Heterogeneous Networks: experimental study of interference between IEEE 802.11 and IEEE 802.15.4 technologies

Réseaux hétérogènes: étude expérimentale de l’intéférence entre les technologies IEEE 802.11 et IEEE 802.15.4

N. de A. Moreira¹,², V. Toldov¹,², R. Igual-Perez¹,², R. Vyas², N. Mitton³, and L. Clavier¹,²,⁴

¹Univ. Lille, CNRS, Centrale Lille, ISEN, Univ. Valenciennes, UMR 8520 - IEMN, F-59000 Lille, France
²IRCICA, CNRS USR 3380
³Inria Lille - Nord Europe, Villeneuve d’Ascq, France
⁴Télécom Lille, Institut Mines Télécom

Keywords: Internet of Things (IoT), Wireless Sensor Networks (WSN), Interference, Energy Consumption
Mots-clefs: Internet des Objets (IoT), Réseauxs de Capteurs, Interférence, Consommation d’énergie

Abstract:

Internet of Things is a key technical and economical challenge for 5G. An important number of technological solutions are developed and deployed (for instance based on the IEEE 802.15.4 standard), specially in the 2.4 GHz ISM band. However this band is shared with other communicating systems, such as WiFi and Bluetooth devices. As a consequence, dealing with interference becomes crucial and has an important impact on the energy consumption. The objective of this work is to experimentally study the nature of interference between IEEE 802.11 and IEEE 802.15.4 devices and to study its impact on the communication reliability. The MAC protocol is based on carrier sense approaches but if listening to a device using the same protocol as yourself in one thing, it can be inefficient when it comes to listening to other types of devices.

Résumé:

L’internet des objets est un défi technique et économique majeur pour la 5G. Diverses solutions technologiques sont développées et déployées (par exemple basées sur la norme IEEE 802.15.4), et en particulier dans la bande ISM à 2,4 GHz. Toutefois, cette bande est partagée avec d’autres systèmes communicants, comme les périphériques WiFi et Bluetooth. En conséquence, la gestion des interférences devient cruciale et a un impact important sur la consommation d’énergie. L’objectif de ce travail est d’étudier expérimentalement la nature de l’interférence entre les dispositifs IEEE 802.11 et IEEE 802.15.4 et son impact sur la fiabilité des communications. Le protocole MAC est basé sur l’écoute de la porteuse, mais si écouter un objet utilisant un protocole identique est une chose, cela peut être inefficace quand il s’agit d’écouter d’autres types d’objets communicants.

1 Introduction: Context and Motivation

Internet of Things is a key technical and economical challenge for 5G: up to 50 billion objects may be connected through wireless networks in 2020. These connections must be low power and must be robust against electromagnetic interferences from different origins, i.e. multi-path interferences resulting from radio propagation, multiple access interference from other nodes in the network [1], and interference from other technologies that share the 2.4 GHz ISM band, such as IEEE 802.11 (WiFi) and 802.15.1 (Bluetooth). This great number of radio technologies using this band overloads this frequency [2, 3, 4, 5].

A sensor network is a network composed by autonomous, eventually intelligent, nodes able to interact with the environment, acquiring physical parameters like temperature, pressure, luminosity and other environmental data. They require physical and MAC layers with very specific constraints, different from more traditional cellular networks. Their low cost, the low data rate each node transmits and the key challenge of nodes’ lifetime necessitates new and specific designs.

According to [6] the energy necessary to transmit one packet may increase up to 4.8 times depending on the level of interference, and due to the low probability of success, the re-transmission policy may be very inefficient. It is important to evaluate the capability of a network to well behave in a certain level of interference, when the usual MAC strategy, based on carrier sensing, mainly attempts to minimize interference. This previous work [6] was based on TelosB to measure the received signal strength, using a similar approach than the one used for
the carrier sensing. The goal was to analyse in a Zigbee network interference created by other Zigbee nodes. The RSSI is a mean value calculated on 128µs duration windows.

If such measurement is relevant when measuring interference from Zigbee packets, we will show that it is rather inefficient when measuring WiFi interference. Indeed, the duration of the measuring window is too long compared to the duration of the WiFi packet and the measured value is a mean over transmission and non-transmission times, lacking of accuracy. To better analyse the impact of interference, we will also use in this work more accurate instruments to measure the interference environment. A good knowledge of interference is important to optimize the decision strategy and could impact the MAC layer strategy.

