Harmful Coexistence Between 802.15.4 and 802.11: A Measurement-based Study

Sofie Pollin [1,2], Ian Tan [1], Bill Hodge [1], Carl Chun [1], Ahmad Bahai [1]
[1] University of California, Berkeley; E-mail : {pollins, iantan, billh, carlchun, bahai}@eecs.berkeley.edu
[2] Interuniversity Micro-Electronics Center (IMEC);

***Abstract*— Due to recent advances in wireless technology, a broad range of standards catering to a diverse set of users are currently emerging. Interoperability and coexistence between these heterogeneous networks are becoming key issues, and proper mitigation of these issues requires a good understanding of how and why heterogeneous networks may harm each other's performance. In this paper, we focus on the coexistence of 802.11 (wireless LAN) and 802.15.4 (sensor networks) in the ISM band. These networks have very different transmission characteristics that result in asymmetric interaction patterns. Consequently, many studies assume that the impact of 802.15.4 on 802.11 is negligible. In this paper, we examine this assumption in detail and show that, in many cases, 802.15.4 significantly impacts 802.11 performance. Even when 802.15.4 is executing a listen-before-send, which should theoretically prevent interference, a significant 802.11 performance degradation frequently occurs due to disparate slot sizes between the two protocols. This is one of the first papers studying the listen-before-send performance for heterogeneous networks with substantial measured data. The results raise important coexistence issues for 802.15.4 and 802.11 in particular, but even more so for dynamic spectrum sharing between heterogeneous devices in general.**

I. Introduction

Interest in wireless technology has experienced explosive growth over the past decade. Due to the finalization of many standards, the development of wireless applications has eased, which has contributed to increased spectrum use by a variety of heterogeneous devices, standards, and applications. This hold especially true for the *Industrial, Scientific and Medical* (ISM) bands that are unlicensed and, hence, host the most heterogeneous mix of networks.

This paper focuses on the coexistence between two major wireless standards that operate in the 2.4 GHz ISM band, namely IEEE 802.11b (wireless LAN) [1] and IEEE 802.15.4 (sensor networks) [2]. Their overlapping frequency allocations are shown in Fig. 1. The characteristics of both networks differ greatly, resulting in an asymmetric coexistence problem. To begin with, the output power of 802.15.4 devices is typically as low as 0 dBm [4], whereas the output power of 802.11b devices is usually 15 dBm or above. Next, although both techniques require a listen-before-send prior to every transmission, the sensing slot for 802.11b networks is 20 μs while the 802.15.4 slot is much larger at 320 μs. As shown in Sections III and IV, this will have a large impact on their collision probabilities. Furthermore, 802.15.4 networks are typically assumed to have very low throughput requirements, resulting in a heavily reduced duty cycle or low channel usage.

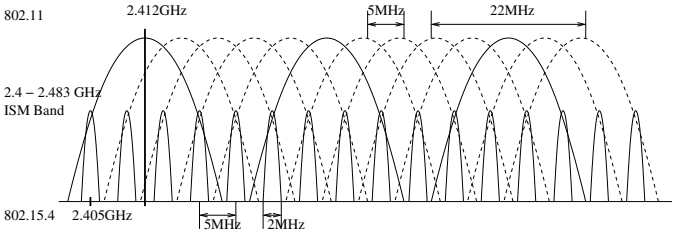

Fig. 1. 802.11 and 802.15.4 channels in the 2.4 GHz ISM band.

Because of the low output power and duty cycle, traditional analysis regularly neglects the impact of 802.15.4 on other networks in the ISM band. However, it is not the output power but the received power that governs interference, and this is a function of the output powers but also the communication distance. Since sensor networks consist typically of a large number of small devices, it is logical to assume that many sensors are near any possible communication device.

