# An Inter-Technology Communication Scheme for WiFi/ZigBee Coexisting Networks *

Daniele Croce[1,2], Natale Galioto[1], Domenico Garlisi[1,2], Fabrizio Giuliano[1,2], Ilenia Tinnirello[1]
[1]Department of Electrical Engineering, Università di Palermo, Italy
[2]Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT), Italy
*name.surname*@unipa.it

## Abstract

In this paper we show how inter-technology interference can be exploited to set-up a low-rate bi-directional communication channel between heterogeneous technologies, which coexist in ISM bands. In particular, we focus on WiFi and ZigBee networks, whose high density deployments make coexistence a critical issue. We monitor the transmission duration of the interference and, after recognizing ZigBee interference from WiFi *off-the-shelf* receivers, we precisely measure the channel busy intervals to map time duration to communication symbols. A similar approach is used on the ZigBee receivers for making the communication channel bi-directional. Extensive experimental results show the feasibility of the inter-technology communication channel.

As a possible application, we designed and implemented a cross-technology TDMA scheme, alternating channel intervals to WiFi and ZigBee nodes. This unconventional communication channel can be very useful not only for coordinating channel access between WiFi and ZigBee networks, but also for other direct link applications, such as reading measurements from ZigBee sensors, or configuring ZigBee actuators (e.g. an on/off power switch) by just using common smartphones or laptops which are only equipped with WiFi interfaces.

## Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]: Wireless communication

## General Terms

Inter-technology communication

*This work has been partially supported by EU funded research projects symbIoTe, H2020-ICT-2015 grant agreement 688156, and Flex5Gware, H2020-ICT-2014-2 grant agreement 671563.

International Conference on Embedded Wireless Systems and Networks (EWSN) 2017
20–22 February, Uppsala, Sweden

ISBN: 978-0-9949886-1-4

*Keywords*

Wireless LAN, ZigBee, coexistence

## 1 Introduction

Traditional contention-based protocols for ISM bands face the problem of coexistence with other nodes by adopting carrier sense mechanisms and dynamic adaptations of channel access probabilities (e.g. exponential backoff). However, these solutions have been mainly designed assuming that all the network nodes are homogeneous and have the same capabilities. In case of coexistence between heterogeneous technologies, such as ZigBee and WiFi, with different carrier sense granularity, transmission power, collision reactions, etc., standard adaptation mechanisms can be ineffective in mitigating performance impairments [1].

Choosing orthogonal channels can be a simple solution for improving the performance of interfering technologies. However, this is becoming impractical because of the increasing number of overlapping networks on ISM bands. Another possibility is introducing some coordination mechanisms by using multi-technology gateways [2], or increasing the robustness of transmission with error correction codes or multiple antennas [3]. Indirect coordination is also possible, for example by transmitting busy tones in an adjacent ZigBee channel for preventing WiFi nodes to interfer with the main ZigBee channel [4]. An alternative communication mean is proposed in [5], where special pulses, detectable by both the technologies, code some simple coordination messages.

A critical aspect for improving the spectrum sharing and mitigating the reciprocal interference, is the correct identification of coexisting networks. Several techniques have been designed for detecting when performance impairments are due to the interference generated by a competing technology. Some solutions are based on the characterization of RSSI samples observed by WiFi or ZigBee nodes at different frequencies and with varying temporal gaps [1, 6], or on the utilization of dedicated hardware [7]. More recently, the analysis of the "error" domain, i.e. the analysis of error events and time intervals between their occurrence, has been proposed in [8, 9] for classifying different interference sources in WiFi networks. Statistics of these errors are available on many WiFi *commodity* cards and can be used to improve interference detection and troubleshooting algorithms of wireless networks. However, the mechanisms proposed for reacting to the detection of an interfering technology [6, 4] are

currently unilateral, because of the lack of a direct communication channel between the coexisting technologies. Bilateral forms of coordination could be much more effective, e.g. based on the knowledge of the expected activity patterns, bandwidth or reliability requirements of each technology.

