LTE2B: Time-Domain Cross-Technology Emulation under LTE Constraints

Ruofeng Liu, Zhimeng Yin, Wenchao Jiang, Tian He
Department of Computer Science and Engineering, University of Minnesota
(liux4189,yinxx283,jiang832,tianhe)@umn.edu

ABSTRACT

Conventional gateway solutions are limited in satisfying the demand for ubiquitous connections among heterogeneous wireless devices, e.g., wide-area and personal-area network devices, due to the deployment complexity, high cost, and the incurred extra traffic. Recent advances propose the physical layer cross-technology communication to address these issues. However, existing CTC techniques commonly emulate the target waveform in the frequency domain (FDE). Despite their success, these FDE based techniques inherently suffer from high quantization errors and are insufficient for IoT applications that require high communication reliability.

To improve the emulation accuracy, we are the first to introduce the time-domain emulation (TDE) that significantly outperforms FDE techniques in reducing quantization errors and offers reliable emulation even with limited sources, e.g., low modulation schemes. To validate our idea, we propose LTE2B, the first TDE based CTC work that enables LTE devices (e.g., smartphones) to transmit data frames demodulatable by ZigBee and Bluetooth low energy (BLE) devices. We implement the LTE2B on commodity devices (Nexus 5X smartphone and CC2530/CC1350 ZigBee/BLE SoC) with only payload embedding by penetrating the extremely complicated LTE stack. Our extensive evaluation demonstrates that TDE outperforms FDE, while LTE2B can achieve a robust (> 99% accuracy), long distance (> 400m) CTC performance under a full range of wireless configurations including indoor/outdoor, mobility, and duty-cycle settings.

CCS CONCEPTS

• **Networks → Wireless access networks**.

KEYWORDS

Cross-Technology Communication; Time-Domain Emulation

ACM Reference Format:
Ruofeng Liu, Zhimeng Yin, Wenchao Jiang, Tian He. 2019. LTE2B: Time-Domain Cross-Technology Emulation under LTE Constraints. In *The 17th ACM Conference on Embedded Networked Sensor Systems (SenSys '19), November 10–13, 2019, New York, NY, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3356250.3360022

1 INTRODUCTION

A wide range of wireless technologies (e.g., WiFi, Bluetooth, ZigBee, and LTE.) have been rapidly and ubiquitously deployed to accommodate diverse application requirements. The net deployment of all kinds of wireless devices is anticipated to grow as large as 50 billion by 2020 [15].

Driven by the emerging deployment and applications of wireless devices, there is an increasing need for pushing information from wide-area network (e.g., LTE and Multefire) to person-area network (e.g., ZigBee and Bluetooth). For example, the lighting condition of ZigBee-enabled smart bulbs may need to be adjusted remotely via LTE network. LTE-based Multefire network [4] needs to share the coordination information to the incumbent low-power IoT devices in the 2.4 GHz unlicensed band in order to mitigate the severe coexistence problem.

To deliver information from WAN to PAN, the de facto solution is a multi-radio gateway, which offers indirect connection [21] since it is assumed that these heterogeneous technologies cannot communicate with each other directly due to the incompatible PHY layers. Although the multi-radio gateway is a viable approach, it suffers a few emerging issues when wireless networks become increasingly ubiquitous, mobile and dense. For instances, to support mobility, either a full coverage of gateways or mobile gateways is needed, introducing high deployment cost and design complexity. In dense networks, extra traffic overhead flowing into and outwards from the gateways escalates the collision and interference in wireless co-existence environments.

Recent advances demonstrate that cross-technology communication [9, 22, 23, 40] holds the promise to address these issues. For example, WEBee [23] supports a high-data-rate Wi-Fi to ZigBee communication without hardware modification at either the sender or receiver side, which is achieved via frequency domain emulation (FDE). By transforming the target ZigBee signal to the frequency domain, WEBee controls the bits at each subcarrier for approximating the ZigBee waveform. However, we notice that WEBee with FDE inherently suffers from high quantization errors, losing near half of the transmitted CTC packets. This inherent unreliability hinders many critical IoT applications, such as channel coordination and controlling IoT devices, since they generally require reliable communication for performance guarantee.

To offer reliable emulation, we are the first to introduce the time-domain emulation (TDE), which approximates the target signal in the time domain. Specifically, after sampling the target signal, TDE chooses the nearest quadrature amplitude modulation (QAM) points in the time domain. Compared with the FDE based techniques such as WEBee, TDE significantly reduces quantization errors, thus improving the CTC reliability. For validating the idea of TDE, we design and implement LTE2B, a PHY-layer CTC technique based

SenSys '19, November 10–13, 2019, New York, NY, USA
© 2019 Association for Computing Machinery.
ACM ISBN 978-1-4503-6950-3/19/11…$15.00
https://doi.org/10.1145/3356250.3360022

on TDE that enables an LTE network to deliver messages via LTE smartphones to commodity ZigBee and BLE devices. As the benefit of TDE, LTE2B offers reliable emulation performance - to emulate a ZigBee packet with more than 99% reliability, it only needs a modulation scheme as low as quadrature phase shift keying (QPSK). In contrast, with FDE, WEBee requires 64 QAM (a much higher modulation scheme than QPSK) for emulating the same waveform, while it still suffers from severe packet losses (around 50%)[23].

In addition, LTE2B is fully compliant to the LTE and ZigBee/BLE protocol, generating the decodable ZigBee/BLE signal purely based on the IP payload of a LTE packet. Specifically, neither the LTE smartphones nor the ZigBee/BLE devices require hardware and firmware modification, indicating this technology can be deployed rapidly in existing network infrastructure. To achieve full compliance, LTE2B addresses multiple practical challenges. Unlike Wi-Fi, ZigBee and BLE, LTE is probably the most complicated wireless standard designed so far, aiming at a high configurability, flexibility, and efficiency. Such complexity introduces *constraints* in multiple dimensions including misaligned sample rates, coding constraints, modulation constraints, and duration constraints, etc. Therefore in order to repurpose a LTE modulator into a time domain signal emulator, LTE2B penetrates each *constraint* and involves tackling a series of highly challenging tasks.

To summarize, our intellectual contributions are:

- LTE2B is the first CTC work that bridges WAN and PAN, so that it leverages the best of both worlds, i.e., the full coverage capability of the LTE devices and energy-efficiency and low-cost of the ZigBee/BLE devices. Such a new wireless architecture will support emerging applications such as lighting, irrigation and access control within smart and connected communities.
- We propose LTE2B, the first CTC based on time-domain emulation (TDE) which emulates the target waveform in the time domain in contrast to existing frequency domain emulation (FDE) such as WEBee [23]. Via TDE, LTE2B significantly improves the emulation accuracy for both ZigBee and BLE signal with limited resources, demonstrating its efficiency and generality.
- To implement LTE2B while being compliant to the LTE protocols, LTE2B penetrates the complicated LTE stack and several practical constraints, e.g., misaligned sample rates, flipped QAM points, and turbo coding constraint. By doing this, LTE2B is a transparent design which is compatible with commodity LTE smartphones, commodity BLE devices, and ZigBee devices, allowing user applications to control these IoT devices purely based on the LTE IP payload. These innovations provide generic guidance for penetrating the constrained layers of other wireless systems.
- Our LTE2B design, implementation, and evaluation are very extensive, given the high complexity of the LTE standard. Specifically, we implement the LTE2B sender on LTE smartphone Nexus 5X and the LTE2B receiver on CC2530/CC1350 Zigbee/BLE SoC without any hardware or firmware modification. Our extensive evaluation demonstrates that LTE2B can achieve a robust, long-distance CTC performance under a full range of wireless configurations.

The rest of the paper is organized as follows. Section 2 motivates the need for time-domain emulation, while Section 3 overviews the design. Sections 4 and 5 describe the key designs, i.e., (i) time-domain emulation and (ii) reverse channel coding. Section 6 presents the evaluation of LTE2B, followed by the related work and conclusion in Section 7 and Section 8 respectively.

2 MOTIVATION

Personal area network (PAN), e.g., ZigBee/BLE are traditionally believed to be private and isolated. However, in the era of the internet of things (IoT), there is an increasing need to push information from the wide-area network (WAN) to these isolated PAN devices. For examples, pushing Internet weather forecast to BLE thermostats makes building temperature control more energy efficient. Switching on/off smart bulbs based on sunset/sunrise times can save the electricity cost for local communities.

