Adaptive 802.15.4 Backoff Procedure to Survive Coexistence with 802.11 in Extreme Conditions

Eugène David Ngangue Ndih, and Soumaya Cherkaoui
Department of Electrical and Computer Engineering
Université de Sherbrooke, Québec, Canada
Email: {eugene.ngangue, soumaya.cherkaoui}@usherbrooke.ca

***Abstract*—With the increasing deployment of smart devices for the Internet of Things (IoT) using 802.15.4 in spaces where 802.11 devices are already deployed, wireless channels are getting densely populated in the 2.4 GHz ISM band, especially when nodes operate in saturation conditions. In addition to the fact that 802.15.4 and 802.11 use different CSMA/CA protocols with considerable different backoff durations, 802.15.4 is designed for ultra-low power, low rate WPAN while 802.11 is designed for higher power and high data rate WLAN. In this paper, we aim to tackle the resulting issues due to this asymmetric coexistence. Especially we propose a simple but efficient backoff mechanism for 802.15.4 in which the backoff duration is adaptively chosen, when WiFi transmissions are detected during the clear channel assessment. Through extensive simulations, we demonstrate the efficiency of the proposed adaptive backoff mechanism and the considerable improvements of the 802.15.4 performance even in case of erroneous decision regarding the type of packet detected during the clear channel assessment.**

I. Introduction

Recent years have been marked by an increasing deployment of both smart devices such as smartphones and tablets for ubiquitous internet access, and sensors - for IoT purposes - which operate in the same 2.4 GHz unlicensed industrial, scientific, and medical (ISM) band. As a consequence, when co-located, these wireless devices experience excessive additional amount of interference known as Cross Technology Interference (CTI) [1]. CTI happens because the technologies involved (802.11 [2] for smartphones, laptop, tablets, etc., and 802.15.4 [3] for wireless sensors) are not designed with the consideration of this coexistence issue.

Indeed, while 802.15.4 (also refer as ZigBee in this paper) is designed for ultra-low power, low rate wireless personal area networks (WPAN), 802.11 (also refer as WiFi in this paper) is designed for higher power and high data rate wireless local area networks (WLAN). In addition, 802.15.4 and 802.11 use different CSMA/CA protocols with considerable different backoff durations. Therefore, as wireless channels are getting densely populated by both 802.11 nodes and 802.15.4 nodes, it becomes important to design efficient protocols that can handle the CTI issues. This is important especially for 802.15.4 nodes whose performance could significantly be deteriorated as it will be shown later on in this paper.

Several studies have been conducted within the last decade to address this coexistence issue. As a matter of fact, there have been new standards which were designed for WiFi such as 802.11n [4] or 802.11ac [5] which basically propose to switch to the 5 GHz ISM band in order to enjoy higher data rates, higher bandwidth and low congestion for the 802.11 nodes. However, because the migration towards the 5 GHz band is not be complete and will not complete in the next few years, and also because of the importance of the 2.4 GHz as a potential frequency candidate for wireless connectivity for the IoT paradigm [6], we keep focusing in this work on solving the coexistence between 802.11 and 802.15.4 in the 2.4 GHz band.

The techniques proposed in the literature to improve the coexistence of WLAN and WPAN in the 2.4 GHz ISM band depend in general on PHY, MAC or networks parameters. The authors in [7] proposed a good survey of some of the proposed techniques. Most techniques can be categorized either as techniques which propose to geographically separate WPAN from WLAN - which is not always possible, or either as techniques implementing additional mechanisms to make ZigBee networks and WiFi networks more friendly. In this last category, some techniques involve additional payload [1], others do not tackle the asymmetric unfairness of coexistence [1] [8], or add complexity to ZigBee network operations by requiring new coordination mechanisms [9]. Another kind of techniques that also fall in the last category are techniques which try to mitigate the effect of packet collisions of ZigBee and WiFi [1], [8]; therefore, they are post-solution by nature, and do not solve CTI problems.

In this paper, different from other works, we tackle the problem of CTI between ZigBee and WiFi nodes while also addressing the problem of unfairness without added complexity.

To this aim, we propose an adaptive backoff procedure technique for 802.15.4. By doing so, we also tackle the problem of starvation of ZigBee nodes in accessing the channel in the presence of WiFi nodes.

