View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Swedish Institute of Computer Science Publications Database

Controllable Radio Interference for Experimental and Testing Purposes in Wireless Sensor Networks

Carlo Alberto Boano, Zhitao He, Yafei Li, Thiemo Voigt
Swedish Institute of Computer Science
Kista, Sweden
{cboano, zhitao, yafei, thiemo}@sics.se

Marco Zúñiga
National University of Ireland
Galway, Ireland
marco.zuniga@deri.org

Andreas Willig
Technische Universität Berlin
Berlin, Germany
awillig@tkn.tu-berlin.de

***Abstract*—We address the problem of generating customized, controlled interference for experimental and testing purposes in Wireless Sensor Networks. The known coexistence problems between electronic devices sharing the same ISM radio band drive the design of new solutions to mitigate interference. The validation of these techniques and the assessment of protocols under external interference require the creation of reproducible and well-controlled interference patterns on real nodes, a non-trivial and time-consuming task.**

In this paper, we study methods to generate a precisely adjustable level of interference on a specific channel, with low-cost equipment and rapid calibration. We focus our work on the platforms carrying the CC2420 radio chip. We show that, by setting the CC2420 in special mode, we can easily generate repeatable and precise patterns of interference.

We show how this method is extremely useful for researchers to quickly investigate the behaviour of sensor network protocols and applications under different patterns of interference. We further evaluate the performance of our proposed method.

***Index Terms*—Interference, Noise, WSN, SNR, Modulated carrier, Unmodulated carrier, Directional antennas.**

I. Introduction

The reliability and robustness of communications in Wireless Sensor Networks (WSN) are affected by radio interference of WLAN [13], Bluetooth [3], IEEE 802.15.4 [14], microwave ovens, and all other electronic devices that share the 2.4 GHz ISM band [21]. This brings some concerns about the robustness of sensor network communications, and limits the wide adoption of WSN by industry.

Several studies and methods have been proposed to reduce the impact of such interference on communication [18]. To investigate new methods, as well as to study the behavior of applications or link quality estimation metrics in presence of interference, experiments on real nodes in a customized interfered scenario are needed. This applies especially where simulators are not enough, for example when dealing with radio hardware parameters such as RSSI and LQI.

However, generating a controlled level of interference on sensor nodes is far from straightforward, and researchers often need an inexpensive, simple, and time-saving way to test their solutions in a precise, repeatable, and customized way.

In this paper, we discuss and evaluate different techniques to generate a controlled level of interference on 802.15.4-compliant sensor devices, focusing on the 2.4 GHz ISM band. We also propose a precise, simple, low-cost solution for the creation of tunable functions of interference or packet loss rate, based on special settings of the popular CC2420 radio chip. We investigate how this method can be used to create a tunable interfered scenario that is repeatable in a straightforward and inexpensive way.

Our results show that this method can be used to higher the noise floor, to vary the packet loss rate, and that only tens of microseconds are necessary to switch on and off interferers. We further show some of its possible applications, such as the validation of protocols and applications under different patterns of interference.

The paper proceeds as follows. Section II explains the problems of generating a controllable level of interference and provides a taxonomy on the existing methods. We describe the limitations of two common techniques used to generate interference in Section III. Thereafter, in Section IV, we identify in the use of carrier-only transmission the best way to generate customized patterns of interference, and we propose a costless and time-efficient solution based on the radio chip test modes. We evaluate this method in Section V with respect to real WSN applications, and we show the benefits it can bring to sensor network research. After reviewing related work in Section VI, we present our conclusions in Section VII.

II. Problem statement

Since the ISM bands are crowded, external interference is a significant problem, and it becomes necessary to add protocol mechanisms capable to adapt a WSN resource usage to the present interference situation, or, more generally, to assess the behaviour of WSN protocols under external interference.

In many studies, simulation is the first crucial step towards such an understanding, but, depending on the capabilities of the simulator, the results are often obtained under simplified or idealized conditions. Therefore, it becomes necessary to perform experiments on real nodes with real interference. In these experiments the need of controlled-interference is two-fold:

- Reproducibility of experiments: it is a generally accepted scientific practice that experimental results should be reproducible by others;

- Validation of simulations or analytical results: in order to validate such results, the interference reproduced on testbeds should be comparable.

However, to create predictable, reproducible and well-controlled interference patterns in a lab setup is not easy to achieve. The major reasons for this are the open-ness of the wireless medium (which means that besides the generated and planned interference often further unplanned interference from neighbored Wi-Fi or Bluetooth systems is catched up) and the practical difficulties to even approximately predict the wave propagation behaviour in realistic environments.

The latter applies even in absence of unwanted interference, since it is hard to find positions, antenna directions, and transmit powers for interferers, giving the desired interference pattern.

It can be a very time-consuming task to generate the desired interference pattern and it is therefore interesting for researchers to obtain tools and techniques allowing to generate desired interference patterns at reasonable effort and costs. To achieve this, a better and more precise understanding of the interference generation problem is needed and we propose a suitable classification for this.