To this purpose, an inter-technology communication channel can be useful to directly notify these parameters and speed up the set-up of any coordination mechanism. More in general, this channel can be used for exchanging simple communication messages between different technologies, bridging two (or more) coexisting networks. Exploiting a recent error-based identification technique, in this paper we build an unconventional communication channel between interfering technologies by artificially provoking such reception errors. We specifically deal with 802.15.4 and 802.11 technologies (commonly referred as ZigBee and WiFi), and we create special interference patterns to be used as in-band messages for inter-technology WiFi/ZigBee communications. This provides network designers the unique opportunity to explicitly send information to a different network, *without the need of an external gateway* or other indirect form of communication. The proposed solution is completely backward compatible towards legacy stations and can be used to send messages *in parallel* to both networks, e.g. to coordinate channel access between the interfering technologies, improving performances in highly congested scenarios. Through extensive testbed experiments, we demonstrate the feasibility of our approach. After a brief review of the some literature solutions (section 2), we present the inter-technology communication channel in section 3. The experimental results, presented in section 4 for validating the proposed approach, show that inter-technology interference can be effectively exploited for improving WiFi and ZigBee coexistence, as described in the application example where WiFi and ZigBee share the channel in a TDMA-like fashon. Finally, section 5 provides some concluding remarks.

## 2 Background and Related Work

The interference scenario between WiFi and ZigBee technologies has been classified as *symmetrical* or *asymmetrical* [10], according to the fact that performance impairments can affect both the technologies or ZigBee nodes only. Symmetrical interference can occur when ZigBee transmitters are in proximity of WiFi receivers, thus originating an interfering signal whose power is comparable with the WiFi signal (although ZigBee transmission power is typically 20dB lower than WiFi). Because of the different granularity in performing the carrier sense, it is likely that ZigBee transmissions collide with WiFi transmissions. Indeed, ZigBee nodes sensing the channel as idle, spend 192$\mu s$ to switch from reception to transmission mode and are not able to detect WiFi transmissions starting during this switching time. Since the WiFi frame duration is shorter than the ZigBee one, the collision affects the initial part of the ZigBee frame, but still prevents the correct demodulation by the ZigBee receiver. Also the WiFi receiver cannot correctly receive its frame in case the ZigBee transmitter is in proximity. The throughput reduction due to this phenomenon can be as high as 70% for WiFi and 50% for ZigBee [9]. It is thus important to find coordination mechanisms capable to mitigate interference, possibly with direct communication between the nodes in order to avoid the need of costly external gateways.

Based on the energy-detection capability of different cards, in [5] an inter-technology communication is proposed by pre-pending a customized preamble to each legacy packet, which contains multiple energy pulses whose gaps convey information for the coexisting technology. The approach is very promising, but cannot be implemented in commercial devices. Another interesting idea, presented in [11], uses specific RF-powered tags able to communicate with commodity WiFi devices. These tags can then use the existing WiFi infrastructure to access the Internet. While a particular hardware design is necessary for the implementation of the RF tags, in our work we use only standard hardware, bridging WiFi and ZigBee nodes.

Inter-technology communication channels between WiFi and ZigBee have been also considered for different applications. In [12], a uni-directional WiFi to ZigBee channel is used for notifying the presence of pending WiFi traffic to a multi-technology WiFi/ZigBee terminal, in which the WiFi interface is switched off for energy saving. The low-power ZigBee interface receives the messages sent by the Access Points, that are opportunistically encoded in terms of interference patterns, and wakes up the WiFi interface when required. Finally, in [13], energy profiles are used to communicate from WiFi to ZigBee with a uni-directional link and an alphabet set of 100 words. In this paper, we propose instead a multi-purpose *bi-directional* scheme for communication between legacy WiFi and ZigBee devices, with an alphabet of 256 words (1 Byte) which makes the implementation much simpler.