To connect these isolated IoT devices to the Internet at low cost, researchers propose cross-technology communication (CTC). In specific, the CTC senders emulates the target waveform of the CTC receivers with incompatible PHY layers. In this section, we first identify that *frequency-domain emulation* (FDE) adopted in the state-of-the-art CTC techniques, e.g., WEBee [23] has inherent limitations for providing reliable CTC between WAN and PAN. After that, we analyze the possibility of *time-domain emulation* (TDE) and its unique advantages for reliable communication in contrast to existing FDE CTC.

2.1 Frequency Domain Emulation

FDE approximates a target waveform from the frequency domain, which is designed for frequency-domain modulator, i.e., orthogonal frequency division multiplexing (OFDM). As Fig. 1 shows, to emulate a target time-domain waveform, FDE first needs to convert it into the frequency domain with Fast Fourier Transform (FFT). Then FDE approximates the FFT results by quantizing them to the nearest predefined discrete QAM points. Quantization changes the frequency domain components from ideal values, thus adding quantization error to the emulated signal. The quantization errors in FDE are non-trivial. Fig.1 plots the distribution of FFT results in the constellation with 'x', which extremely disperse. Hence, some frequency components are significantly far away from the legitimate QAM points (grey rectangles), leading to severe quantization errors.

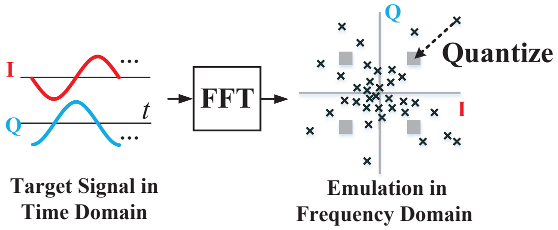


Figure 1: Frequency Domain Signal Emulation.

To reduce the quantization errors, FDE usually requires sender to use high modulation schemes with dense QAM points. Fig.2 compares the ZigBee signal emulated by WEBee using different modulation schemes. When reducing the modulation scheme from

64QAM to QPSK, the number of QAM points available for emulation decreases from 64 to 4. With less available QAM points, the quantization errors are significantly increased, causing severe distortion in the emulated signal. Thus, WEBee fixes transmitter to use 64QAM while it still loses 50% of the CTC packets due to inevitable quantization error.

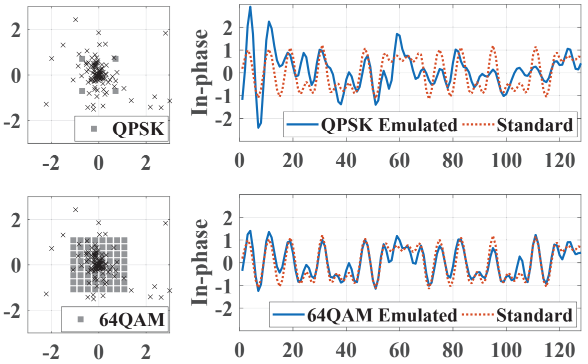


Figure 2: FDE-emulated Signal vs. Standard.

The inherent inaccuracy and stringent requirement of high modulation schemes limit FDE's applicability. For example, LTE devices only support up to 16QAM in the uplink, while they cannot set the modulation schemes freely due to the central control of the base station. Thus, it is still an open and critical question whether WAN technology, e.g., LTE can emulate low-power IoT waveform with limited resources while achieving high accuracy.

2.2 Time Domain Emulation

Besides FDE, transmitters, e.g., LTE and WiFi may also be capable to emulate IoT signal directly in the time domain using the time domain emulation (TDE). We observe that in addition to OFDM which modulates QAM points in the frequency subcarriers, SC-FDMA in LTE (as we will discuss in Section 4) and DSSS/CCK in 802.11 can transmit a sequence of QAM in the time domain.

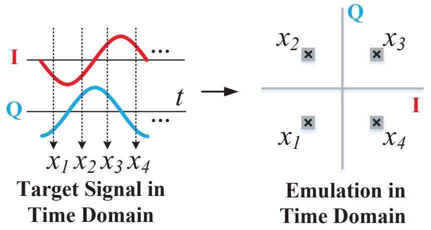


Figure 3: Time Domain Signal Emulation.

The benefit of TDE is obvious. In contrast to the disperse distribution in the frequency domain, waveforms of IoT transmissions are typically extremely simple in the time domain. This is because IoT devices are designed for low cost and complexity and thus the IoT waveforms must be simple enough to be decoded directly in the time domain with robustness. We take OQPSK waveform depicted in the Fig.3 as an example. The ideal samples in the time domain, i.e., x_n are located right at the 4 QAM points (grey rectangles). Thus, mapping the ideal samples to discrete QAM in the time domain for the emulation incurs zero quantization errors.

Because of this reason, by using significantly lower modulation schemes, e.g., four QAM points in QPSK, TDE is able to perfectly track the waveform of the ideal signal, significantly improving the accuracy of the emulation. Compared to the stringent requirement for modulation schemes in FDE, TDE can be generically applied to wide range of settings, which significantly outperforms FDE in the applicability.

This fundamental difference between FDE and TDE inspires us to explore the possibility of performing TDE on the *commodity* device, e.g., LTE smartphone for offering reliable CTC with limited resources, e.g., modulation schemes.

3 OVERVIEW

This section presents the overview of LTE2B, a transparent time domain emulation from **commodity** LTE to both **commodity** ZigBee and BLE. For the illustration purpose, our design description focuses on using ZigBee receivers as an example, while the evaluations of both ZigBee and BLE are introduced in Section 6.

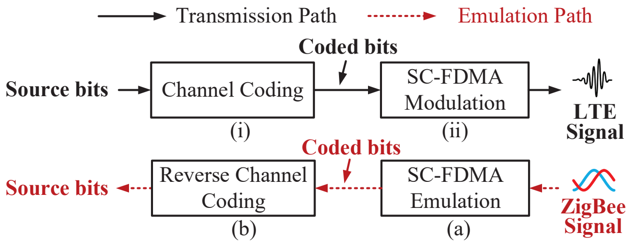


Figure 4: Architecture of LTE2B.

Fig.4 compares the high-level structure of the LTE transmitter and LTE2B. The LTE transmitter converts source bits to the baseband signal in two steps: (i) source bits are encoded by channel coding into coded bits for robustness. (ii) These coded bits are modulated by Single-Carrier Frequency Division Multiple Access modulation (SC-FDMA) into a LTE baseband signal.

LTE2B is completely transparent time-domain emulation that is fully compliant with LTE system, i.e., it takes the emulation path to figure out the source bits which generate special waveform decodable by ZigBee. Specifically, in Section 4 LTE2B emulates the ZigBee waveform in the time domain for offering accurate emulation. Then in section 5, we discuss how to penetrate complicated LTE coding stack to provide desired coded bits for time-domain signal emulator.

4 SC-FDMA EMULATION

In this section, we introduce how LTE2B emulates the ZigBee signal in the time domain, while being transparent to the SC-FDMA modulation in the LTE stack. Specifically, we address several challenges, such as mismatched sample rate, time-domain QAM flip, duration and guarding interval constraints. As a generic method, time-domain emulation is also applicable to other CTC scenarios (e.g., LTE to BLE and 802.11 CCK to ZigBee) as evaluated in Section 6, while we focus on the LTE to ZigBee in the section.

4.1 Opportunity

Note that LTE2B requires the frequency overlap between LTE and ZigBee/BLE devices. Although the current 3GPP standards limit LTE to the licensed bands, the recent LTE-based MulteFire[5], proposes to work at the 2.4 GHz for extending the LTE ecosystem. Since LTE2B is validated via the current 3GPP specifications and commodity smartphones and MulteFire is based on 3GPP specifications, LTE2B can be directly applied to the emerging MulteFire in the near future for enabling CTC.

In addition, LTE UEs are controlled by the LTE base station at the running time, i.e., the allocated central frequency and the bandwidth are allocated by the LTE base station. To enable LTE2B, the LTE base station could configure the UEs running LTE2B specifically for the CTC purpose, while this configuration can be achieved easily by setting the LTE resource scheduler without violating the 3GPP specifications.