In the rest of the paper we call the interfering node the *interferer*, and the interfered node the *interferee*. To be of relevance for the sensor network community, we specifically consider the problem of generating interference for nodes equipped with an IEEE 802.15.4-compliant transceiver like the ChipCon CC2420 [14], [6], operating in the 2.4 GHz ISM band. Some important attributes are the following:

- **Spectral characteristics of interferer.** The interferer(s) can occupy bandwidth in three different ways. A *broad-band interferer* such as Wi-Fi occupies a spectrum that overlaps with several neighbored 802.15.4 channels including the target channel. A *matched interferer* occupies exactly one 802.15.4 channel (although with an 802.15.4 interferer we might still have some limited co-channel interference [23]). Lastly, a *sub-band interferer* occupies an amount of spectrum significantly smaller than a 802.15.4 channel.
- **Frequency-agility of interferer.** We distinguish between a *static interferer*, not changing its center frequency over time, and a *frequency-hopping interferer* which changes its center frequency periodically. Wi-Fi is a static interferer while Bluetooth is a frequency-hopper.
- **Generation target.** The goal for interference generation depends very much on the application. One goal could be to directly influence the Signal-to-Noise Ratio (SNR) at a node (where interference is regarded as noise). Another goal would be to impact derived and node-dependent measures like the Packet Loss Rate (PLR).
- **Spatio-temporal power profile.** In full generality, the interferer may follow any interference pattern, e.g. a time stamped sequence of on-off signals. These series lead to time periods with and without interference.
- **Interaction between interferer and interferees.** The interferer can be *blind*, *responsive*, or *informed*. A blind interferer does not interact at all with the interferee: it does not perform any carrier-sensing nor possess a schedule of the interferees transmissions. A responsive interferer does not possess a-priori knowledge about the interferees transmissions, but performs carrier-sensing for its own transmissions and stays away from the medium if the interferee has started transmitting. An informed interferer either knows in advance the precise transmission schedule of the interferee and is well time-synchronized with it or is explicitly triggered by the interferee.
- **Equipment cost.** The equipment cost characterizes the economic cost and time effort required to set up the interferer. Cost can vary a lot depending on the use of accurate and costly signal generators that permit fine-grained generation. We show that we can use inexpensive peer-sensor nodes to generate controlled interference.
- **Calibration cost.** The calibration costs characterizes the cost and effort required to achieve the desired spectral characteristics and spatio-temporal power profile with the given equipment. It can be reasonably assumed that there is a tradeoff between equipment cost and calibration costs: the less you spend on equipment the more you have to work on calibration.

In these terms, we can state our goal as follows: we are interested in methods having low equipment and calibration costs that generate static, matched interference (so to avoid distortion of neighbored channels), that can influence either the SNR or the PLR at the interferee and with no interaction between interferer and interferee.

It is perhaps not too surprising that the cost constraints and the other goals are chosen such that using an IEEE 802.15.4-compliant node as an interferer provides a natural starting point. The different interference generation methods are then judged on two grounds: first, the precision with which the desired spatial-temporal power-profile can be achieved, and second, the calibration costs and effort required to do so.

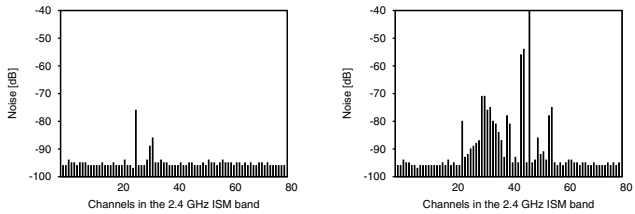
III. Limitations of current techniques

This section describes the limitations of two simple approaches: the creation of inter-network interference using Wi-Fi devices, and the creation of intra-network interference with the transmission of a packet storm from an 802.15.4 device.

A. Wi-Fi based techniques

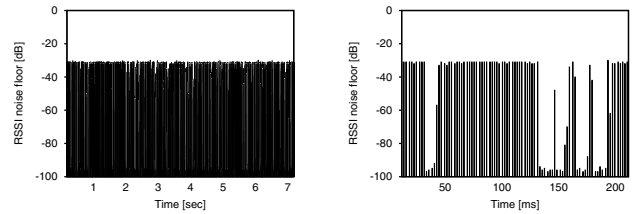
A simple way to create interference in the 2.4 GHz band is to generate traffic using an 802.11-enabled device, given the coexistence problem with the 802.15.4 devices.

However, this method is not suitable if the goal is to generate a tunable, static, matched interference, due to the spectral characteristics of Wi-Fi, that uses different radio frequencies with respect to the sensor nodes. Despite 802.15.4 and Wi-Fi channels overlap, there is no one-to-one mapping, as shown in Figure 1 in [18]. Channel 1 of Wi-Fi corresponds to channels 11,12,13, and 14 in sensors, while Wi-Fi frequencies do not overlap with IEEE 802.15.4 channels 25 and 26.



(a) Noise floor with WLAN off (b) Noise floor with WLAN on

Fig. 1. RSSI noise floor in a 802.15.4 device when WLAN is active and when it is off. The interference generated in a Wi-Fi channel is spread over multiple frequencies that do not match the ones of a single 802.15.4 channel, and this makes impossible to control in a precise way the generated interference. The X-axis of the two plots shows the 80 channels in the 2.4 GHz spectrum as 2.402 GHz + k MHz, with $k = 0, ..., 78$.