Our contribution can be summarized as follows:

- We propose an adaptive backoff mechanism for 802.15.4 in which the backoff duration is uniformly selected within 0 and twice the CCA duration, when WiFi transmissions are detected during the CCA.
- Through extensive simulations conducted in MATLAB, we demonstrate the efficiency of the proposed adaptive 802.15.4 backoff mechanism.
- We demonstrate that even in case of erroneous decision regarding the type of packet detected during the CCA, the adaptive 802.15.4 backoff procedure still provides significant

978-1-4673-9292-1/16/$31.00 ©2016 IEEE

improvements regarding the performance of the ZigBee nodes compared to the standard 802.15.4 backoff procedure.

A. Literature Review

As example of previous works belonging to the category of our concern, the authors in [1] quantified the interference patterns between 802.11 networks and 802.15.4 networks at a bit-level granularity, and they introduced a mechanism, named BuzzBuzz, which aims to improve the reception rate of the 802.15.4 nodes through header and payload redundancy. Contrary to our proposed technique, the efficiency of BuzzBuzz relies mostly on the interference patterns and does not tackle the unfairness suffered by 802.15.4 nodes due to the significant difference of rates between 802.11 and 802.15.4.

In the same vein, authors in [8] presented WizBee (i.e. Wise ZigBee system) as extension to current ZigBee networks with intelligent sink node. WizBee is based on the observation that WiFi signal is much stronger than ZigBee signal when they collide, leaving much room for applying interference cancellation technique, especially in symmetric area. To recover ZigBee packet during WiFi/ZigBee collision, WizBee first extracts WiFi packet, then subtracts WiFi interference and decodes ZigBee packet. As BuzzBuzz, WizBee is a collision-based post-solution. It tries to recover 802.15.4 packets involved in collision with 802.11 packets. We propose instead a predictive approach, and most important, we address the unfairness due to larger backoff durations of ZigBee nodes.

In [10], the authors proposed WiCop, a policing framework to address the coexistence problem between 802.15.4 and 802.11 in the 2.4 GHz band. WiCop aims to control the temporal white-spaces between consecutive WiFi transmissions, and utilizes them to deliver low duty cycle medical WPAN traffic with minimum impacts on WiFi. However, if no such spaces are not available, ZigBee nodes will have more difficulties in accessing the channel.

In [9], a technique which aims to notify WiFi nodes of the presence of ZigBee nodes has been proposed. Referred to as cooperative carrier signaling (CCS), the technique implements a separate ZigBee node called signaler which behaves as a proxy to perform the carrier signaling. The signaler has a higher power than normal ZigBee transmitters, thus allowing the WiFi nodes to sense the ZigBee transmitter's presence indirectly by detecting the busy tone. This technique requires additional complexity to manage the busy tone.

B. Paper Organisation

The rest of the paper is organized as follows. In Section II, we present the system model with the main assumptions considered. In Section III, we present a brief overview of the CSMA/CA mechanisms for 802.11 and 802.15.4, and we describe the proposed adaptive backoff procedure. In Section IV, we present some numerical results, and we discuss about the performance of both 802.11 nodes and 802.15.4 nodes when the adaptive backoff scheme is used. Finally, in Section V, we conclude this work.

II. System model, and Assumptions

We consider a homogeneous WLAN network co-located with a homogeneous WPAN network, and coexisting in the same 2.4 GHz spectrum band. All ZigBee nodes are in the communication range of WiFi nodes. The topology of the network is constant, and the number of nodes does not change during the analysis. The size of 802.15.4 packets is assumed to be fixed as well as the size of 802.11 packets but the ratio between these two sizes varies. Both ZigBee nodes and WiFi nodes operate in saturation conditions, that is, they always have a packet ready for transmission. We consider constant and equal packet size for each type of node. We assume ideal channel conditions, that is, a failure of transmission occurs only upon collisions. These assumptions are consistent with previous literature. Further, we assume that ZigBee nodes can predict using appropriate energy/preamble detectors [3], [11] during the CCA if the detected transmission comes from other ZigBee nodes or not. However, this assumption is relaxed further on the paper, and we demonstrate that it might have a negligible impact for relative good prediction.