In [3] Petrova et. al. experimentally test the impact of 802.15.4 on 802.11 by using a Chipcon CC2420EB board [4]. The CC2420EB can only achieve a channel occupancy rate of 5% by using the largest possible packet size of 127 bytes. Consequently, they noted that the interference impact on 802.11b could only be seen when the offset between the central frequencies is minimal (2 MHz) and the 802.11b packet length is larger than 600 bytes. However, they did not specify the level of impact, nor did they explain why smaller 802.11b packets were not affected. Furthermore, they did not test for potential interference with smaller 802.15.4 packet sizes and larger channel occupancy rates. We address this shortcoming by studying scenarios with small 802.15.4 packets and occupancy rates up to 43%. In [5] Muoung et. al. evaluate the packet loss rate and throughput for an 802.11b network when interfered with by 802.15.4 traffic. They show that when the distance between the 802.11 reciever and 802.15.4 transmitter is small, performance degradation can be large. In their analysis, however, they assume that the transmissions between networks are independent, which implies that the listen-before-send algorithm for one network does not hear packets from the other network. Neither this assumption nor their analytical results were validated through measurements.

The purpose of this paper is to study the impact of a heavily loaded 802.15.4 network on an 802.11 network. This

study is motivated by two reasons. First, because of the very low bit rate at the physical layer of 802.15.4 networks (250 Kbps in the ISM band), applications with low throughput requirements will still cause the duty cycle at the physical layer to easily exceed 5%. For example, assume we want to transmit application layer measurement packets of 10 bytes at 250 Kbps, which takes a transmission time 320 μs. Next, each such packet involves a minimal header overhead of another 15 bytes (480 μs) [6]. As a result, each small packet of 10 bytes will need 800 μs of channel occupancy time, even in the absence of acknowledgements. A one packet per second rate is equivalent to a 0.08% duty cycle. Increasing to a 12 packets per second (pkt/s) rate results in a 1% duty cycle. This can occur when a single node reports 12 times every second or in a sensor network of 12 nodes where every node reports once a second. One application of 802.15.4 sensor networks is for health monitoring, in which the required data transfer rate can be considerably higher. For instance, the EEG, EKG, and EMG sensor nodes developed at IMEC [7] require transmitting 1024×12 bits (i.e., 12 bit samples 1024 times per second) or approximately 160 of these 10 byte packets a second, per sensor. Thus, a realistic scenario motivating this paper is such a health monitoring application, where an individual wearing a body area network is also working near a WiFi-enabled computer.

More generally, the measurements presented in this paper help illuminate how the listen-before-send mechanisms of two unsynchronized networks interact to (ideally) prevent inter-network collisions. For this second motivation of the study, other listen-before-send protocols could be used to examine coexistence. We choose 802.15.4 and 802.11 since those technologies exist in cheap, off-the-shelf solutions, and allow us to study the coexistence of heterogeneous networks in practice.

Traditional approaches for distributed channel sharing between wireless networks rely on a listen-before-sense or carrier sense technique. The first successful example of this access scheme was found in the Distributed Coordination Function (DCF) for 802.11 networks. Assuming that all 802.11 networks can hear each other, it is possible to assume that all 802.11 nodes are time-sychronized and collisions only occur by accident, i.e., when two 802.11 nodes pick the same random backoff counter. Such collisions have been studied in great detail, and they follow an analytical model to compute the collision probability proposed in [8]. However, when heterogeneous networks are sharing the medium, such time-synchronization of the nodes can no longer be assumed. Especially in the case of 802.15.4 coexisting with 802.11, we will show that the listen-before-send of 802.15.4 and 802.11 nodes is insufficient to prevent collisions and interference.

The remainder of this paper is organized as follows. First, we detail the measurement setup in Section II. Next, in Section III we present results indicating that 802.15.4 can significantly impact the performance of 802.11, even when 802.15.4 is doing a listen-before-send. Section IV explains why those collisions occur, and Section V concludes the paper.