## 3 Exploiting interference for unconventional WiFi/ZigBee communications

In this section we show how the capability of detecting interfering signals originated by a competing technology can be exploited for activating an inter-technology communication channel. Clearly, classification and communication are two independent tasks and can be executed in different ways. However, classification is necessary to implement the inter-technology communication, isolating the interfering traffic of interest. In our work, we adopt *ErrorSense* [8, 9], a recent technique to detect ZigBee frames in WiFi networks with the analysis of the error patterns caused by this interference. Errors occurring while demodulating a WiFi packet are categorized into: *i*) an error on the PLCP parity check; *ii*) an error on the FCS checksum of the MAC frame; *iii*) one or more errors in the header fields which make them invalid (either in the PLCP or MAC headers). These errors have different probabilities to occur depending on the channel conditions and on the power of the received WiFi signal. However, the errors generated by inter-technology interference have much different patterns compared to errors typical of WiFi transmissions. As discussed in [8, 9], this information can be exploited to identify the source of interference on off-the-shelf WiFi devices. The types of errors raised by the WiFi bcm4318 card used are listed in Table 1. Similar capabilities have also been demonstrated for ZigBee commercial

**Table 1. Receiver events reported by bcm4318 cards.**

| Receiver Event | Description |
|---|---|
| Too Long | Frame longer than 2346 bytes |
| Too Short | Frame shorter than 16 bytes |
| Invalid MAC Header | Protocol Version is not 0 |
| Bad FCS | Checksum Failure on frame payload |
| Bad PLCP | Parity Check Failure on PLCP Header |
| Good PLCP | PLCP headers and Parity Check OK |
| Good FCS and RA match | Correct FCS matching the Receiver Address |
| Good FCS and not RA match | Correct FCS not matching the Receiver Address |

receivers, recognizing WiFi transmissions by monitoring the interference patterns and measuring the duration of interfering transmissions [10].

The basic idea for the set-up of the inter-technology communication channel is exploiting these capabilities for coding a message into an interference signal with variable duration. This can be achieved by defining a transmission scheme in which each inter-technology data symbol is mapped into a WiFi or ZigBee frame of different length. Receivers that cannot demodulate the frame (because their technology is different from the transmitter one) measure the busy time duration and decode the associated symbol.

Similar approaches have been investigated in [5] and [12]. However, in the first case the nodes are based on Software-Defined-Radio, rather than commercial devices, because it is required to transmit a customized preamble with energy pulses opportunistically spaced. In the second case, the inter-technology communication channel is unidirectional (from WiFi to ZigBee) because it has been designed for a specific power-saving application in which a feedback channel is not required. We argue that working with commercial devices and supporting a bi-directional channel can be very useful in many practical scenarios and in particular for enabling inter-technology coordination mechanisms.

We consider a scenario in which ZigBee and WiFi networks interfere in a symmetrical way, with performance impairments for both the networks. In case each network is able to infer about the presence of the coexisting heterogeneous technology, for example by monitoring the statistics of the receiver errors, we propose to exploit this capability for setting-up an inter-technology communication channel. The basic idea is modulating the duration of the inter-technology interference for coding simple messages to be exploited for improving coexistence. Since interference is due to the transmission of frames built according to a different standard, such a modulation can be achieved by transmitting frames with variable transmission times.

Note that intra-technology data can be carried in parallel by the same frames used for inter-technology communication. Fragmentation and/or zero padding allows the adaptation of the payload to the desired frame lengths. Therefore, the inter-technology channel is *transparent* to standard communications and backward-compatible with legacy stations already present in the network.

## 3.1 Frame Length Modulation

We designed two different modulation schemes for the ZigBee-to-WiFi and WiFi-to-ZigBee links, taking into account the different features of the two technologies. On one side, the accuracy on the measurement of the channel busy intervals depends on the carrier sense granularity of the receivers, which is much smaller for WiFi (less than $10\mu s$) than ZigBee (more than $100\mu s$). On the other side, the variability range of the frame duration depends on the maximum payload size (2304 byte for WiFi, 127 byte for ZigBee), while the frame duration granularity depends on the maximum data rate of the transmitters, which lead to a granularity lower than $1\mu s$ for WiFi transmissions (1 byte at 54 Mbps) and $32\mu s$ for ZigBee transmissions (1 byte at 250Kbps).