4.2 Background: Modulation in LTE

To explain how to enable time-domain emulation in LTE, it is necessary to first introduce the SC-FDMA modulation in the transmitter of LTE UE (user equipments). Fig.5 shows the detailed procedures of SC-FDMA: (i) Coded bits are mapped to a sequence of time-domain discrete QAM points based on the assigned modulation scheme, typically QPSK. (ii) The sequence of QAM points are then converted to the frequency domain using Discrete Fourier Transform (DFT). (iii) Once in the frequency domain, they are mapped to the desired subcarriers in the overall LTE spectrum. (iv) Finally, to create the transmitted signal, Inverse Discrete Fourier Transform (IDFT) is performed creating a time-domain SC-FDMA symbol. As we will further discuss in section 4.7, twelve SC-FDMA symbols will be concatenated with guarding intervals and reference signal into an uplink subframe.

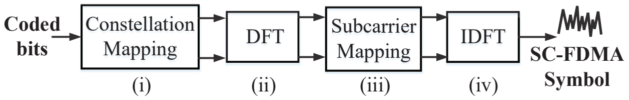


Figure 5: SC-FDMA Modulation.

As the procedure demonstrates, SC-FDMA modulates coded bits into a sequence of *time-domain* QAM and transmits them sequentially in a single carrier. This is significantly distinct from orthogonal frequency division multiplexing (OFDM), where bits are modulated into a set of QAM points in the *frequency domain* and transmitted parallelly in multiple subcarriers. This unique capability of producing QAM sequence in time domain enables time-domain signal emulation in LTE.

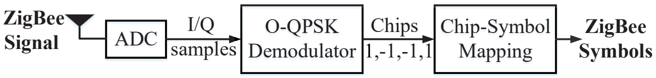


Figure 6: How a ZigBee Receiver Demodulates.

4.3 Background: Demodulation in ZigBee

To quantify the accuracy of emulated ZigBee signal, we demonstrate how ZigBee devices demodulate the OQPSK signal in Fig.6. First, the baseband signal is sampled by ADC using 2MHz sample rate to generate discrete I/Q samples of the ZigBee signal. Second, OQPSK demodulator decodes chips from I/Q samples.

Last, a set of 32 ZigBee chips are mapped to one of 16 ZigBee symbols by matching the received chip sequences with the ideal direct-sequence spread spectrum (DSSS) sequences of each symbol defined in a symbol-to-chip mapping table. Note due to the inherent redundancy in DSSS, a small number of chips errors due to imperfect emulation can be tolerated by DSSS.

4.4 Emulation Challenges

In Section 2, we demonstrate that a sequence of time-domain QPSK points are able to perfectly emulate time-domain samples of ideal ZigBee waveform. In addition, our analysis of the SC-FDMA modulation procedure in section 4.2 shows that such QAM points sequence can indeed be produced by SC-FDMA modulator in the time domain. As a result, LTE2B is able to emulate the ZigBee waveform in the time domain. However, the complicated LTE stack imposes several practical constraints and challenges which must be addressed. Specifically, LTE2B needs to emulate ZigBee signal with different sample rates (The sample rate is directly decided by the allocated bandwidths from the LTE base station), as demonstrated in Section 4.5. In addition, we need to solve the unique challenges of using TDE with LTE's SC-FDMA modulation.

4.5 TDE under Misaligned Sample Rates

TDE is able to perform perfect one-to-one mapping in the time domain when ZigBee and LTE have the same sample rate. However, LTE standard specifies that the sample rate of LTE uplink must be a multiple of 180 kHz because the granularity of bandwidth allocation is 180kHz. Since the ZigBee sample rate is 2 MHz, the sample rates of ZigBee and LTE are misaligned, resulting in inevitable quantization errors in TDE as well. In this section, we introduce how LTE2B offers generic TDE under misaligned samples rates, and why TDE is better than FDE.

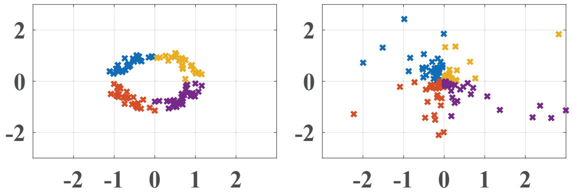


Figure 7: Sample Distribution: Time vs. Frequency.

In Fig.7 and Fig.8, we study the impact of misaligned sample rate on TDE and FDE. We demonstrate by emulating the ZigBee waveform sampled at one legitimate LTE sample rate: 1.8MHz with both QPSK TDE and QPSK FDE. As shown in the left part of Fig.7, due to the misaligned sample rate, the ZigBee samples no longer concentrate on the four discrete QAM values, i.e., ±1 ± i. Instead, they form four concentrated clusters closely around the four ideal QAM values. The misaligned sample rates bring ZigBee samples

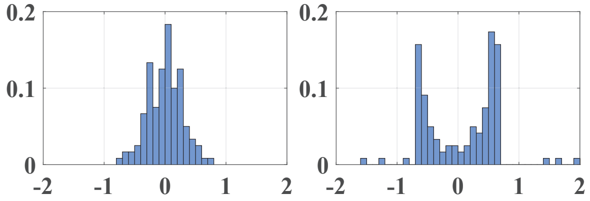


Figure 8: Emulation Error Distribution: TDE vs. FDE.

small and bounded quantization errors when they are mapped to the closest LTE QAMs in TDE. In comparison, the frequency equivalence of ZigBee samples shown in the right part of Fig.7 keep disperse under the LTE sample rate, making them hard to be well represented by a limited number of, e.g., four, frequency-domain QAM points in FDE.

In Fig.8, we quantitatively illustrate the quantization errors in "In-phase" when the normalized signal is emulated by TDE and FDE respectively. We find that the TDE quantization error is concentrated near 0 and bounded by 0.7, while its FDE counterpart is far more disperse and can be as large as 2.2. The comparison in Fig.8 clearly shows TDE outperforms FDE in quantization error for the ZigBee waveform under the mismatched LTE sample rate.

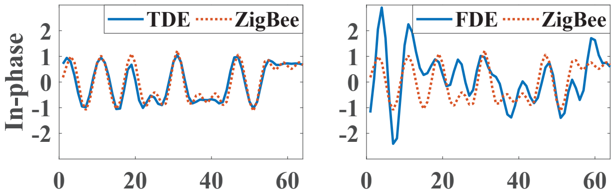


Figure 9: Emulated Signal: TDE vs. FDE.

To have a perceptual comparison of the waveform emulated by FDE and TDE, we depict the ideal and emulated waveforms of ZigBee symbol '0' under 1.8MHz sample rate in Fig.9 as a proof-of-concept example. In each subfigure of Fig.9, the ideal ZigBee waveform is with the red dotted line while the emulated one is with the blue concrete line. We find the TDE emulated waveform better matches the ideal waveform compared to the FDE emulated one, although the latter shows the correct trend. The waveform comparison perceptually proves that TDE achieves better emulation than FDE under misaligned sample rate.

In addition to the waveform comparison, we also evaluate the ZigBee receiver's performance with the signal emulated from TDE and FDE. In the experiment, we emulate the waveform of ZigBee frames consisting of over 100 random ZigBee symbols with QPSK TDE and QPSK FDE respectively under various valid LTE sample rates range from 1.08 MHz to 4.5 MHz. We collect the demodulated ZigBee frames and calculate the average chip errors per ZigBee symbol at the receiver side. From Fig.10, we find the average chip errors of TDE is about 8 out of the 32 chips per ZigBee symbol under the sample rate of 1.08MHz and dramatically decrease as the sample rate increases. The chip errors reach zero when the sample rate is over 2MHz, which is the standard ZigBee sample rate. It shows that TDE can emulate ZigBee waveform with no chip error under large enough sample rate.

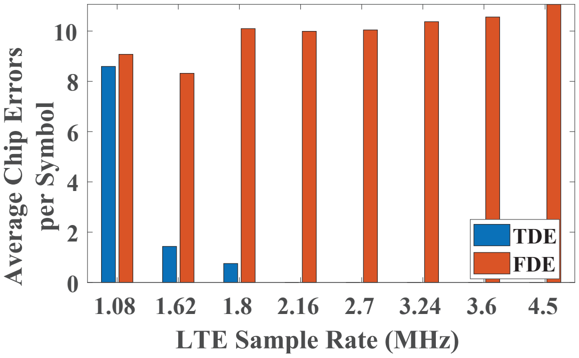
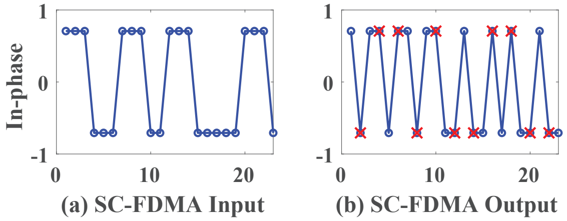


Figure 10: Chip Errors: TDE vs. FDE.

