signal ρ, also known as the duty cycle of the square wave, by means of Equation 1:

$$\rho = \frac{T_{busy}}{T_{busy} + T_{idle}} \tag{1}$$

By properly varying these two parameters, different levels of interference can be achieved.

4. Radio duty cycling protocols for WSNs

The need to save energy and extend the network lifetime is crucial in WSNs and one of the most promising ways to achieve it is to reduce the idle listening of the radio chip. It has been shown that the energy spent by a node to listen the wireless medium, even though no packets are being transmitted, is one of the most significant contributions in its energy budget [23,24]. Accordingly, a great attention has been paid, in the last years, to the design of low-power MAC protocols which, generally, shut-down the radio chip and periodically wake-up it to sense the wireless medium by means of a CCA. For this reason they are also called Radio Duty Cycling (RDC) protocols.

Popular RDC protocols can be roughly categorized into *synchronous* and *asynchronous* approaches, along with hybrid

combinations. Synchronous protocols, define a schedule that specifies when a node should be awake and asleep within a communication frame. Nodes, in fact, periodically exchange synchronization packets to share a schedule information in order to coordinate the periods of wake-up/sleep and to reduce the unnecessary time in idle listening. However the generated overhead could in principle increase network traffic and energy consumption. On the other hand, asynchronous protocols rely on preamble sampling, also called *Low Power Listening* (LPL), to negotiate a transmission between sender and receiver nodes. This family of protocols shows no control overhead (unlike synchronous approaches) but, as a counterpart, it could lead to significant increase of delay for the sender to meet the receiver's active period [25]. Indeed, because of the above mentioned overhead, synchronous protocols like the recently developed and standardized Time Synchronized Channel Hopping (TSCH) [26] pose significant challenges (for instance in the computation of scheduling schemes [27]) thus making their adoption questionable especially in low-rate traffic scenarios; moreover, asynchronous protocols facilitate dynamic applications, where nodes may flexibly join and leave the network [28] and also provide a low-complexity design choice for applications which are not latency-critical but with strong energy efficiency requirements [29]. Hence, at time of this writing, asynchronous duty-cycling solutions still represent a reference choice in many research and industrial deployments, making it interesting to evaluate their performance in an interference environment. In this work, we therefore decided to focus on asynchronous protocols to assess the impact of packet length on some performance metrics

The asynchronous RDC protocols can furthermore be divided in *sender-initiated* and *receiver-initiated* protocols based on the fact that the rendezvous, between the transmitter and the receiver, is initiated by the sender rather than by the receiver.

In a sender-initiated protocol, when a sender has data to be sent, it transmits a preamble that is at least as long as the sleep period of the receiver. When the receiver will wake up, if it detects the preamble, it will stay awake to receive the data. This class of protocols implements mechanisms aimed at reducing the collision probability between different sender such as the Carrier-sense Multiple Access with Collision Avoidance (CSMA/CA).

In a receiver-initiated protocols every time a node wakes up from its sleep period it sends a small packet (called *probe*) containing its own ID to notify its presence to a possible sender. If a node has a packet to be sent it wakes up and waits for a probe from the receiver before start to send. The aim of the receiver-initiated protocols is to reduce the overhead of collision between two or more sender which, in a sender-initiated protocol would compete for the channel, by leaving to the receivers the task of reserving a channel time slot. Receiver-initiated protocols can also make use of CSMA/CA mechanisms before probes sending.

Despite the large number of protocols introduced by the scientific community, we focus the presented work on the three popular asynchronous RDC mechanisms provided by Contiki which is one of the most widespread operating systems for wireless sensor networks [30]. In particular we analyse the impact of packet length on the communication performance for ContikiMAC [18], X-MAC [16], and LPP [17] protocols under interference. It is worth noticing that the choice of these three MAC protocols allows us to compare different protocols running on the same hardware-software platform, adding to the consistency of the experimental framework.

4.1. ContikiMAC

ContikiMAC is an asynchronous sender-initiated RDC protocol. In particular, a sender which has a packet to be transmitted, instead of sending a long preamble to meet the wake-up period of the receiver, it repeatedly sends a copy of the data packet to be sent until either an acknowledge (ACK) is received or the total transmission time exceeds the receiver wake-up interval. Every reply of the packet is called strobe.

In order to receive a packet, a node must wake up periodically to sense the wireless channel by means of two consecutive CCA. If both succeed (clear channel) there is no data packet to be received and the node can go back to sleep to save power. If at least one CCA fails (busy channel), the node must stay awake to receive the incoming packet.

When the node receives the data packet it looks at the target node ID and, in case of mismatch, it immediately returns to sleep. Otherwise the packet will be completely decoded, then an ACK will be sent to sender, and the receiver will be switched off until the next wake up interval [18,31].

Unicast transmission fails if no ACK is received after a time which corresponds to a wake-up interval. In this case, ContikiMAC notify the upper network stack level which can decide if schedule a retransmission or not.

In the broadcast communication no ACK is sent by the receiver and, as we must guarantee that each node in the range can receive the packet, the sender must keep 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).

The ContikiMAC protocol provides a number of optimization strategies dedicated to further reduce energy consumption. For instance, the *fast sleep optimization* strategy is aimed to help a receiver node to determine if a negative CCA (channel busy) was caused by noise rather than an incoming packet. In the first case, in fact, the node can be immediately switched off, with no consequence on the communication, in order to save power. This strategy is based on the ContikiMAC timing constraints, and, in particular, it tries to identify those radio patterns which are not related to a real transmission but which are the result of interfering signals [4]. 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. This *reception window* is defined as $2 * t_l + t_i$, where t_l is the transmission time of the longest possible packet and t_i is the interval between each strobe transmission [18].

Another mechanism, called *phase-lock* allows senders to optimize the energy spent in sending strobes. In particular, a sender learns the wake-up schedule of a neighbor, so that it start sending strobes only in proximity of its wake-up time. This results in a strong reduction of strobes required to achieve a transmission. Once the sender knows the neighbor wake-up time, the phase-lock is established and, on average, two strobes are sufficient: the first one is needed to notify the receiver and the second one is the data which is successfully received. Obviously, reducing the average number of strobes reduces the channel utilization with a direct benefit on the communication reliability and energy consumption [32].

Finally, also the CSMA/CA mechanism adopted in ContikiMAC has been optimized to further reduce data collision and to increase communication reliability. In fact, ContikiMAC checks the availability of the channel before and during strobes transmission by performing several CCAs. Since the interval covered by the CCAs is slightly longer than the time between two successive strobe transmissions, if a CCA succeeds after the transmission of a strobe, it informs the sender that apparently no other transmission is occurring so that it can keeps sending strobes. On the other hand, if one

CCA fails (channel busy), the node stops sending strobes that will be resumed after a while [32].