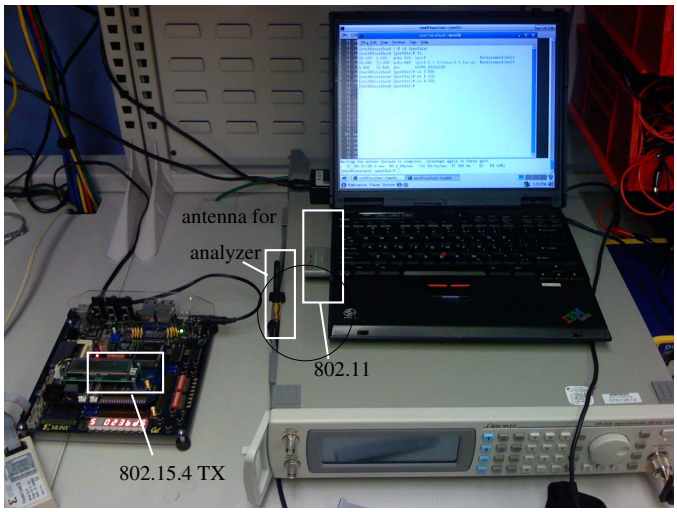

Fig. 2. CaLinx expansion board with 802.15.4 TX, Litepoint IQview antenna, and 802.11 laptop. For scenarios one and two, the laptop is the RX; for scenario three, it is the TX.

II. Measurement Setup

In this section we detail the measurement equipment: the 802.11b link, the 802.15.4 transmitter, and the spectrum analyzer (Fig. 2). Different test scenarios then follow in Section II-D.

A. 802.11 Link

For the 802.11b network, we use a point-to-point transmission link where the physical layer bit rate can be fixed to 1, 2, 5.5, or 11 Mbps. Additionally, an automatic bit rate mode (*auto*) is possible that falls back to lower rates on noisy channels (i.e., when packets are lost). We use two D-Link AirPremier DWL-A6660 PCMCIA 802.11 cards in 802.11b mode with an output power of 15 dBm. Over the link UDP packets of 1480 bytes are sent at as quickly as possible using the *iperf* tool ([10]), on channel 1. Although we could not completely avoid 802.11 traffic on that channel due to our environment, the achieved throughput was very close to the maximum possible (saturation) throughput. During every measurement, we periodically turn on the 802.15.4 traffic to demonstrate the impact on 802.11's saturation throughput. Every measurement lasted for 180 s, and the 802.15.4 traffic was on during the intervals $[30, 60]$, $[90, 120]$ and $[150, 180]$.

B. 802.15.4 Transmission

The 802.15.4 transmission was implemented using a CaLinx expansion board with a Chipcon CC2420 RF Transceiver [4]. The transceiver was controlled via a Xilinx VirtexE FPGA onboard the CaLinx board. For the measurement, we set the 802.15.4 transceiver to send short packets of 15 bytes periodically (15 bytes is only the header) at 250 Kbps. The 802.15.4 transmissions are on channel 12, with a center frequency of 2.410 GHz. This is closest to 802.11's channel 1 (center frequency 2.412 GHz). Each transmission lasted 480 μs. The period is adjustable to achieve different 802.15.4 transmission

TABLE I

MEASUREMENT SCENARIOS: 802.15.4 DUTY CYCLE INFORMATION.

Packets/s	160	320	450	640	820
Duty Cycle (%)	7.6	15.36	21.6	30.72	39.36

TABLE II

MEASUREMENT SCENARIOS: AMPLITUDE INFORMATION.

Amplitude of (-5 dB)	Scenario 1	Scenario 2	Scenario 3
Noise	-66 dBm	-66 dBm	-66 dBm
802.11 Packet	-39 dBm	-47 dBm	-19 dBm
802.15.4 Packet	-36 dBm	-36 dBm	-36 dBm

rates, as listed in Table I, and compliance with the 802.15.4 protocol is ensured by the Chipcon CC2420 chip. Before every packet, the 802.15.4 transmitter listens to the channel during two consecutive slots of length 320 μs, to detect if there is energy on the channel. Only when the channel is detected to be free a transmission may occur. As a result, the maximum channel occupancy with such short packets is $\frac{480}{1120}$, which is 42.9%.