In comparison, the average chip errors per ZigBee symbol are always within the range of [8, 12] for FDE under the sample rate from 1.08MHz to 4.5 MHz. Considering that the ZigBee receiver cannot correctly demodulate a ZigBee symbol when the average chip errors are larger than 6 [39], QPSK FDE fails to emulate decodable ZigBee frames. From the comparison in Fig. 10, we find the performance of FDE does not improve even with large enough sample rate, which is due to the inherent errors during the FDE. Surprisingly, when the bandwidth is 1.62 MHz or 1.8 MHz, our TDE is able to successfully emulate the ZigBee waveform, although the bandwidth is smaller than the 2 MHz ZigBee bandwidth, demonstrating the unique advantages of TDE.

4.6 TDE under SC-FDMA

In Section 4.4, we introduce the TDE with misaligned sample rates. Since LTE2B needs to be fully transparent with existing LTE stack, it has to consider the impacts of LTE PHY layer. Specifically, to allow multiple LTE user equipments (UE), such as smartphones, to access the spectrum at the same time, SC-FDMA utilizes "subcarrier mapping" to shift the signal from the baseband to the target frequency. However, this frequency shift also modifies the time-domain QAM points used in the emulation procedure. As a result, LTE2B needs to address this constraint for emulating the target signal.



(a) SC-FDMA Input (b) SC-FDMA Output

Figure 11: Emulated Signal in SC-FDMA.

The Phenomenon: Due to the SC-FDMA modulation in LTE, the time-domain signal before and after this procedure are different, leading to errors in the time domain emulation. To begin with, we analyze the change of time-domain waveform. Fig.11(a) depicts the emulation of the ZigBee symbol 0 using QPSK. However, after the SC-FDMA modulation, some QAM points are flipped around the origin, while the other QAM points remain the same as shown in Fig.11(b). As a result, LTE2B needs to address this phenomenon so that its time domain emulation is accurate.

The Solution: To enable time-domain emulation under SC-FDMA, we analyze its impacts on the signal. Specifically, we compare the time-domain QAM points before and after the SC-FDMA. With a time-domain QAM point series $S_0, S_1, S_2, ...S_i, ...$, where i means the index ,we have the following interesting conclusions: (1) the QAM points with even indices are kept the same; (2) the QAM points with odd indices are flipped w.r.t. the origin in the constellation. Note that the detailed analysis of SC-FDMA and the theoretical proof of the interesting phenomenon are in the Appendix.

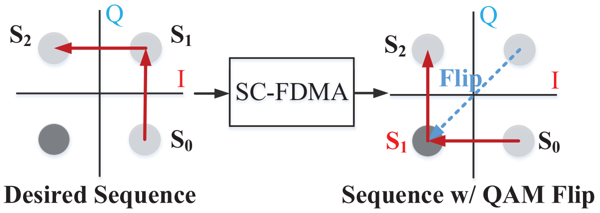


Figure 12: QAM point Flip in SC-FDMA.

Take Fig 12 as an example. With the original input sequence S_0, S_1, S_2, the SC-FDMA will change the QAM points with odd indices. Specifically, both S_0 and S_2 are kept the same, while S_1 is flipped by rotating the QAM point with 180 degrees around the origin point.

This discovery leads to our key design that solves the problem in the time-domain emulation. For the targeted time-domain sequence $S_0, S_1, ..., S_{N-1}$, LTE2B produces a sequence $S'_0, S'_1, ..., S'_{N-1}$, where $S_{2k} = S'_{2k}$, and $S_{2k+1} = -S'_{2k+1}$ $(0 \leq k\&k \in Z)$ as SC-FDMA input. In other words, we flip the samples with odd indices to cancel out the impacts of SC-FDMA and produce the desired sequence at the output.

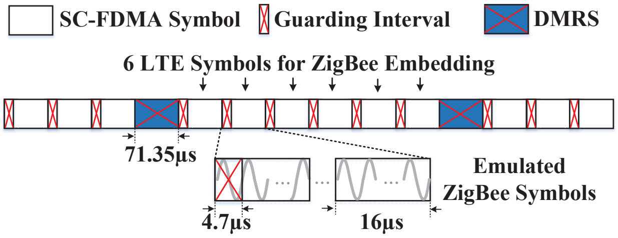


Figure 13: LTE Uplink Subframe Structure.

4.7 TDE under Duration Constraints

So far, we have shown that a SC-FDMA symbol can be used to emulate OQPSK signal. Yet, one single SC-FDMA symbol is still not long enough for one ZigBee frame so LTE2B embed one ZigBee frame in one LTE subframe which consists of 12 SC-FDMA symbols. Due to the existence of reference signal (DMRS) and guarding intervals (GI) in the predefined subframe structure, we cannot control the entire waveform in one subframe. As shown in Fig.13, DMRS are in the 4th and 11th SC-FDMA symbols and the duration of each DMRS is 71.35μs, which will destroy four ZigBee symbols (16μs) if the emulated signal tries to cover these regions. Thus in order to maximize the duration of ZigBee frame, LTE2B embeds the ZigBee waveform in the middle six LTE symbols. LTE signal in the other six symbols and DMRS are incompatible to ZigBee and will be naturally ignored by ZigBee receiver. The maximum duration of the emulated frame is 428.6μs, which can support 26 ZigBee symbols.

Besides DMRS, LTE appends a 4.7μs guarding interval in front of each symbol to eliminate inter-symbol interference (ISI). GI signal is also out of our control. But luckily it has a much shorter duration than DMRS and only overlaps with 9 ZigBee chips. Our empirical study in Section 6.3 demonstrates that GI only influences 6 out of 26 emulated ZigBee symbols with maximum 6 chip errors which are tolerable due to the redundancy in DSSS.

Finally, other IoT technology, e.g., BLE does not provide the redundancy like ZigBee. Luckily, due to the lack of redundant code, the duration of BLE frame is also much shorter. For example, LTE2B can emulate a 16-byte BLE frame of 128us duration with only 2 LTE symbols. Thus, the emulation of BLE signal avoids DMRS and only needs to deal with one LTE GI. Since GI is a cyclic copy of the LTE symbol, LTE2B carefully manipulates the LTE symbol to create the specific signal in GI. Due to the space limitation of the paper, we put the details into the technical report[1].

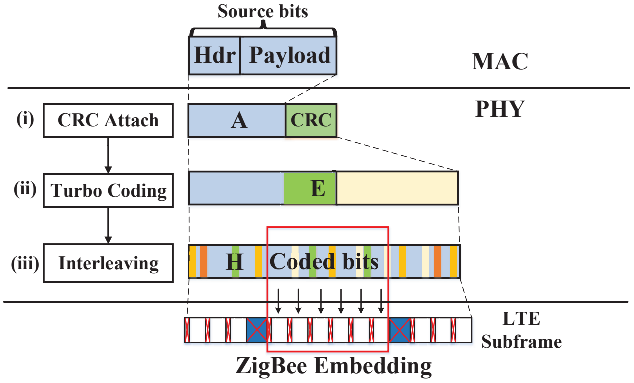


Figure 14: Channel Coding Data Flow.

5 REVERSE LTE CHANNEL CODING

Section 4 shows how LTE2B emulates the target ZigBee signal in the time domain with given coded bits. However, we are still halfway to success, because LTE2B are designed to emulate ZigBee signal purely based on the payload in IP packets (i.e., via socket programming). Thus, given desired code bits, we need to penetrate multiple LTE channel coding layers, as shown in Fig.14, reversely and figure out the right payload.

5.1 Background: LTE Channel Coding

To explain the reverse engineering process in detail, we need first introduce the extremely complicated channel coding scheme in LTE. In Fig.14, we illustrate three main steps in LTE channel coding: CRC attachment, turbo coding, and interleaving. Note that although the real LTE channel coding is much more complex and may repeat each step multiple times, our discussion about how to reverse engineer each channel coding step still satisfies. The functionality of the three steps are as follows.