For the WiFi-to-ZigBee link, the main limit is due to the ZigBee receiver that is able to distinguish only interference intervals whose difference is higher than $32\mu s$. This makes the system vulnerable to the environmental noise, i.e. to transmissions originated by other coexisting networks (not involved in the inter-technology communication) that can be erroneously mapped into valid symbols. To cope with these features, we defined 4 constellations of 16 data symbols; in each constellation, symbols are equally spaced of 128 $\mu s$ (i.e. 16 bytes of difference from one frame length to the next one, transmitted at 1 Mbps). Constellations are selected dynamically according to the environment traffic and node for avoiding *collisions* with intervals of equal duration due to other interferers. Decisions on symbol demodulation are based on the usual minimum distance approach, while interference intervals not corresponding to the range values of the selected constellation are simply discarded. The maximum gross rate of the channel is about 1 kbps (i.e. 4 bit/frame, with a maximum inter-frame time of about 4 *ms* for the first constellation with the smaller payloads).

For the ZigBee-to-WiFi link, the main limit is due to the WiFi receiver behavior, which performs periodic resets in case of long interference intervals (every 1 *ms*) and measures wrong busy times when a Good PLCP event is erroneously triggered (with probability 1/4, as discussed in [8]). To cope with these features, we limited ZigBee symbols to frame durations lower than 1 *ms* (maximum packet length of 31 bytes), and defined a single constellation of 8 symbols spaced of 1 byte (i.e. 24–31 bytes). Indeed, since interfering transmissions due to other WiFi networks are generally longer than 1 *ms* and WiFi receivers have a very high carrier sense granularity, the probability to have a *collision* with intervals of equal duration due to other interferers is very low. The minimum gross rate of the channel is about 3 Kbit/s (i.e. 3 bit/frame, with a frame duration lower than 1 *ms*). However, there is a very high probability to have a wrong measurement of the interference duration in case of Good PLCP events. To mitigate this problem, it is necessary to use a channel coding scheme which reduces the channel rate according to the introduced redundancy level.

## 3.2 Communication Protocol

Different communication protocols can be defined on top of the inter-technology communication scheme, according to the specific application that exploits the WiFi/ZigBee communication channel. For example, ZigBee nodes involved

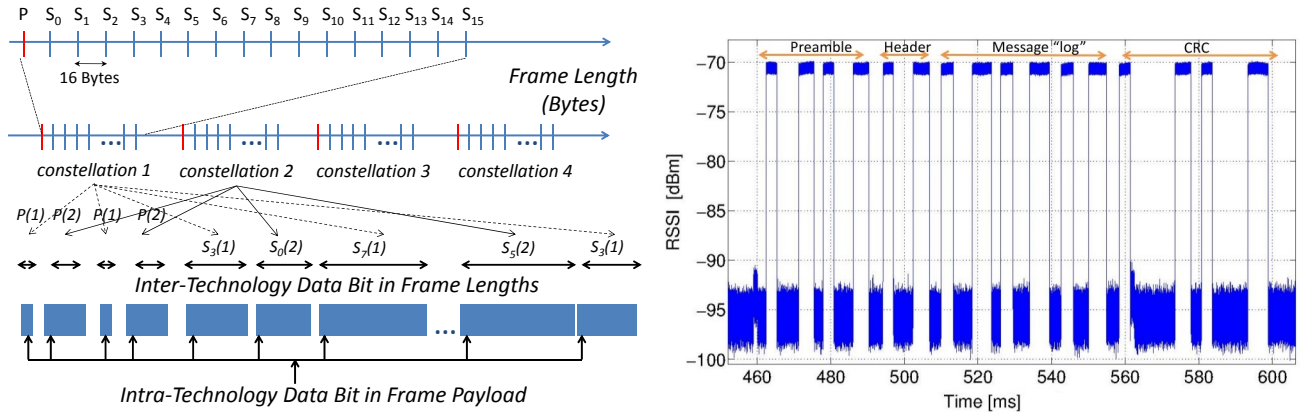


**Figure 1. Inter-technology communications: (a) modulation scheme and (b) exemplary message for the WiFi-to-ZigBee link.**

