Cross-Technology WiFi/ZigBee Communications: Dealing With Channel Insertions and Deletions

Ilenia Tinnirello, Daniele Croce, Natale Galioto, Domenico Garlisi, and Fabrizio Giuliano

***Abstract*— In this letter, we show how cross-technology interference can be exploited to set up a low-rate bidirectional communication channel between heterogeneous WiFi and ZigBee networks. Because of the environment noise and receivers' implementation, the cross-technology channel can be severely affected by *insertions* and *deletions* of symbols, whose effects need to be taken into account by the coding scheme and communication protocol.**

***Index Terms*— WLAN, interference, wireless coexistence.**

I. Introduction

MANY wireless technologies for local area networks, such as 802.11 and 802.15.4 considered in this letter (commonly referred as WiFi and ZigBee), make use of unlicensed ISM radio bands which are becoming increasingly crowded. Despite the fact that many mechanisms have been included in the relevant standards to cope with interference, such as carrier sense and signal spreading, these technologies can significantly suffer in case of coexistence. For this reason, several techniques have been designed for detecting when performance impairments are due to a competing technology, by monitoring RSSI measurements [1], utilizing dedicated hardware [2], [3], or analyzing the statistics of receiver errors [4]. However, the mechanisms proposed for reacting to the detection of an interfering technology [5], [6] are currently unilateral, because of the lack of a direct communication channel between technologies. Bilateral forms of coordination can be much more effective, e.g. based on the knowledge of the expected activity patterns, or bandwidth requirements of each technology.

We propose to exploit interference for building an unconventional communication channel between WiFi and ZigBee interfering networks, which can be used for improving coordination. A similar principle has been applied in [7], by exploiting the energy-detection capability of heterogeneous receivers and special non-standard preambles conveying information symbols. Cross-technology communications based on off-the-shelf devices and energy detection have been demonstrated in [8], with an alphabet of 100 words, and in [9] with more complex messages. However, in both the cases the communication channel is unidirectional, from WiFi to ZigBee networks. The reason is that information symbols in the opposite direction can be missed with high probability, as discussed also in §III.

In this letter, we show that it is possible to set-up a *bi-directional* communication channel between off-the-shelf WiFi and ZigBee devices by exploiting interference as a communication mean, although such a channel can be critically affected by *insertions* and *deletions* due to environment noise and hardware limits. Capacity of insertion and deletion channels is still unknown, although there are some bounds and coding solutions for dealing with binary channels (which model synchronization errors between the transmitter and the receiver) or symbols carrying large number of bits (which model packet losses in Internet) [10]. Our cross-technology channel falls in the middle between these two cases, because symbols carry multiple bits in both the channel directions, but such a number is limited to a few units. Specific coding and communication schemes, based on repetition codes and multiple constellations, are envisioned for this channel and evaluated by means of a Markov model. We expect that similar channel behaviors can occur for other cross-technology communications based on interference modulation.

II. Background

A. Effects of Cross-Technology Interference

The interference between WiFi and ZigBee technologies has been classified as *symmetrical* or *asymmetrical* [11], 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*. The throughput reduction due to this phenomenon can be as high as 70% for WiFi and 50% for ZigBee [4].

B. Error-Based Interference Identification

Previous work has demonstrated that WiFi networks can recognize the presence of a coexisting ZigBee network [4] and vice versa [11], by monitoring the receiver errors. Indeed, the errors generated by cross-technology interference have different patterns compared to errors typical of standard frame demodulation. While for standard frames the error probability varies during the frame reception in different frame fields

Manuscript received July 20, 2016; accepted August 8, 2016. Date of publication August 29, 2016; date of current version November 9, 2016. This work has been partially supported by EU funded research projects sym-bIoTe, H2020-ICT-2015 grant agreement 688156, and Flex5Gware, H2020-ICT-2014-2 grant agreement 671563. The associate editor coordinating the review of this letter and approving it for publication was B. Rong. *(Corresponding author: Ilenia Tinnirello.)*

The authors are with the Department of Electrical Engineering, Università di Palermo, 90133 Palermo, Italy, and the CNIT Consortium, Italy (e-mail: ilenia.tinnirello@unipa.it).