(i) CRC attachment: CRC parity bits are calculated from the source bits, denoted as code block A, which contains the entire IP packet including the headers. The CRC parity bits are then appended to the trailer of code block A.
(ii) Turbo coding: Code block A and its appended CRC code block are then encoded by a *turbo encoder* into code block E, which contains the whole input bits, i.e., code block A and CRC, as well as some redundant bits generated by the turbo coding.
(iii) Interleaving: Finally, bits in the code block E will go through a complex interleaving process, including the rate matching, concatenation, and permutation as detailed in [3]. The output code block H is coded bits which are modulated into the LTE subframe shown in Fig.14, where the middle six SC-FDMA symbols are used to emulate ZigBee frames..

5.2 Challenges in Reversing Turbo Coding

The reverse of channel coding includes reversing both the interleaving process and the turbo coding. The former is fully reversible because interleaving by definition does not insert or remove data bits but only reorder them. The reverse of turbo coding, however, is much more complicated.

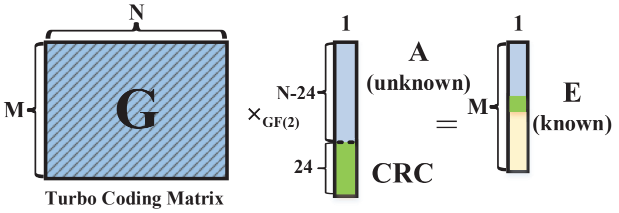


Figure 15: Turbo Coding Matrix

We find the procedures of turbo coding can be represented via matrix multiplications in Galois field GF(2) because turbo coding involves only linear operations, as illustrated in Fig.15. In the figure, the matrix G is an $M \times N$ (typically 7200×10680) coding matrix derived from the turbo encoder utilized in LTE, E is an $M \times 1$ output matrix of turbo coding, and A is an $(N-24) \times 1$ matrix containing $(N-24)$ LTE source bits followed by 24 CRC parity bits. Our goal is to find the unknown code block A from the coded block E. However, we observe two phenomena that make the task challenging.

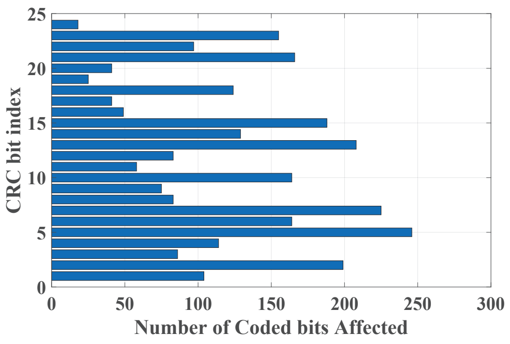


Figure 16: Non-negligible Impacts of CRC on Coded Bits.

(i) Simple solution does not work: The simple solution of matrix inverse, i.e., $\left[A \quad CRC\right]^T = inv(G) \times_{GF(2)} E$ does not work, because *the CRC bits are uncontrollable.* In other words, we can only control block A instead of $\left[A \quad CRC\right]^T$ for the CRC block is determined following the LTE standard. It is a constraint that LTE2B must satisfy to be fully compliant to the LTE standard.
(ii) Impact of CRC bits is non-negligible: One may expect we can simply ignore the 24-bit CRC, for its length is relatively small compared to the source bits N or the coded bits M, so its impact on the coded bits may be limited. It is true for some coding schemes, such as the convolutional code widely used in WiFi, where each CRC bit will affect only several (typically < 10) coded bits [32]. However, in the turbo code, the impact of each CRC bit spreads to the whole coded bits due to turbo code's internal feedback mechanism [3]. In Fig.16, we illustrate the impact of each CRC bit on the final coded bits. In the figure, the Y-axis is the index of the 24 CRC bits, while the X-axis is the number of coded bits each CRC bit will affect. We find that although there are only 24 CRC bits, one CRC bit may affect up to 250 coded bits, leading to significant TDE error if we do not deal with them carefully.

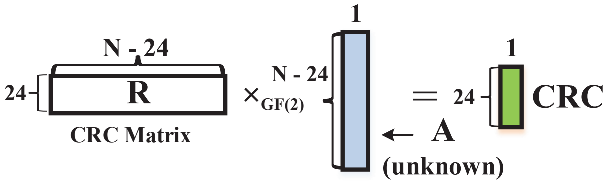


Figure 17: Computation of CRC Bits.

5.3 Reverse Turbo Coding

To tackle the uncontrollable CRC issue, we have to formulate the CRC and use that as a constraint when calculating code block A. We find the calculation of CRC from the source bits, i.e., code block A, can also be expressed as the matrix multiplication. As shown in Fig. 17, R is a $24 \times (N-24)$ matrix indicating the LTE CRC calculation operations. We substitute CRC in Fig. 15 with this formula:

$$(G \times_{GF(2)} \left[I_{N-24} \quad R^T\right]^T) \times_{GF(2)} A = E, \qquad (1)$$

where I_{N-24} is an identity matrix. With this equation, LTE2B is able to compute the code block A with any wanted coded bits E while satisfying the CRC constraints.

We also notice that solving a large system of equations is time-consuming. To provide real-time performance, LTE2B computes the specific inverse matrixes offline. The inverse matrix is only required to be calculated once while online calculation only involves matrix multiplication which requires significantly less computation.

6 PERFORMANCE EVALUATION

This section presents the implementation and evaluation of LTE2B over commodity devices.

6.1 System Implementation

LTE2B sender has been implemented on a commodity LTE smartphone LG Nexus 5X. Since LTE2B works completely in the application layer and only uses socket system calls, it is compliant with

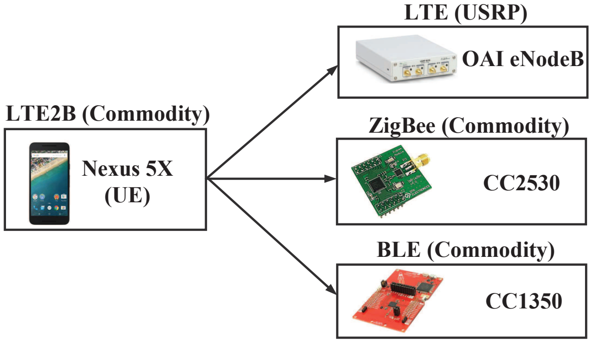


Figure 18: Experiment Setting for LTE2B

any LTE UEs with any chipsets. Specifically, LTE2B computes its LTE packet payload with the target IoT signal at the application layer, and then transmits the packet following the whole LTE stack.

Implementation of LTE2B in the application layer is extremely challenging because source bits in the turbo coding will not only contain IP payload but also various types of protocol headers, e.g, TCP/IP. Similar to CRC, these protocol headers have a non-trivial impact on the decoded bits. Since we cannot control these coded bits via modifying the IP payload, LTE2B leverages the segmentation feature [2] to eliminate protocol header bits in the source bits.

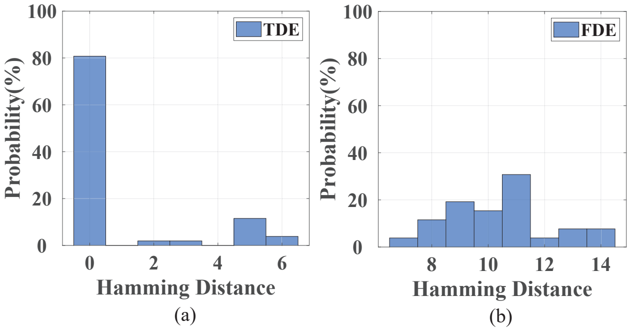
In specific, when the size of the source bits is larger than the capacity of a single subframe, LTE encoder will segment them into two partitions, which are then individually encoded and modulated into subframes. Thus, in order to create a subframe without upper layer protocol headers, LTE2B generate IP payload with large enough size such that the headers and the source bits for TDE will be separated into different partitions and modulated into different subframe. In this way, LTE2B is enable to fully control the coded bits of a subframe from the application layer and generate desired TDE waveform that can be demodulated by commodity ZigBee and BLE devices. Due to the space limitation, we omit other implementation details, which can be found in our website[1].