This paper will focus on two important facts about interference in wireless sensor and ad hoc networks.

— Interference will generate long sensing period (most of the protocols are based on Carrier Sensing), difficulties to initiate the communication and an increased number of transmissions. In particular, if we want to keep the same quality of service (at least in terms of packet error rate) this will significantly increase the objects consumption and reduce their life duration. We will experimentally show the link between interference level; reliability and energy consumption and show that the sensing period is an important parameter in heterogeneous networks.

— Interference exhibits statistical properties that are different from the classical thermal noise that is encountered in all communication systems. It has been shown in many papers [7, 8] that this interference exhibits an impulsive nature, but this will be specifically important in the heterogeneous environment we consider. This importantly impacts the performance of the receiver that needs to be adapted to keep good performance in such environments.

The reminder of this paper is organized as follows: in section 2 we jointly analyse interference, reliability and consumption; we use two types of measurements, one based on low accuracy TelosB mote and another using more accurate USRP cognitive radio modules; we show the difficulty for the IEEE 802.15.4 nodes to efficiently detect the IEEE 802.11 interferers. In section 3 we discuss the impulsive nature of the interference. We then show how a receiver can be designed to better behave in such an environment. The paper ends with a short conclusion.

2 Reliability, consumption and Wi-Fi Interference

We experimentally studied in [6] interference in a Zigbee network. We showed its impact on the reliability and energy consumption of the objects. In this work we address the problem of interference coming from another network [9]. The useful link uses an IEEE 802.15.4 based protocol. Interference comes from an IEEE 802.11 (WiFi) network. Both standards can use the 2.4 GHz band and interact on each other. However, the physical layer characteristics are highly different - symbol duration, carrier frequencies are different, there is no time synchronization between the systems, the bandwidth and modulation schemes are different. We analyse the impact of interference on the reliability and energy consumption. Experiments show that, contrarily to interference coming from the Zigbee network, the WiFi interference has an impact which is more difficult to analyse. Our first conclusion is that a Zigbee node is not efficient in listening a WiFi interferer. The differences in the physical layers make it difficult for the Zigbee node to make appropriate decisions and the sensing method is not suited.

2.1 Experimental set-up

The tests with Wi-Fi interference have been carried out in a laboratory environment. We use the experimental setup described in Figure 1. Two sets of devices are used to complete the experiments: one for the transmission part (TX) and the other for the reception part (RX). Both sets are composed of three different devices:

1. **WSN430 node** as the node under evaluation.

2. **TelosB mote** is used to measure the interference in the channel. It reads Received Signal Strength Indicator (RSSI) values at the center frequency of the channel used by the WSN430 nodes. This option is implemented in the CC2420 chip, which provides average values of electromagnetic energy measured during 128 µs intervals.

3. **Synergie platform**, as the energy measurements platform. The node under evaluation and the measurement platform are connected by the resistor interface which makes the measurement unit compatible with different WSN nodes. The node is also connected to the Synergie platform via two General Purpose Input-Output (GPIO) lines in order to synchronize energy measurement data with different states of the device (e.g. beginning of the retransmission, dropped packet). GPIO lines provide this information directly from the embedded code of the microcontroller of WSN430.
In this work, we analyze the average values of RSSI and energy consumption for each application layer packet (including retransmissions). These values are calculated between the end of the previous packet transmission and the end of current one, which are delimited using GPIO signals.

We have carried out a unicast communication between two Contiki-driven WSN430 nodes. Both use Rime protocol [10] on a network layer, X-MAC [11] Radio Duty Cycle (RDC) management strategy and Carrier Sense Multiple Access (CSMA) Medium Access Control (MAC) algorithm as parameters of Contiki communication stack. At the physical layer, the data are included in IEEE 802.15.4 packets. The packets are generated every second by the transmitting node. They are composed of a payload with the current packet number. The total size of the payload is 19 bytes. Moreover, 6 bytes of a Rime network layer header and 15 bytes of IEEE 802.15.4 data link layer header (for 16-bit addressing) are added. Thus, the total size of each packet is 40 bytes. Packets to be sent are placed in a buffer which can store up to 24 packets.