4.2. X-MAC

X-MAC is another well-known asynchronous sender-initiated RDC protocol. The unicast transmission is obtained by means of a preamble sampling techniques introduced by B-MAC and LPL protocols [33,34]. While in B-MAC the receivers are notified of incoming frames by means of the transmission of a long preamble, the duration of which must be greater than the wake-up interval, in X-MAC the long preamble is replaced by a stream of short packets, called strobes, containing only the destination address. A receiver periodically wakes-up and listens the medium looking for a strobe. As soon as it catches a matching strobe (containing its address) it replies with a strobe-ACK to notify the sender. When the sender receives the strobe-ACK it can stop sending strobes and proceed to send the data packet [16].

In this case, the transmission can fail in two different conditions: (i) the sender does not receive a strobe-ACK after a time corresponding to a wake-up interval; (ii) the receiver does not receive the data packet transmitted by the sender. In both cases X-MAC does not plan any retransmission that, possibly, will be required by the upper network-stack layer. Notice that, the original definition of X-MAC does not require sending a data-ACK after the reception of a data packet.

The broadcast transmission makes use of a stream of strobes containing a null destination address and that must last longer than a wake-up interval to allow all the receivers to hear it. Of course, no strobe-ACK is sent by receivers.

The X-MAC implementation provided by Contiki slightly differs from the original version described in [16]. In particular, the most significant changes are the *encounter optimization*, the *reliable data transmission*, the *collision avoidance mechanism*, and the *broadcast mechanism*.

The encounter optimization is a mechanism similar to the Contiki phase-lock which allows a sender to learn the wake-up schedule of the neighboring receivers in order to reduce the number of strobes to be sent during unicast transmission.

The reliable data transmission, on the other hand, aims to increase the communication robustness by introducing a data-ACK after packet reception. For such transmissions the sender stays awake waiting for the ACK.

For what concerns the collision avoidance mechanism, we must highlight that Contiki does not provide a full implementation of the X-MAC but it limits the carrier sensing to the sending of the strobes. This involves that, after receiving a strobe, the sender will start transmitting the packet without worrying about channel occupation, thus increasing the risk of collision [32].

Finally, it is critical to point out that Contiki X-MAC provides two different implementation of the broadcast mechanism. The first implementation is the pure X-MAC broadcast mechanism which entails the use of strobe packets containing the null address as destination address. When a node hears one of these strobe packets, it does not shut down the radio but it waits for the packet transmission. This mechanism ensures that all nodes that have listened the strobe will receive the broadcast packet at the same time (the time the broadcast packet arrives), but it increases the energy spent by the receivers which have to be awake until the data packet arrives. In a second available implementation (the default), the sender instead of sending strobes, simply sends the broadcast packet itself. This entails that receivers do not need to keep their radio on for a time longer than a check interval and they can save valuable energy. The only weakness of this mechanism is that the broadcast reception is no more atomic because the nodes receive their broadcast packet at different times. This makes it impossible to use broadcast packets to perform some kind of fine synchronization at the application level.

4.3. LPP

LPP stands for *Low Power Probing* and it is a receiver-initiated RDC protocol [17]. It replaces the passive channel probing at the receiver level, usually made by means of a CCA, with an active probing which consists of periodically sending broadcast packets that contain only the node ID. In particular, each receiver node, at wake-up, sends a probe to announce its presence to a potential sender. If a sender hears the probe, and if it has a packet to be delivered to the probing node, it acknowledges the probe and then sends the packet to the destination. From the receiver point of view, if an acknowledge is received after the probe the node remains active waiting for the packet, otherwise it goes back to sleep. Replacing the CCA with the active probing obviates the need for long or repeated preambles thus reducing the average channel occupation.

In LPP the transmission can fail in two different conditions: (i) the sender does not receive a probe from the receiver so that it does not send the packet; (ii) the receiver does not receive the data packet once transmitted. In the first case, the sender can buffer the packets (compatibly with the available memory) for future transmissions, while, in the second case, as the original implementation of LPP does not require sending a data-ACK after a packet reception, no retransmission can be triggered and the packet will be definitely lost.

The broadcast transmission is simply obtained by replaying the send of the packet for each received probe. Of course, for LPP the broadcast transmission is intrinsically not atomic.

Potentially, LPP protocol can make use of CSMA/CA strategies both for probes and data sending to reduce collision and increase reliability. The implementation of LPP provided by Contiki OS, however, carries out the channel sensing only before sending the probe, leaving the actual transmission more prone to collide. Finally, in order to increase the reliability, Contiki LPP (contrarily to the original version) requires a data-ACK after packet reception that allows the upper stack layer to implement a retransmission.

5. Experimental set-up

To gauge communication and energy performance of low power WSN, we conceived a set-up composed of: *(i)* a sender node (*Sender*), continuously transmitting packets of given, specified, length; *(ii)* a receiver node (*Receiver*) that listens to channel for incoming transmissions; *(iii)* an interference generator in charge of emitting a signal according to specific patterns.

Regarding the position of the interference source with respect to that of transmitter and receiver nodes, we can identify two operating conditions for the system under study, as depicted in Fig. 2(a) and .(b). Namely, Fig. 2(a) refers to a situation where the interference signal both affects the sender and the receiver, while Fig. 2(b) corresponds to a situation where the interference only impacts the receiver. Since low power protocols usually implement carrier sensing and collision avoidance (CSMA/CA) solutions, the two conditions result into different communication dynamics. Indeed, the transmitter could decide to immediately send a packet or to postpone it (according to the measured Signal-to-Noise ratio (SNR)), while the receiver, after having listened to the wireless channel, could optionally shutdown the radio transceiver in order to save energy if it doesn't detect any ongoing transmission.

As a consequence, in the case of Fig. 2(a) the transmitter can react to the interference signal by adapting to its dynamics, hence mitigating its effect. Conversely, in the case illustrated in Fig. 2(b), the sender node cannot enforce any compensation.

