Strategies and Demonstration to Support Multiple Wireless Protocols with a Single RF Front-End

Mohamed Mohamed, Suranga Handagala, Jieming Xu, Miriam Leeser, and Marvin Onabajo

Abstract

In an increasingly interconnected world, the demand for smartphones, tablets, and other wireless devices in the IoT has surged over the last few years. This high demand has increased mobile data usage and wireless communication, resulting in an explosion of traffic demand in the limited 2.4 GHz frequency band. This traffic demand and the limitations of existing wireless devices operating in the same frequency range have resulted in a spectrum congestion problem. To utilize the available spectrum more efficiently, it becomes important to detect the desired signals and support flexible communications. After reviewing relevant characteristics of the protocols of interest, this article introduces a new approach for spectrum sharing with a hardware implementation to support the coexistence of WiFi, LTE, and ZigBee in the congested 2.4 GHz band using a single RF front-end. A detection method was developed to resample the preambles of both WiFi and ZigBee to the LTE sampling rate to avoid continuous resampling of the received signal. Further processing steps such as synchronization and demodulation for each protocol are described. Measurement results are provided to demonstrate the techniques showing a low symbol error rate tested over the air in a laboratory environment with interference.

Introduction

The rapid growth of wireless devices and wireless traffic has significantly increased data usage, creating severe spectrum congestion. The increased types of devices, including IoT, have resulted in an increase in the number of protocols for wireless communications, some occupying the same bandwidth. Typically, different hardware radios are designed for each protocol in the spectrum, which can be quite expensive, especially with more protocols.

Spectrum congestion is more severely impacted by the inefficient use of the spectrum rather than spectrum scarcity. Researchers have introduced the idea of spectrum sharing or spectrum coexistence, in which more than one application can be used in the same bandwidth. The main challenge is to manage interference, such that the Primary User (PU) is not affected by the Secondary User's (SU) communication. Ongoing research in cognitive radio technology focuses on addressing the challenging issue of low power signal detection from within interference. Detection is a critical part of managing interference, while frequency coordination and access by different types of communication systems are also challenging.

This article outlines a new method for detecting and processing multiple wireless protocols, focusing on WiFi, LTE, and ZigBee using the same RF sample rate and spectrum bandwidth. An Analog Devices transceiver front-end on a Xilinx ZC706 evaluation board setup is used as a first demonstration of the method. This setup represents a flexible software-defined radio (SDR) that can be used for multiple protocols, but currently researchers tend to use it for one protocol at a time. Our approach achieves spectrum reuse with multiple protocols that share the same bandwidth, namely 2.4 GHz. First, the WiFi and ZigBee matched filter coefficients are resampled since the RF front-end is set to one of the LTE sampling rates (30.72 MHz). The protocols are transmitted over the air using a random sequence, and the received signal is analyzed for detection of the protocols using matched filtering (preamble detection for both WiFi and ZigBee, and primary synchronization signal (PSS) detection for LTE). Further synchronization and demodulation steps are taken for each of the protocols depending on whether the detection flag is set. Figure 1 illustrates our approach.

Background

Coexistence studies among different protocols have been ongoing for a number of years, such as the ones summarized in Table 1. In [1], a coexistence between WLAN and WPAN is presented in the ISM band using traffic scheduling, but performed at the expense of an additional delay in data transfer. Studies in [2] and [3] present coexistence methods using traffic scheduling between ZigBee and other protocols in both the ISM and unlicensed frequency bands, but both require prior knowledge of the transmitted protocol. Another more recent example for WiFi and LTE coexistence in the unlicensed band is presented in [4] using a newly-designed fairness criterion. Note that none of these studies perform tests with heterogeneous systems and none of them present WiFi, LTE, and ZigBee coexistence in the same bandwidth like

Digital Object Identifier:
10.1109/MWC.001.1900224

Mohamed Mohamed is with Massachusetts Institute of Technology;
Suranga Handagala, Jieming Xu, Miriam Leeser, and Marvin Onabajo are with Northeastern University, Boston.