III. Description of Proposed Backoff Procedure

A. Overview of 802.11 DCF

According to the standard [2], a WiFi node which uses the 802.11 DCF (Distributed Coordination Function) scheme (802.11 node) to transmit a new packet first has to sense the channel activity. If it finds the channel idle for a period of time corresponding to the Distributed InterFrame Space (DIFS)[1], the node transmits, otherwise the node set its backoff counter to a random backoff time uniformly chosen between 0 and $CW - 1$, where CW, the contention window, is set to the minimum value CW_{min} at the initiation of the transmission of a new packet. At any backoff state, if the channel is found busy, the backoff counter is frozen until the channel is sensed idle for a DIFS period, and the backoff counter is then decremented by one. When the backoff counter reaches zero, the node proceeds to the transmission. Upon successfully received a packet, the receiver has to acknowledge the source node by transmitting a short ACK packet after the channel being sensed idle for a Short InterFrame Space (SIFS) time. If the source node does not receive the ACK packet, the CW for backoff time is doubled up to the maximum value CW_{max}. When the value of CW exceeds CW_{max}, we assume that the packet is dropped.

B. Overview of the unslotted 802.15.4

In the unslotted 802.15.4 CSMA/CA, the WPAN coordinator does not send beacons every cycle. According to the standard [3], when a ZigBee node, using the unslotted 802.15.4 mode, wants to transmit a packet, it waits for a random number of *backoff Periods* (BP) between 0 and $2^{BE} - 1$, where BE, the backoff exponent, is $3 \leq BE \leq 5$. For simplicity of presentation, we use the following notations:

[1]To avoid channel capture, even if the channel is sensed idle for a DIFS period, a node must delay a random backoff time between two consecutive new packets transmissions.

$BE_{min} = macMinBE = 3$, and $BE_{max} = macMaxBE = 5$. At the end of the backoff stage, the ZigBee node performs a *Clear Channel Assessment* (CCA) over a duration of 8 symbols. If the channel is sensed busy during this step, both BE and the number of backoffs (NB) are incremented by one up to BE_{max} and NB_{max} =*macMaxCSMABackoffs* respectively. Once BE reaches the value BE_{max}, it remains at this value until the packet is dropped or successfully transmitted. The packet is dropped either if NB exceeds its maximum value allowed, that is, $NB > NB_{max}$, or if the number of retransmission (RT) exceeds the limit allowed ($RT > RT_{max} = macMaxFrameRetries$). Note that, for a given packet, the variable RT is incremented by one each time the node fails to receive ACK after transmitting the packet.

C. Description of the Adaptive 802.15.4 Backoff Procedure

The goal of the Adaptive 802.15.4 Backoff Procedure is to improve the performance of the ZigBee nodes when coexisting with WiFi nodes. In general, the proposed adaptive backoff mechanism is similar to the standard backoff procedure described above. The difference is observed only when ZigBee nodes detect a WiFi transmission during the CCA. To summarize, when a ZigBee node which uses the adaptive 802.15.4 backoff procedure wants to transmit a packet, it waits for a random number BP between 0 and $2^{BE}-1$, with $3 \leq BE \leq 5$. When the counter reaches zero, the ZigBee node performs a CCA over a duration of 8 symbols. We assume that with the adaptive backoff procedure, a zigBee node can determine whether the detected transmission comes from a ZigBee node or not, in which case the transmission comes from a WiFi node. If the channel is sensed busy by a ZigBee transmission during this step, both BE and NB are incremented by one up to BE_{max} and NB_{max} =*macMaxCSMABackoffs* respectively. Once BE reaches the value BE_{max}, it remains at this value until the packet is dropped or successfully transmitted. If the channel is sensed busy by a WiFi transmission instead, both BE and NB do not change, and the backoff window is adjusted accordingly. The node waits for a random BP uniformly chosen between 0 and $2CCA$ (twice the CCA duration). Fig. 1 presents the main changes between the adaptive backoff procedure and the standard backoff procedure.