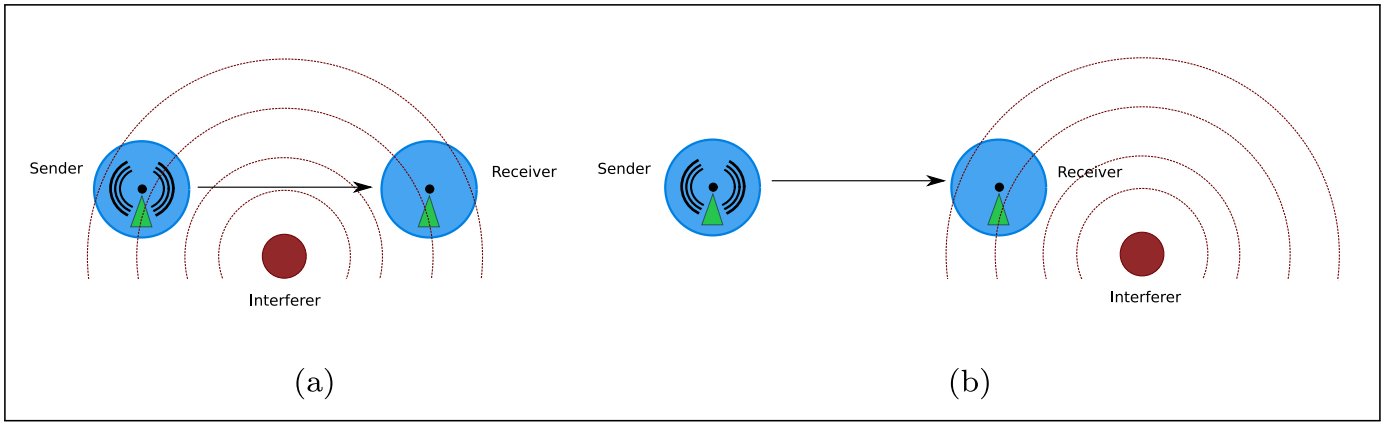

Fig. 2. Reference scheme of the system. (a) The activity of the interferer affects either the sender and the receiver; (b) Only the receiver is located within the influence range of the interference source.

The measurement set-up that we used for the experimental assessment is composed of two sensor nodes and an interference source, placed in an office environment in proximity to each other ($< 1m$). The features of sensor nodes and interference generator are described in the following subsections.

Results and statistics were collected from experiments lasting 30 min. Each trial was conducted on the IEEE 802.15.4 channel 26 (thus avoiding any overlap with WiFi communications) and consisted of the transmission of about 1000 broadcast and unicast packets.

5.1. Wireless sensor node

The sensor node chosen for the transmitter and the receiver is VirtualSense [35], an ultra low-power sensor platform based on the TI CC2538 system-on-chip designed for 2.4-GHz IEEE 802.15.4 applications [36]. Its software stack is built around the Contiki operating system [30] and the Darjeeling java compatible virtual machine [37], which have been properly modified in order to enable concurrent execution of typical WSN tasks with reduced power consumption (about few μW on average) [31]. Indeed, VirtualSense inherits the low-power Contiki network stack called *Rime*, 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 contains the application, the transport and the routing layers as expected in 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, together, constitute the physical layer. In particular, the Radio layer provides software drivers needed to manage the RF chip while the RDC layer defines power saving strategies by means of three implemented mechanisms which are X-MAC, ContikiMAC, and LPP [16–18].

5.2. Interference source

A third VirtualSense node has been exploited for setting up the interference source. Particularly, we modified the radio layer to emulate an internal frequency matching interferer. The mote has been programmed by means of a Contiki task in charge of: *(i)* initializing the RF chip to generate a randomly modulated signal; *(ii)* repeatedly turning on and off transmission according to two parameters, namely T_{busy} and T_{idle}. Fig. 3 reports a snapshot of the C code of the Contiki process. The code consists of a main loop (rows from 8 to 25) that continuously runs the following steps:

- The radio transmitter is switched on by sending the related command (row 12);
- The transmitter is kept active until a specific amount of time (defined by the parameter `MS_ON`) has elapsed (rows 15–17);
- The transmitter is switched off (row 20);
- Radio activity is silenced for `MS_OFF` msec (rows 23–25).

The implementation of the system illustrated in Fig. 2 entails the modification of the position of the interference source with respect to transmitter and receiver nodes. Indeed, the configuration of Fig. 2(a) can be obtained by suitably positioning sender, receiver, and interferer close enough to be each one within the connectivity range of the others. Conversely, the configuration of Fig. 2(b) is subject to the variability of the communication range, thus making it more difficult its attainment. We therefore decided to modify the radio layer of the transmitter node in a way that always returns, independently from the measured SNR, a true value for the CCA, thus ensuring a decoupling of the transmissions with the interference dynamics.

5.3. Power measurement

In order to monitor the energy expenditure of the motes, we measured the current consumption of a sensing resistor (39Ω) placed in series with the sensor nodes. Each node was powered at 3.3V through a NGMO2 Rohde & Schwarz dual-channel power supply [38], and we sampled the signals to be monitored during the experiments by means of a National Instruments NI-DAQmx PCI-6251 16-channel data acquisition board connected to a BNC-2120 shielded connector block [39,40].

6. Results and discussion

In this section, we present the results of extensive experiments aimed at investigating the impact of packet length on the performance of a IEEE 802.15.4 wireless communication link subject to internal interferences. In particular, we compare the performances achieved by X-MAC, ContikiMAC, and LPP radio duty cycling protocols in broadcast and unicast communication and, finally, we evaluate the sensitivity of the system to the interference level. In each experiment we also show the performances achieved by an always-on CSMA/CA configuration (without any radio duty cycling protocol) that can be considered as a performance baseline.

For each radio duty cycling protocol two different sets of experiments have been carried out according to the two configurations described in Section 5. As a reminder, in the first configuration, both the sender and the receiver nodes are subject to the interference while in the second one the interference is perceived only by the receiver. The results obtained in this second configuration are reported by adding to the corresponding plot the suffix "−R".

```
PROCESS_THREAD(cc2538_rf_interferer_process, ev, data)
{
  rtimer_clock_t t0;
  PROCESS_BEGIN();

  PRINTF("Starting RF-interferer main loop\n");

  while(1){

      /* send to the Command Strobe Processor the ISTXON opcode *
       * to immediately enable TX                                */
      CC2538_RF_CSP_ISTXON();

      /* actively wait for MS_ON milliseconds */
      t0 = RTIMER_NOW();
      while(RTIMER_CLOCK_LT(RTIMER_NOW(), t0 + MS_CLOCK*MS_ON)){}

      /* send to the Command Strobe Processor the ISROFF opcode *
       * to immediately disable TX                               */
      CC2538_RF_CSP_ISRFOFF();

      /* actively wait for MS_OFF milliseconds */
      t0 = RTIMER_NOW();
      while(RTIMER_CLOCK_LT(RTIMER_NOW(), t0 + MS_CLOCK*MS_OFF)){}
  }
  PROCESS_END();
}
```

Fig. 3. C code of the Contiki interferer process.