(a) Macro view (b) Micro view

Fig. 2. At first glance, it may seem that the interference generated by an 802.15.4 device transmitting a packet storm is continuous (a). Instead, the lack of a real continuous carrier is translated into several fluctuations between different levels of interference over time (b). The X-axis of the two plots shows the 80 channels in the 2.4 GHz spectrum as 2.402 GHz + k MHz, with $k = 0, ..., 78$.

This makes impossible to control in a precise way the interference generated in a single 802.15.4 channel. Moreover, we run the risk of affecting the connectivity of other devices using adjacent channels. Figure 1 illustrates how the interference generated in a Wi-Fi channel is spread over multiple frequencies and it does not match a single 802.15.4 channel.

The spectral limitations apply also when using Microwaves to generate noise, (because there is no control at all of the generated noise), or Bluetooth devices, since it uses Frequency Hopping Spread Spectrum (FHSS), and this means that it is allowed to hop between all the seventy-nine 1 MHz-wide channels in the 2.4 GHz band.

B. Packet-storm techniques

An intuitive and fast way to generate intra-network interference is to use a neighboring 802.15.4 device to send a packet storm, i.e. to use a sender node to broadcasts packets at a predefined transmission rate in order to interfere the other ongoing communications. This would introduce packet jamming and would increase the latency of the transmissions between the interfered nodes.

Packet-storm is a matched interference since it affects only the sensor nodes that use the same radio channel. The interference generated by the packet storm is, however, far from being controllable and tunable. This type of interference is based on four independent variables: the transmission power T_P, the packet length P_L, the elapsed time between broadcasted packets t_p, and the distance d of the interferer from the motes to be interfered. We call the interference generated by a packet storm I_{ps} the combination of these independent variables: $I_{ps} = \{P_L, d, T_P, t_p\}$.

Combining these variables in a satisfactory way is extremely time-consuming, because it is hard to foresee the effects brought by a change of one of the parameters. Redeploying the network by e.g. changing distance between nodes and interferer to obtain the desired I_{ps} requires a lot of time.

A second problem is the impossibility to control the exact time at which packets are transmitted. Packets are sent in the wireless medium after a certain amount of CPU and physical layer operations. Even with a deep understanding of the implementation details of the lower layers it is difficult to achieve a continuous batch transmission of packets. In other words, the problem could be stated as lack of continuous carrier. Given a long temporal window, it may appear that the interference or noise generated by the packet storm is continuous, but we have in reality some cases in which packets collide with the other ongoing transmissions, and some other cases in which there are gaps left by the processing operation of CPU and PHY.

Figure 2a shows that at first glance, it may seem that the interference generated by an 802.15.4 device transmitting a packet storm is continuous. However, the lack of a real continuous carrier is translated into a fluctuation between different levels of interference over time (Figure 2b).

The consequence of the lack of a continuous carrier is that there is no guarantee to hit every or a specific packet that is transmitted, if this is the goal of the interference. Moreover, it is also not possible to just raise the RSSI noise floor to a predefined value.

However, one of the biggest advantages in the use of packet storm technique is the creation of the same kind of interference that may be generated by several transmissions from neighboring 802.15.4 nodes.

IV. Broadcasting a continuous carrier

The spectral and temporal limitations described in Section III are the main limitation for the generation of a really controllable, repeatable, and tunable interference. In this section, we show how the introduction of a continuous signal is the key to achieve such solution. We use also mechanisms that guarantee a static, matched interference, so to avoid distortion of neighbored channels.

A. Software defined radio

A possible way to create a continuous tunable amount of interference is to design an interferer using Software Defined Radio (SDR). Through the Universal Software Radio Peripheral (USRP) [17], we can generate signals to interfere the communication in specific instants of time, with a given transmission power, thus having only two independent variables involved: the distance d and the transmission power

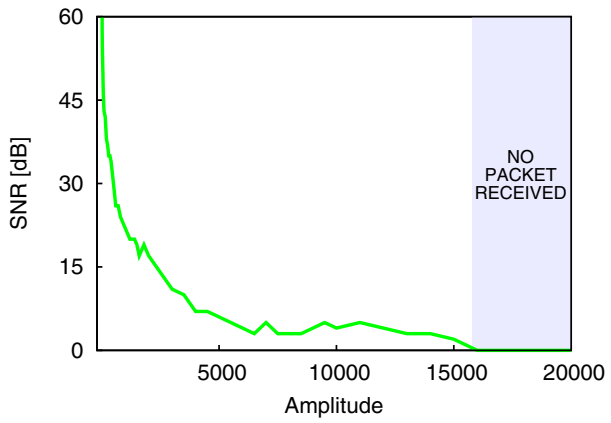


Fig. 3. Tunable interference generated using Software Defined Radio (SDR). The SNR of an ongoing communication between sensor nodes can be decreased to a specific value by playing with the amplitude of the signal.

T_P. We tested the interference level produced by SDR on two communicating Tmote Sky nodes placed at a distance of 1 meter, by measuring their SNR when varying the T_P of an Hamza USRP [11]. T_P is changed by setting the transmit amplitude of the signal, since we can not control the transmit power directly.

Figure 3 shows the results, in particular how it is possible to decrease the SNR of the communication in a tunable way.

Despite this method is controllable in a very fine-grained way, the equipment needed for SDR is far from being cheap, so we investigated a method that involves a simple 802.15.4 sensor node, and we describe it in the next subsection.