1536-1284/20/$25.00 © 2020 IEEE

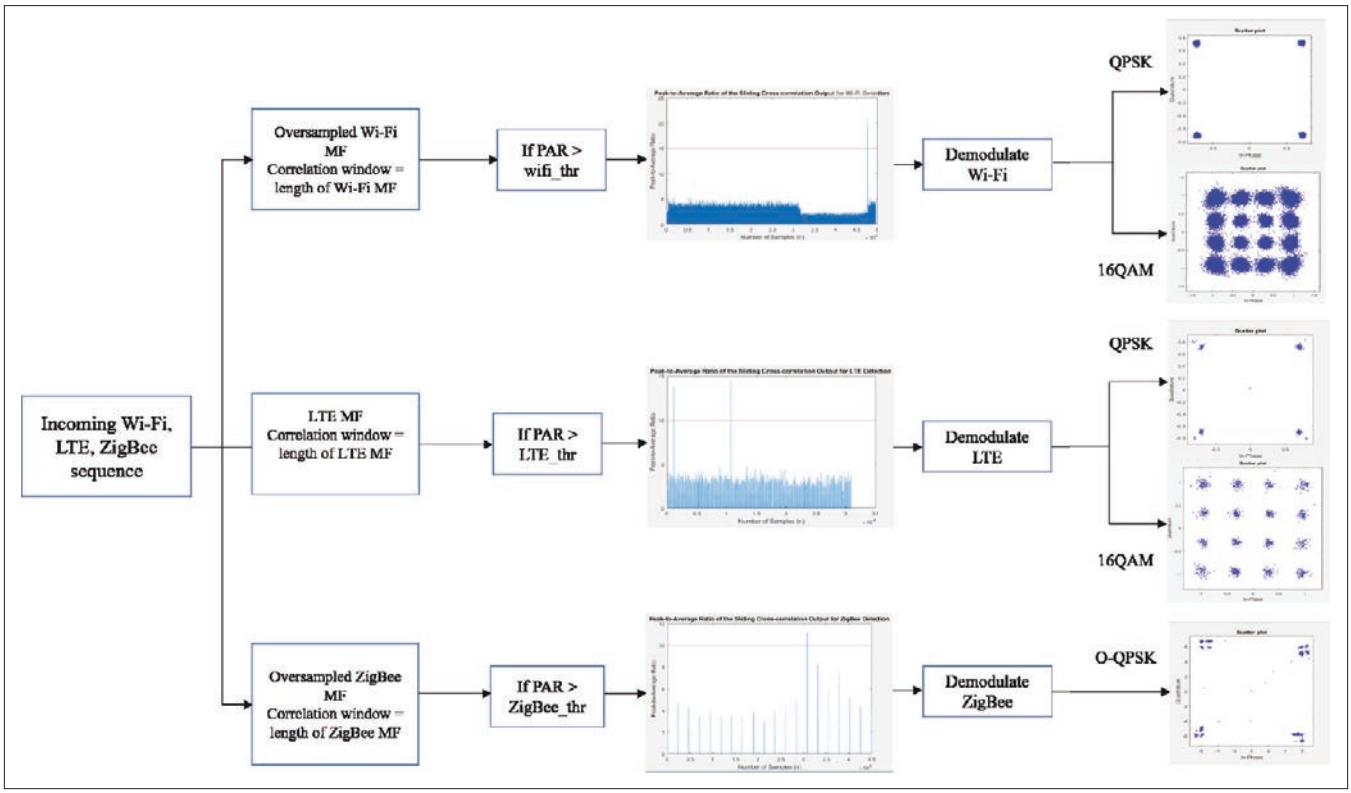

FIGURE 1. WiFi, LTE, and ZigBee coexistence flowchart showing detection and demodulation of each protocol. Top (WiFi), middle (LTE), and bottom (ZigBee).

the studies presented in this article combined with over the air experiments using online radio equipment. Similar coexistence research presented in [5] demonstrates the use of the same setup for WiFi, ZigBee and Bluetooth Low Energy (BLE) coexistence using a single transceiver board, minimizing different board mismatches and delay when using independent transmitter and receiver boards such as the setup presented in this article, but does not present a coexistence method including LTE. To the best of our knowledge, the work described in this article is the first to support WiFi, LTE, and ZigBee with the same RF front-end.

In addition to providing support for multiple protocols with the same RF front-end, the research presented in this article enables the capability to detect a received protocol among WiFi, LTE, and ZigBee without prior knowledge of the transmitted signal. It demonstrates successful processing of each protocol with low error rate and high demodulation accuracy. One advantage of using the proposed approach is that it eliminates the requirement of a sampling rate converter, which would have been necessary if these protocols were to be detected at sampling rates specified in their standards. Another benefit is that the same ADC bandwidth can be used, and that the technique circumvents the use of multiple antennas and analog RF front-ends tuned to different center frequencies to receive the different protocols.

Property	ISM band	Wi-Fi	LTE	ZigBee	Implemented using common RF front-end	Implementation method
[1]	Y	Y	N	N	N	Simulation
[2]	Y	Y	N	Y	N	Over the air
[3]	Y	Y	N	Y	N	Theory
[4]	N	Y	Y	N	N	Simulation
[5]	Y	Y	N	Y	Y	Over the air
[6]	N	Y	Y	N	N	Simulation
This work	Y	Y	Y	Y	Y	Over the air

TABLE 1. Comparison of spectrum sharing works.

Coexistence Protocols Structures

802.11n (WiFi)

802.11 is the IEEE standard that defines WiFi. It specifies the media access control (MAC) and physical (PHY) layer for implementing wireless local area networking for wireless communication at radio frequencies ranging from 900 MHz up to 60 GHz.

The WiFi 802.11n protocol structure (Fig. 2a) starts with an 8 μs short training field (STF) consisting of 10 short training symbols (16 samples each), followed by an 8 μs long training field (LTF) consisting of a guard interval (32 samples) and two long training symbols (64 samples each) to form the packet preamble. The LTF is followed by an 4 μs legacy signal (L-SIG) field, which is used to transfer rate and length information. In addition, 802.11n has an 8 μs high throughput (HT) signal (HT-SIG) field that is similar to the L-SIG field. The HT-SIG field is followed by a 4 μs HT-STF and a 4 μs HT-LTF. The longer preamble used in 802.11n is compatible with both HT-mixed (802.11n) and non-HT (802.11a) receivers, making it a more flexible protocol than other 802.11 protocols. 802.11n operates in both 2.4 GHz and 5 GHz frequency

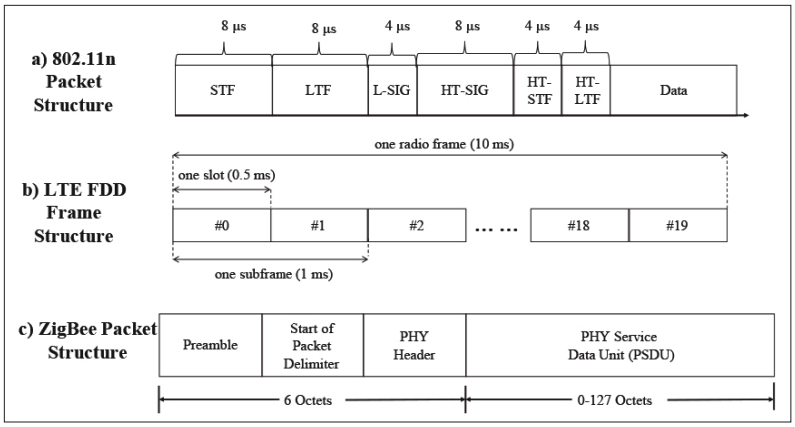

FIGURE 2. Protocol packet structures: a) WiFi; b) LTE; c) ZigBee.

bands. We refer to 802.11n as WiFi when it is used for the coexistence experiment at 2.4 GHz.