C. Spectrum Analyzer

To obtain information on what happens on the channel during the experiment, we used a spectrum analyzer. A LitePoint IQview 802.11a/b/g WLAN tester was used to sample the ISM band at 66 MSamples/sec (complex I and Q per sample), centered around 2.412 GHz (WLAN channel 1). The antenna was connected to the spectrum analyzer through a coax cable causing an extra attenuation of 5 dB. This spectrum analyzer provided a detailed time-domain view of the channel and enabled tracking of collisions between different transmissions. However, the analyzer could only capture 15 ms, after which approximately six seconds were needed to empty the buffer for a new measurement. In Fig. 2, an overview is given of the CaLinx expansion board, one of the 802.11b laptops, and the spectrum analyzer antenna between the laptop and the board.

D. Measurement Scenarios

For the first test, we were interested in the impact of 802.15.4 on 802.11 performance. To test this, we placed the 802.15.4 transmitter close to the 802.11 receiver. Such a setup is used in scenario one and scenario two, as we will refer to them later. The respective noise powers for 802.11 packets and 802.15.4 packets as measured by the spectrum analyzer are given in Table II for each of the scenarios. The difference between scenario one and scenario two is that the 802.11 power at the reciever is lower for scenario two. We achieve the lower receive power by increasing the RX-TX distance.

Next in scenario three, the laptop closest to the 802.15.4 transceiver becomes the 802.11b transmitter. This setup tests if 802.11 will backoff for 802.15.4. An 802.11 transmitter, when undergoing a listen-before-send, has the highest probability of picking up the transmitted 802.15.4 signal if that signal is transmitted very close to the 802.11 transmitter.

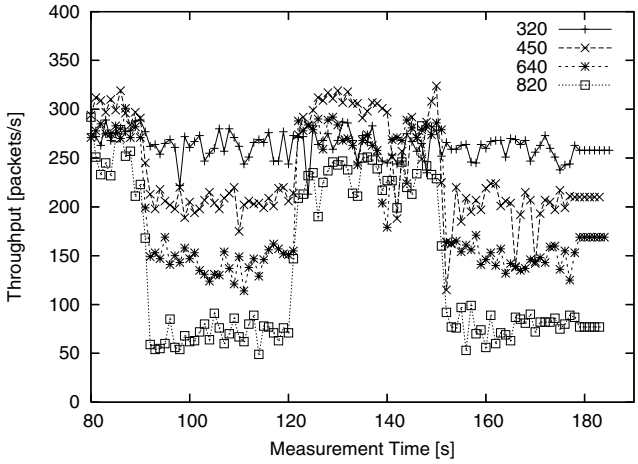

Fig. 4. 802.11 throughput over time for scenario one. Intervals with and without 802.15.4 interference can be distinguished clearly. The lower the 802.15.4 rate, the lower the impact. 802.11 rate is fixed at 11 Mbps.

III. 802.11 PERFORMANCE DEGRADATION

In this section, we discuss the performance loss of 802.11 in our scenarios. Although the 802.15.4 transmitter performs a listen-before-send based on energy levels that should theoretically avoid 802.11 packets, the performance loss may still be significant. We first look at the impact on 802.11 for scenario two in Fig. 3. The intervals with 802.15.4 traffic can be seen clearly. For each of the 802.11 physical layer bit rates, the actual throughput is lower when the 802.15.4 transmitter is on. Fig. 3 shows the results when the 802.15.4 transmitter sends at 640 pkt/s.

For comparison, in Fig. 4 we show the results for scenario one over a range of 802.15.4 rates and a fixed 802.11 physical layer bit rate of 11 Mbps. At 640 pkt/s, the impact is very similar, which implies that an 8 dB increase of 802.11 SNR does not help mitigate interference for 802.11 transmissions at 11 Mbps. From Fig. 4 it is also clear that the larger the 802.15.4 rate, the larger the performance degradation. For a 320 pkt/s 802.15.4 rate, the impact is small but still noticeable. We also plot the impact for scenario one as function of 802.11 rate in Fig. 5. Although 802.11 transmissions at 11 Mbps suffer greatly, the impact for 1 Mbps transmissions is hardly noticeable. Thus, 1 Mbps transmissions benefit from the large SNR and are more tolerant to interference noise.