Code sample 1 Reset() function: reset the changes and set back the CC2420 radio chip in normal mode.

```
setreg(CC2420_MANOR, 0x0000);
setreg(CC2420_TOPTST, 0x0010);
setreg(CC2420_MDMCTRL1, 0x0500);
setreg(CC2420_DACTST, 0x0000);
strobe(CC2420_STXON);
```

Code sample 2 Creating an unmodulated carrier with the CC2420 radio chip.

```
setreg(CC2420_MANOR, 0x0100);
setreg(CC2420_TOPTST, 0x0004);
setreg(CC2420_MDMCTRL1, 0x0508);
setreg(CC2420_DACTST, 0x1800);
strobe(CC2420_STXON);
```

Code sample 3 Creating a modulated carrier with the CC2420 radio chip.

```
Reset();
setreg(CC2420_MDMCTRL1, 0x000C);
strobe(CC2420_STXON);
```

B. Special modes of Chipcon radio chips

In the recent past, the radio chips of sensor nodes were sending continuous streams of bits such as the TR1000 bit-based transceiver [19]. Bit-based transceivers can transmit continuous streams of information, thus eliminating the temporal gaps shown in Section III.

Last generation sensor network platforms use instead packet-based radio chips, such as the Chipcon radio chips. Many Chipcon radios, such as the popular CC2420 radio chip [6] can be set into different transmit test modes for performance evaluation or lab testing. In particular, it is possible to send a continuous carrier without the need of adding any external hardware. The radio transceiver can generate other than normal packets, also an unmodulated carrier and a modulated a carrier (created as pseudorandom sequence using the CRC generator). This can be made simply changing the value of the register CC2420_MDMCTRL1 as shown in the Code samples 1, 2, and 3.

Different types of interference. The transmission of an unmodulated and a randomly-modulated signal enable the generation of two different kinds of interference dependent only on two variables: the distance of the interferer d and the transmission power T_P. The unmodulated carrier has a highly concentrated power spectrum peaking at the center frequency, whereas the randomly-modulated signal's power spectrum spreads out evenly across the channel bandwidth. The CC2420's randomly-modulated signal can even emulate short bursts of interfering packets by prefixing a matching synchronization header to the random data, resulting in a hardware interrupt on the receiver. For this reason, it can be used to emulate the interference generated by neighbor transmissions, switching on and off the interferer in a intermittent way, as explained in Section V-B. We can thus use an unmodulated carrier to generate an interference pattern similar to the background noise and tune the SNR of ongoing transmissions, while the modulated carrier can be used to generate the same kind of intra-network interference generated by IEEE 802.15.4 packet transmissions. Our experiments show that the use of the unmodulated carrier is very useful to avoid phenomena like jamming, overflow of buffers, packet loss rate, since the unmodulated carrier does not trigger the interrupt that handles a received packet.

Tune the amount of interference. As with the SDR, assuming a fixed distance of the interferer, we can generate different amount of interference by simply varying the transmission power of the Chipcon radio chip. The amount of interference can be thus lowered in a customized way, and we are even able to lower the SNR of the communication between a pair of 802.15.4 nodes with a good granularity, as shown in Figure 4. Given that it is possible to select only 31 values of transmission power in the CC2420, we may vary also d, and obtain higher levels of precision. This set of experiments has been carried out with the communicating motes placed at a distance of one meter and the interferer at a few meters distance from the interferees.

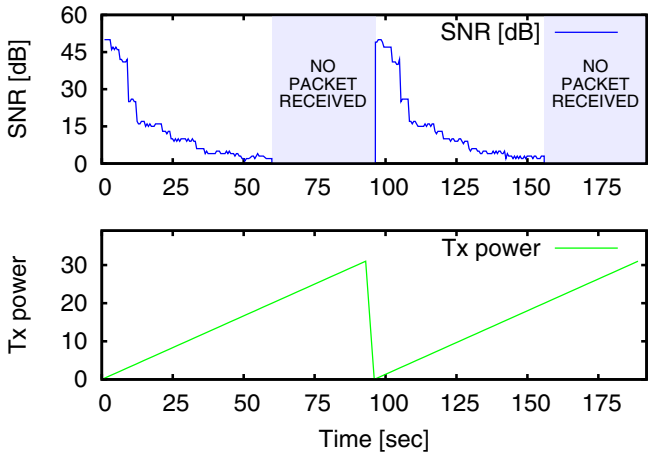


Fig. 4. Increasing the transmission power of the radio chip is the key to increase easily and quickly the amount of interference. The highest transmission power values may drop the communication if the distance between interferer and interferee(s) is short.

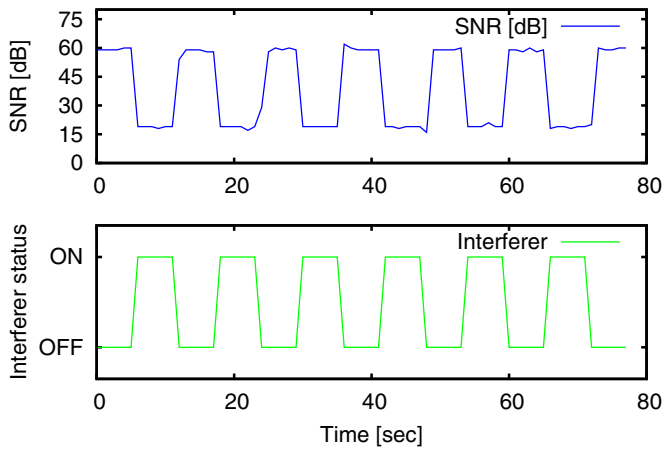


Fig. 5. Intermittent interferer. Here you can see the effects on the SNR given static transmitter and receivers interfered by a third intermittent node. The SNR drops accordingly only when the interferer is ON. This may be used to let the SNR fall only at given instants of time.