LTE

Long Term Evolution (LTE) transmissions are in blocks known as packets. LTE uses orthogonal frequency-division multiple access (OFDMA) on the downlink (DL), where the spectrum is divided into resource blocks (RBs). OFDMA allows multiple users on the available bandwidth. Each user is assigned a specific time-frequency resource or a resource block in the LTE specification. LTE has two frame structure types: frequency-division duplexing (FDD) and time-division duplexing (TDD) [7]. In FDD mode (used in this work), the 10 ms LTE radio frame is divided into 20 equally sized slots of 0.5 ms each as shown in Fig. 2b. Each slot has seven OFDM symbols for the normal cyclic prefix and six OFDM symbols for the extended cyclic prefix.

ZigBee

ZigBee is an IEEE 802.15.4-based specification that operates at multiple frequencies. Here, we use the 2.4 GHz ISM band, which consists of 16 channels [8]. This band supports a data rate of 250 kb/s, and is modulated by Offset Quadrature Phase Shift Keying (OQPSK).

Similar to 802.11 protocols, the first part of a ZigBee packet is the preamble used by the receiver for synchronization (Fig. 2c). The length of the preamble for the OQPSK PHY is eight symbols (four octets). Following the preamble is the Start of Packet Delimiter (SPD) and the PHY header, which specifies the length of the PHY Service Data Unit (PSDU) [9]. The last section of the packet is the PSDU, which can range from 0 to 127 octets in length. This section contains the main data to be transmitted. The complete frame forms the physical protocol data unit (PPDU).

Packet Detection and Coexistence Approach

In this experiment, cross-correlation is used for packet detection, which is useful when the signal is corrupted by noise, such that the signal detection from a noisy signal has to be performed. For time-domain signals, cross-correlation is computed between the received time-domain signal and a known periodic sequence, resulting in a peak to indicate the position of the periodic sequence (preamble for WiFi and Zigbee, and PSS for LTE). We employ a flexible method that handles different signal lengths to detect different protocols without prior knowledge of which packet is transmitted.

WiFi Detection

The 802.11n specification dictates that the LTF should be derived from a combination of 52 non-zero subcarriers. The 802.11n LTF consists of two long training symbols of 3.2 µs each that are concatenated and preceded by a guard interval of 1.6 µs. The LTF consists of a particular combination of 1 and −1 values for the orientation of the 52 tones. The combination of 1 and −1 gives the LTF a low peak to average ratio, minimizing nonlinear distortion in the analog transmitter chain. To detect a received WiFi waveform, the received waveform is cross-correlated with the LTF. The correlation result yields three peaks indicating the positions of a guard interval and two training symbols in the received waveform, which are utilized in this detection method.

LTE Detection

Similar to preamble detection in WiFi, LTE detection is also done in the time domain using a repeated periodic sequence. LTE uses a synchronization channel (SCH) inserted periodically in the LTE DL radio frame. The SCH is composed of a primary synchronization signal (PSS) and a secondary synchronization signal (SSS). The PSS is received in 1.4 MHz bandwidth based on a 1.92 MHz OFDM sampling rate, meaning that any incoming LTE waveform must be downsampled to 1.92 MHz in order to detect the PSS. The PSS provides subframe timing information and sector index by identifying which primary sequence has been transmitted out of the three possible alternatives. In FDD operating mode, the PSS is present in two locations in each 10 ms LTE DL radio frame. The first one is located in the last OFDM symbol of the first time slot of the first subframe, where each subframe is 1 ms long and each slot is 0.5 ms long. The PSS is repeated in the last OFDM symbol in subframe 5 [10]. The PSS is generated from a 63-length frequency-domain Zadoff-Chu (ZC) sequence whose root index determines the sector identity. Detection of the PSS in the time domain (TD) is implemented by cross-correlating the TD signal with the three possibilities of PSS coefficients in which one of the three correlation outputs will display two peaks depending on the cell ID, indicating both PSS positions within the LTE frame [11].

ZigBee Detection

ZigBee packet detection is done using preamble detection, where the preamble sequence present in the received packet is correlated with a fixed reference sequence to identify whether or not a valid packet has been received. The received packet is cross-correlated by taking a 32 bit window (preamble length) with the fixed preamble sequence. In every correlation, a peak to average ratio is calculated and compared with a predefined threshold. The number of samples per chip used commonly with ZigBee frames is 12, and frames are captured at 12 x chip rate, equating to 12 MHz. The number of samples per chip is digitally reduced in the receiver in order to increase processing speed.

