International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Review on Techniques for Establishing Coexistence between WiFi and Zigbee

Garima Khanna[1], Gaurav Gupta[2]

[1]PG Student ECE Department, MIT, Ujjain, India

[2]Associate Professor, ECE Department, MIT Ujjain, India

Abstract: ***The ISM spectrum is becoming increasingly populated by emerging wireless networks. Spectrum sharing among the same network of devices can be arbitrated by MAC protocols (e.g., CSMA), but the coexistence between heterogeneous networks remains a challenge. The disparate power levels, asynchronous time slots, and incompatible PHY layers of heterogeneous networks severely degrade the effectiveness of traditional MAC. CBT allows a separate ZigBee node to schedule a busy tone concurrently with the desired transmission, thereby improving the visibility of ZigBee devices to WiFi. Its core components include a frequency flip scheme that prevents the mutual interference between cooperative ZigBee nodes, and a busy tone scheduler that minimizes the interference to WiFi, for both CSMA and TDMA packets. To optimize CBT, we establish an analytical framework that relates its key design parameters to performance and cost. Both the analytical and detailed simulation results demonstrate CBT's significant throughput improvement over the legacy ZigBee protocol, with negligible performance loss to WiFi. The results are validated further by implementing CBT on sensor motes and software radios.***

Keywords: 802.11 Interference Mitigation, 802.15.4, Wireless Measurement Study, Error Correction , coexistence

1. Introduction

Spectrum scarcity is known to be a main obstacle to the scaling of wireless network capacity. Spectrum sharing has been advocated as a key remedy for this problem, especially after the successful deployment of WLAN and WPAN devices on an unlicensed band. However, severe performance degradation has been observed when heterogeneous devices share the same frequency band (e.g., WiFi & Bluetooth [13], WiFi & ZigBee [18], WiFi & WiMax [22]). Such a coexistence problem is rooted at their mutual interference due to the lack of coordination. Although most systems incorporate interference avoidance mechanisms, such as listen before- alk, they are designed to resolve the collision between the same type of networks. These built-in mechanisms become less effective for heterogeneous MAC/PHY protocols/standards, which adopt asynchronous time slots, different scheduling modes (e.g., TDMA vs. CSMA), disparate transmission/interference ranges, and incompatible communication mechanisms. The problem is likely to persist and exacerbate in future, especially within the recently opened-up TV white- space [10] for unlicensed users. We address a key question related to this trend: how should heterogeneous wireless MAC/PHY protocols coexist to share spectrum? We will focus on two such protocols, WiFi (IEEE 802.11) and ZigBee (IEEE 802.15.4), that share the 2.4GHz ISM band. WiFi is typically deployed for pervasive Internet access or medium-scale WLANs, whereas ZigBee targets monitoring and control applications for home, hospital, or enterprise environments [14]. The conflicting coexistence between them has been observed in existing measurement studies [12, 18], and their underlying cause is representative of many other coexisting networks. In particular, ZigBee packets are transmitted with 20dB lower power than WiFi packets, and tend to be invisible to, and often interrupted by, WiFi transmitters. Even when it can be sensed by WiFi, a ZigBee transceiver has a 16× longer response time, and is often preempted by WiFi, when it switches from sensing to transmission, or transmission to reception mode. Besides, ZigBee allows for TDMA mode, which operates without carrier sensing, and may arbitrarily collide with an ongoing WiFi transmission. Therefore, by resolving the coexistence between ZigBee and WiFi, one could naturally extend the solution to other heterogeneous networks facing similar problems.