Digital Object Identifier 10.1109/LCOMM.2016.2603978

(PHY, MAC headers, payloads) protected with heterogeneous coding, errors may appear randomly at any point during the reception of signals generated by a different technology. Random errors imply that the WiFi receivers trigger a bad PLCP event with probability 3/4 or a good PLCP event followed by another error (failed checksum or too long frames) with probability 1/4[1] [4]. The occurrence of these events with these statistics allow to identify the presence of non-WiFi modulated signals. For ZigBee receivers, random errors in the frame header (i.e. at the beginning of the ZigBee frame) allow to infer about the existence of a coexisting WiFi network.

III. Cross-Technology WiFi/ZigBee Channel

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, a simple idea for setting-up a cross-technology communication channel is modulating the duration of the cross-technology interference for coding information symbols. 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. Receivers that cannot demodulate the frame (because their technology is different from the transmitter one) measure the interference duration and decode the associated symbol. Intra-technology data can be carried in parallel by the same frames used for cross-technology communication by exploiting fragmentation and/or zero padding.

A. Frame Length Modulation

Symbol constellations for the WiFi-to-ZigBee and ZigBee-to-WiFi links can be built by considering the physical parameters of two standards. On one side, the interference duration can be measured with a different accuracy according to the carrier sense granularity of the receivers, which is much smaller for WiFi (a few μs) than ZigBee (about $128\mu s$). On the other side, the variability range of the interference duration depends on the maximum payload size (2304 byte for WiFi, 127 byte for ZigBee), which can be mapped into a maximum number of potential communication symbols by opportunistically spacing the frame transmission times. For example, figure 1 shows that in the WiFi-to-ZigBee link a space of $128\mu s$ between symbols can be achieved by transmitting frames at 1 Mbps with 16 bytes of difference between consecutive symbols, thus leading to a maximum number of 2304/16=144 symbols. In the opposite direction, the minimum space between the symbols is $32\mu s$ (1 byte at 250Kbps), with a total number of 127 symbols. As discussed in §IV, the valid set of symbols can be restricted for increasing robustness to other interfering sources, which can cause insertions and deletions of symbols.

1) Channel Insertions: Channel insertions can occur when a receiver erroneously considers interference intervals due to other interfering sources and coexisting networks as a cross-technology symbol. This phenomenon can be relevant in the WiFi-to-ZigBee direction, because of the density of coexisting WiFi networks. Although symbols can be chosen with durations different from environment traffic, it may happen that channel busy times due to the overlapping of multiple interference sources are mapped by the ZigBee receiver (which moreover works with a carrier sense granularity of only 128 μs) into valid symbol durations. In the other direction, the probability to have an insertion due to other ZigBee networks is very low because they need to be in proximity of the WiFi receiver. Moreover, WiFi receivers can distinguish channel busy intervals with an accuracy of $1\mu s$.

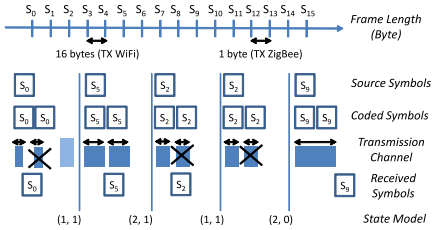

Fig. 1. An example of cross-technology constellation and transmission channel with insertions (shaded frame) and deletions (frames with crosses).

2) Channel Deletions: Channel deletions can occur when the cross-technology symbol is missed by the intended receiver because the interference is not detected or its duration measurement is wrong. This phenomenon can be very critical in the ZigBee-to-WiFi direction, because with probability 1/4 the WiFi receivers assume that ZigBee frames are valid WiFi frames and read the duration from the relevant frame field (rather than measuring it on the channel). This corresponds to a wrong measurement and, generally, to the loss of the symbol. Moreover, in this direction the ZigBee interference power is 20dB lower than other coexisting WiFi networks.

B. Experimental Characterization of the Channel

For demonstrating the feasibility of cross-technology communications and quantifying the impact of insertions and deletions, we implemented an exemplary WiFi-to-ZigBee and ZigBee-to-WiFi modulation and demodulation schemes on commercial off-the-shelf devices. More into details, we programmed WiFi nodes based on the Broadcom bcm4318 card, and ZigBee nodes based on the Texas Instrument system-on-chip CC2530 with Z-Stack. We modified the firmware of both cards for reporting low-level measurements of busy channel time at the host, where the cross-technology modulator and demodulator are implemented.