Blocking ongoing communications. Figure 4 also shows that given a proper distance between the interferer and the interferee, we can stop the ongoing communication when using the highest transmission power values. Such interruption of connectivity would be continuous as it is the radio chip transmission.

Tune the intervals of interference. The transmission of both modulated and unmodulated carrier can be made in specific instants of time, i.e. we can decide to keep the interferer active only for a periodic fixed interval of time (a, b). We can decide to switch on interference for an interval of time in order to, for example, manipulate communication protocol states. Differently from the case show in Figure 2, the interference will remain constant for the whole (a, b) thanks to the continuous transmission. Figure 5 shows an example of such an interference pattern: the stability of the interference level in the whole interval of time in which the interferer is active is the added value of this method.

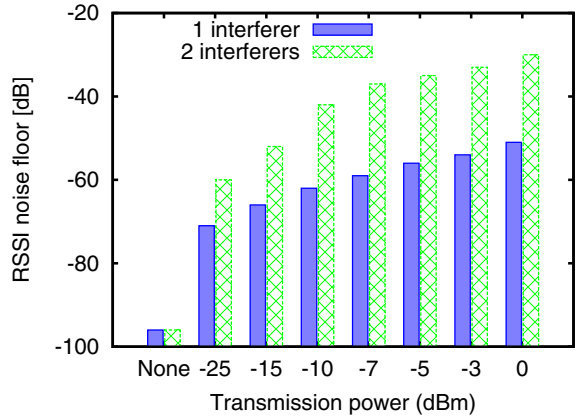


Fig. 6. Environmental RSSI noise floor measured by a sensor node placed at two meters distance from different interferers running a continuous unmodulated carrier. The picture show that the additive interference property applies: the total interference is the sum of different contributions.

TABLE I
GENERATING CONTINUOUS INTERFERENCE USING CHIPCON RADIOS

Model	Modulation	Single Carrier	Arb. data	Random data
CC1000	2-FSK	serial	serial	NA
CC1020	2-FSK	serial	serial	yes
CC1100	2-FSK	serial	serial	yes
CC2400	2-FSK	serial	serial	yes
CC2420	DSSS/O-QPSK	SPI	NA	yes
CC2500	2-FSK	serial	serial	yes

Multiple interferers. In case the interferer cannot be placed close to the interferee(s), we may decide to use multiple interferers to increase the level of generated noise. We can do this exploiting the *additive interference* property that states that the total interference is the sum (in dB) of each individual interferer. Figure 6 shows that the additive interference property applies when using multiple nodes as interferers. In other words if one of the interfering nodes rises its transmission power of 3 dBm, the overall noise floor is highered approximately of 3 dB. However, it is hard to obtain an exact increase of interference, due to the uncertainness of radio propagation issues among the interferers. We noticed that it is easier to control the additive interference at low transmission powers.

Generating interference with other platforms. Despite our work is focused on the CC2420 platform [6], it is possible to create continuous interference also using other Chipcon radios even at different frequencies. Creating continuous interference can be done by respective register settings of the transmission mode and data pins of the chip. Serial-interface radios such as CC1000 [5] and CC1020 [7] can continuously send an arbitrary bit sequence fed by the user; some newer radios that normally transmitting from a packet buffer, such as CC1100 [9] and CC2500 [8], can be set to fall back to serial mode to send continuous bit sequences, but this usually requires changes to pin settings as well; additionally, many of these radios have a built-in pseudo-random sequence generator. We summarize the capability of generating continuous interference of various radio chips in Table I.

Fig. 7. The Cantenna used in the experiment.

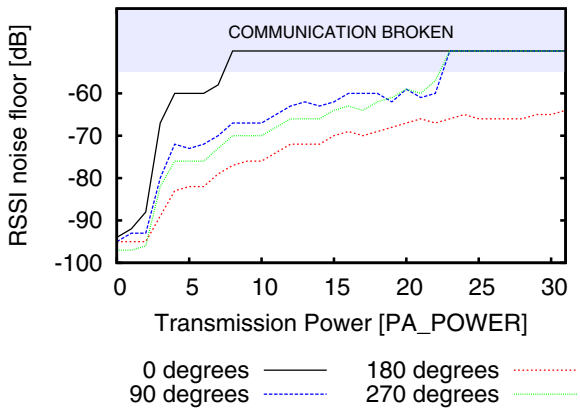


Fig. 8. Using a directional antenna, we can direct the range of interference. The communication between two nodes is not broken when pointing the antenna 180 degrees far from such area.

Table II summarizes the characteristics of the interferers based on the different hardware and methods described so far with respect to the taxonomy provided in Section II.