In Fig. 6 we plot the throughput loss as function of 802.15.4 interference rate. The throughput loss is determined as the throughput during interference versus the throughput when no interference is present. Even for 802.15.4 at 320 pkt/s (duty cycle of only 15.36%), the throughput loss can be up to 30%. For slower 802.11 transmission rates, packets are large in time, and hence, each packet can potentially collide with 802.15.4 packets due to higher channel occupancy. Faster transmission rates suffer less since there is a high probability that 802.11 packets will fit between the periodic 802.15.4 transmissions (see Fig. 7). For even larger 802.15.4 duty cycles, the loss goes up to 60% for fixed bit rates. When the automatic rate

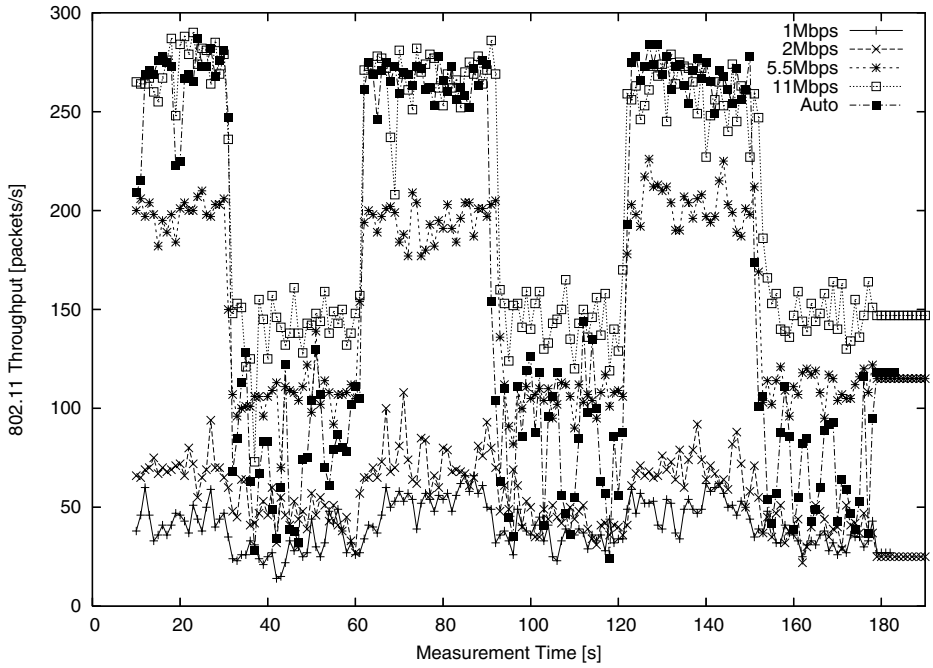

Fig. 3. 802.11 throughput versus time for scenario two. Intervals with and without 802.15.4 interference are clearly distinguishable. 802.15.4 rate set to 640 pkt/s.

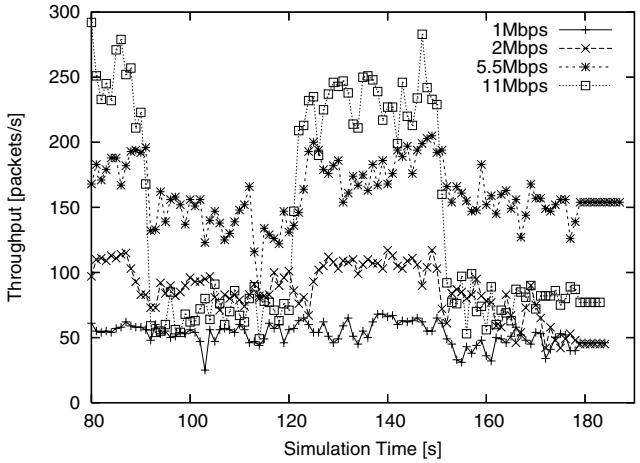

Fig. 5. 802.11 throughput over time for scenario one. 802.15.4 rate fixed at 820 pkt/s. Intervals with and without 802.15.4 interference can be distinguished clearly. While 802.11 transmissions at 11 Mbps clearly suffer, the intervals with 802.15.4 interference are less clearly noted for the 1 Mbps physical layer bit rate.