We run several tests in our lab, under *uncontrolled* environmental noise due to coexisting WiFi networks. We configured different scenarios by varying the distance of the ZigBee and WiFi nodes involved in the cross-technology link, and by activating an additional *controlled* WiFi interferer. In different experiments, the transmission power of both the WiFi cross-technology transmitter and interferer is tuned to -24dBm (high level, H) or -42dBm (low level, L), while the source rate of the WiFi interferer is increased from 1Mbps to saturation conditions, with frames of varying payloads transmitted at 6Mbps. Before characterizing the link reliability, we eliminated the channel insertions in the WiFi-to-ZigBee link by filtering valid symbols on the basis of the received power. We also observed, as expected, that insertions in the opposite direction are very rare. Tables I and II quantify

[1]These are ZigBee frames which pass the PLCP parity check (with probability 1/2 because the PLCP includes only one parity bit) and have a valid RATE field (with probability 1/2 because the field is 4 bits long, while only 8 modulations are admitted).

TABLE I

PERCENTAGE OF DELETIONS AND ERRORS FOR WiFi-to-ZigBee Links

	WiFi_H		WiFi_L		WiFi_H+interf_L		WiFi_L+interf_H	
Symb.	Del	Err	Del	Err	Del	Err	Del	Err
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 II

PERCENTAGE OF DELETIONS AND ERRORS FOR ZigBee-to-WiFi Links

	ZigBee only		ZigBee+WiFi_1		ZigBee+WiFi_5		ZigBee+WiFi_s	
Symb.	Del	Err	Del	Err	Del	Err	Del	Err
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

the cross-technology link reliability, respectively, for the WiFi-to-ZigBee and ZigBee-to-WiFi links. In particular, the tables show the symbol error probability and deletion probability for eight different symbols. The deletion probability is the probability of completely missing the reception of the symbol, while the error rate is the probability of detecting one symbol different from the transmitted one.

1) WiFi-to-ZigBee Link: We varied the power of the WiFi cross-technology transmitter and interferer. Table I shows that in most of the considered scenarios the symbol errors are below 5%, and only with a powerful source of interference the error rate raises to 14%. Deletions are due to the filter used for mitigating channel insertions. They are usually below 1%, apart from the last experiment in which some symbols have been erroneously deleted because the transmission power of the cross-technology transmitter can be comparable with the interference power.

2) ZigBee-to-WiFi Link: We configured four different scenarios, in which ZigBee is transmitting to WiFi without interference or with an environmental WiFi traffic of increasing intensity. Table II shows that errors are very low even in saturated conditions thanks to the higher precision in the busy time measurements. However, deletions are higher because good PLCP events trigger the virtual busy time mechanism based on the frame duration field, which destructs the real airtime measurement of symbol transmissions. Moreover, as the rate of the WiFi environmental traffic increases, it is likely that ZigBee transmissions collide with an ongoing WiFi transmission, thus resulting in a channel busy time longer than the cross-technology symbol duration.

IV. CROSS-TECHNOLOGY COMMUNICATION SCHEME

A. Deletion Channel With Repetiton Codes

In presence of symbols carrying large number of bits, the usual approach for dealing with channel deletions is numbering the symbols for detecting the occurrence of deletions and enabling selective retransmissions. This approach cannot be applied in our case, because we can rely on alphabets of only few symbols (namely, 8 symbols in our implementation). A possible solution is transmitting the same symbol multiple times. If l is the number of copies used for each source symbol, the residual probability to lose a symbol after the repetition code is given by the probability to lose all the copies of a given symbol, or to consider as a single symbol $r \leq l$ received copies of two or more consecutive identical symbols.

To model the channel history, we consider a discrete-time Markov chain evolving at the transmission of each source symbol, which in turns implies the transmission of l copies of the symbol. The system memory is modeled by a bi-dimensional state (i, j), where i represents the number of copies of the last received symbol (with $i = 1, 2, \cdots l$), and j is a binary variable indicating if the last received symbol is the one transmitted at the current time ($j = 1$) or not ($j = 0$). The last row in figure 1 shows an example of state evolutions for $l = 2$. At the end of the third time interval, the system state switches from $(2, 1)$ (two copies of the source symbol S_5 transmitted in the previous interval) to $(1, 1)$ (one copy of the current symbol S_2). When an additional copy of S_2 is received in the next time interval, the state switches to $(2, 0)$ because the second source symbol S_2 is not received.