Direct the range of interference. Although the continuous carrier enables a good control of the interference level with an acceptable customization level, the interferer will interfere on its whole radio range. If the scenario needs that only a specific number of nodes are affected, we can use directional antennas to direct the interference. Since our goal is to keep the hardware costs as low as possible, we tested if it is possible to interfere only a specific region by using a Cantenna [20], a low-cost and homemadeable antenna shown in Figure 7. Our results confirm the results obtained in [20], and show that we can minimize the interference level in the region opposite to the one pointed by the antenna (180 degrees from that region), if playing correctly with T_P and d.

Figure 8 shows how the level of interference decreases when rotating the Cantenna away from the area that should not be interfered. If the antenna is pointed towards that area (0 degrees), the communication is broken easily (i.e. even with low transmission powers). A rotation of 90 and 270 degrees will make the communication much harder to break (i.e. higher transmission powers are needed), while if the antenna is rotated completely, the transmission is not broken even when using the maximum transmission power. We can conclude that we can avoid some nodes to be interfered with low-cost equipment as well.

V. Evaluation

In this section, we show some possible applications of the controlled interference generation based on the CC2420 test modes. Firstly, we show first how to evaluate a simple link quality metric, and secondly how to generate a responsive interference so to create an exact amount of packet loss rate in a selected communication.

Given the easiness on how we can create the interference, the presented evaluations can be extended to many other applications areas, ranging from protocols validation under certain patterns of interference, to solutions to increase the robustness of a deployed network. As an example, given the known impact of temperature on communication [1], [4], we could emulate an increase of temperature during the deployment phases through the use of a smart controlled interferer, so to increase the robustness of the deployment.

A. Performance of Link quality metrics

The tuning of the noise floor through the use of an unmodulated carrier can be exploited to decrease the SNR of an ongoing communication to match a specific value. For example, we can test the behaviour of an RSSI-based link quality metric L_m. The L_m metric is based on the information encapsulated in the ACK of each packet sent, which contains the information about the SNR at the receiver side. Based on such information, the sender can decrease the sending rate in case the SNR is too low. In our simple example, the communication is delayed with a sort of penalties in time as follows:

- if $SNR > T_1$, there is no penalty and the next packet is transmitted immediately (No_Penalty);
- if $T_2 \leq SNR \leq T_1$, the next packet is delayed of t_1 ms (Penalty lev. 1);
- if $SNR < T_2$, the next packet is delayed of t_1 ms (Penalty lev. 2).

Supposing the values to be $T_1 = 10dB$ and $T_2 = 5dB$, and $t_1 = 78,5ms$ and $t_2 = 157ms$, we want to compute the latency for a burst transmission of k packets on real nodes.

This simple protocol would be very difficult to test without a way to tune the noise floor and the SNR. We experimentally noticed that even if T_1 and T_2 differs only of 2-3 dB, with static conditions, we are able to create a situation in which we can decrease/increase the SNR of the communication in such a way the thresholds will be triggered as desired. Figure 9 shows the latency measured on real nodes given a pool of $k = 5$ packets. The experiment is carried out using Contiki on two Sentilla Tmote Sky nodes.

B. Responsive interference

If we know the transmission pattern of the interferees, we could use either a modulated or an unmodulated carrier to interfere the communication in such a way that the packet loss rate of the communication is approximately the desired one. Figure 5 shows that it is possible to create intermittent intervals in which interference is created. If the transmission power is sufficient to break the communication, we can synchronize

TABLE II
SUMMARY OF THE DIFFERENT METHODS OF INTERFERENCE

Interferer type	Spectral char.	Freq. agility	Interaction	Equip. cost	Calibr. cost
CC2420 in special modes	Matched	Static	Blind, Responsive, Informed	Very low	Very low
Packet-storm based	Matched	Static	Blind, Responsive, Informed	Very low	High
Wi-Fi	Broadband	Static	Blind	Average	High
Bluetooth	Sub-band	F. hopping	Blind	Average	High
Software Defined Radio	Matched	Static	Blind, Responsive, Informed	High	Average

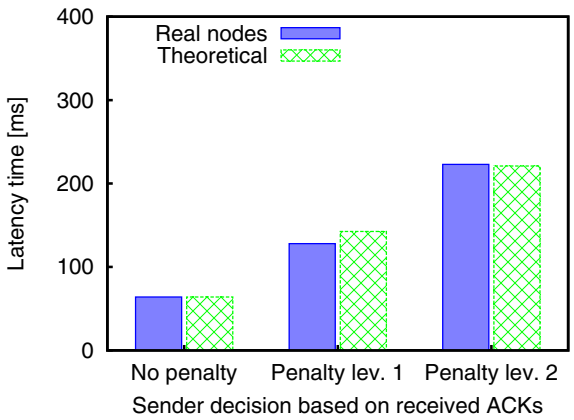


Fig. 9. Latency time for the transmission of a packet burst when using the link quality metric L_m. With our smart interferer we are able to recreate on real nodes a specific amount of SNR by triggering the desired thresholds. In this way we can test the behaviour of our file transfer application.