IV. Simulation Analysis

A. Simulation scenarios

To provide deep insights on the adaptive 802.15.4 backoff procedure, we consider several scenarios for simulation. Unless stated otherwise, the PHY and MAC parameters of ZigBee and WiFi are derived from their respective standards [3], [2]. In the first scenario, the number N of ZigBee nodes is set to 10 and we vary the number M of WiFi nodes from 0 to 10, and we set the ratio of ZigBee/WiFi packet durations to 50. For the second scenario, we consider a fixed number of nodes within the network, and we vary the proportion of WiFi/ZigBee nodes. Also, to analyze the impact of the packet duration of both WiFi/ZigBee nodes, for each WiFi/ZigBee nodes distribution, we vary the ratio of ZigBee/WiFi packet durations. For each simulation, we determine for both the

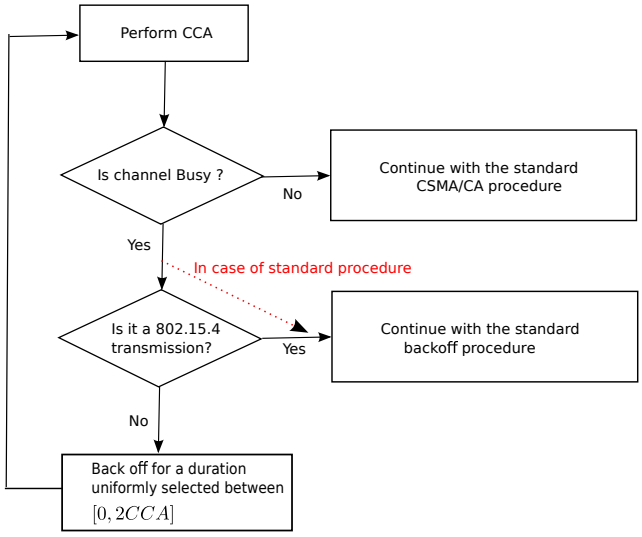

Fig. 1: Adaptive 802.15.4 Backoff Procedure.

802.1.5.4 standard backoff procedure and the 802.1.5.4 adaptive backoff procedure the fractions of successful/unsuccessful transmissions of WiFi/ZigBee nodes among the total number of transmitted packets. The total number of transmitted packets is determined either when the simulation duration expires, or when the maximum number of packets to be transmitted within the simulation is reached.

B. Discussion

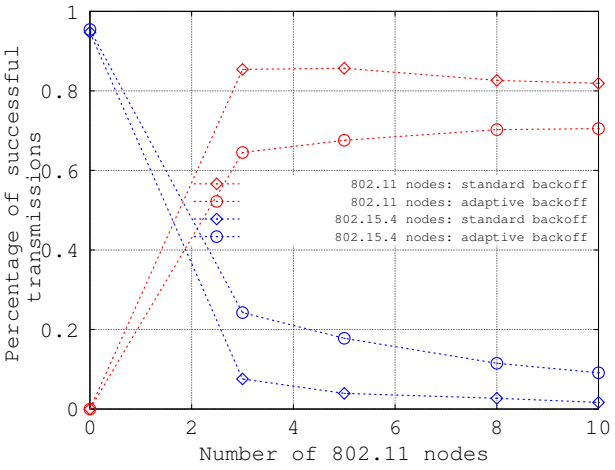

Fig. 2: Fraction of successful transmission with respect to the number of 802.11 nodes.

The simulation results of the first scenario are presented in Fig. 2. We observe that as the number of WiFi nodes increases in the network, the gap between the percentage of successful transmissions from WiFi nodes and ZigBee nodes decreases. For instance, for the ZigBee/WiFi distribution 10/3, the gap decreses from 11 (in the case of standard 802.15.4 backoff procedure) to 2 (for the case of adaptive backoff), and for the

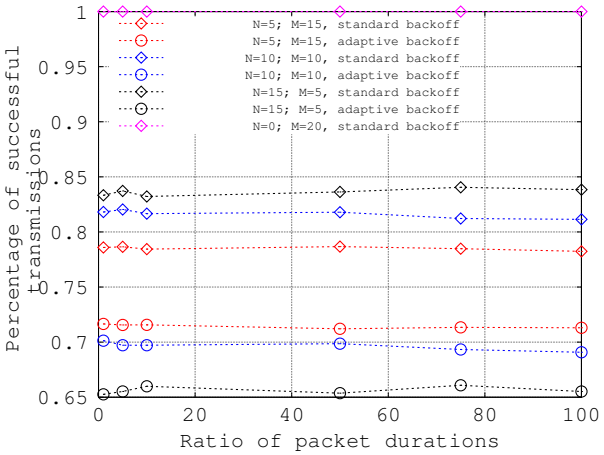

Fig. 3: Fraction of successful WiFi transmission with respect to the ratio of ZigBee/WiFi packet durations.