2. Multiheader Approach to Solving Coexistence

Wireless sensor networks will play an important role in Cyber-Physical system, whose applications typically fall under sensor-based systems and autonomous systems. For example, many wireless sensor networks monitor some aspects of the environment and relay the processed information to a central node. Many different wireless communication technologies, such as ZigBee and WiFi, have been witnessed recently to be deployed in more and more applications. Thus, the cross technology interference has draw attention of the researchers. Now, the WSN community has acknowledged the impact of WiFi interference on WSN applications in various settings. Roughly, the current research can be classified as the following three categories based on the research points: The works in the first category are focus on the mechanism or principle of interference. An empirical results was found in [4] in a hospital setting. The results show that running CTP on a 15.4 network that overlapped with an active 802.11 channel decreased the end to end goodput by a factor of three. The impact of 802.11 interference on ZigBee networks was studied in [5] and the authors found that the position distribution of bit errors in 15.4 packets is temporally correlated with 802.11 traffic. The authors in [6] found that 15.4 packet loss as high as 87%, with an 802.11b sender located in between two 15.4 nodes five meters apart. Currently, under the existence of WiFi sources, the existing

works predict 15.4 link performance based on SINR. A passive interference measurement method based on the PPR-SINR model is proposed in [6]. However, performance prediction model solely based on SINR is inaccurate. The second kind of works focuses on how to avoid the WiFi interference for ZigBee networks. The common approach for 802.15.4 networks to mitigate 802.11 interference is to switch the network to channels that do not overlap with an active 802.11 channel. According to IEEE 802.15.4 specification, the coordinator can scan the energy level in each channel so that the quietest channel could be chosen. However, all the nodes will work with the same channel and thus can not avoid the interference from WiFi hotspots which varies in different space over different time. In [7], Adaptive Frequency Hopping (AFH) is proposed for Bluetooth and WiFi coexistence. In [8], the authors proposed a distributed channel selection mechanism that detects 802.11 interference using periodic RSSI samples. However, these works did not consider the locality of interference and thus can not provide a good link performance. Moreover, static channel assignment may not work as planned due to node mobility and incremental WiFi deployments.There are also some works focusing on the dynamic channel assignment schemes. Different nodes in a sensor network, or the same node over different points in time, will use different 15.4 channels to avoid interference from nearby WiFi sources. However, accurately assessing the interference is a key problem. The current methods do not present efficient method. Our paper aims to fill this gap and proposes a novel method.Recently, more and more researchers found that improving the coexistence of 15.4 and 802.11 networks is beneficial to the spectrum efficiency. Through the statistical analysis of data traces, WiFi frames are highly clustered and the arrival process of clusters has the feature of selfsimilarity. Based on this find, the authors in [9] proposed a method to predict the length of white space in WiFi traffic. The ZigBee intelligently adapts frame size to maximize the throughput efficiency while achieving assured packet delivery ratio. Literature [10] designed a BuzzBuzz protocol to mitigate WiFi interference through header and payload redundancy. These methods are complementary to our method.

3. Buzz Buzz Protocol Method for Solving Coexistence Problem

Most of the previous work that has examined the interaction between 802.11 and 802.15.4 networks has focused on high-level metrics such as packet reception rate (PRR) [4, 23]. In contrast, we examine the interaction between the two radio technologies by accurately detecting and measuring various packet transmission events. Giventhe packet and interval durations shown in Table 1, this task requires instruments that detect and measure RF events that are as short as a few µs. The RFMD ML2724 narrow band radio gives us the ability to detect RF transmissions with the desired timing accuracy and precision [22]. The ML2724 can be tuned to acentral frequency between 2400 and 2485 MHz and generates an analog voltage on its RSSI OUT pin that is directly proportional to the RF signal energy received in a 2 MHz frequency band centered at the tuned frequency. Given the relative widths of the channels used by 802.11, 15.4, and the ML2724 radio, it is possible to detect 802.11 packets thatcollide with 15.4 transmissions without being affected by the later transmissions. In practice, we use 15.4 channel 22, 802.11 channel 11 , and set the ML2724's center frequencyto 2465.792 MHz (equivalent of 15.4 channel 23).We selected the ML2724 for two key reasons. First, RSSI measurements are directly available as analog voltage outputs, which makes it possible to detect RSSI changes quickly by sampling this signal at a high frequency. In contrast, the CC2420 radio exposes the measured RSSI value as the contents of an internal register; due to the delays associated with accessing CC2420 registers over the SPI bus, it is impossible to detect most of the 802.11 RF events by reading this RSSI register. The second reason for using the ML2724 is its fast RSSI response. According to the datasheet, the maximum rise and fall times of the RSSI OUT are 4.5 µs and 3 µs respectively, hich make ML2724 an excellent candidate for detecting the RF activity we are interested in. While we use the ML2724 radio to detect 802.11 packets, we detect events related to the transmission of 15.4 packets using the GPIO pins of TelosB motes equipped with CC2420 radios [20]. Specifically, we leverage the observation that the TinyOS event, CaptureSFD.captured is invoked at the beginning and the end of 15.4 packet transmissions respectively. This event is the interrupt service handler that is triggered when the CC2420 radio toggles its pin at specific points during a radio packet transmission. Under light load, when interrupts are disabled only for short durations, we can accurately detect these CC2420 events by toggling processor GPIO pins from within these TinyOS events. There is however a fixed offset between the actual RF transmissions and the toggling of pins on the CC2420 radio. We measured these offsets by observing the RSSI OUT of a properly tuned ML2724 and the GPIO pin activities of a TelosB mote using an oscilloscope; during these measurements, we also verified that these offsets are constant. To accurately correlate 802.11 and 802.15.4 transmissions over time we connected the RSSI OUT pin of the ML2724 radio and the mote's GPIO pins to the same Data Acquisition (DAQ) card that samples and logs analog inputs at 1 MHz frequency [17].