Following the X-MAC protocol, a transmitting node wakes up when it has a packet to transmit. Then, it sends a sequence of beacons (X-MAC preamble) containing the MAC address of the destination node in order to establish a connection. Once the receiver node is awaken, it decodes the MAC address from the beacon and if it is the packet destination, it sends an X-MAC early acknowledgment (ACK) packet back to the TX node. After reception of the X-MAC early ACK message, the transmitting node starts to send a packet with data, which should be acknowledged by the receiver in case of correct reception. Otherwise, it repeats the procedure of sending the same packet starting from X-MAC connection establishment after a random back-off time. It is important to mention that the size of a data ACK message is 11 bytes [12], which is about 4 times smaller than a data packet in our case. According to the IEEE 802.15.4 protocol, transmitting nodes can have up to three tries to send each packet. If after three transmissions there is still no ACK message received, the current data packet is discarded and deleted from the buffer. A 125 ms duty cycle is set as a parameter of X-MAC protocol. Then, the receiving node wakes up every 125 ms to check whether there is any packet to receive on the channel.

The interference source is a laptop situated 30 cm away from the TX node. This computer uses its WiFi module to communicate with the WiFi access point 10 m away. In order to send the IEEE 802.11 packets in a controlled manner, we use the D-ITG [13] (Distributed Internet Traffic Generator) tool, with which it is possible to choose the length of packet and the number of packets per second to be sent.

The IEEE 802.11 frame is composed of a fixed header of 34 bytes and maximum payload of 2312 bytes. In this test, we chose a payload of 250 bytes with a data rate of 54 Mbps, then, the on-air time is $t_{\text{paq1}} = 42.07 \mu s$. To compare, the IEEE 802.15.4 frame is 40 bytes and the data rate is $R = 250$ kbps, resulting in an on-air time of $t_{\text{paq2}} = 1.28$ ms.

2.2 Measurements

In this experiment, the channel starts without interference from the laptop during 2 minutes 30 seconds (2'30") and, then, we increase the frequency of sending the IEEE 802.11 packets every 2'30" in 100, 300, 500, 700, 900 packets per second.

During the experiments, we have collected the packet statistics information as number of retransmissions (on TX side) and number of received duplicated packets (on RX side) for each generated application layer packet. We identify the different possibilities (number of physical transmissions of a single application layer packet) with the following notation:
— type ‘1’ corresponds to the situation when a single packet is sent once, well received by RX and the ACK sent by RX is also well received by TX. This is the ideal situation, normally for the lowest interference levels;
— type ‘2’ corresponds to two transmissions of a single packet, whether a data packet or an ACK packet is lost;
— type ‘3’ corresponds to three transmissions of the same packet and the ACK is only received after the third transmission;
— type ‘4’ corresponds to lost packets: three transmissions have been done but TX has not received the ACK packet to confirm the good reception. In this case, two options are possible: either one or several data frames are received by RX but the ACK messages are lost or, more probable, the data frame has not been received by the RX.

Things are slightly different at the receiver side. Type ‘1’ describes the situation when a packet is received once, the best situation. However, type ‘2’ occurs when a single packet arrives twice to RX due to the loss of an ACK. Then, type ‘3’ represents one packet received and two duplicates of the same packet. Finally, type ‘4’ corresponds to "no packet received".

2.3 Results

We observe the energy used to transmit one packet as a function of the Received Signal Strength (as measured by a Zigbee module) at the TX side (Fig. 2) and at the RX side (Fig. 3). The different markers indicate the packet type as described in the previous section.

![Figure 2 – Energy consumption versus RSSI per packet type with WiFi interference at the transmitter.](image)

![Figure 3 – Energy consumption versus RSSI per packet type with WiFi interference at the receiver.](image)

We observe that, at the TX as well as at the RX, the energy consumed by the packets according to their packet type is coherent, since type ‘1’ (in red) remains the less energy-hungry, when type ‘2’ (black), ‘3’ (green) and ‘4’ (blue) consume more and more energy. However, the observed values in abscissa make things difficult to correlate with the interference level. This is very different from the interference coming from the IEEE 8012.15.4 devices as studied in [6]. Indeed, the range between the lowest and the highest RSSI values is small (around 7 dB), and the measurements seem not coherent: success at the first trial or repeated fails occur independently of the interference level.

The average energy, the number of packets and the total energy values per packet type in this experiment are summarized in Table 4.