6.2 Evaluation Setting

Fig.18 illustrates the evaluation settings of LTE2B. LTE2B sender is commodity LTE smartphone LG Nexus 5X. The receivers we use are commodity ZigBee CC2530 and commodity BLE CC1350. In the experiment, Nexus 5X connects to a base station running Openairinterface(OAI) LTE base station [28]. We deploy the open-source LTE base station in order to control the carrier frequency of LTE devices. Specifically, the base station operates on LTE band 7 with 2505MHz central frequency and 10MHz bandwidth. Commodity ZigBee and BLE devices are tuned to 2503MHz which overlaps with LTE spectrum, which can be done by configuring the "FREQCTRL" register in software without modifying the hardware. Note that the emerging LTE-based MulteFire will operate at 2.4 GHz unlicensed band and also follow the 3GPP specifications, enabling LTE2B to work directly between MulteFire and ZigBee/BLE. However, due to the lack of MulteFire equipment, we conduct the experiments on commodity LTE smartphones in 2.5 GHz as a proof of concept.

The results provided are based on QPSK modulation schemes and 2.16MHz bandwidth if there is no extra explanation. We note that TDE's emulation performance increases with higher modulation schemes (less quantization error), while we evaluate QPSK as the bottom line for our design. The evaluations start with the detailed measurements of LTE2B's performance in PHY layers (i.e., chip error rate and symbol error rate). Then link-layer experiments (i.e., frame reception ratio) are conducted under a wide range of settings including indoor/outdoor, Line-of-Sight(LOS)/None-Line-of-Sight(NLOS), mobile and low duty cycle. Each experiment is repeated 10 times. Each time, 10000 LTE2B frames are sent and the statistical results are obtained.

To demonstrate the generality of TDE, we also evaluate TDE with other technologies, e.g., WiFi and BLE in Section 6.9 and 6.10.



(a)

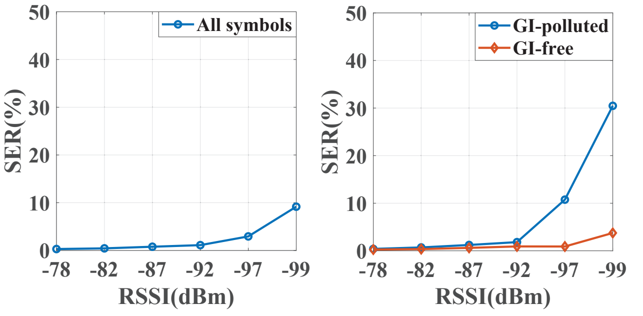
(b)

Figure 19: Hamming Distance (a) TDE (b) FDE.

6.3 Chip Error Rate

Chip is the basic unit in ZigBee demodulation. ZigBee receiver collects 32 ZigBee chips and maps them to the nearest ZigBee symbol with minimum chip errors in Hamming distance. To examine the accuracy of the time-domain signal emulation, we emulate random ZigBee frames with both LTE2B (TDE-QPSK) and WEBee (FDE-QPSK) and collect chip errors in the received ZigBee symbols. We use Nexus 5X as LTE2B transmitter and USRP B210 as WEBee transmitter. The received signal strength at ZigBee side is fixed to -72dBm. As depicted in Fig.19(a), 80% symbols have no chip errors while the rest have tolerable chip errors caused by guarding intervals (GI). While one GI overlaps with 9 chips, our empirical study shows it only flip at most 6 chips, which can be corrected by DSSS. In contrast, as shown by Fig.19(b), FDE causes significantly more chip errors. Symbols emulated by FDE may suffer from 14 chip errors, which definitely lead to demodulation failure. In order to improve the accuracy of emulation and produce demodulatable ZigBee signal, WEBee fix the modulation scheme of WiFi to 64QAM. In contrast, LTE2B works well under any modulation schemes that LTE supports and is well suitable for LTE system where the modulation schemes are dynamically controlled by the base station.

This gives us an interesting insight that emulating OQPSK signal defined in *time domain* directly via QAM samples that are also in time-domain can yield significantly fewer emulation errors than approximating the converted *frequency domain* version of the signal using frequency-domain QAM.



(a) (b)

Figure 20: Symbol Error Ratio (a) All symbols (b) GI-polluted vs. GI-free Symbols.

6.4 Symbol Error Rate

In ZigBee, one symbol error leads to CRC check failure and thus failure of the whole packet. Hence symbol error rate (SER) is an important criterion of the accuracy of signal emulation. We collect the SER of ZigBee frames emulated by LTE2B in a wide range of received signal strengths (RSSI). Fig.20(a) demonstrates that LTE2B achieves nearly zero SER when RSSI is as low as -92dBm. SER begins to increase when RSSI goes below -92dBm, which coincides with the increase of error rate for those symbols overlapped with guarding interval as shown in Fig.20(b). In contrast, SER of GI-free symbols remains stable, which again demonstrate the stability of TDE. As the positions of GI are fixed, the application of LTE2B may optionally forbid the usage of these vulnerable symbols or adopt coding technology to reduce the frame errors. In contrast, the majority of symbols in FDE-QPSK emulated ZigBee frame have more than eight chip errors even in the high RSSI (-72dBm) as demonstrate in Fig.19(b). Thus most of them fail to be demodulated at ZigBee receiver.

6.5 Frame Reception Rate

The section evaluates the performance of the frame reception rate (FRR) by conducting experiments with LTE2B, WEBee and standard ZigBee under varied settings. One frame is considered lost if any received symbol is wrong.

6.5.1 *Impact of RSSI (vs. FDE & Standard ZigBee).*

Fig.21 compares the frame reception rate of LTE2B frames, WEBee frames and the standard ZigBee frames under the same RSSI. Since FDE introduces high quantization errors, it is not feasible for emulating ZigBee signal with QPSK modulation. Instead, WEBee frames are generated with FDE-64QAM, a much higher modulation scheme than QPSK with dense QAM points for reducing the quantization errors. It is clear that when RSSI is above -92dBm, LTE2B achieves the same performance as the standard ZigBee. The FRR of both LTE2B and standard ZigBee drops at -92dBm. LTE2B's FRR drops faster mainly due to the increasing failures in GI-polluted symbols discussed in section 6.4. In the extremely low SNR (i.e, -99dBm), ZigBee receiver can still receive 25% of LTE2B frames. In contrast, even with 64QAM, the FRR of WEBee drops dramatically when RSSI is below -80dBm. This result demonstrates that TDE is inherently more reliable than FDE when emulating the IoT signal.

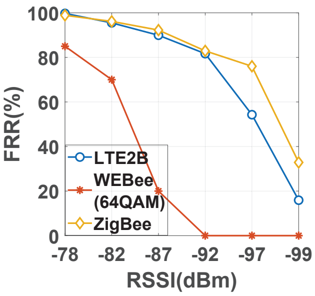


Figure 21: FRR vs. RSSI.

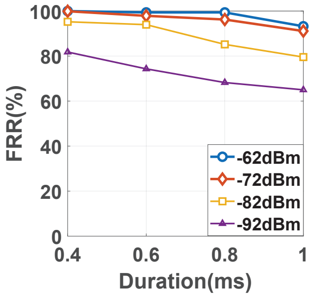


Figure 22: FRR vs. Duration.

6.5.2 *Impact of Frame Duration.*

In the previous experiment, we fix the duration of frames to be 0.42ms, which is the maximum length achievable for the emulated signal in commodity LTE UE. To further evaluate the performance of our time-domain emulation method, we use MATLAB LTE System toolbox [26] to generate emulated ZigBee signal with various lengths and transmit via USRP. As Fig. 22 shows, the impact of frame length on the FRR is almost negligible when signal strength is high. When the receive signal strength is low ($\leq -92dBm$), increasing frame duration shows more impact on frame errors, which is clearly because the longer frame overlaps with more guarding intervals.

6.6 LTE2B Performance: Indoor and Outdoor

In this section, we evaluate LTE2B in various real-life scenarios. The transmission power of LTE UE is about 16dBm. Note that this 16dBm is legitimate in LTE standards, while the maximum allowed power for UE is 23dBm. Also, 16dBm conforms to FCC's requirement on transmission power in the unlicensed band (typically 30dBm) and complies with ZigBee or BLE standard.

