DEMO: Unconventional WiFi-ZigBee Communications without Gateways [*]

Daniele Croce, Natale Galioto, Domenico Garlisi,
Costantino Giaconia, Fabrizio Giuliano, Ilenia Tinnirello
University of Palermo, Italy
name.lastname@unipa.it

ABSTRACT

Nowadays, the overcrowding of ISM bands is becoming an evident limitation for the performance and widespread usage of 802.11 and 802.15.4 technologies. In this demo, we prove that it is possible to opportunistically exploit the inter-technology interference between 802.11 and 802.15.4 to build an unconventional low-rate communication channel and signalling protocol, devised to improve the performance of each contending technology. Differently from previous solutions, inter-technology communications do not require the deployment of a gateway with two network interfaces, but can be activated (when needed) directly between two heterogeneous nodes, e.g. a WiFi node and a ZigBee node. This capability can be very useful for coordinating channel access between WiFi and ZigBee networks, reading measurements from ZigBee sensors, or configuring ZigBee actuators (e.g. an on/off power switch) directly by using common smartphones or laptops which are only equipped with WiFi interfaces.

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.

Differently from [5], which works on Software-Defined-Radios (SDRs), in this demo we show that direct communications between *commodity* WiFi and ZigBee interfaces is possible and can be used for interference mitigation. Rather than transmitting busy tones or extra RF pulses, we exploit data transmissions with variable payload lengths (not readable by the other competing technology) as in-band multi-symbol busy tones. The payload length is modulated for coding simple signalling messages that can opportunistically configure channel access parameters (such as the contention free periods, the beacon intervals, etc.) of MAC protocols as a function of the reciprocal interference. In this way we can *explicitly* coordinate channel access between the interfering technologies without the need of external gateways, SDRs or other indirect form of communication. The demonstration has been possible thanks to the availability of programmable MAC architectures for WiFi and ZigBee cards [6, 7], which allowed to implement the inter-technology communication system on the commodity hardware.

2. COMMUNICATION SYSTEM

We now present a novel inter-technology communication system, called BusyBee, which defines a modulation scheme and a message-oriented protocol that can be correctly interpreted by WiFi and ZigBee nodes.

2.1 Frame Length Modulation

In case of reciprocal interference, each technology can be configured for detecting the channel busy intervals due to the *exogenous* transmissions. This allows to define a modulation scheme in which each data symbol is mapped into a 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 by means of usual minimum distance decisions. We used a constellation of 16 data symbols, which correspond to an inter-technology transmission rate of 4 bits/frame (i.e. about 1Kbit/s for the longest ZigBee frames lasting 4 ms in case of negligible inter-frame spaces). Intra-technology data can be carried in parallel by the same frames (piggy-backing), by using fragmentation and/or zero padding, adapting the payload to the desired frame lengths.

[*] This work has been partially supported by the Italian national research project PON 04 i-NEXT.

WiNTECH'14, September 7, 2014, Maui, Hawaii, USA.
ACM 978-1-4503-3072-5/14/09.
http://dx.doi.org/10.1145/2643230.2643245.

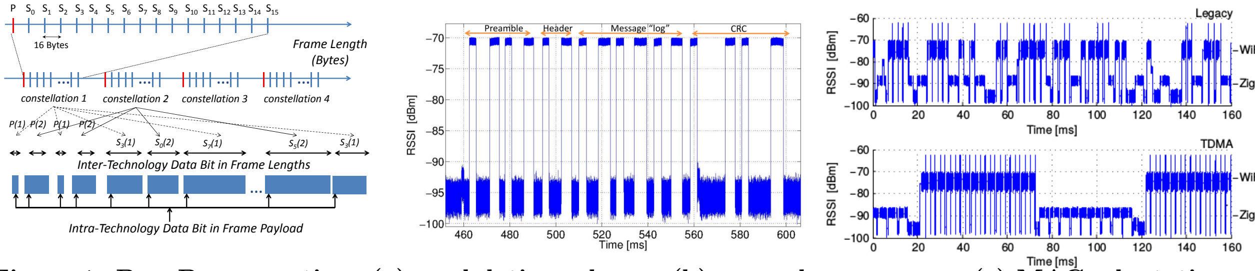

Figure 1: BusyBee operation: (a) modulation scheme, (b) exemplary message, (c) MAC adaptations.