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>‘1’</th>
<th>‘2’</th>
<th>‘3’</th>
<th>‘4’</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg. Energy (mJ)</td>
<td>1.60</td>
<td>4.76</td>
<td>8.86</td>
<td>9.65</td>
</tr>
<tr>
<td>No. packets (%)</td>
<td>63.0%</td>
<td>23.2%</td>
<td>7.6%</td>
<td>6.1%</td>
</tr>
<tr>
<td>Total energy (%)</td>
<td>29.9%</td>
<td>32.6%</td>
<td>20.0%</td>
<td>17.4%</td>
</tr>
</tbody>
</table>

We observe that two retransmissions consume significantly more than twice a single transmission. This is because our set-up takes into account all the different mechanisms included in the communication mechanism. The second observation is the amount of energy used for unsuccessful transmissions.
The first conclusion is the inefficiency of the sensing process in case of heterogeneous networks. One possible explanation is that RSSI measurements are carried out every 128 $\mu$s whereas the IEEE 802.11 packet on-air time is shorter, $t_{\text{paq1}} = 42.07 \mu$s. Then, CC2420 radio module and, generally, the IEEE 802.15.4 transceivers are not able to clearly detect if the channel is or not occupied by other electromagnetic sources, and especially the IEEE 802.11 devices. This is a serious problem in WSN applications where many packets may be corrupted because of these interference sources and the WSN nodes cannot detect these perturbations in the channel.

3 Impulsive interference

3.1 Further considerations

Coming back to the packet durations, we can evaluate the number of bits in a IEEE 802.15.4 packet that will be impacted by a WiFi packet. The ratio of a IEEE 802.15.4 packet duration $t_{\text{paq2}}$ over a WiFi packet duration $t_{\text{paq1}}$ (as defined in the previous section, depending on the payload the packets could have a different duration) is: $\frac{t_{\text{paq2}}}{t_{\text{paq1}}} = 30.43$. This means that the on-air time for IEEE 802.11 is much shorter. In fact, the considered IEEE 802.11 frame occupies $\frac{40 \text{ bytes}}{1 \text{ byte}} = 1.31$ bytes of IEEE 802.15.4 frame or, thus, $1.31 \times 8 \text{ bits} = 10.51$ bits. This is enough to corrupt a IEEE 802.15.4 packet as seen in the previous section. However such a dynamic interference does not result in Gaussian interference and can be mitigated with appropriate receiver design.

To further understand the impact of interference, we substitute the TelosB as channel sniffer used in the previous section with a high-performance device as a NI USRP (National Instruments Universal Software Radio Peripheral). We measured the channel with a frequency band from 400 MHz to 4.4 GHz. The test was made in IRCICA laboratory. The USRP is placed close to a XBee node which sends a 100-byte payload packet every 100 ms to the coordinator node. A Wi-Fi point access is situated at a distance of 10 meters from the XBee node and a smart-phone with the Bluetooth module activated is placed at 2 meters and communicates via Bluetooth with another smart-phone in the same room. Figure 5 shows the amplitude in ordinate axis and the time in abscissa axis of the IEEE 802.15.4 channel 12, centered in 2.410 GHz. We can identify a long IEEE 802.15.4 packet, a small Wi-Fi control packet and a Bluetooth packet. Although the Bluetooth packet is much smaller, it corrupts the IEEE 802.15.4 packet. Thus, a retransmission is done and the time in active mode of the XBee node increases. This also confirms that an impulsive noise, which can be very difficult to sense by the IEEE 802.15.4 transceivers, may corrupt a packet and, consequently, increase the energy consumption and decrease the lifetime of the node.

3.2 Detection problem statement

Let us consider the detection problem in a block fading scenario. Each data symbol is transmitted over wireless channels and $K$ versions of each symbol are received (like with the DS-CDMA structure in IEEE 802.15.4). We use in this paper a simplified version: for a single transmitted symbol, the received signal $Y \in \mathbb{R}^K$ is:

$$Y = s_h + I + N,$$

where $s$ is the unknown transmitted symbol, $h \in \mathbb{R}^K$ is the block fading channel coefficients, $I \in \mathbb{R}^K$ is the interference and $N_k \sim \mathcal{N}(0, \sigma^2)$ is the thermal noise.