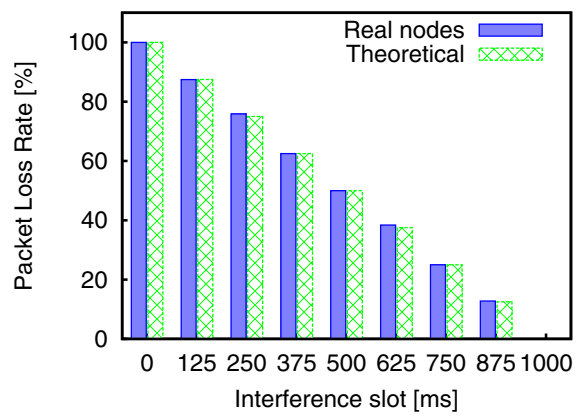


Fig. 10. Responsive interference for tunable packet loss rate generation. The interferee transmits continuously and periodically one packet every $3.9ms$, and the interferer is activated in time slots of Xms/sec, so to generate a specific percentage of packet loss rate.

TABLE III
APPROXIMATE TIME NEEDED TO SWITCH ON AND OFF THE RADIO TEST MODES ON THE TMOTE SKY PLATFORM WHEN USING CONTIKI.

Type of carrier	Time to switch on	Time to switch off
Unmodulated carrier	142.82 us	142.82 us
Modulated carrier	52.08 us	52.08 us

interferer and interferee and create an exact amount of packet loss rate. If, for example, the sensor nodes are sending data in a continuous linear fashion, e.g. 256 packets per second, i.e. one every $3.9ms$, we can set up an intermittent interferer that generates interference in time slots and obtain a predefined amount of packet loss rate. For example, if we keep the interferer on only for $125ms$ every second, we can get a PRR of 87.5%. At the same way, an interferer on for $875ms$ will generate a PRR of 12.5% only. Figure 10 shows how a periodic responsive interferer can be used to generate a PLR persistent over time that is very close or equal to the theoretical value.

This is possible because of the little time needed to switch on and off the interferer. We evaluated the time needed to perform these operations in the Tmote Sky nodes using the Contiki operating system.

The results in Table III show that it takes around 100 us to switch on and around 50 us to switch off the interferer making it possible to emulate the transmission of a single packets.

VI. RELATED WORK

Radio interference has been studied in several areas on wireless communication, ranging from cellular networks [25] to mobile ad-hoc networks [24]. Radio interference is an important topic of study due to its impact on the overall performance of the network in terms of delay, throughput, and security (jamming and denial of service).

In the area of wireless sensor networks, the study of radio interference has centered around the topics of link quality [22], MAC performance [27], and security [15]. Our work does not focus on evaluating the impact of interference on these topics, but rather we propose a simpler method to generate specific interference-patterns based on the carrier-only transmission of the CC2420 radio chip [6].

A well-known technique to generate customized radio interference is the use of external hardware. For example, Bertocco *et al.* [2] use a signal generator and a log-periodic antenna to optimize the performance of CSMA/CA in WSN deployed in industrial environments. Signal generators permit a significant flexibility in generating interference because the output power, bandwidth, and time cycles can be generated with a high granularity. However, the main disadvantage of this method is the cost required by the extra hardware. In this work, we studied the use of carrier-only transmission capability of the platforms carrying a Chipcon CC2420 radio chip, such as the Sentilla Tmote Sky.

Another widespread alternative to generate interference is

to disable the MAC carrier sense and send a sequence of packets. In [23], the authors evaluate the impact of cross-channel interference on packet reception rate by sending a synchronized sequence of packets. On a similar line of work, Zhou *et al.* [10] study interference of strong and weak links by using three motes (sender, receiver and interferer) and synchronizing the packet transmission between sender and interferer.

Packet storms have also been used to study the capture effect in WSN, whereby a packet with a strong signal can be received in spite of interference or collisions. In [26], the authors present collision detection and recovery techniques to improve the behavior of MAC schemes by leveraging on the capture effect. Son *et al.* [22] provide further insight on the capture effect by quantifying the SINR under which the capture effect can be observed. These works required the generation of synchronization methods to guarantee the collision of concurrent transmissions. By using the capabilities of the CC2420 radio, the significant work involved in synchronizing packet transmissions could be removed to a large extent.

The method proposed in this paper can also be used to re-create interference patterns obtained on particular scenarios. For instance, on a recent paper by Hauer *et al.* [12], two motes were used to capture the interference spectrum of a public plaza. Our method could be potentially used to replicate on real nodes the interference observed in this scenario.

The use of the MDMCTRL1 pin in the CC2420 radio chip has been mentioned in the TinyOS Manual [16] and in [15] as a mean to generate a continuous carrier. Our work uses this capability to provide a thorough method for generating repeatable and tunable interference patterns.

VII. Conclusions

In this paper we address the problem of generating customized controlled interference for experimental and testing purposes in wireless sensor networks. We show that by using Chipcon's CC2420 radio transceivers in special mode, we can quickly and easily generate repeatable and precise patterns of interference in an easy and inexpensive way.

Acknowledgments

We would like to thank Pedro José Marrón, Jonas Meyer, Olga Saukh and Robert Sauter for lending us the cantenna.

This work has been partially supported by CONET, the Cooperating Objects Network of Excellence, funded by the European Commission under FP7 with contract number FP7-2007-2-224053.

This work has been partially supported by the European Commission under the contract FP7-ICT-224282 (GINSENG) and was in part financed by VINNOVA, the Swedish Agency for Innovation Systems.

This work has been partially supported by an IRCSET Postdoctoral fellow Grant PD200857, SFI Grant No. SFI08CEI1380.