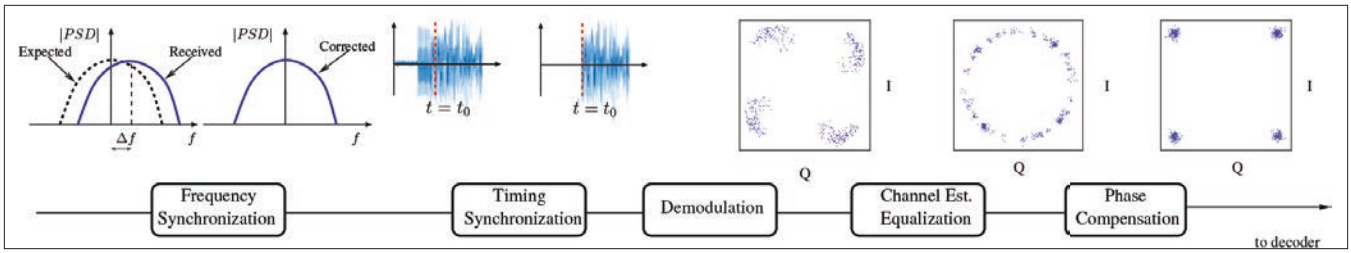

FIGURE 3. Major signal processing stages in a receiver chain: frequency/timing synchronization, demodulation, channel estimation and phase compensation [12–14]. For WiFi and LTE, demodulation was performed using FFTs of size 64 and 2048, respectively. For ZigBee, a 2048 FFT size was used for demodulation, and a zero-crossing timing error detector was used for timing synchronization. The frequency domain Least Square (LS) and minimum mean squared error (MMSE) channel equalizations were used for WiFi and LTE, respectively.

Coexistence Design

After exploring packet detection for each of the protocols described here (WiFi, LTE, and ZigBee), it is important to highlight that these methods are successful only if the RF front-end settings are compatible with each protocol. One common RF front-end is used with the same RF carrier frequency (2.4 GHz) and bandwidth (20 MHz). However, the sampling rate is that of LTE (30.72 MHz), which is faster than the 20 MHz WiFi and ZigBee baseband sampling rates. Suppose we want to resample the LTE signal at a WiFi signal rate. The rate conversion ratio from LTE to WiFi is 125/192. If we were to perform rate conversion on the received signal with this ratio, the hardware complexity would be excessively high. If we were to directly implement this rate converter for a signal with clock rate of 20 MHz, then the maximum clock rate of this converter could reach around 3 GHz, which is too high for baseband processing. In order to avoid continuous sample conversion of the received signal, the original WiFi and ZigBee matched filters are oversampled to 30.72 MHz. Oversampling the matched filter is more efficient than resampling the received oversampled WiFi or ZigBee signal because the filter coefficients are fixed, and therefore repetitive resampling is no longer required when following the technique from [10]. The resample ratio for WiFi is:

$$\frac{30.72\ \text{MHz}}{20\ \text{MHz}} = \frac{192}{125}$$

This ratio shows that the 20 MHz preamble is upsampled by 192 and downsampled by 125 to achieve the new oversampled 30.72 MHz WiFi preamble. Similarly for ZigBee, the resample ratio is:

$$\frac{30.72\ \text{MHz}}{12\ \text{MHz}} = \frac{64}{25}$$

The ZigBee preamble is upsampled by 64 and downsampled by 25 to achieve the oversampled 30.72 MHz ZigBee preamble.

In this experiment, an incoming WiFi, LTE, and ZigBee sequence (formed using a random combination of the three protocols) is received using the AD9361 FMComms3 SDR at 30.72 MHz. This sequence is then processed in parallel for each of the protocols using different correlation windows. For WiFi, cross-correlation is computed with a correlation window equal to the length of the oversampled WiFi matched filter (MF) and a peak-to-average value is computed and compared to a predefined threshold. If that threshold is passed, the packet proceeds for the WiFi processing chain to produce the demodulated QPSK symbols. The process developed in this research is shown in Fig. 1. Similarly, these steps are completed in parallel for LTE and ZigBee to produce the demodulated symbols. 16QAM demodulated symbols are processed as well for WiFi and LTE. Higher modulation schemes are not displayed for ZigBee because it is always O-QPSK modulated.

Synchronization and Demodulation

Once a packet is detected and a peak-to-average ratio of the matched filter output exceeds a predefined threshold, synchronization and demodulation of the received packet extract the symbols (Fig. 1). The receiver functions (Fig. 3) are used to obtain the constellation that serves as the input to the decoder. Frequency synchronization compensates for carrier frequency offsets that occur either due to mismatch between TX and RX local oscillator frequencies or Doppler shift, which could affect the orthogonality between subcarriers. Channel estimation and equalization reverse channel effects acting on the signal that otherwise would degrade the accuracy of the constellation points. Residual phase offsets are corrected through phase compensation.

WiFi Synchronization and Demodulation: WiFi synchronization steps include coarse and fine frequency offset compensation, timing detection and correction, channel estimation and phase noise correction [12].

If frequency offsets are not corrected, each FFT output symbol represents not only the orientation and magnitude of a single subcarrier, but also contains trace information from all other carriers.

Timing error is a type of linear distortion that occurs because the receiver does not know the perfect sampling instant, creating a timing offset in the Analog-to-Digital Converter (ADC). Fortunately, the correlation result described earlier can be used to obtain the timing reference, where we cross correlate the sample stream with a local copy of the LTF.

Channel estimation determines the impact of the multipath channel on the frequency response of the received signal. Since the long training symbols' subcarrier orientation is known, it can be compared to the received subcarriers (FFT outputs) of the long training symbols.

LTE Synchronization and Demodulation: LTE specification defines different (but similar) synchronization and demodulation steps compared to WiFi: timing correction, frequency offset compen-

Transmitting a signal at a high modulation rate in a narrow band increases the likelihood of Inter-Symbol Interference (ISI). Pulse shaping changes the transmitted pulses by limiting the effective bandwidth using a pulse filter. This process is essential for making signals fit within a frequency band.