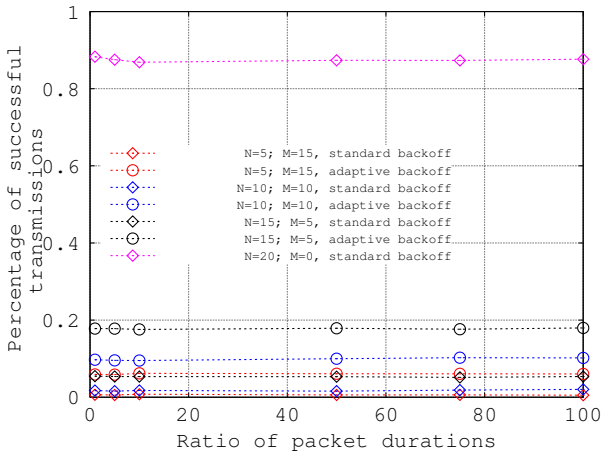

Fig. 4: Fraction of successful ZigBee transmission with respect to the ratio of ZigBee/WiFi packet durations.

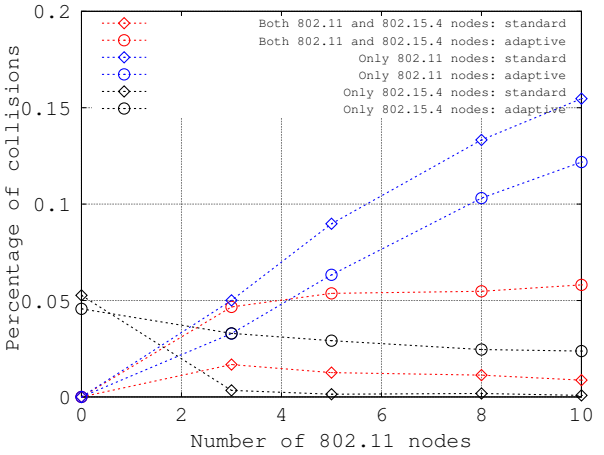

Fig. 5: Fraction of different collision types with respect to the number of WiFi nodes.

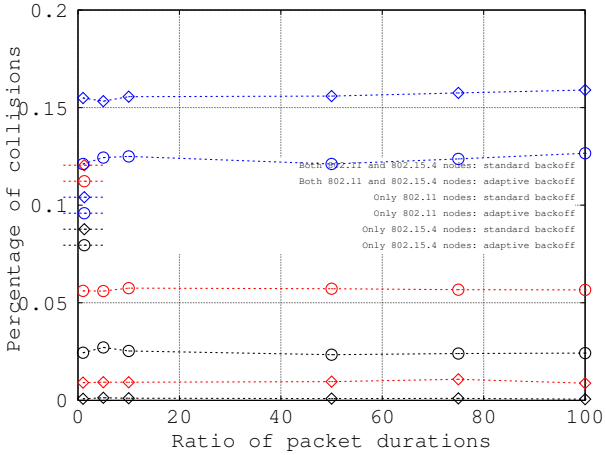

Fig. 6: Fraction of different collision types with respect to the ratio of ZigBee/WiFi packet durations.

ZigBee/WiFi distribution 10/5 and 10/10, the gap decreases from 21 to 3, and from 48 to 7, respectively.