References

[1] K. Bannister, G. Giorgetti, and S. Gupta. Wireless sensor networking for hot applications: Effects of temperature on signal strength, data collection and localization. In *Proc. of the 5th Workshop on Emb. Networked Sensors (HotEmNets)*, Charlottesville, Virginia, June 2008.

[2] Matteo Bertocco, Giovanni Gamba, Alessandro Sona, and Stefano Vitturi. Experimental characterization of wireless sensor networks for industrial applications. *IEEE Transactions on Instrumentation and Measurement*, 57(8):1537–1546, August 2008.

[3] Bluetooth SIG. *Bluetooth Specifications*, 2.1 edition, July 2007.

[4] C.A. Boano, J. Brown, Z. He, U. Roedig, and T. Voigt. Low-Power Radio Communication in Industrial Outdoor Deployments: The Impact of Weather Conditions and ATEX-compliance. In *Proceedings of the 1st International Conf. on Sensor Networks Applications, Experimentation and Logistics (Sensappeal'09)*, Athens, Greece, September 2009.

[5] Chipcon AS. *CC1000 datasheet - Single Chip Very Low Power RF Transceiver (Rev. 2.4)*, January 2007.

[6] Chipcon AS. *CC2420 datasheet - 2.4 GHz IEEE 802.15.4 / ZigBee-Ready RF Transceiver (Rev. B)*, March 2007.

[7] Chipcon AS. *CC1020 datasheet - Low-Power RF Transceiver for Narrowband Systems (Rev. B)*, July 2008.

[8] Chipcon AS. *CC2500 datasheet - Low-Cost Low-Power 2.4 GHz RF Transceiver (Rev. SWRS040C)*, May 2008.

[9] Chipcon AS. *CC1100 datasheet - Low-Power Sub- 1 GHz RF Transceiver (Rev. SWRS038D)*, May 2009.

[10] G. Zhou et al. RID: Radio interference detection in wireless sensor networks. In *Proc. of the 24th Conference of the IEEE Computer and Comm. Societies (INFOCOM'05)*, volume 2, pages 891–901, 2005.

[11] Firas Abbas Hamza. The USRP under 1.5X Magnifying Lens. Web page, http://gnuradio.org/trac/wiki/UsrpFAQ. Visited 2009-05-31.

[12] Jan-Hinrich Hauer, Vlado Handziski, and Adam Wolisz. Experimental study of the impact of wlan interference on ieee 802.15.4 body area networks. In *Proceedings of 6th European Conference on Wireless Sensor Networks (EWSN'09)*, Cork, Ireland, February 2009.

[13] IEEE 802.11 Working Group. *Wireless LAN MAC and PHY Specifications*, ieee std 802.11-2007 edition, June 2007.

[14] IEEE 802.15.4 Working Group. *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*, rev. 802.15.4-2006 edition, September 2006.

[15] Y.W. Law, P. Hartel, J. den Hartog, and P. Havinga. Link-layer jamming attacks on s-mac. In *Proceeedings of the Second European Workshop on Wireless Sensor Networks (EWSN'05)*, pages 217–225, Jan 2005.

[16] Philip Levis. TinyOS Programming, Jun 2006.

[17] Ettus Research LLC. Universal software radio peripheral (USRP). Web page, http://www.ettus.com. Visited 2009-05-31.

[18] Razvan Musaloiu-E. and Andreas Terzis. Minimising the effect of wifi interference in 802.15.4 wireless sensor networks. *International Journal of Sensor Networks (IJSNet)*, 3(1):43–54, December 2007.

[19] RF Monolithics, Inc. *916.50 MHz Hybrid Transceiver TR1000 Data Sheet*, April 2008.

[20] O. Saukh, R. Sauter, J. Meyer, and P. Marrón. Motefinder: A deployment tool for sensor networks. In *Proc. of the Workshop on Real-World Wireless Sensor Networks (REALWSN)*, Glasgow, UK, April 2008.

[21] A. Sikora and V. Groza. Coexistence of IEEE 802.15.4 with other systems in the 2.4 GHz-ISM-band. In *IEEE Instrumentation and Measurement Technology*, pages 1786–1791, Ottawa, Canada, May 2005.

[22] D. Son, B. Krishnamachari, and J. Heidemann. Experimental study of concurrent transmission in wsn. In *Proc. of the 4th Conf. on Embedded Networked Sensor Systems (SenSys'06)*, pages 237–250, 2006.

[23] Emanuele Toscano and Lucia Lo Bello. Cross-channel interference in ieee 802.15.4 networks. In *Proc. 7th IEEE International Workshop on Factory Communication Systems*, Dresden, Germany, May 2008.

[24] Y. Tseng, S. Ni, Y. Chen, and J. Sheu. The broadcast storm problem in a mobile ad-hoc network. *Wireless networks*, 8(2):153–167, 2002.

[25] H. Viswanathan, S. Venkatesan, and H. Huang. Downlink capacity evaluation of cellular networks with known-interference cancellation. *Journal on Sel. Areas in Communications*, 21(5):802–811, June 2003.

[26] K. Whitehouse, A. Woo, F. Jiang, J. Polastre, and D. Culler. Exploiting the capture effect for collision detection and recovery. In *Proc. of the 2nd Workshop on Embedded Networked Sensors (Emnets)*, Sydney, 2005.

[27] Wei Ye, John Heidemann, and Deborah Estrin. Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Trans. Netw.*, 12(3), 2004.