**Table 2. Loss rate and false positive rate for WiFi-to-ZigBee links (in percentage).**

| | $WiFi_H$ | | $WiFi_L$ | | $WiFi_H$+$interf_L$ | | $WiFi_L$+$interf_H$ | |
|---|---|---|---|---|---|---|---|---|
| Symb. | Loss | False | Loss | False | Loss | False | Loss | False |
| $S_1$ | 0.00 | 0.45 | 0.00 | 0.20 | 0.00 | 3.30 | 1.10 | 14.95 |
| $S_2$ | 0.39 | 1.55 | 0.00 | 0.20 | 0.00 | 3.30 | 3.40 | 14.55 |
| $S_3$ | 0.00 | 0.30 | 0.00 | 0.20 | 0.00 | 3.15 | 3.85 | 14.05 |
| $S_4$ | 0.00 | 0.10 | 0.00 | 0.25 | 0.00 | 2.40 | 7.75 | 14.35 |
| $S_5$ | 0.00 | 0.10 | 0.05 | 0.25 | 0.00 | 2.00 | 0.00 | 13.40 |
| $S_6$ | 0.00 | 0.40 | 0.05 | 0.25 | 0.00 | 2.20 | 0.00 | 14.85 |
| $S_7$ | 0.00 | 0.20 | 0.00 | 0.35 | 0.00 | 2.70 | 0.95 | 14.65 |
| $S_8$ | 0.00 | 0.10 | 0.00 | 0.50 | 2.05 | 0.20 | 0.95 | 14.70 |

**Table 3. Loss rate and false positive rate for ZigBee-to-WiFi links (in percentage).**

| | ZigBee only | | ZigB.+$WiFi_{1Mb/s}$ | | ZigB.+$WiFi_{5Mb/s}$ | | ZigB.+$WiFi_{sat.}$ | |
|---|---|---|---|---|---|---|---|---|
| Symb. | Loss | False | Loss | False | Loss | False | Loss | False |
| $S_1$ | 33.13 | 0.00 | 29.37 | 2.68 | 40.30 | 0.40 | 52.50 | 0.70 |
| $S_2$ | 31.26 | 0.00 | 31.26 | 1.71 | 38.60 | 0.70 | 57.60 | 0.50 |
| $S_3$ | 31.89 | 0.00 | 28.20 | 3.33 | 41.50 | 0.30 | 56.10 | 0.50 |
| $S_4$ | 31.80 | 0.00 | 26.67 | 2.97 | 39.80 | 0.40 | 56.60 | 1.00 |
| $S_5$ | 31.62 | 0.18 | 33.06 | 0.45 | 39.60 | 2.20 | 61.60 | 2.20 |
| $S_6$ | 33.78 | 0.09 | 31.44 | 0.99 | 39.60 | 2.10 | 50.60 | 4.10 |
| $S_7$ | 32.70 | 0.18 | 30.63 | 0.54 | 38.90 | 2.00 | 52.70 | 4.00 |
| $S_8$ | 32.61 | 0.36 | 29.82 | 0.81 | 41.20 | 3.20 | 56.40 | 6.40 |

in periodic (and sporadic) traffic could reserve in advance some channel access intervals for protecting the traffic from WiFi interference. The channel allocations can also be negotiated dynamically to adapt to traffic changes or give priority to a particular application. The channel can also be used for exchanging simple data: for example, common laptops or smart-phones, only equipped with WiFi interfaces, could read the measurements performed by ZigBee sensors or configure ZigBee actuators directly (e.g. an on/off power switch).