In Fig. 3 and Fig. 4, we observe that for either the 802.15.4 standard backoff case or the 802.15.4 adaptive backoff case, the fraction of successful/unsuccessful transmission of ZigBee/WiFi nodes does not vary with respect to the ratio of ZigBee/WiFi packet durations. Also, for any given ZigBee/WiFi distribution, we observe that when considering the 802.15.4 adaptive backoff case, the fraction of successful ZigBee (resp. WiFi) transmissions increases (resp. decreases) for an average of 500% to 900% (resp. 10% to 15%). Because of the smaller backoff durations of WiFi nodes compared to ZigBee nodes, the probability that WiFi nodes access the channel is very high compared to the probability that ZigBee nodes access the channel. In addition, ZigBee nodes fail to access the channel most of the time due to WiFi transmissions. The improvement observed in ZigBee nodes performance when the adaptive backoff procedure is used is due to the fact that the backoff duration in the backoff duration is very small compared to backoff durations in the standard backoff procedure; as a consequence, the probability of accessing the channel of the ZigBee nodes drastically increases resulting in the increase of both the fraction of successful and failed ZigBee transmissions. We also observe that the unsuccessful transmissions of WiFi nodes depends on the type of backoff procedure used. For the standard (resp. adaptive) backoff procedure case, the unsuccessful transmissions of WiFi nodes are mainly due to collisions occurring between WiFi nodes' transmissions (resp. WiFi nodes and ZigBee nodes transmissions). Therefore, as the number of WiFi (resp. ZigBee) nodes increases, the percentage of successful WiFi transmission will decrease. On the contrary, the performance of ZigBee nodes mainly depends on the

number of ZigBee nodes present in the network. That is, both for the standard backoff procedure case and for the adaptive backoff procedure case, when the number of ZigBee nodes increases, the percentage of successful ZigBee transmissions increases.

In Fig. 5 and Fig. 6, the fractions of collisions between WiFi transmissions only, WiFi/ZigBee, and ZigBee only are presented with respect to the number of WiFi nodes (Fig. 5), and with respect to the ratio of packet durations (Fig. 6). We observe that the percentage of collisions for each type does not vary with respect to the ratio of packet durations. However, we notice that for both simulations shown in Fig. 5 and Fig. 6, when the adaptive backoff procedure is used, the probability that a ZigBee node initiates a transmission increases, resulting in the increase of both the fraction of successful transmissions and the percentage of collisions.

C. Impact of erroneous packet type detections in the CCA

The decision to use either the standard 802.1.5.4 backoff scheme or the adaptive 802.15.4 scheme depends on the decision made concerning the type of packet detected during the CCA. We have assumed so far that there is no decision error regarding the type of packet detected. In this scenario, we assume that there exists a non zero probability (0.1 and 0.3) that the decision regarding the type of packet detected is wrong. The ZigBee/WiFi nodes distribution is similar to the one described in the first scenario, that is, the number of ZigBee nodes is set constant to 10 and the number of WiFi nodes varies from 0 to 10.

We further consider the cases where the ratio of ZigBee/wiFi packet durations is 10 and 50 in order to analyze the impact of the packet durations in the context of erroneous decisions. The results of the simulations are depicted in Fig. 7 and Fig. 8. We observe that the ratio of packet durations may have an impact on the performance of both the ZigBee nodes and WiFi nodes when there is a probability of error in the decision regarding the type of packet detected during the CCA. One notices that as the duration of ZigBee nodes packets approaches the duration of WiFi nodes packets, the percentage of successful ZigBee transmissions increases while the one of WiFi transmissions decreases. However, we observe that as the probability p of making a wrong decision regarding the type of packet detected during the CCA increases, the performance improvement of ZigBee nodes is still considerable, but may approach the value of the standard backoff procedure case if the wiFi nodes packet duration is negligible compared to ZigBee nodes packet duration.

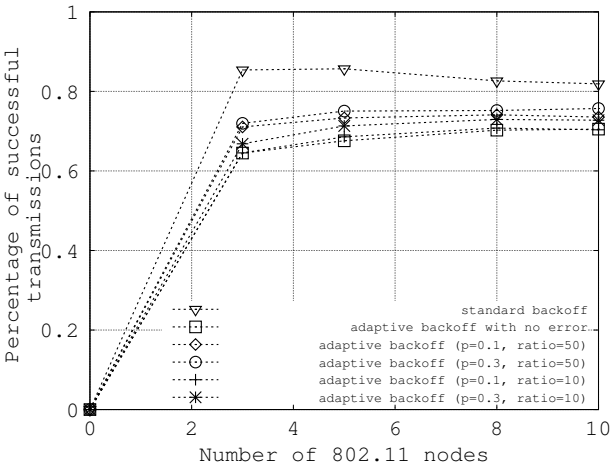

Fig. 7: Fraction of successful WiFi transmission with respect to the number of WiFi nodes when considering decision error during the CCA.