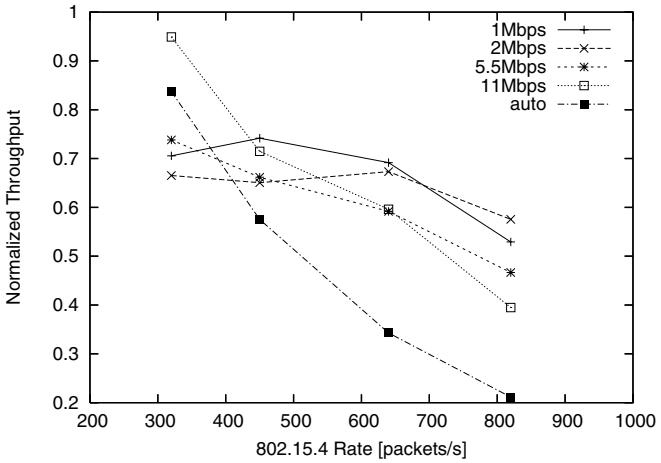

Fig. 6. Normalized 802.11 throughput loss for each 802.11 bit rate. As expected, the *auto* rate suffers most since it misclassifies losses due to interference as losses due to fading, and hence reduces the transmission rate. Data from scenario two.

control is used, the throughput degradation is even larger, up to 80%. This is because losses due to 802.15.4 collisions are misinterpreted as fading losses, causing the rate control algorithm to choose a lower physical layer bit rate.

Finally, in Fig. 8 we show that in addition to a significant throughput loss, interference caused packet losses at the UDP layer. This suggests that MAC layer retransmissions were insufficient or that 802.15.4 interference was too high to be overcome. In the next section, we will evaluate what causes those losses, even when 802.15.4 is doing a listen-before-send.

IV. Analysis of Listen-Before-Send

In this section we study why 802.15.4, while doing a listen-before-send, can harm the 802.11 transmissions. The primary cause is shown clearly in Fig. 9. In that figure we see that the collision between the short 802.15.4 packet and the long 802.11 packet occurs only at the beginning of the 802.11 packet. Indeed, during the remainder of the 802.11 packet, no 802.15.4 transmissions happen, proving that 802.15.4 does

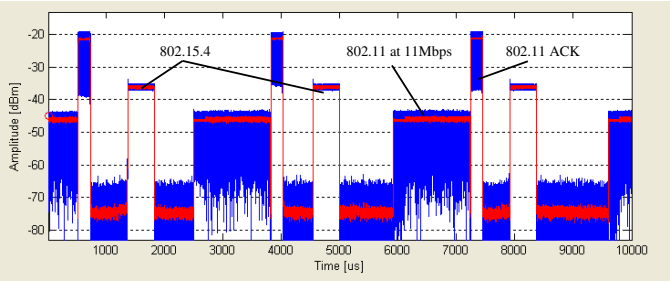

Fig. 7. Not every 11 Mbps packet suffers a potential collision with 802.15.4, since the 802.11 packets may fit between 802.15.4 transmissions. As a result, the collision probability, and hence performance degradation (at low interference rates), is lower for 11 Mbps in Fig. 6. For larger 802.15.4 rates, this benefit is no longer valid and the 802.11 performance for high physical layer bit rates degrades. Data taken from scenario two.