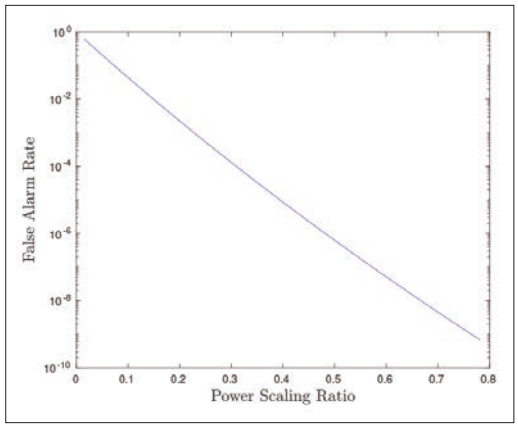

FIGURE 4. False alarm rate estimation example.

sation, channel estimation, and phase drift correction [13].

Any frequency offset must be removed prior to OFDM demodulation, and is estimated by means of correlation of the cyclic prefix.

The LTE specifications define a channel estimation method using pilot symbols within reference signals such as Cell Reference Signal (CellRS). Pilot symbols in CellRS in OFDM symbol 0 and 4 of each time slot are used instead of the PSS and SSS. An MMSE method is used for equalization as shown Fig. 3.

ZigBee Synchronization and Demodulation: Similar to WiFi and LTE, ZigBee also requires synchronization before demodulation, and these steps include coarse/fine frequency offset compensation and timing synchronization [14].

Transmitting a signal at a high modulation rate in a narrow band increases the likelihood of Inter-Symbol Interference (ISI). Pulse shaping changes the transmitted pulses by limiting the effective bandwidth using a pulse filter. This process is essential for making signals fit within a frequency band. In ZigBee, the 2.4 GHz OQPSK PHY uses half-sine pulses, therefore a half-sine receive filter is required. This filter also improves the signal-to-noise ratio (SNR).

For ZigBee, a coarse frequency offset compensator employs an FFT-based method that squares the received OQPSK signal to reveal two spectral peaks. The coarse frequency offset is obtained by averaging and halving the frequencies of these two spectral peaks. To obtain a more accurate estimate of the frequency offset, a fine frequency offset compensator is used, which uses a closed-loop phase-locked loop (PLL) approach to reduce frequency offset and phase rotation.

Synchronized symbols are demodulated using OQPSK to convert [−1 1] to [0 1]. The result of preamble detection is used to obtain Start of Packet Delimiter (SPD) and PHY header positions. Each 32-chip pseudo-noise (PN) sequence is then mapped to a data symbol by finding the chip sequence that is the most similar to the one received. For symbol to bit mapping, each data symbol is mapped sequentially to 4 bits (despreading) to form the MAC protocol data unit (MPDU).

Threshold Selection

A signal that is detected that is not received is a false alarm; a signal that is present but not detected is a missed detection. If more than one signal is detected simultaneously, we report this as a collision to the MAC layer for decision-making.

False alarm rate and missed detection rate depend on the threshold value. We assume that any noise (including interference from undesired signals) is a Gaussian random process. Since the power of the received signals depends on the scenario, a fixed threshold is not a good choice to decide the presence of a synchronization signal. The threshold should be adaptive; the approach we adopt is based on the power of the matched filter's output compared to the signal that is being received. We scale the output power of the matched filter, and compare it to the average power of the received signal using a power scaling ratio c. The appropriate power scaling ratio c varies depending on the signal sample lengths and the power of the synchronization signals for different protocols. Figure 4 visualizes the relationship between the power scaling ratio and the false alarm rate.

The higher the threshold (i.e., power scaling ratio), the lower will be the false alarm rate. On the other hand, a higher threshold will result in a higher missed detection rate. For different protocols and users, the requirements are different to balance the false alarm and missed detection rates. For this reason, the adjustable power scaling ratio value can be selected by the user, such that it can be changed to meet different requirements. We used power scaling ratios of 0.04 for LTE, 0.16 for WiFi, and 0.03 for ZigBee, which balanced the missed detection rates and false alarm rates well during the experiments. Situations such as multiple positive decisions are detected as collisions, and can be reported to the MAC layer when the method is employed in a complete system.

Experimental Setup and Results

We utilized the MATLAB WLAN, LTE, and Communications toolboxes to generate WiFi, LTE, and ZigBee transmit signals. This was done by executing toolbox functions on binary data to be transmitted. These functions perform data scrambling, encoding, interleaving, bit-to-symbol mapping and modulation to create the transmit side complex baseband signals that are up-converted to the RF frequency by the AD9361 prior to transmission. As an example, we created a sequence consisting of the generated signals in a random order to produce a sequence of WiFi, LTE, and ZigBee signals separated by zeros between them. For the results presented here, the signal starts with 5000 zeros followed by an LTE packet, 5000 zeros, a ZigBee packet, 5000 zeros, and a WiFi packet. The WiFi and LTE packets are both QPSK modulated, and the ZigBee packet is O-QPSK modulated. Furthermore, 16QAM modulation was utilized for WiFi and LTE packets to test this approach with an exemplary higher modulation scheme. Other higher-order QAM formats can also be accommodated and decoded with sufficient EVM accuracy provided that the received SNR is acceptably high, and that the distance between the transmitter and receiver is sufficiently short. This sequence is then transmitted and received using the experimental setup shown in Fig. 5d, consisting of two AD9361 FMCOMMS3 transceiver modules, one used as a transmitter and the other as a receiver with a 12-bit resolu-