Let S be the number of symbols of the alphabet, and d be the deletion probability of each symbol copy (that can be assumed constant for all the symbols, for the reasons and the experimental results presented in §III). State transitions depend on the probability to receive a number $c = 0, 1, \cdots l$ of copies, with probability $r(c) = \binom{l}{c}(1-d)^c d^{(l-c)}$, and on the probability $1/S$ that the source symbol generated at the current time is equal to the last received one. There are two mutually exclusive events which correspond to the reception of the source symbol generated at the current time: either 1) it is different from the last received symbol and at least one copy out of l copies is correctly received, or 2) it is equal to the last received symbol and the sum of the new copies with the system state is higher than l. In the first case, the first state component switches to the number of copies which are correctly received at the current time, while in the second case to the sum of old and new copies modulo l. It follows that the transition probability $\Pi(i, j)^{(m,1)}$ form a generic state (i, j) to state $(m, 1)$ can be expressed as

$$\Pi(i, j)^{(m,1)} = (1 - 1/S) \cdot r(m) + 1/S \cdot u(i - m) \cdot r(l - m + i)$$

where $u(i - m)$ is the step function equal to 1 when $m \leq i$ and 0 otherwise. When the source symbol at the current time is lost, the first state component does not change if the symbol is different from the previously received one and no copy is received, while it is increased if the symbol is equal to the previous one and the sum of old and new copies is lower or equal to l. Therefore, $\Pi(i, j)^{(m,0)}$ is given by:

$$\Pi(i, j)^{(m,0)} = 1/S \cdot u(m-i) \cdot r(m-i) + (1-1/S) \cdot \delta(m-i) \cdot r(0)$$

where $\delta(m-i)$ is equal to 1 only when $m = i$ and 0 otherwise.

Since the Markov chain is aperiodic and includes a finite number of $l \cdot 2$ states, it exists a steady-state probability vector $P(i, j)$ to be in state (i, j), from which the symbol loss probability P_{loss} can be derived as $\sum_{i=1}^{l} P(i, 0)$.

Figure 2 shows the residual P_{loss} probability as a function of the redundancy factor l and for different deletion rates, by comparing the results obtained by the model (lines) with simulations (points), for an alphabet of $S = 8$ symbols.

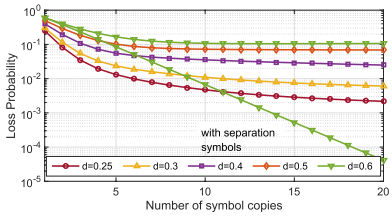

Fig. 2. P_{loss} evaluation: analysis (line) vs. simulation results (points), for different rates of the repetition code.

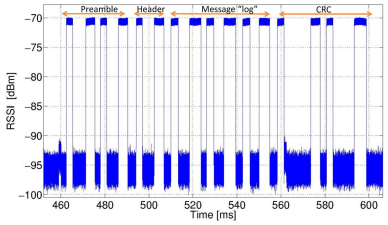

Fig. 3. Exemplary message for the WiFi-to-ZigBee link.

Because of the channel memory, the loss probability can be higher than d^l, especially for large l values where the curves exhibit a floor. This implies that the loss rate cannot be simply reduced by acting on the coding rate. However, using special separation symbols, external to the alphabet, between consecutive identical symbol it is possible to correct this phenomenon, by introducing an additional overhead proportional to $1/S$. The previous model can be easily extended to this coding variant. An exemplary curve obtained for $d = 0.6$ with this coding scheme is also shown in figure 2, where it is evident that in this case P_{loss} can be approximated by d^l.