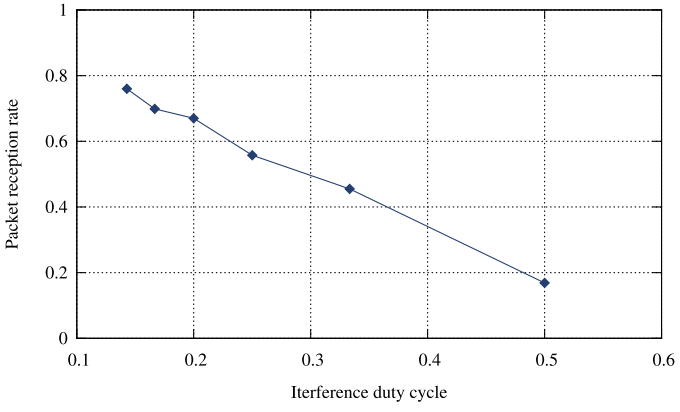

Fig. 4. Packet reception rate as a function of the interference duty cycle.

In order to tune the generation of the interference a first set of experiments has been carried out where the sender node was delivering 70 bytes's broadcast packets to the receiver in the always-on configuration and subject to the interference. At each experiment, the duty cycle of the interferer has been changed by vary the T_{idle} parameter and the related packet reception rate has been measured. Fig. 4 shows the measured packet reception rate when the interferer duty cycle increases from about 0.14 (corresponding to $T_{idle} = 24$ ms and $T_{busy} = 4$ ms) to 0.5 (corresponding to $T_{idle} = T_{busy} = 4$ ms). As expected, increasing the duty cycle (i.e. decreasing the T_{idle}) increases the collision probability and therefore the packet reception rate decreases. Notice that the transmission time of a 70 bytes packet is about 2.2 ms according to the 250 Kbit/s bit rate of the 802.15.4 standard. This means that at least a window longer than 2.2 ms without interference is needed to successfully deliver a packet. In real experiments we found that no packet has been delivered for a window shorter than 4ms. An interferer with a fixed duty cycle of about 0.22, corresponding to a T_{idle} of 14 ms, has been used to build all the subsequent experiments.

6.1. Broadcast communication

The following results have been obtained by programming the sender node to repeatedly send broadcast packets. First of all we report several statistics aimed at highlighting the impact of the packet length on the protocols behavior, and then we point out

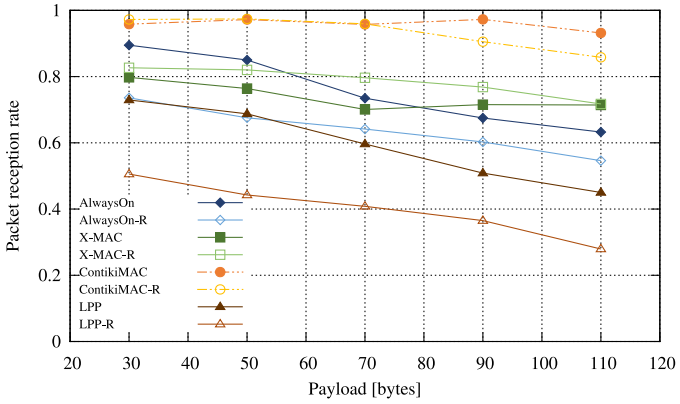

Fig. 5. Packet reception rate as a function of the payload length in different radio duty cycling protocols.

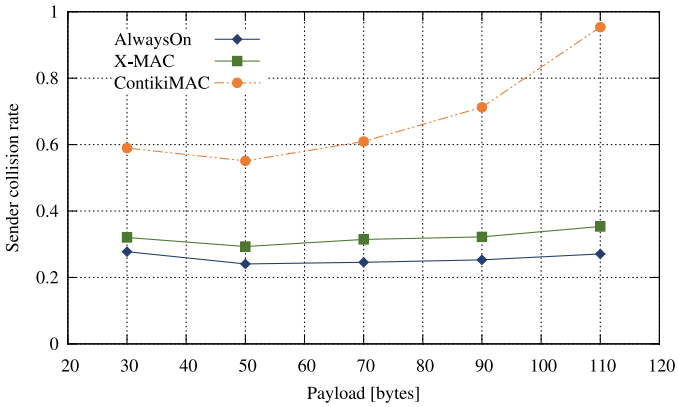

Fig. 6. Collision rate detected by the sender versus payload length in different communication protocols.

how the packet length impacts the energy consumption of the receiver node.

6.1.1. Packet reception rate

Fig. 5 shows the packet reception rate obtained while varying the length of the packet payload for different radio duty cycling protocols. Each point has been computed from experiments lasting 30 min, for a total of around 1000 packet for each experiment (approximately 1 packet every half second). In total, experiments (for either broadcast and unicast scenarios) refer to around 16,000 transmitted packets. In this setting, we can reasonably assume each single communication event to be independent from the others.

The AlwaysOn (CSMA/CA without radio duty cycling), the LPP, and the X-MAC protocols show a strong dependency of the packet reception rate from the length of the packet payload while the ContikiMAC appears to be less influenced. In effect, in the case of the largest payload, all protocols show the lower packet reception rate, which, in the case of LPP-R, falls below about 30%. In all protocols, when no collision avoidance strategies can be performed ("−R" configurations), we measure a lower packet reception rate with respect to the corresponding non "−R" configuration which demonstrates the effectiveness of the collision avoidance mechanism. Moreover, it is interesting to point out how the use of the data packet as a wake up strobe, performed both by X-MAC and by ContikiMAC, increases the communication reliability so that, despite their low-power nature, these protocols reach and even exceed the performances of the always-on configuration. For instance, in the ContikiMAC, this strategy, together with the CSMA/CA mechanism, strongly increases the packet reception rate which, in the worst case, does not fall below about 93%.

A separate consideration must be made for the LPP protocol to better understand its weak results achieved in this experiment. In fact, LPP is the only receiver-initiated protocol tested in this work, and, as previously described, a broadcast transmission using LPP can fail for several reasons in presence of an interference. For instance a collision can be generated both by the transmission and by acknowledgment of the probe or, definitely, by the data packet itself thus reducing the communication reliability. Moreover, the implementation of LPP provided by Contiki OS carries out the channel sensing only before sending the probe and not before sending the data packet which, because of its larger size, is more prone to collide.

If, on the one side, the design choice to send several replies of the data packet as wake up strobes allows ContikiMAC and X-MAC to reach a high degree of reliability, on the other side, it forces the sender to sustain a great workload which results in an increased energy consumption. An indirect measure of this workload can be obtained by counting the number of collision detected by the sender node during each experiment when it is subject to the interferer signal. Fig. 6 plots the sender collision rate versus the payload length for AlwaysOn, X-MAC, and ContikiMAC protocol. Since LPP does not apply CSMA/CA strategies before sending a data packet, its collision count refers to sending beacon instead of data packets, and it is not reported in the plot.