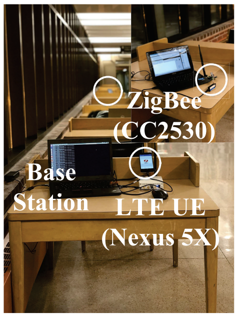


Figure 23: Hallway

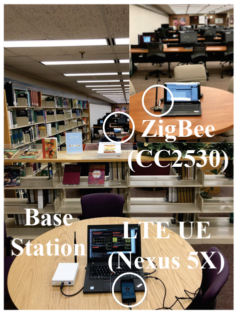


Figure 24: Library

We first compare the indoor performance of LTE2B with WEBee in two settings, i.e., hallway (LOS, depicted in Fig.23) and library (NLOS, depicted in Fig.24). For a fair comparison, the transmission power of WEBee is also configured to be 16dBm. Fig.25 demonstrates that in all the distances, LTE2B achieves above 97% FRR. Thus, with one LTE device, we can control all IoT devices equipped with low power ZigBee on a large scale. We also notice that the indoor FRR of LTE2B is significantly higher than WEBee [23] (50%) while the LTE2B uses much lower modulation schemes than WEBee. This demonstrates the benefit of TDE in both applicability and reliability.

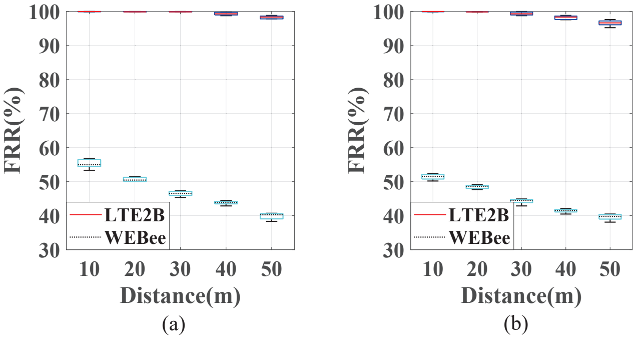


Figure 25: Indoor FRR (a) Hallway (b) Library.

One key advantage of LTE2B is long distance (supporting outdoor applications in the scale). So we extensively evaluate the gain of communication range from LTE2B in the outdoor environment by comparing it with a commodity ZigBee transmitter with 1dBm maximum transmission power. Fig.26 depicts the outlook of the experiment scenario, which is a 1340-foot long bridge. For a fair comparison, we fix both the CC2530 transmitter and LTE UE at the one end of the bridge, while moving ZigBee receiver to the other end. The FRR experiments are tested every 15 meters.

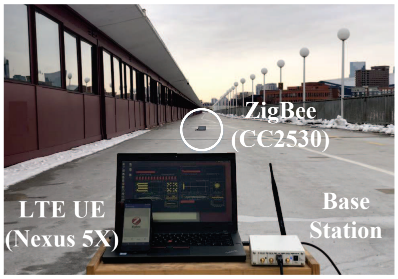


Figure 26: Outdoor Experiment Site

Fig.27 demonstrates the frame reception ratio for both standard ZigBee communication from CC2530 and LTE2B at different distances. It is clear that the standard ZigBee has limited transmission distance: the maximum communication range is 120m. In contrast, LTE2B is able to deliver the ZigBee message to a much longer distance. For example, LTE2B achieves an FRR of 94% at a distance of 180m, while it still manages to maintain 52% FRR at 400m. This huge distance discrepancy demonstrates that LTE2B can cover IoT sensors in large scale in one hop. This unique benefit removes the requirement of relay nodes in the ZigBee network, which significantly reduces the hardware cost, and maintenance cost. In addition, LTE2B also removes the bottleneck problem on the relay nodes, improving the overall system life time.

6.7 Repeated Transmission

Because of the accurate signal emulation, LTE2B works extremely reliably in the indoor scenarios and outdoor scenarios when the communication distance is less than 180m. To further support reliable communication for longer distance, e.g., 400m, we can transmit LTE2B frame multiple times for improving the overall reliability. Fig.28 shows the frame reception ratio of LTE2B frame with varying number of transmission at the 4 different distances, from 250 m to 400 m. Specifically, LTE2B can achieve 99% frame reception rate via repeating the frame 3 times for 300m and 4 times for 400m, demonstrating the reliable communication of LTE2B. In addition to the transmission distance, we also study the performance of retransmission for frames with different durations. In this experiment, the transmission distance between the sender and receiver is fixed to 400m, while LTE2B transmits frames from 0.4 ms to 1 ms. From Fig.29, we can see repeated transmission performs similarly for these 4 frame durations, suggesting that LTE2B's robust performance.

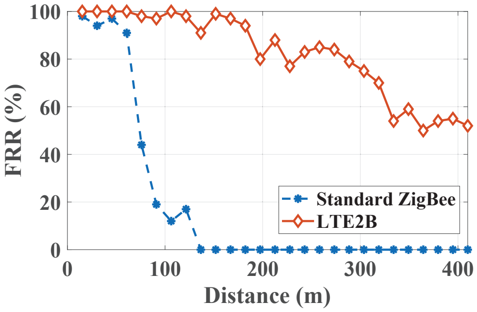


Figure 27: FRR vs. Distances

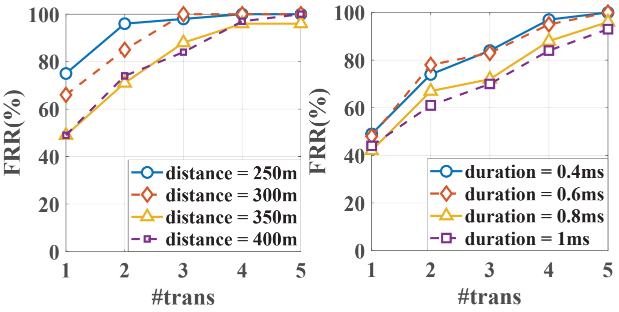


Figure 28: FRR vs. Tx Distance (retransmission)

Figure 29: FRR vs. Frame Duration (retransmission)

6.8 LTE2B Performance: Mobility

LTE2B is designed to work with the mobile applications. For example, with LTE2B ambulances equipped with in-vehicle LTE can directly control the ZigBee traffic lights. In this experiment, we test mobility performance LTE2B with different moving speeds: walking (4mph), bicycling (10mph) and driving (30mph). Moreover, the ZigBee receiver performs low power listening with varying duty cycle ratios, e.g., the ZigBee turn off the wireless radio periodically for preserving energy, while one LTE2B frame is repeated 50 times from the smartphone. In Fig.30, we demonstrate that when the user walk or bicycle, 5% duty cycle ratio is enough to guarantee reliable message delivery from LTE2B to ZigBee sensors at low power mode. Even in the driving scenarios with the moving speed of 30 mph, LTE2B achieves reliable communication with only 10% duty cycle ratio. This series of experiments demonstrate the reliability of TDE in LTE2B, and the potential deployment of LTE2B for emerging mobile IoT applications, e.g., smart city and autonomous driving.

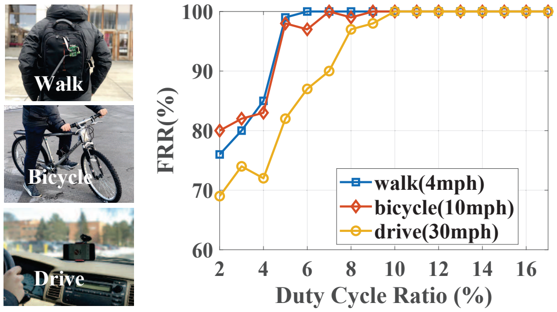


Figure 30: FRR in Mobility and Duty Cycle

6.9 LTE2B in Bluetooth Low Energy

In addition to the emulation of OQPSK ZigBee signal, we also implement LTE2B to enable the CTC from LTE to Bluetooth Low Energy (BLE) following the TDE described in Section 4. This emulation of Gaussian frequency shift keying (GFSK) waveform demonstrates that the TDE is generic and can be generally applied to various scenarios for enabling CTC. Note that although existing commodity smartphones generally adopt BLE transceivers, LTE transceivers with the higher transmission power (23dBm) can significantly improve the coverage of BLE signal, which will come in handy in the applications such as advertising, neighbor discovery and control, while commodity BLE receivers generally have limited transmission energy. In addition, the emerging LTE-based Multefire devices in the 2.4 GHz band may not be equipped with BLE transceivers[27], while LTE2B enables direct communication among them.