B. Design of the Communication Scheme

The design of the cross-technology modulation and coding scheme has been based on our previous considerations on the cross-technology channel. In the WiFi-to-ZigBee direction, for minimizing the probability of insertions, we defined four different constellations of 16 alphabet symbols and two additional symbols (for helping in the delimitation of the messages), that can be dynamically selected according to the most probable durations of the environmental interference. The first symbol of each constellation has been set to 300, 570, 900 and 1170 bytes. Moreover, two different constellations can be interleaved for detecting single insertions. By considering that 16 symbols carry 4 bits and that the average frame transmission time including the backoff time is about $4ms$ for the first constellation with the smallest payloads, the maximum gross rate of the channel is about 1 kbps. In the ZigBee-to-WiFi direction, we defined a single constellation, because insertion probability was practically zero. Since we observed that some WiFi cards perform a periodic reset after an interference duration of 1ms, we decided to limit the constellation size to 8 alphabet symbols and two additional external symbols (corresponding to ZigBee frames whose payload vary from 1 to 10 byte and to a maximum symbol duration lower than 1ms). Assuming that in practical conditions the deletion rate is about 0.3, from previous results we decided to use a repetition code with $l = 4$ and separation symbols, thus obtaining a channel gross rate of 3 bits/4 ms=0.750kbps.

Different communication protocols can be defined on top of the proposed scheme for frame length modulation and coding, according to the application which exploits the cross-technology communication channel. As a demonstrative example, we implemented a message-based and byte-oriented communication protocol devised to send text data or configuration commands to the nodes. Figure 3 shows the temporal RSSI trace acquired by a USRP monitoring node during the transmission of a cross-technology message sent by a WiFi node. In the example, the message length is equal to 10 symbols (4 preamble + 2 header + 4 CRC symbols) and the payload is coding a control command activating a *logging* mode on the ZigBee node.

V. CONCLUSIONS

In this letter, we have shown how to exploit the capability of recognizing cross-technology interference for building low-rate communication channels between ZigBee and WiFi coexisting networks. A demonstrative modulation and demodulation scheme has been implemented by working on *commodity* WiFi and ZigBee cards. We experimentally characterized the cross-technology channel, by dissecting the origin of asymmetrical *insertions* and *deletions* problems due to the environment noise and receiver implementations. Finally, we have discussed some possible approaches for dealing with channel insertions and deletions, based on multiple constellations and repetition codes. We argue that cross-technology communications pave the way to the improvement of coexistence in ISM bands and even to innovative applications, e.g. reading measurements from ZigBee sensors directly by using common smart-phones with WiFi interfaces.

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. 3rd Int. Conf. Cognitive Radio Oriented Wireless Netw. Commun. CrownCom*, May 2008, pp. 1–6.

[2] K. Lakshminarayanan, S. Sapra, S. Seshan, and P. Steenkiste, "RFDump: An architecture for monitoring the wireless eTHER," in *Proc. 5th Int. Conf. Emerging Netw. Experiments Technol.*, Dec. 2009pp. 253–264.

[3] Y. Gao, J. Niu, R. Zhou, and G. Xing, "ZiFind: Exploiting cross-technology interference signatures for energy-efficient indoor localization," in *Proc. IEEE INFOCOM*, Turin, Italy, Apr. 2013, pp. 2940–2948.

[4] D. Croce, D. Garlisi, F. Giuliano, and I. Tinnirello, "Learning from errors: Detecting ZigBee interference in WiFi networks," in *Proc. 13th Annu. Mediterranean Ad Hoc Netw. Workshop (MED-HOC-NET)*, Jun. 2014, pp. 158–163.

[5] J. Huang, G. Xing, G. Zhou, and R. Zhou, "Beyond co-existence: Exploiting WiFi white space for ZigBee performance assurance," in *Proc. ICNP*, Oct. 2010pp. 305–314.

[6] X. Zhang and K. G. Shin, "Enabling coexistence of heterogeneous wireless systems: Case for ZigBee and WiFi," in *Proc. 12th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2011, pp. 6:1–6:11.

[7] X. Zhang and K. G. Shin, "Gap sense: Lightweight coordination of heterogeneous wireless devices," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 3094–3101.

[8] K. Chebrolu and A. Dhekne, "Esense: Communication through energy sensing," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw.*, Beijing, China, 2009, pp. 85–96.

[9] Y. Zhang and Q. Li, "HoWiES: A holistic approach to ZigBee assisted WiFi energy savings in mobile devices," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 1366–1374.

[10] R. Yazdani and M. Ardakani, "Reliable communication over non-binary insertion/deletion channels," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3597–3608, Dec. 2012.

[11] C.-J. M. Liang, N. B. Priyantha, J. Liu, and A. Terzis, "Surviving Wi-Fi interference in low power ZigBee networks," in *Proc. 8th ACM Conf. Embedded Netw. Sensor Syst.*, 2010, pp. 309–322.