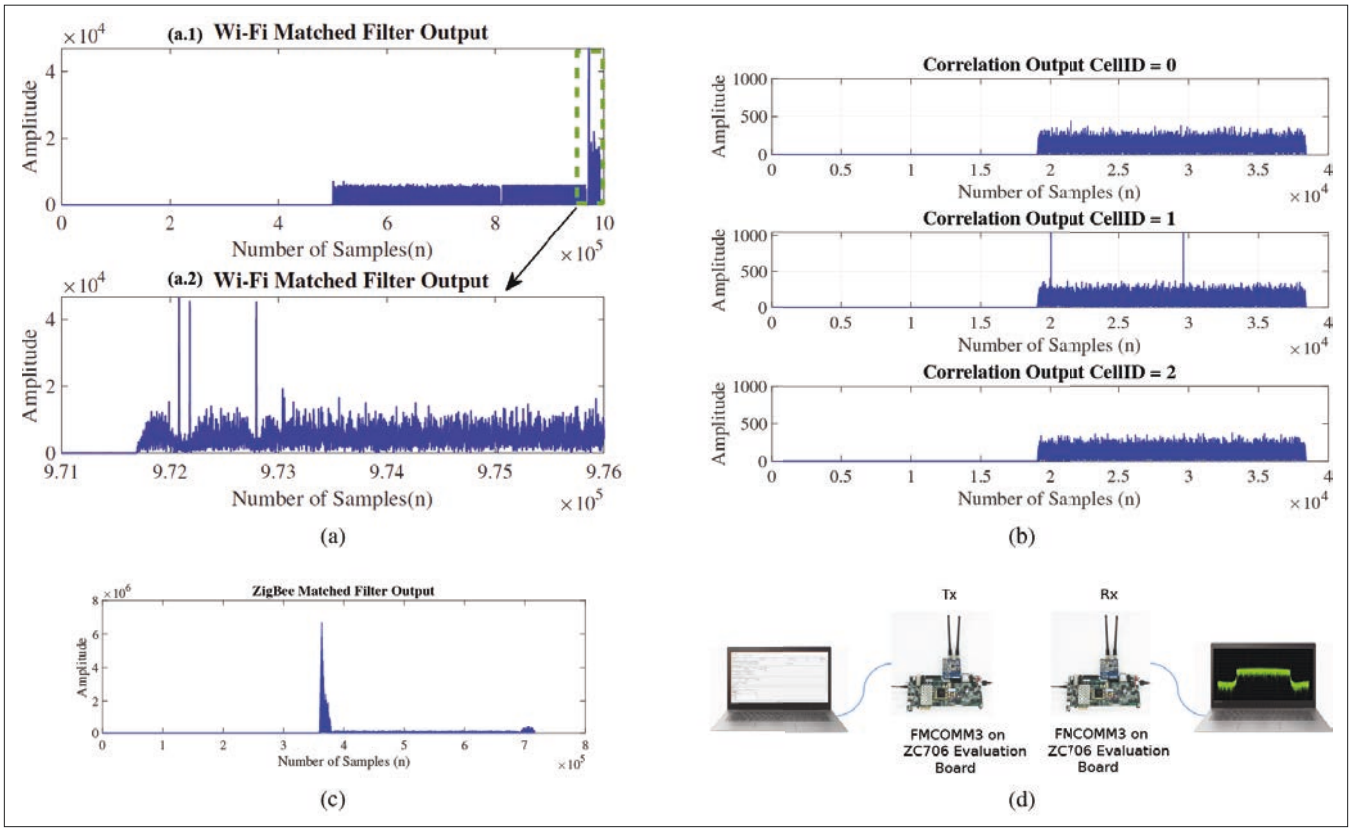

FIGURE 5. a) WiFi matched filter output when cross-correlated with the WiFi, LTE, and ZigBee sequence for: a.1) all samples, a.2) samples in the region containing the WiFi signal between 9.71 x 10^5 and 9.76 x 10^5; b) LTE matched filter output; c) ZigBee matched filter output; d) experimental setup.

tion Σ-Δ ADC (one antenna for each). Additional TX and RX antenna ports of the SDR can be leveraged to support transmit/receive diversity, and hence can be used to accommodate multiple modes. The RF sampling rate for the transmitter and receiver are 30.72 MHz with an 20 MHz RF bandwidth. Both TX and RX local oscillators were configured to operate at 2.4 GHz. The experiments were performed in a mixed-use lab and office environment, where interference signals were present from two nearby WiFi routers located at ~10 m and ~20 m from the setup, as well as from 8 to 12 people using devices with WiFi and Bluetooth of varying activity throughout the experiments.

Packet Detection Results

For WiFi detection, cross-correlation between the received sequence and oversampled WiFi preamble is calculated with a window size equal to the length of the oversampled WiFi preamble. The matched filter output result is shown in Fig. 5a1, where the peaks are present toward the end in the dotted green rectangle. Fig. 5a2 shows the same matched filter output within the dashed green section to clearly show three correlation peaks, which show the position of the guard interval as well as the first and second long training symbols, indicating a successful detection of a WiFi packet in the received sequence.

Similar to WiFi detection, LTE detection involves cross-correlation between the received sequence and the three PSS matched filter coefficients: *CellID* = 0, 1, *and* 2. However, since the PSS is present within the smallest LTE bandwidth (1.4 MHz) corresponding to a sample rate of 1.92 MHz, a downsample operation is required before detection. The received sequence is sampled at 30.72 MHz and then downsampled by 16 in order to achieve a sample rate of 1.92 MHz. After downsampling, the calculation of all three correlation outputs is required since the receiver has no prior knowledge of which primary sequence has been transmitted out of the three possible alternatives. The cross-correlation outputs of the three coefficients (see Fig. 5b) reveal the correlation output with *CellID* = 1 containing two clear peaks indicating the positions of the two PSSs in the received signal.