![Figure 5 – Coexistence of technologies in 2.4-Ghz band. Measurements by NI USRP.](image)
The optimal receiver in terms of minimizing the Bit Error Rate (BER) is the Maximum Likelihood (ML) detector, given by:

\[ \hat{s} = \arg \max_{s \in \Omega} \mathbb{P}_Y(y|s; h) = \arg \max_{s \in \Omega} \sum_{k=1}^K \log \mathbb{P}_{Y_k}(y_k|s; h_k), \]

the second equality assuming independent noise samples. Let us now assume the following:

1. The unknown transmitted symbol, \( s \), is defined on a discrete support \( \Omega = \{-1, 1\} \) with equally likely elements to be transmitted.
2. The block fading channel coefficients are a random vector (RV) denoted by \( h \in \mathbb{R}^K \). The distribution of the coefficients depends on the considered channel model (e.g. Rayleigh, Nakagami, Rician etc.). We assume perfect channel state information at the receiver.
3. The impulsive interference is denoted by a RV \( I \in \mathbb{R}^K \) in which all elements are assumed independent and identically distributed (i.i.d.).
4. The thermal noise at the receiver is a RV \( N \in \mathbb{R}^K \) in which all elements are assumed i.i.d. with a Gaussian distribution, \( N_k \overset{i.i.d.}{\sim} \mathcal{N}(0, \sigma^2) \).
5. The interference is independent of the thermal noise, i.e., \( I \perp N \).

With these assumptions, the ML detector in (2) is given by:

\[ \sum_{k=1}^K \log \frac{\mathbb{P}_{Y_k}(y_k|s=1, h_k)}{\mathbb{P}_{Y_k}(y_k|s=-1, h_k)} \overset{z=-1}{\gtrless} 0. \] (3)

### 3.3 Standard Interference modeling

In many previous papers, it has been shown that the interference term is not adequately modelled with a simple Gaussian distribution assumption. Middleton [14, 15] derived one of the first impulsive noise model. Difficult to handle in practice, several approximation models have been proposed. The main approach is to consider only the most significant terms [16] leading to a Gaussian mixture [17]. The two terms case is often denoted as the \( \epsilon \)-contaminated noise [18, 19].

Many works have also proposed empirical choices that allow analytical analysis of the receiver, justified by simulations, observations of the estimated PDF and/or gains in BER. Some surveys can be found in [20, 21].

Recently, the network analysis attracted a lot of works relying on stochastic geometry. As in Middleton’s work, interferers are assumed spatially distributed according to a Poisson field. The heavy-tailed \( \alpha \)-stable law results from such a theoretical analysis and can also be in some cases a good model for impulsive interference.

### 3.4 Receiver design

Using the classical linear receiver in impulsive noise results in poor performance. However we do not really know what interference model to use (this highly depends on the transmission environment). The network configuration is set as follows: \( K = 5 \) repetitions are available at the destination. Representing all interference situations is not possible but we propose here to study a moderately impulsive case: a mixture of \( \alpha \)-stable \( \mathcal{S}_\alpha(0, \gamma, 0) \) and Gaussian \( \mathcal{N}(0, \sigma^2) \) noises with \( \alpha = 1.5 \), \( \text{NIR}=\sigma^2/(2\gamma) = 1 \). We compare in the following different receiver strategies. They all introduce in different manners a non-linearity that will make them more robust in the impulsive noise. We do not detail how they are derived due to lack of space in this paper but details can be found in the literature and in the mentioned references.

In Fig. 6, \( \alpha \) is set to 1.5 and NIR is 0 dB. The MRC receiver (linear receiver, optimal in Gaussian noise) has difficulties in dealing with the impulsive interference. Non linear approaches significantly improve the performances. The Cauchy [22] receiver shows a significant improvement compared to linear approaches due to the increased impact of the large samples. The Myriad [23], \( p \)-norm [24] and NIG receivers [25] give the best performances and are very close to each other. The Myriad has a slight advantage at high 1/\( \gamma \), probably due to a greater robustness to estimation errors in this mixture of impulsive and Gaussian noises.

### 4 Conclusion

In this paper we studied the coexistence of an IEEE 802.15.4 network surrounded by other types of networks, especially 802.11 devices. We showed that the sensing strategy is not necessarily adapted to this heterogeneous configuration due to a dynamic nature of the interference: the different packet duration and physical layer parameters require adapted sensing methods. It also results in an impulsive interference. In that case, the traditional linear receiver is not adapted. However, the introduction of non linear detection solution, if it increases the receiver complexity, significantly improves the performances.

A better knowledge of the interference statistical properties is necessary to adapt both the medium access protocols and the physical layer of a communication.
Acknowledgment

This work is partially supported by a grant from CPER Hauts-de-France / FEDER Campus Intelligence Ambiance and by European Commission through the program Erasmus Mundus EBW+, coordinated by Porto University. This work is part of the research project PERSEPTEUR supported by the French Agence Nationale de la Recherche ANR.

5 References