Interestingly, for AlwaysOn and X-MAC the number of collisions detected does not show a dependency on the size of the data packet because the CSMA is performed only once before starting the transmission. Conversely, in ContikiMAC, the CCA is performed for each strobe and if a collision is detected, the transmission of the following strobes is suspended and postponed for a while. This reiterated channel sensing facilitates the adaptation of the train of strobes to a possible interference pattern. The results of this strategy is an increasing of the sender collision rate while the packet length increases. For instance, in ContikiMAC we measure a sender collision rate which grows up to 95% for a payload of 110 bytes. This ensures a higher reliability at a strong energy cost that has to be sustained by the transmitter node.

6.1.2. Packet corruption rate

We now describe the relation between the packet corruption rate, measured at the receiver level, and the payload size for different protocols. The packet corruption rate has been obtained as the ratio between the number of corrupted packets received at the radio layer (*badcrc* in Contiki operating system) and the total number of received packets (*llrx*). The aim of this metric is to highlight if there is or not an appreciable dependence of the impact of the interferer from a particular communication protocol. If a dependence is found, we must conclude that there is a coupling phenomenon between the interference and a certain protocol mechanism which involves a non-homogeneous effectiveness of the interferer. Notice that, for protocols that send several replies of the same data packet as strobes (ContikiMAC and X-MAC), this metric does not correspond to one minus the packet reception rate previously described.

Fig. 7 shows the packet corruption rate measured when varying the payload length for different RDC methods. All the plots show no appreciable correlation with the communication mechanism but, in all cases, the packet corruption rate increases while the packet length increases. This allow us to state that the generated interference can be considered homogeneous with respect to the tested protocols and that it depends only on the packet length.

In order to thoroughly evaluate the effectiveness of the interferer we also measured the Estimated Bit Error Rate (EBER) by dividing the packet corruption rate, shown in Fig. 7, by the bit

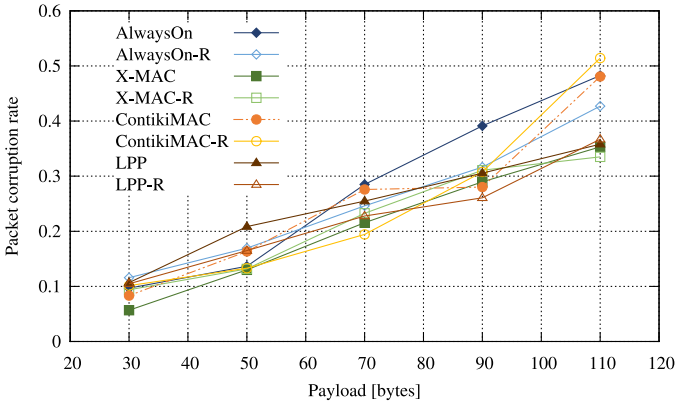

Fig. 7. Comparison of the packet corruption rate Vs payload length in different communication protocols.

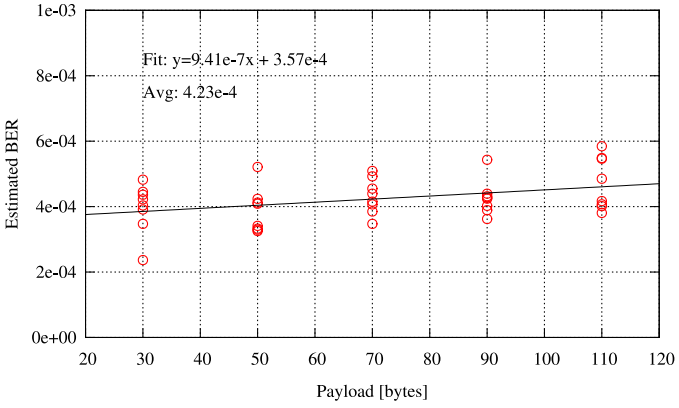

Fig. 8. Comparison of the Estimated Bit Error Rate (EBER) Vs payload length in different communication protocols.

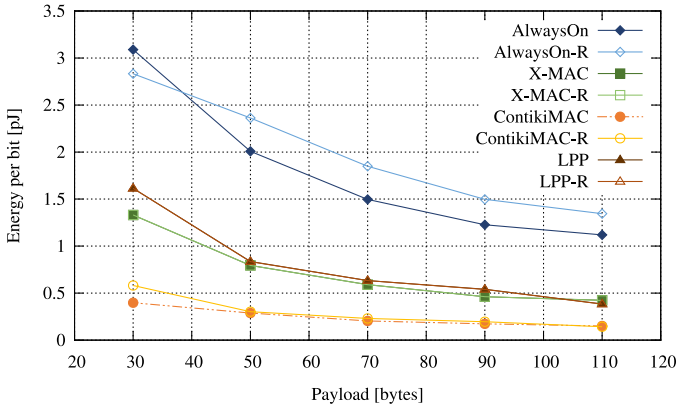

Fig. 9. Average energy spent by the receiver node for a delivered bit versus payload length in different communication protocols.

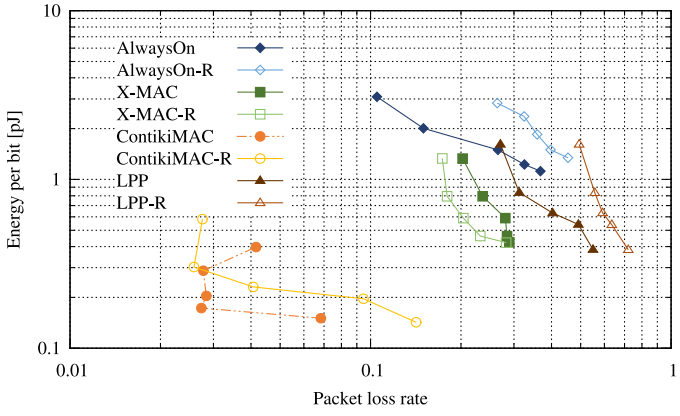

Fig. 10. Pareto curve showing the trade-off between energy spent per delivered bit and packet loss rate in different communication protocols.

length of the payload. Fig. 8 shows the EBER measured in each experiment and fitted by means of a linear interpolation function. Interestingly, the dependence of the EBER from the payload length is about $9.41 * 10^{-7}$ which is almost three order of magnitude lower than the average value (about $4.23 * 10^{-4}$). For this reason we can consider the probability of corrupting a bit not related to the length of the packet.

6.1.3. Energy consumption

Another set of experiments has been performed to investigate the impact of the packet length on the energy consumed by the receiver node under interference. To this purpose the current drawn by the receiver node has been sampled to calculate the average energy consumed per delivered bit. Notice that the energy spent to receive a corrupted packet (which is then discarded) is attributed to the packets effectively delivered so that the greater the number of corrupted packets received and the greater will be the resulting average energy per bit.