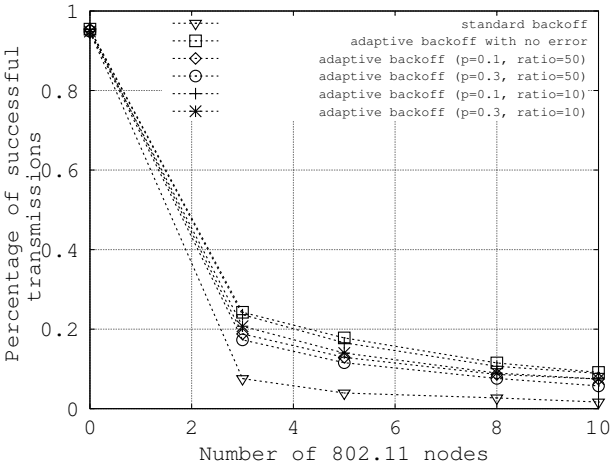

Fig. 8: Fraction of successful ZigBee transmission with respect to the number of WiFi nodes when considering decision error during the CCA.

V. Conclusion

In this paper, we addressed the problem of the unfair asymmetric coexistence between WiFi and ZigBee in the 2.4 GHz band. We proposed a simple but efficient 802.15.4 backoff mechanism in which the backoff duration is adaptively chosen when WiFi transmissions are detected during the CCA. We performed extensive simulations to assess the impact of the adaptive procedure in saturation conditions where the coexistence of both technologies is particularly problematic. The results of simulations demonstrate the efficiency of the proposed adaptive backoff mechanism and the considerable improvements of the 802.15.4 performance even in case of erroneous decisions regarding the type of packet detected during the CCA.

References

[1] A. Iyer, C. Rosenberg, and A. Karnik, “What is the right model for Wireless Channel Interference?” IEEE Transactions on Wireless Communications, Vol. 8, No. 5, pp. 2662–2671, 2009.

[2] ”Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, IEEE Std 802.11-2007.

[3] Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPAN), 2006, IEEE 802.15.4 Std.

[4] 802.11n-2009 - IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput

[5] 802.11ac-2013 - IEEE Standard for Information technology– Telecommunications and information exchange between systems—Local and metropolitan area networks– Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications–Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.

[6] Gil Reite, "Wireless connectivity for the Internet of Things", Texas Instruments, http://www.ti.com/lit/wp/swry010/swry010.pdf, June 2014.

[7] Yang, Dong, Youzhi Xu, and Mikael Gidlund. "Wireless coexistence between IEEE 802.11-and IEEE 802.15. 4-based networks: A survey." International Journal of Distributed Sensor Networks, 2011.

[8] Yan, Yubo, Panlong Yang, X. Li, Zhang Yafei, Lu Jianjiang, Lizhao You, Jiliang Wang, Jinsong Han, and Yan Xiong. "Wizbee: Wise zigbee coexistence via interference cancelation in single antenna." DOI 10.1109/TMC.2014.2359673, IEEE Transactions on Mobile Computing, 2014.

[9] Zhang, Xinyu, and Kang G. Shin. "Cooperative carrier signaling: Harmonizing coexisting WPAN and WLAN devices." Networking, IEEE/ACM Transactions on 21, no. 2, pp. 426-439, 2013.

[10] Wang, Yufei, Qixin Wang, Guanbo Zheng, Zheng Zeng, Rong Zheng, and Qian Zhang. "WiCop: Engineering WiFi Temporal White-Spaces for Safe Operations of Wireless Personal Area Networks in Medical Applications." IEEE Transactions on Mobile Computing, Vol. 13, No. 5, pp. 1145-1158, May 2014.

[11] Shin, Soo Young, Iyappan Ramachandran, Sumit Roy, and Wook Hyun Kwon. "Cascaded clear channel assessment: Enhanced carrier sensing for cognitive radios." In Communications, 2007. ICC'07. IEEE International Conference on, pp. 6532-6537. IEEE, 2007.