For ZigBee detection, the received sequence is cross-correlated with the oversampled preamble with a window size equal to the oversampled preamble length. The matched filter output (Fig. 5c) has a clear peak in the middle to indicate that a ZigBee packet is present.

Demodulation and Synchronization Results

During WiFi synchronization, the following operations are executed: coarse and fine frequency offset compensation, timing error detection and correction, channel estimation and equalization, and phase drift correction. These steps are required in order to minimize bit errors and maximize demodulation accuracy. After synchronization, the signal is demodulated by applying a 64 point FFT on the baseband IQ data to extract QPSK and 16QAM symbols as exemplified in Fig. 1 (top).

Spectrum sharing is likely to continue into the future [15], for which efficient spectrum coexistence between LTE and 5G-NR is under discussion. Implementing our method in real time minimizes hardware complexity and power consumption. Furthermore, this technique is complementary to coexistence methods like traffic scheduling while demonstrating spectrum efficiency and low latency.

Similar to WiFi, synchronization steps including frequency offset estimation and correction, demodulation (using a 2048-point FFT), channel estimation, phase correction, frame synchronization, cell identification, bandwidth determination, and channel decoding are performed for LTE. After synchronization, the decoded OFDM symbols of the Physical Downlink Shared Channel (PDSCH) for both QPSK and 16QAM modulations are plotted (see Fig. 1 (middle)).

Similar to WiFi and LTE, ZigBee synchronization and demodulation is performed if the peak-to-average ratio from detection is exceeded. The steps include half-sine pulse filtering, frequency offset compensation, and timing recovery to produce the OQPSK synchronized symbols shown in Fig. 1 (bottom). Despreading of the demodulated symbols is used to output the MAC Protocol Data Unit (MPDU) bits that are used for Bit Error Rate (BER) calculations. The Symbol Error Rate (SER) was calculated in comparison to the transmitted symbols for all the protocols, and an SER of zero was achieved in all cases. To gain further insights, an experiment was performed using WiFi and LTE with 16QAM modulation as an example. While maintaining the same distance between the transmitter and receiver, the following BER results were obtained for WiFi with different transmitter attenuations of 0 dB, 10 dB, 15 dB, and 20 dB: 0, $5.57 \cdot 10^{-4}$, $5.72 \cdot 10^{-4}$, and $6.03 \cdot 10^{-4}$ (respectively). Similarly for LTE, transmitter attenuation values of 0 dB, 20 dB, 22 dB, 24 dB, 27 dB, and 30 dB resulted in the following BER: 0, $5.61 \cdot 10^{-5}$, $1.68 \cdot 10^{-4}$, $8.03 \cdot 10^{-4}$, $7 \cdot 10^{-3}$, and 0.007 (respectively). In this experiment, we only emulate the effect of changing the distance by changing the attenuation. In reality, the multipath structure depends on changing obstacles as the distance varies, which affects BER measurements.

To evaluate the effects of interference between two concurrent protocols transmitted with the same carrier frequency without idle periods, we performed an experiment where LTE and WiFi are transmitted simultaneously on the same channel with varying power levels for WiFi. The signal-to-interference-plus-noise ratio (SINR) between LTE and WiFi was used as a metric to determine the minimum power levels at which LTE and WiFi can be detected under the test conditions. Note that this co-channel interference with varying SINR was created in addition to the environmental interference described above. For SINR values of 34 dB, 26 dB, 14 dB, 8 dB, and 2 dB, the obtained BER values are as follows: 0, 3.55·10–4, 0.0581, 0.107, and 0.158, respectively. WiFi packets were detectable for SINR values down to 8 dB, and LTE packets were detectable for SINR values of 2 dB and higher. These results demonstrate the ability to detect WiFi and LTE during concurrent transmissions. They also show that the lower the SINR is, the higher will be the BER as expected with increased interference.

Conclusion

We have demonstrated the ability to differentiate among, detect, synchronize, and demodulate WiFi, LTE, and ZigBee signals using the same RF front-end in the 2.4 GHz ISM band tested over the air in a lab environment that is susceptible to interference. Cross-correlation windows are used in parallel for detection of the listed protocols with a window length equal to the preamble/PSS length. The original WiFi and ZigBee matched filters are oversampled to 30.72 MHz in order to avoid data sample conversion before matched filtering. Rather than continuous resampling of the received signal, the WiFi and ZigBee matched filters are resampled only once.

In the future, this approach will be extended to support more protocols such as Bluetooth Low Energy (BLE) and further applications in the ISM band. Current wireless devices like smartphones use multiple hardware resources to support WiFi and LTE. Spectrum sharing is likely to continue into the future [15], for which efficient spectrum coexistence between LTE and 5G-NR is under discussion. Implementing our method in real time minimizes hardware complexity and power consumption. Furthermore, this technique is complementary to coexistence methods like traffic scheduling while demonstrating spectrum efficiency and low latency.

Acknowledgments

This research is funded in part with support from MathWorks, Analog Devices and Xilinx. Handagala and Leeser were funded in part by NSF grant CNS-1836880. The opinions and views expressed in this article are those of the authors, and not necessarily that of the funding bodies.

References

[1] C.-F. Chiasserini and R. R Rao, "Coexistence Mechanisms for Interference Mitigation in the 2.4-GHz ISM Band," *IEEE Trans. Wireless Commun.*, vol. 2, no. 5, 2003, pp. 964–75.

[2] J. Kruys and L. Qian, *Sharing RF Spectrum with Commodity Wireless Technologies: Theory and Practice*, Springer Science & Business Media, 2011.