In order to correctly consider a busy interval as an inter-technology data symbol, the constellation of frame lengths needs to be adapted to the environment traffic and noise for avoiding *collisions* with intervals of equal duration due to other interferers. For this purpose, we defined four different sets of possible frame lengths and a mechanism for monitoring the duration of all the interfering transmissions. The final modulation is obtained by considering the two constellations with the lowest interference level, and by interleaving symbol transmissions belonging to each one.

In each constellation, the symbols are equally spaced and clustered as much as possible into a small interval of values. The minimum space depends on the carrier sense granularity. Measurements not falling in the constellation interval (e.g. due to other interferers) are simply discarded. Figure 1-a shows the symbol constellations and the interleaved symbol transmissions in case the first two constellations are selected. For the link WiFi to ZigBee, in which the carrier sense granularity of the receiver is lower, the symbol lengths are spaced of 16 bytes (about $60\mu s$ tolerance).

2.2 Message Organization

The envisioned signaling protocol is message-based and byte-oriented. 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 message 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 10 different frames.

The message preamble is built by transmitting special symbols not used for inter-technology data. As indicated in figure 1-a, the special symbols are placed right before the starting of each constellation. The preamble is given by alternating the special symbols of the two selected constellations. An example of a real message is shown in the temporal RSSI trace of figure 1-b that has been acquired by an USRP monitoring node. In the example, the payload is coding a control command activating a default log mode.

3. DEMONSTRATION DESCRIPTION

Our demonstration has two main goals: (a) validating the BusyBee communication system by proving that messages can be reliably exchanged between WiFi and ZigBee nodes for supporting different inter-technology applications; (b) showing an application example in which performance benefits are achieved thanks to the coordination messages exchanged between WiFi and ZigBee transmissions.

For demonstration purposes, we developed a simple application for sending text messages between a WiFi node and a ZigBee node, and an ASCII coder for transmitting these messages over BusyBee messages. Being the maximum message length equal to 255 bytes, we can transmit up to 255 characters per message. We show how the system reliability is affected by the environment congestion level and noise and by the constellation choice.

As an example of interesting application exploiting BusyBee, we implemented an inter-technology 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. Control messages are exchanged between the nodes for activating this transmission mode and configuring the slot size allocated to each technology as a function of the traffic conditions and requirements. The bottom trace shown in figure 1-c is a channel access trace captured when the TDMA mode is activated with an equal slot size for both the technologies. Different transmitters are identified by different RSSI values measured by the 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.

Although BusyBee has been mainly envisioned for supporting coordination strategies between WiFi and ZigBee networks, we are also considering other promising use cases in which BusyBee messages are used for sending data. The idea is to read the measurements performed by ZigBee sensors, or configuring ZigBee actuators (e.g. an on/off power switch) by using common smartphones or laptops which are only equipped with WiFi interfaces.

4. 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 CrownCom, 2008.

[2] R. Gummadi, H. Balakrishnan, and S. Seshan. Metronome: Coordinating Spectrum Sharing in Heterogeneous Wireless 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. ACM SIGCOMM 2011.

[4] X. Zhang, K. G. Shin. Enabling Coexistence of Heterogeneous Wireless Systems: Case for ZigBee and WiFi. ACM MobiHoc '11.

[5] —. Gap Sense: Lightweight coordination of heterogeneous wireless devices. IEEE INFOCOM 2013.

[6] I. Tinnirello, G. Bianchi, P. Gallo, D. Garlisi, F. Giuliano, F. Gringoli. Wireless MAC Processors: Programming MAC Protocols on Commodity Hardware. IEEE INFOCOM 2012.

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