Figure 1 shows an exemplary message-based and byte-oriented communication protocol. Each message starts with a preamble (4 symbols following a pre-defined pattern) and includes the following fields: an header of 1 byte (i.e. two symbols) for specifying the message length; the payload, whose length may vary in the range 0-255 bytes; a final CRC of 2 bytes. It follows that the minimum message has a length of 10 symbols (4 preamble + 2 header + 4 CRC symbols) and requires the transmission of at least 10 different frames. The message preamble is built by transmitting special symbols not used for inter-technology data. As indicated in Figure 1-a for the WiFi-to-ZigBee link, the special symbols $P(i)$ are placed right before the starting of each constellation $i \in [0,3]$ and symbols $S_j(i)$ of two different constellations are interleaved ($j \in [0,15]$). Figure 1-b shows the temporal RSSI trace acquired by a USRP monitoring node corresponding to a real message. In the example, the payload is coding a control command activating a default log mode.

# 4 Experimental results

We implemented our WiFi-to-ZigBee and ZigBee-to-WiFi modulation and demodulation scheme on commercial devices. More into details, we built the inter-technology communication link by using an embedded Alix PC with a Broadcom bcm4318 WiFi card, and system-on-chip by Texas Instruments (CC2530) with Z-Stack [14]. An additional WiFi node has been used for producing environmental background traffic, which is the most common scenario. For the sake of simplicity, we avoided experiments with ZigBee background traffic, which could be added in a future work.

## 4.1 Link Reliability

Tables 2 and 3 quantify the inter-technology link reliability, respectively, for the WiFi-to-ZigBee and ZigBee-to-WiFi links. In particular, the tables show the symbol error probability for eight different symbols, which correspond to eight symbols selected in one of the available constellation for the WiFi-to-ZigBee link, and to the whole set of available symbols for the ZigBee-to-WiFi link. The error probability is decomposed into two different figures: the loss rate, that is the probability of completely missing the reception of the symbol, because the interference is not recognized as a different technology interference or because the measured duration is not recognized as a valid symbol; the false positive rate, that is the probability of detecting one symbol different from the transmitted one.

In the first WiFi-to-ZigBee experiment, we configured different scenarios by varying the distance from the WiFi