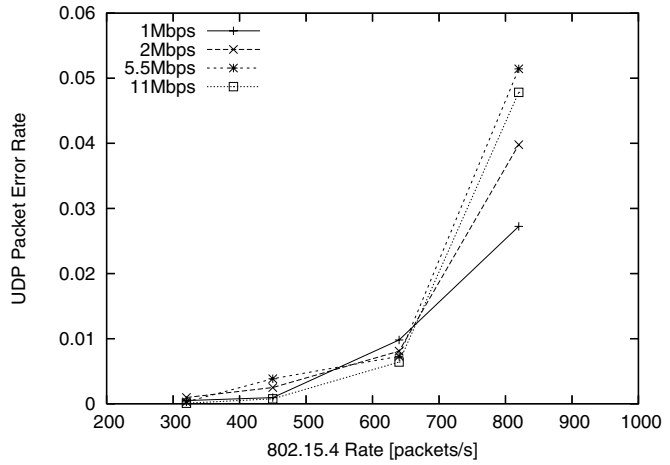

Fig. 8. Aside from a throughput loss, the UDP packet error rate rises with increasing 802.15.4 interference. Data from scenario two.

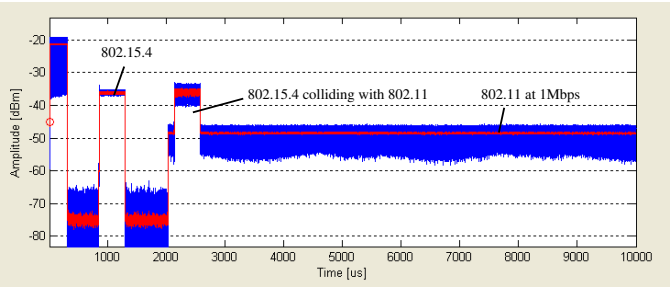

Fig. 9. 802.15.4 does not back off for 802.11 when an 802.11 packet has just started. Later, during long 802.11 packet transmissions, the 802.15.4 listen-before-send does avoid collisions. 802.11 rate set at 1 Mbps, 802.15.4 set at 450 pkt/sec.

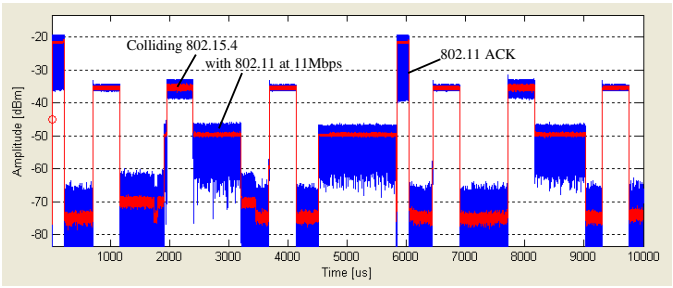

Fig. 10. Collisions with 802.15.4 does cause packet losses for 802.11 since the 802.11 packets are not acknowledged. 802.11 rate set at 11 Mbps, 802.15.4 at 900 pkt/sec.

back off for 802.11. However, the responsiveness of the 802.15.4 sensing is too slow to avoid collisions with the start of an 802.11 packet. Indeed, the 802.15.4 backoff sensing slot is 320 μs, which is very long compared to the 20 μs sensing slot for 802.11b. An 802.11 packet starting during an 802.15.4's sensing slot will not be detected quickly enough, and therefore, each network's own listen-before-send algorithm is insufficient to avoid inter-network collisions. Fig. 10 proves that an 802.15.4 collision with 802.11 results in a packet loss. Indeed, the acknowledgement (the short high-power packet just after the 802.11 data packet) is missing when 802.15.4 collides. We note that the 802.11 packets in this figure are much shorter compared to Fig. 9 because a higher 802.11 physical layer bit rate is used. This result shows that using a listen-before-sensing scheme for heterogeneous networks is inadequate for preventing unwanted interactions, especially when the data rates of the technologies are very different and synchronization is loose. Also, we note that for spectrum sharing applications, the required sensing time might be very large, which could aggravate the problem further [9].

To test the inverse situation - the ability of 802.11 to sense and backoff for 802.15.4 - we put the 802.15.4 transmitter very close to the 802.11 transmitter. The result is plotted in Fig. 11. Clearly, an 802.11 transmission happens after the start of an 802.15.4 packet, thereby showing a lack of backoff after carrier sense. The collision does not result in a packet loss for 802.11, since the 802.15.4 power is much lower (by 15 dB). This is further confirmed with the presence of the 802.11 acknowledgment from the distant receiver (the low power short packet just after the 802.11 transmission).