[3] N. Azmi *et al.*, "Interference Issues and Mitigation Method in WSN 2.4 GHz ISM Band: A Survey," *Proc. 2014 2nd Int'l. conf. Electronic Design (ICED)*, IEEE, 2014, pp. 403–08.

[4] Z. Guan and T. Melodia, "CU-LTE: Spectrally-Efficient and Fair Coexistence Between LTE and Wi-Fi in Unlicensed Bands," *Proc. 2016 35th Annual IEEE Int'l. Conf. Computer Commun., INFOCOM 2016*, IEEE, 2016, pp. 1–9.

[5] X. Jiao *et al.*, "Radio Hardware Virtualization for Coping with Dynamic Heterogeneous Wireless Environments," *Proc. Int'l. Conf. Cognitive Radio Oriented Wireless Networks*, Springer, 2017, pp. 287–97.

[6] T. Nihtilä *et al.*, "System Performance of LTE and IEEE 802.11 Coexisting on a Shared Frequency Band," *Proc. 2013 IEEE Wireless Commun. Networking Conf. (WCNC)*, IEEE, 2013, pp. 1038–43.

[7] S. Antipolis, "Evolved Universal Terrestrial Radio Access (E-UTRA): Physical Channels and Modulation," vol. 3, GPP TS 36.211, version 8.7.0, Release 8. 3GPP Technical Specification Group Radio Access Network, 2009.

[8] I. Parvez *et al.*, "LAA-based LTE and ZigBee Coexistence for Unlicensed-band Smart Grid Communications," *Proc. 2016 IEEE SoutheastCon*, IEEE, 2016, pp. 1–6.

[9] IEEE 802 Working Group and Others, "EEE Standard for Local and Metropolitan Area Networks — Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANS)," IEEE Std., 802:4–225, 2011.

[10] M. Leeser *et al.*, "An FPGA Design Technique to Receive Multiple Wireless Protocols with the Same RF Front End," *Wireless Days*, IEEE, 2019.

[11] H. Setiawan and H. Ochi, "A Low Complexity Physical-Layer Identity Detection for 3GPP LTE," *Advanced Commun. Technology (ICACT)*, IEEE, 2010.

[12] "802.11n Packet Error Rate Simulation for 2x2 TGn Channel," https://www.mathworks.com/help/wlan/examples/802-11n-packet-error-rate-simulation-for-2x2-tgn-channel.html; accessed: 2019-10-06.

[13] "Cell Search, MIB and SIB1 Recovery," https://www.mathworks.com/ help/lte/examples/cell-search-mib-and-sib1-recovery.html; accessed: 2019-10-06.

[14] Recovery of IEEE 802.15.4 OQPSK Signals, https: //www.mathworks.com/help/supportpkg/zigbee/examples/ recovery-of-ieee-802-15-4-oqpsk-signals.html; accessed: 2019-10-06.

[15] L. Wan, Z. Guo, and X. Chen, "Enabling Efficient 5G NR and 4G LTE Coexistence," *IEEE Wireless Commun.*, vol. 26, no. 1, 2019, pp. 6–8.

Biographies

Mohamed Mohamed received the B.Sc. degree in electrical engineering from The University of Massachusetts at Amherst in 2017 and the M.Sc. degree in electrical engineering from Northeastern University in 2019. His research interests include RF wireless communication systems and signal processing. He is currently an RF engineer at the Plasma Science and Fusion Center at Massachusetts Institute of Technology.

Suranga Handagala received the B.Sc. degree in electronic and telecommunication engineering from the University of Moratuwa, Sri Lanka in 2009, and the M.S. degree in electrical engineering from the University of Akron, OH in 2016. He is currently pursuing the Ph.D. degree in electrical engineering with Northeastern University, Boston, MA. His research interests focus on software defined radio and implementation of wireless communication algorithms on FPGAs.

Jieming Xu is a Ph.D. student in the Department of Electrical and Computer Engineering at Northeastern University. He received his master's degree from Northeastern University in 2017 and he graduated from Southeast University, Nanjing, China in 2014.

Miriam Leeser [SM'97] is professor of electrical and computer engineering at Northeastern University. She has been doing research in hardware accelerators, including FPGAs and GPUs, for decades, and has done groundbreaking research in floating point implementations, unsupervised learning, medical imaging, privacy preserving data processing and wireless networking. She received her B.S. degree in electrical engineering from Cornell University, and Diploma and Ph.D. degrees in computer science from Cambridge University in England. She has been a faculty member at Northeastern since 1996, where she is head of the Reconfigurable Computing Laboratory and a member of the Computer Engineering group. She serves on the editorial board of *ACM Transactions on Reconfigurable Technology and Systems*. She is the recipient of an NSF Young Investigator Award, and was named a Fulbright Scholar in 2018.

Marvin Onabajo [SM'14] is an associate professor in the Electrical and Computer Engineering Department at Northeastern University. He completed a B.S. degree in electrical engineering at The University of Texas at Arlington in 2003, as well as M.S. and Ph.D. degrees in electrical engineering from Texas A&M University in 2007 and 2011, respectively. He currently serves as an associate editor on the editorial boards of *IEEE Transactions on Circuits and Systems I* (TCAS-I, 2016-2017, 2018-2019, and 2020-2021 terms) and of *IEEE Circuits and Systems Magazine* (2016-2017, 2018-2019, and 2020-2021 terms). During the 2014-2015 term, he was on the editorial board of *IEEE Transactions on Circuits and Systems II* (TCAS-II). He received a CAREER Award from the National Science Foundation, a Young Investigator Program Award from the Army Research Office, and the Martin Essigman Outstanding Teaching Award from the College of Engineering at Northeastern University.