Fig. 9 shows the average energy spent for a delivered bit when the payload length increases. As expected the energy consumed per bit decreases while the packet size increases for all tested protocols. This reflects the fact that, from an energy point of view, it is always convenient to send large packets despite its greater probability of collision because of the higher overhead that the system incurs in case of fragmentation. Obviously, the Always-on configuration protocol shows an energy consumption of about one order of magnitude greater than the low-power RDC protocols since it never turns off the radio chip. Moreover, these results show that the energy needed to deliver a bit using LPP or X-MAC is very close especially when the packet size increases while ContikiMAC obtains greater performances overcoming all the other protocols in all conditions. It is interesting to note that AlwaysOn, in the configuration in which the interference is perceived only by the receiver ("−R" plots), shows a greater energy consumption with respect to the corresponding not "−R" configuration. This must be clearly attributed to the increased number of corrupted packet received which are due to the impossibility, for the sender node, of implementing any collision avoidance strategies. This trend, even if of reduced entity, is also evident for ContikiMAC while, for both LPP and X-MAC, the two configuration practically overlap. This is not surprising because, as previously described, these two protocols make a very limited use of the CSMA/CA strategy.

In order to highlight the relationship between packet length, energy efficiency, and packet loss we introduce Fig. 10, showing a Pareto curve which illustrates 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 the lower energy per bit, are not the optimal design choice when subject to the interference because of their higher loss rates. On the other hand, too short packets provide a low loss rate but rapidly increase energy expenditure. Therefore, 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 by means of the choice to use an intermediate packet length. Finally, these results show even more the supremacy of ContikiMAC, both in terms of energy and loss rate, if compared with the others tested protocols.

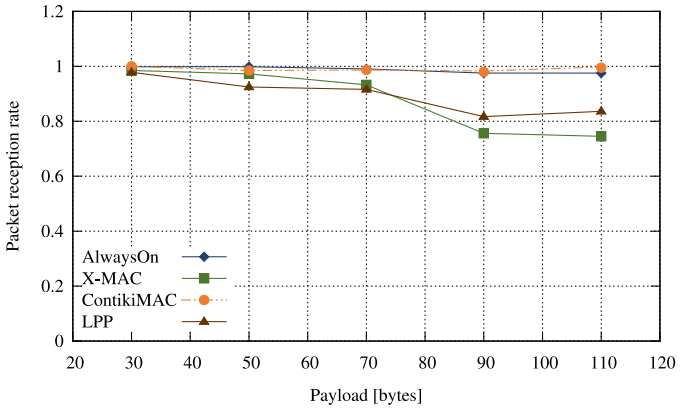

Fig. 11. Packet reception rate as a function of the payload length in different communication protocols using unicast communication.

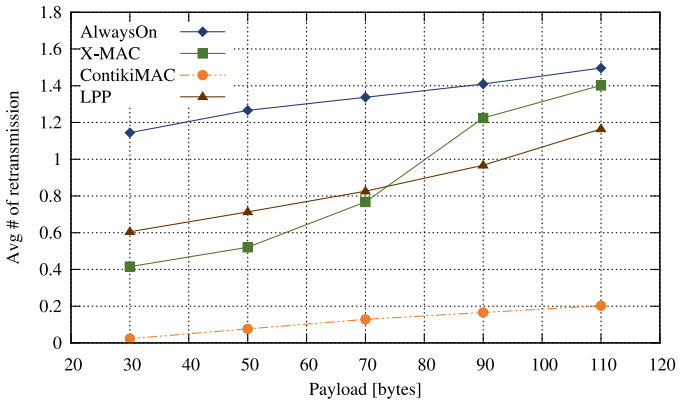

Fig. 12. Average number of packet retransmission as a function of the payload length in different communication protocols using unicast.

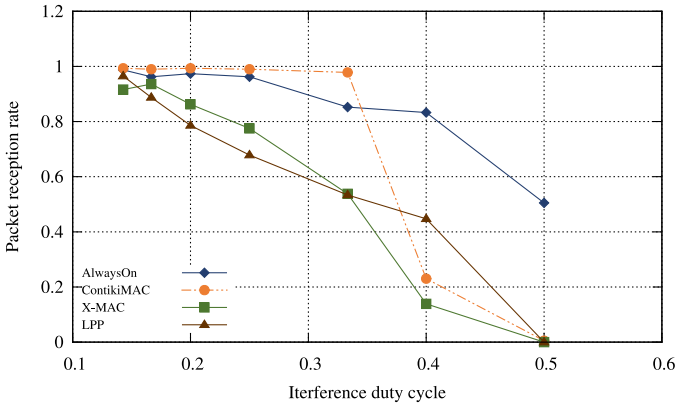

Fig. 13. Packet reception rate as a function of the duty cycle of the interferer in different communication protocols using unicast.

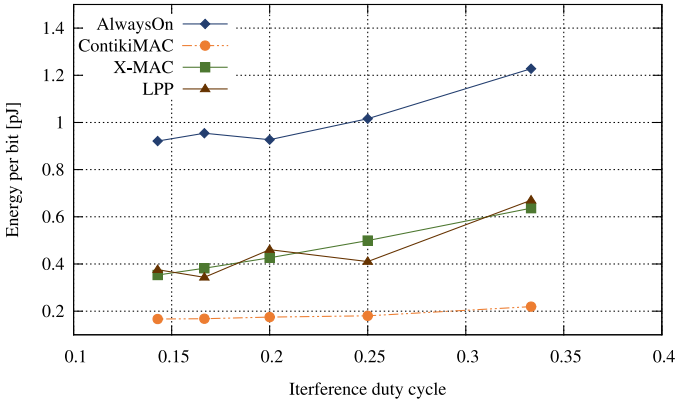

Fig. 14. Average energy spent by the receiver node for a delivered bit versus duty cycle of the interferer in different communication protocols using unicast.

6.2. Unicast

In this section we report the results obtained while the sender node was repeatedly send a unicast packet to the receiver. For the sake of readability we report only experiments in which the interference is perceived both by the sender and by the receiver nodes and we show only results that appreciably differ from the already discussed broadcast communication. In particular we focus on the communication reliability by leaving out the discussion on the energy efficiency which broadly overlaps the broadcast case.

6.2.1. Packet reception rate

In unicast communication subject to interference, the measured packet reception rate, as expected, shows a greater value with respect to the broadcast configuration such that for many packet length values it is close to one (see Fig. 11). Only for LPP and X-MAC protocols, when the packet length exceeds 90 bytes, the packet reception rate falls respectively below about 90% and about 80%. Obviously, the greater reliability of the unicast communication depends on the retransmission of the data packet in case of the acknowledge failure which, in the default Contiki OS configuration, can be reiterated for just three times. Despite this limit applies to all the tested protocols, since it depends on the upper software layer, it is interesting to note that only ContikiMAC can match the performance of the AlwaysOn configuration.