4. 802.11 Overview

WiFi networks are almost ubiquitous in office buildings, homes, and even outdoors in urban areas. Considering that 802.11b, 802.11g, and 802.11n share the same 2.4 GHz ISM band with 802.15.4, 802.11 transmissions can interfere with co-located 802.15.4 networks. In the U.S., only 15.4 channels 25 and 26 do not overlap with WiFi and even these channels are covered in other parts of the world. In practice, since most WiFi networks use channels 1, 6, and 11, 15.4 channels 15 and 20 can also be interference-free [16]. The potential for 802.11 transmissions to overwhelm 15.4 receivers is amplified by the fact that 802.11 radios transmit at 10 to 100 times higher power than 15.4 radios. Figure 4, which presents the key features of the 802.11 MAC protocol through a timing diagram, helps us understand how WiFi nodes use the wireless edium. The 802.11 standard specifies using CSMA/CA with ACKs as the MACprotocol, optionally with the addition of RTS/CTS packets [10]. The protocol also specifies the SIFS and DIFS intervals when nodes should defer using the medium. A time period, called the contention window, follows the DIFS shown in Figure 4.

This window is divided into slots.Nodes use a uniform random distribution to select a slot and wait for that slot before attempting to access the medium. The node that selects the earliest slot wins while others defer. Nodes initialize their contention window (CW) to 31 slots and double it every time they fail to access the medium, until CW reaches a maximum size of 1023 slots. Table 1 summarizes the duration of the DIFS, SIFS, and backoff slots for 802.11b and 802.11g. Also shown are the maximum and minimum packet sizes for 802.11b, 802.11g, and 802.15.4. It is worth noting that for many 802.11b and 802.11g packets, the entire air time is smaller than a 802.15.4 slot time.

5. 802.15.4 Overview

The IEEE 802.15.4 standard defines a PHY layer for low-rate wireless networks operating in the 2.4 GHz ISM band [9]. The standard defines 16 channels within this band, each 2 MHz wide with 3 MHz inter-channel gap-bands (see Figure 2). According to the standard, outgoing bytes are divided into two 4-bit symbols and each symbol is mapped to one of 16 pseudo-random, 32-chip sequences. The radio encodes these chip sequences using orthogonal quadrature phase shift keying (O-QPSK) and transmits them at 2 Mchips/s (i.e., 250 kbps). Figure 3 shows the format of a 15.4 packet including the Synchronization Header (SHR) and the PHY Header (PHR), shown in grey. The SHR header includes a 4-byte preamble sequence (all bytes set to 0x00) and a 1-byte Start of Frame Delimiter (SFD) set to 0x7A. The PHR includes a 1- byte Length field that describes the number of bytes in the packet's payload, including the 2-byte CRC. The maximum packet size is 133 bytes, including all the headers. The MAC protocol in the 802.15.4 standard defines both beacon-enabled and non-beacon modes. In the beaconless mode, the standard specifies using a CSMA/CA protocol [9]. While the CSMA/CA protocol uses binary exponential backoff, in practice the CSMA/CA protocol implemented in Tiny OS uses a fixed-length backoff interval [29]. On the receiving side, a 15.4 radio synchronizes to incoming zero-symbols and searches for the SFD sequence to receive incoming packets. Interference and noise can corrupt the incoming chip stream, leading to 32-chip sequences that do not match one of the 16 valid sequences.