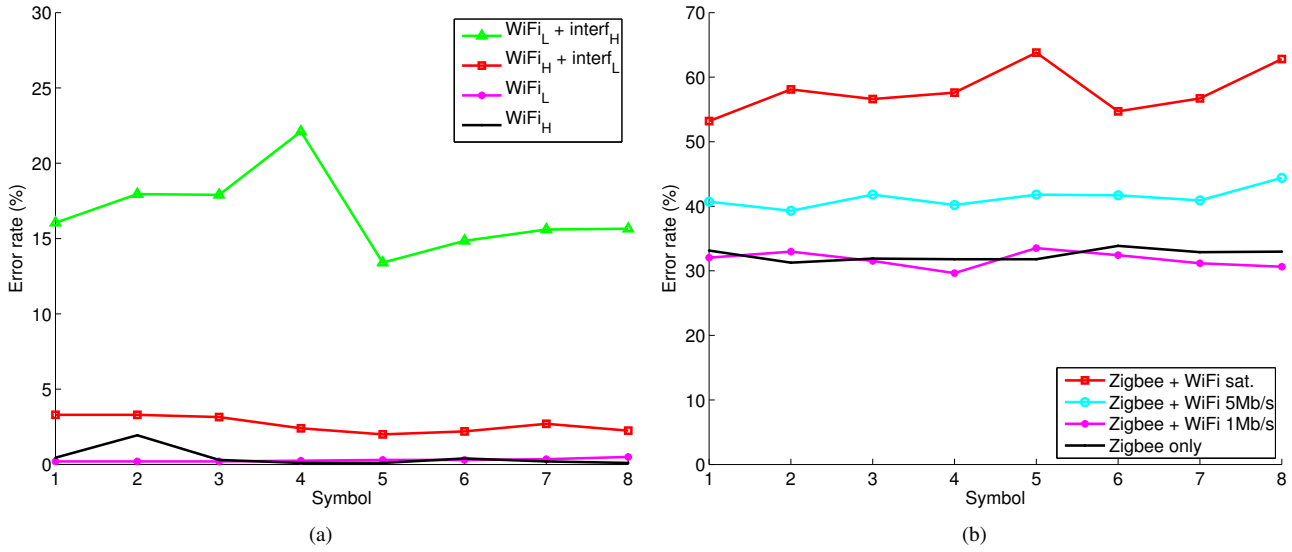


**Figure 2. Total error rate for WiFi-to-ZigBee links (a) and ZigBee-to-WiFi links (b).**

transmitter to the ZigBee receiver, as well as to the additional WiFi interferer. We classified two different levels of received powers (either the useful power or the interfering power) as high power and low power. Each level has been indicated with a subscript: the high level power is -24dBm and the low level power is -42dBm. For example, $\text{WiFi}_H$ means that the power received from the WiFi transmitter is -24dBm, while $\text{interf}_L$ means that the power received from the WiFi interferer is -42dBm. The WiFi interferer has been configured with a data rate of 1 Mbps, saturation traffic, and variable payload lengths (but different from the values of the constellation spaces). As evident from the table, in most of the considered scenarios the symbol errors are below 5%, and only with a powerful source of interference false positives raise to 14%.

In the second ZigBee-to-WiFi experiment, we configured four different scenarios, in which ZigBee is transmitting to WiFi without interference or with an environmental traffic of increasing intensity (namely, 1 Mbps, 5 Mbps and saturation traffic with a fixed payload of 1500 bytes). The data rate of the WiFi interferer has been set to 36 Mbps, which leads a packet transmission interval lower than the inter-technology constellation space. From table 3, it is evident that false positives are very low even in saturated conditions thanks to the higher precision in the busy time measurements. However, losses are higher because Good PLCP events trigger the virtual busy time mechanism which destruct the real airtime measurement of symbol transmissions. It follows that in this direction redundancy schemes are necessary. However, since the communication speed is at least three times faster than in the other direction, the inter-technology channel capacity can be opportunistically balanced, leading to a symmetric bidirectional channel rate of approximately 1 kbps.

Figure 2 summaries the above results by showing the total symbol error rate, in the two directions, for all the described scenarios.

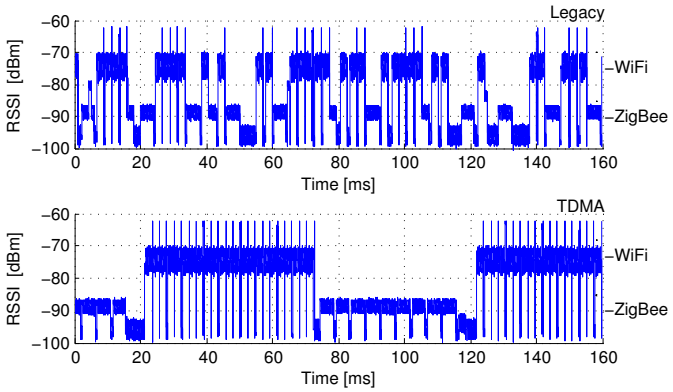


**Figure 3. Coexistence between WiFi and ZigBee networks: standard protocols (top trace) and inter-technology TDMA (bottom trace).**

## 4.2 Application Example

As an example of interesting application exploiting the inter-technology communication channel, we consider the possibility to set-up a TDMA scheme in which different technologies are allowed to transmit in non-overlapping periodic time intervals (with a frame structure), following their legacy MAC protocol within their slot. A control message is sent from the WiFi transmitter to the ZigBee nodes, coding a special command for activating this access mode. In case of positive feedback from the ZigBee coordinator, the WiFi transmitter sends a further command for configuring the slot size allocated to each technology and specifying the duration of a synchronization WiFi frame. ZigBee coordinator can confirm this allocation or asking for increasing or reducing its slot. In our experiments, such a negotiation lasts less than 0.5s. The bottom trace shown in Figure 3 is a channel access trace captured by the USRP monitoring node after the

negotiation, when the TDMA mode is activated with a equal slot size for both the technologies. Different transmitters are identified by different RSSI values measured by the USRP channel sniffer. By comparing this trace with the upper one showing normal access operations, it can be inferred that the inter-technology TDMA scheme increases the rate of ACK transmissions (i.e. successful transmissions), which are represented by the narrow spikes following WiFi frames.