Fig. 12 reports the average number of packets retransmission while the payload increases. Interestingly, despite ContikiMAC achieves the best performance in terms of reliability, it exhibits the lower average number of retransmission demonstrating that the design choice to use data packets as strobes is itself able to guarantee a strong reliability so that it rarely recurs to the upper level retransmission.

6.3. Sensitivity to interference

The last part of this study is devoted to investigate the sensitivity of the radio duty cycling protocols w.r.t. the interference levels, by conceiving a set of experiments in which the unicast transmission of a 70B-long data packet is subject to an increasing interference. In particular, for each experiment, the duty cycle of the interferer has been changed starting from about 0.14 up to about 0.5 (by varying the T_{idle} from 24 ms up to 4 ms with a fixed T_{busy} of 4 ms).

Fig. 13 shows the packet reception rate as a function of the duty cycle of the interferer. It is interesting to point out how each protocol reacts to the increased interference. For instance, ContikiMAC is able to cope with an increase of interference up to a duty cycle of about 0.33 (corresponding to a T_{idle} of 8 ms), with a packet reception rate practically close to 1. A further increase in the interference leads however to a rapid fall up to zero in the communication reliability (no packets delivered for an interference duty cycle of 0.5). It is interesting to note that ContikiMAC, despite its low-power nature, appears to be more robust with respect to the AlwaysOn configuration. X-MAC and LPP, on the contrary, show a gradual reduction in performance as soon as the interference increases.

From the energy point of view, it is intuitive that an increase on the interference leads to an increase on the energy spent to receive a valid bit because of the greater number of corrupted packet to be processed. Fig. 14 reports the comparison of the energy spent

per bit by the different protocols while the interference increases. Also in this case it is noteworthy that ContikiMAC shows a stronger performance with respect to the others protocols by reporting a weak dependency of the energy spent with the interference duty cycle.

7. Conclusions

Electromagnetic interference impairs communication and limits the lifetime of WSN. Indeed, to design reliable and flexible networked embedded system, detailed understanding of the role of parameters of the design space on performance, in environments subject to interference, is decisive. In this work we presented an experimental assessment aimed at evaluating the impact of payload size on the reliability of the communication and on the energy expenditure of a link composed by a pair of sensor nodes affected by controlled interference levels. We have conducted experiments to explore different scenarios (e.g. with various low-power MAC protocols and according to different communication patterns) by measuring the packet reception rate and the energy consumption of the system under study.

Results confirm that longer packets negatively affect reliability (being more prone to corruption from interfering sources) while they are more efficient in terms of energy consumption, as illustrated by the reported Pareto curves. As a consequence, intermediate values of the payload size can be identified, which represent the best trade-off between energy expenditure and communication success probability. Specifically, experimental results highlight a given number of features of the investigated systems which can be summarized as follows:

- Broadcast transmissions:
  - ContikiMAC shows higher resilience in terms of dependability (i.e. in terms of packet reception rate) w.r.t. LPP and X-MAC when the payload length is increased;
  - The strategy of sending data packets as wake-up strobes adopted by either X-MAC and ContikiMAC results into increased levels of reliability, enabling to reach or outperform AlwaysOn configurations at the cost of higher energy consumption on the sender side;
  - The number of collisions detected by the sender is relatively stable (w.r.t to packet lengths) for always-on and X-MAC, while it increases for ContikiMAC (due presumably to the execution of CCA for each strobe to be sent);
  - The energy spent by the receiver for a delivered bit is very similar for LPP and X-MAC, and much lower for ContikiMAC in all tested scenarios; in all protocols the receiver node incurs higher energy expenditures when the sender doesn't perceive the interference, w.r.t. the case of both nodes affected by interference.
- Unicast transmissions:
  - ContikiMAC matches the performance of the AlwaysOn protocol in terms of packet reception rate (as a function of payload length), outperforming both LPP and X-MAC despite it needs, on average, a lower number of retransmissions (because of the use of data packets as strobes which avoids to resort to upper level retransmissions in the stack);
  - X-MAC and LPP gradually decrease their reliability when interference grows, while ContikiMAC is more robust up to a certain degree of interference and more steeply degrades after a given threshold (for a duty-cycle of the interference source around 0.33).

In conclusion, the presented study provides a thorough characterisation of the impact of packet length on basic performance metrics, thus yielding to a better support in the selection of points of the design space.

Regarding the possibility of extending this research in other directions for future work, it could be interesting to study the interplay between interference, packet length, reliability, energy efficiency, and MAC protocols on different network topologies. Several challenges need to be faced for a full evaluation, ranging from the choice of topology and traffic (e.g. multi-hop or clique networks, collection or dissemination primitives, etc.) to the definition of adequate metrics (e.g. end-to-end reliability) which, however, are expected to be strongly influenced from other system-level design choices that should be, therefore, carefully evaluated. Moreover, also spatial characteristic (e.g. the presence of obstacles and the distances between nodes) should be taken into account to properly address the effect of the physical environment on wireless propagation (fading, multi-path effects). Finally, the positioning of interference sources represents itself a problem to be considered, which could require the subdivision of the deployment into several cells of given area and the choice of proper transmission power level for nodes acting as interference sources (as suggested, for instance, in [3]), to enable sufficient coverage in terms of interference over the whole network while minimizing cross-talk effects between adjacent cells.

Declaration of Competing Interest

The authors declare that they do not have any financial or non-financial conflict of interests.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.comnet.2019.106986.

References

[1] M. Dong, K. Ota, A. Liu, RMER: reliable and energy-efficient data collection for large-scale wireless sensor networks, IEEE Internet Things J. 3 (4) (2016) 511–519.
[2] A. Sikora, 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, 22, IEEE; 1999, 2005, p. 1786.
[3] C.A. Boano, T. Voigt, C. Noda, K. Romer, M. Zuniga, JamLab: augmenting sensornet testbeds with realistic and controlled interference generation, in: Proceedings of the 10th ACM/IEEE International Conference on Information Processing in Sensor Networks, 2011, pp. 175–186.
[4] M. Michel, T. Voigt, L. Mottola, N. Tsiftes, B. Quoitin, Predictable MAC-level performance in low-power wireless under interference, in: EWSN '16 Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks, 2016, pp. 13–22.
[5] P. Lettieri, 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, 2, IEEE, 1998, pp. 564–571.
[6] M.C. Vuran, 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.
[7] J.-S. Han, Y.-H. Lee, Interference-robust transmission in wireless sensor networks, Sensors 16 (11) (2016) 1910.
[8] J. Brown, U. Roedig, C.A. Boano, 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.
[9] D. Son, B. Krishnamachari, J. Heidemann, Experimental study of concurrent transmission in wireless sensor networks, in: Proceedings of the 4th international Conference on Embedded Networked Sensor Systems, ACM, 2006, pp. 237–250.
[10] W. Ye, J. Heidemann, D. Estrin, An energy-efficient mac protocol for wireless sensor networks, in: INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, 3, IEEE, 2002, pp. 1567–1576.
[11] W. Guo, W.M. Healy, M. Zhou, Performance measurement and analysis of low data rate wireless communication under interference sources in buildings, in: Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on, IEEE, 2010, pp. 2473–2478.
[12] W. Dong, C. Chen, X. Liu, Y. He, Y. Liu, J. Bu, X. Xu, Dynamic packet length control in wireless sensor networks, IEEE Trans. Wirel. Commun. 13 (3) (2014) 1172–1181.