6. Conclusion

This paper presents a careful analysis of the IEEE 802.15.4 and 802.11 interference patterns at 2.4 GHz ISM band. We examine these interference patterns at a bit-level granularity, and we explain how a 15.4 node may change the behavior of nearby 802.11 transmitters under certain conditions. Also it has been observed that there exists ways to mitigate the coexistence problem in this area of communication engineering, such methods have been carefully studied and a general review has been given.

References

[1] Atmel Corporation. Low Power 2.4 GHz Transceiver for ZigBee, IEEE 802.15.4, 6LoWPAN, RF4CE and ISM applications. Available at http://www.atmel.com/dyn/resources/prod_ documents/doc5131.pdf, 2009.
[2] C. A. Boano, T. Voigt, N. Tsiftes, L. Mottola, K. Romer, and M. A. Zuniga. Making Sensornet MAC Protocols Robust Against Interference. In EWSN, 2010.
[3] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis. Collection Tree Protocol. In SenSys, 2009.
[4] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan. Understanding and Mitigating the Impact of RF Interference on 802.11 Networks. In SIGCOMM, 2007.
[5] B. Han, A. Schulman, F. Gringoli, N. Spril, B. Bhattacharjee, L. Nava, L. Ji, S. Lee, and R. Miller. Maranello: Practical Partial Packet Recovery for 802.11. In NSDI, 2010.
[6] J.-H. Hauer, V. Handziski, and A. Wolisz. Experimental Study of the Impact of WLAN Interference on IEEE 802.15.4 Body Area Networks. In EWSN, 2009.
[7] J. Hou, B. Chang, D.-K. Cho, and M. Gerla. Minimizing 802.11 Interference on Zigbee Medical Sensors. In BodyNets, 2009.
[8] I. Howitt and J. Gutierrez. IEEE 802.15.4 Low Rate - Wireless Personal Area Network Coexistence Issues. In WCNC, 2003.
[9] IEEE Computer Society. 802.15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for LowRate Wireless Personal Area Networks (LR-WPANs). Available at: http://standards.ieee.org/getieee802/download/ 802.15.4-2003.pdf.
[10] IEEE Computer Society. Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Available at: http://standards.ieee.org/getieee802/download/ 802.11-2007.pdf.
[11] IEEE Computer Society. Local and metropolitan area networks - Specific requirements Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs). Available at: http://standards.ieee.org/ getieee802/download/802.15.1-2005_part1.pdf.
[12] K. Jamieson and H. Balakrishnan. PPR: Partial Packet Recovery for Wireless Networks. In SIGCOMM, 2007.
[13] J. Jeong and C.-T. Ee. Forward Error Correction in Sensor Networks. In WWSN, 2007.
[14] S. Kim, R. Fonseca, and D. Culler. Reliable Transfer on Wireless Sensor Networks. In SECON, 2004.
[15] J. Ko, T. Gao, and A. Terzis. Empirical Study of a Medical Sensor Application in an Urban Emergency Department. In BodyNets, 2009.
[16] C.-J. M. Liang, J. Liu, L. Luo, A. Terzis, and F. Zhao. RACNet: A High-Fidelity Data Center Sensing Network. In SenSys, 2009.
[17] Measurement Computing Corp. USB-2523: USB-Based 16 SE/8 DI Multifunction Measurement and Control Board. Available from: http://www.mccdaq.com/usb-data-acquisition/ USB-2523.aspx, 2009.