# 5 Conclusions

In this paper, we have shown how to exploit the capability of recognizing inter-technology interference for building low-rate communication channels between ZigBee and WiFi coexisting networks. Leveraging on an emerging identification technique based on error patterns analysis and busy time measurements, we used *commodity* WiFi and ZigBee cards and simply monitored the appearance of reception errors together with their duration. Then, we mapped interference durations to communication symbols, to build a bi-directional communication channel between the two coexisting networks. Our experimental results show the feasibility of this inter-technology communication channel, achieving nominal speeds of about 1Kbps.

This feature paves the way to innovative applications (e.g. reading measurements from ZigBee sensors directly by using common smart-phones with WiFi interfaces) and offers network designers the great opportunity to explicitly coordinate channel access between the interfering technologies (improving performances in highly congested scenarios), without the need of an external gateway or other indirect form of communication.

# 6 References


[1] S. Pollin, I. Tan, B. Hodge, C. Chun, and A. Bahai. Harmful Coexistence Between 802.15.4 and 802.11: A Measurement-based Study. In Proc. of CrownCom, 2008.

[2] R. Gummadi, H. Balakrishnan, and S. Seshan. Metronome: Coordinating Spectrum Sharing in Heterogeneous Wireless Networks. 1st Int. Workshop on Communication Systems and Networks (COMSNETS), 2009.

[3] S. Gollakota, F. Adib, D. Katabi, and S. Seshan. Clearing the RF smog: making 802.11n robust to cross-technology interference. In Proc. of ACM SIGCOMM 2011, pages 170-181, 2011

[4] X. Zhang, K. G. Shin. Enabling Coexistence of Heterogeneous Wireless Systems: Case for ZigBee and WiFi. ACM MobiHoc 2011.

[5] Xinyu Zhang, K.G. Shin. Gap Sense: Lightweight coordination of heterogeneous wireless devices. in Proc. of IEEE INFOCOM 2013, Turin Italy, pp.3094-3101.

[6] J. Huang; G. Xing; G. Zhou; R. Zhou. Beyond Co-existence: Exploiting WiFi White Space for ZigBee Performance Assurance. ICNP, 2010.

[7] K. Lakshminarayanan, S. Sapra, S. Seshan, and P. Steenkiste. RFDump: An Architecture for Monitoring the Wireless Ether. In Procs. of CoNEXT 09, Dec. 2009.

[8] D. Croce, P. Gallo, D. Garlisi, F. Giuliano, S. Mangione, I. Tinnirello, "ErrorSense: Characterizing WiFi Error Patterns for Detecting ZigBee Interference", International Wireless Communications and Mobile Computing Conference (IWCMC), TRAC Workshop, 2014.

[9] D. Croce, D. Garlisi, F. Giuliano and I. Tinnirello, Learning from Errors: Detecting ZigBee Interference in WiFi networks, in Proc. 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOCNET) 2014. Piran (Slovenia), 2014, pp. 158163.

[10] C.-J. M. Liang, N. B. Priyantha, J. Liu, and A. Terzis. Surviving Wi-Fi Interference in Low Power ZigBee Networks. In Proc. of SenSys 10, pages 309-322, 2010.

[11] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, D. Wetherall. Wi-fi backscatter: internet connectivity for RF-powered devices. In Proc. ACM SIGCOMM 2014, Chicago, USA, pp. 607-618.

[12] Yifan Zhang and Qun Li. HoWiES: A holistic approach to ZigBee assisted WiFi energy savings in mobile devices. In Proc. IEEE INFOCOM 2013, Turin Italy, pp. 1366-1374.

[13] Kameswari Chebrolu and Ashutosh Dhekne. Esense: communication through energy sensing. In Proc. 15th international conference on Mobile computing and networking (MobiCom '09). Beijing, China.

[14] CC2530 Development Kit and Z-Stack (see http://www.ti.com/tool/cc2530dk).