[13] A. King, J. Brown, J. Vidler, U. Roedig, Estimating node lifetime in interference environments, in: Local Computer Networks Conference Workshops (LCN Workshops), 2015 IEEE 40th, IEEE, 2015, pp. 796–803.
[14] M.Y. Naderi, K.R. Chowdhury, S. Basagni, W. Heinzelman, S. De, S. Jana, Surviving wireless energy interference in RF-harvesting sensor networks: an empirical study, in: Sensing, Communication, and Networking Workshops (SECON Workshops), 2014 Eleventh Annual IEEE International Conference on, IEEE, 2014, pp. 39–44.
[15] V. Toldov, R. Igual-Pérez, R. Vyas, A. Boé, L. Clavier, N. Mitton, Experimental evaluation of interference impact on the energy consumption in wireless sensor networks, in: World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2016 IEEE 17th International Symposium on A, IEEE, 2016, pp. 1–6.
[16] M. Buettner, G.V. Yee, E. Anderson, 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, in: SenSys '06, ACM, New York, NY, USA, 2006, pp. 307–320, doi:10.1145/1182807.1182838.
[17] R. Musaloiu-E., C.-J.M. Liang, 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, doi:10.1109/IPSN.2008.10.
[18] A. Dunkels, The ContikiMAC Radio Duty Cycling Protocol, SICS Technical Report T2011:13, ISSN 1100-3154, 2011. 1–11
[19] E. Callaway, P. Gorday, L. Hester, J.A. Gutierrez, M. Naeve, B. Heile, V. Bahl, Home networking with ieee 802.15. 4: a developing standard for low-rate wireless personal area networks, IEEE Commun. Mag. 40 (8) (2002) 70–77.
[20] A. Iyer, C. Rosenberg, A. Karnik, What is the right model for wireless channel interference? IEEE Trans. Wirel. Commun. 8 (5) (2009).
[21] Universal Software Radio Peripheral (USRP).
[22] C.A. Boano, Z. He, Y. Li, T. Voigt, M. Zúñiga, A. Willig, Controllable radio interference for experimental and testing purposes in wireless sensor networks, in: Proceedings - Conference on Local Computer Networks, LCN, 2009, pp. 865–872, doi:10.1109/LCN.2009.5355013.
[23] L.M. Feeney, M. Nilsson, Investigating the energy consumption of a wireless network interface in an ad hoc networking environment, in: INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, 3, IEEE, 2001, pp. 1548–1557.
[24] A. Bogliolo, E. Lattanzi, V. Freschi, Idleness as a resource in energy-neutral WSNs, in: ENSSys '13: Proceedings of the 1st International Workshop on Energy Neutral Sensing Systems, ACM, New York, NY, USA, 2013, pp. 1–6. http://doi.acm.org/10.1145/2534208.2534214.
[25] M. Doudou, D. Djenouri, N. Badache, A. Bouabdallah, Synchronous contention-based MAC protocols for delay-sensitive wireless sensor networks: a review and taxonomy, J. Netw. Comput. Appl. 38 (1) (2014) 172–184, doi:10.1016/j.jnca.2013.03.012.
[26] D. De Guglielmo, S. Brienza, G. Anastasi, IEEE 802.15. 4e: a survey, Comput. Commun. 88 (2016) 1–24.
[27] Y. Jin, U. Raza, M. Sooriyabandara, BOOST: bringing opportunistic routing and effortless-scheduling to TSCH MAC, in: 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1–7, doi:10.1109/GLOCOM.2018.8647851.
[28] S. Duquennoy, B. Al Nahas, O. Landsiedel, 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.
[29] C. Sarkar, R.V. Prasad, K. Langendoen, Fleet: when time-bounded communication meets high energy-efficiency, IEEE Access 7 (2019) 77555–77568, doi:10.1109/ACCESS.2019.2920937.
[30] A. Dunkels, B. Gronvall, 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, in: LCN '04, IEEE Computer Society, Washington, DC, USA, 2004, pp. 455–462.
[31] E. Lattanzi, A. Bogliolo, Hardware filtering of non-intended frames for energy optimisation in wireless sensor networks, Int. J. Sensor Netw. 15 (2) (2014) 10, doi:10.1504/IJSNET.2014.060725.
[32] M. Michel, B. Quoitin, Technical Report : ContikiMAC vs X-MAC Performance Analysis, 2014.
[33] J. Polastre, J. Hill, D. Culler, Versatile low power media access for wireless sensor networks, in: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, ACM, 2004, pp. 95–107.
[34] J.L. Hill, D.E. Culler, Mica: a wireless platform for deeply embedded networks, IEEE Micro 22 (6) (2002) 12–24.
[35] U. Raza, A. Bogliolo, V. Freschi, E. Lattanzi, A.L. Murphy, A two-prong approach to energy-efficient WSNs: wake-up receivers plus dedicated, model-based sensing, Ad Hoc Netw. 45 (2016) 1–12.
[36] Cc2538 powerful wireless microcontroller system-on-chip for 2.4-GHz IEEE 802.15.4, 6lowpan, and zigbee applications.
[37] N. Brouwers, K. Langendoen, P. Corke, Darjeeling, a feature-rich VM for the resource poor, in: Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, in: SenSys '09, ACM, New York, NY, USA, 2009, pp. 169–182.
[38] Ngmo2 Datasheet.
[39] Pc-6251 Datasheet.
[40] Installation Guide bnc-2120.

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 at the Department of Pure and Applied Sciences (DiSPeA) of 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.

Paolo Capellacci graduated in applied computer science at University of Urbino, Italy, in 2019. His research interests include wireless sensor networks, embedded systems, algorithms, and geomatics.

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, networked embedded systems, graph algorithms, bioinformatics, optimization.