V. Conclusions

This paper presents a measurement study to empirically examine some assumptions about the coexistence of heterogeneous networks. First, we check if the widespread assumption that 802.15.4 cannot harm an 802.11b network holds. Most studies assume that an 802.15.4 network may harm an 802.11 network only when the former does *not* execute an 802.11-aware listen-before-send. Our results clearly disprove this assumption using real measurements and data. Even in the case when 802.15.4 is listening for 802.11 (which is not always true in reality since it is an 802.15.4 configuration option), a

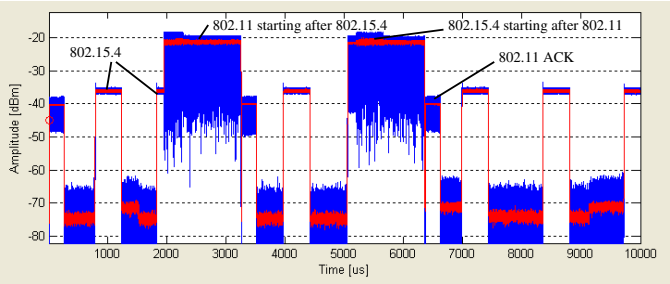

Fig. 11. 802.11 does not back off for 802.15.4, although the 802.15.4 transmitter is very close to the 802.11 transmitter. This does not cause a packet loss for 802.11 since the output power of 802.15.4 is 15 dB lower than that of 802.11 (transmitters colocated). 802.11 rate set at 11 Mbps, 802.15.4 at 640 pkt/sec.

significant and measurable performance degradation of 802.11 results when the two networks coexist, leading to a throughput degradation of 802.11 by up to 80%. In addition, packet losses at UDP layer are also observed.

More importantly, this paper shows that when designing coexistence rules for heterogeneous networks, experimental validation of assumptions and models is absolutely essential.

VI. Acknowledgements

The authors would like to thank Ferenc Kovac for supplying the CaLinx expansion board. Sofie Pollin is supported by a Marie Curie OIF fellowship of the EU.

References

[1] IEEE Standard for Information technology, *Telecommunications and information exchange between systems - LAN and MAN - Specific requirements - Part 11: Wireless LAN MAC and PHY specifications*, 1999

[2] S.C.Ergen, *ZigBEe/IEEE 802.15.4 Summary, www.eecs.berkeley.edu/ csinem/academic/publications/zigbee.pdf*

[3] M. Petrova, J. Riihijarvi, P. MAhonen, S. Labella, *Performance Study of IEEE 802.15.4 Using Measurements and Simulations,* WCNC 2006.

[4] http://www.chipcon.com/files/CC2420_Data_Sheet_1_2.pdf

[5] K.-J. Muoung, S.-Y. Shin, H.-S. Park, W.-H. Kwon, *802.11b Performance Analysis in the Presence of IEEE 802.15.4 Interference,* IEICE Trans. Commun., Vol. E90-B, No.1 Jan. 2007.

[6] S. Pollin, M. Ergen, S. C. Ergen, B. Bougard, L. Van der Perre, I. Moerman, F. Catthoor, A. Bahai, P. Varaiya, *Performance Analysis of Slotted Carrier Sense IEEE 802.15.4 Medium Access Layer,* IEEE Globecom 2006.

[7] Bert Gyselinckx and Sofie Pollin, *Wireless sensor nodes: potential and challenges,* Embedded Systems West Conference 2007

[8] G. Bianchi. *Performance Analysis of the IEEE 802.11 Distributed Coordination Function.* IEEE Journal on Selected Areas in Communications, vol.18, March 2000.

[9] A. Sahai, N. Hoven, and R. Tandra, *Some fundamental limits on cognitive radio,* Allerton Conference on Communication, Control, and Computing, October 2004.

[10] A. Tirumala, F. Qin, J. Dugan, J. Ferguson, K. Gibbs, *http://dast.nlanr.net/projects/Iperf/*