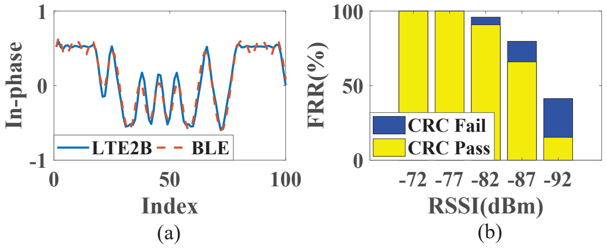


Figure 31: LTE2B in BLE (a) Emulation (b) FRR.

In Fig.31, we demonstrate the emulated GFSK waveform of BLE and frame reception ratio of a 14 Bytes BLE advertisement frame. BLE does not provide redundancy mechanism (e.g., DSSS) and thus any bit error will lead to packet corruption. Due to the simplicity of GFSK in the time domain, TDE is able to emulate it accurately. Thus, with high RSSI, i.e., above -77 dBm, LTE2B is able to achieve 100% FRR, while still offering good reliability in low RSSI conditions.

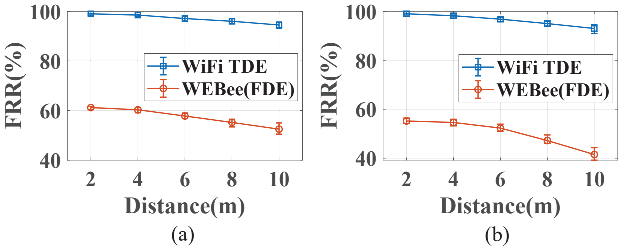


Figure 32: FRR WiFi TDE vs FDE (a) ZigBee (b) BLE.

6.10 Time-Domain Emulation in WiFi

Time-domain emulation is a generic method that can be applied to other technology, i.e., WiFi. Besides OFDM modulation for FDE, commodity WiFi devices also support DSSS/CCK modulation that can be utilized for TDE. Due to the space limitation, we omit the implementation details and demonstrate the performance with CC3200 commodity WiFi in this section. In Fig. 32, we compare the frame reception ratio of emulated ZigBee and BLE signal using TDE (802.11 QPSK-CCK) and FDE (802.11 64QAM). In both cases, TDE significantly outperforms FDE even if the modulation scheme, i.e., QPSK is much lower. This further proofs that TDE is a generic technique that dramatically improve the accuracy of CTC.

6.11 Application

In this section, we implement LTE2B to control the color and intensity of a ZigBee-equipped light bulb for demonstrating its potential benefits. When receiving the ZigBee control messages from users, the ZigBee sensor adjusts the light bulb to a specific color and light intensity. To enable CTC, LTE2B is running as an Android application in the application layer, and receives the user commands for computing the payload in the UDP packet used for emulation. Following Section 4 and Section 5, LTE2B computes the needed LTE payload for any ZigBee control messages, and then transmit this packet for emulating the ZigBee waveform. Our experiments validate that LTE2B achieves reliable control of the lighting condition of the smart bulb in real-time, suggesting that LTE2B can be directly applied to emerging IoT applications.

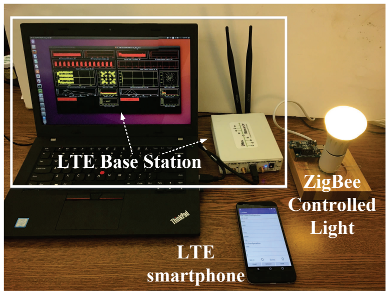


Figure 33: Light Control Application of LTE2B

7 RELATED WORK

Traditional research on wireless coexistence focused mostly on inference avoidance, cancellation, and detection [4, 6, 7, 11–14, 16, 18, 21, 24, 25, 29–31, 33–38, 41–47]. Recently Cross-technology communications (CTC) has emerged as a promising mechanism for explicit coordination and collaboration between heterogeneous wireless communications. Based on the principles, in early designs, the wireless sender transmits packets for creating the unique energy pattern in the wireless channel, e.g., FreeBee [22], Esense [10] and GSense [44]. Although effective, these methods suffer from the low data rate due to the limited energy sample rate. To remedy this drawback, the recent advances in CTC [8, 19, 20, 23] directly emulate the targeted signal, so that the emulated signal can be recognized as the legacy communication at the target receiver. Among them, WEBee [23] is the first to generate ZigBee signals by emulating the target ZigBee waveform at the WiFi sender. Since WEBee is based on frequency domain emulation (FDE), it inherently suffers from high quantization errors during the emulation procedure, and lose near half of the transmitted CTC packets. The recent work [17] introduces digital emulation to improve performance of WEBee, which still suffers from the errors due to FDE. In addition, the work in [8] takes advantage of the LTE downlink PHY to emulate WiFi CTS packets for reducing the cross-technology interference. However, this design requires modification of the LTE stack, since it essentially by-passes the LTE protocol constraints (e.g., header, CRC and coding constraints). The work in [19, 20] achieves CTC between BLE and ZigBee by taking advantage of the phase shift in ZigBee and BLE communication, and is different from directly emulating the waveform in LTE2B.

LTE2B is first to introduce the time-domain emulation (TDE). By adopting idea of TDE, LTE2B significantly reduces the quantization errors, leading to more reliable CTC. In addition, LTE2B is fully compliant with the LTE standard, which is achieved by penetrating through the complicated LTE stack with a set of constraints such as misaligned sample rates, subcarrier mapping, and CRC pollution in reverse turbo coding. Note that LTE2B doesn't require modification of both hardware and firmware as evidenced by our implementation on the commodity WAN and PAN devices.

8 CONCLUSION

This paper presents LTE2B, the first work that bridges the WAN technology (e.g., LTE) with PAN technology (e.g., ZigBee and BLE). In contrast with previous CTC approaches with high errors in the frequency domain, LTE2B comes up with time-domain emulation for offering reliable CTC even with limited modulation schemes such as QPSK. To realize time-domain emulation in the LTE system, LTE2B tackles several practical challenges so that it is completely compliant with existing standards and has been implemented in commercial COTS devices (e.g., LG Nexus 5X) with > 99% accuracy over a long distance (e.g., 400m). We also demonstrate the feasibility of using the IP payload via a commercial smartphone to control and configure a commodity ZigBee-enabled light bulb.

9 ACKNOWLEDGEMENTS

This work was supported by the NSF CNS-1525235, NSF CNS-1718456 and NSF CNS-1717059. We sincerely thank the shepherd and reviewers for their valuable comments.

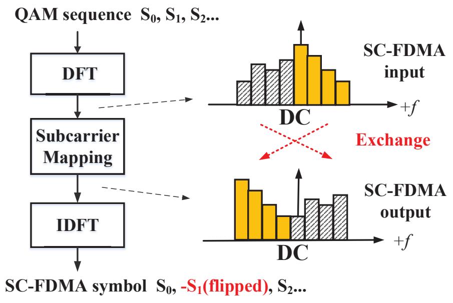


Figure 34: Subcarrier Mapping in SC-FDMA.

APPENDIX

This section analyzes the SC-FDMA modulation. With a time-domain signal, LTE first computes the frequency components of this time-domain signal using DFT, and then exchanges the positive and negative frequency components, followed by the inverse-DFT to generate the final time-domain signal. Due to the exchange of the positive and negative frequency components shown in Fig. 34, the positive components in the input signal become negative components in the output while the original negative components become the DC and positive components, leading to a different waveform. Specifically, the QAM points with odd indices are flipped around the origin, which is theoretically proofed as follows.

Proof. By Inverse Fourier Transform (IDFT) theorem, a N-point IDFT represent the relationship between time-domain samples and frequency components as:

$$x[n] = \frac{1}{N} \times \sum_{k=0}^{N-1} f[k] e^{j\frac{2\pi k \times n}{N}}, n = 0 \dots N-1 \tag{2}$$

, where $x[n]$ is the n^{th} samples in the time domain, $f[k]$ is the k^{th} component in the frequency domain, and $f[0]$ is the DC component. For each $x[n]$, the summation in equation 2 can be rewritten as:

$$x[n] = \frac{1}{N} \times \sum_{k'=0}^{\frac{N}{2}-1} (f[k'] + f[k' + \frac{N}{2}] \times e^{j\pi n}) \times e^{j\frac{2\pi k' \times n}{N}} \tag{3}$$

, where we group all the frequency components into $\frac{N}{2}$ pairs, each of which contains one positive component $f[k']$ and one negative component $f[k' + \frac{N}{2}]$. The coefficient of negative component (i.e., $e^{j\pi n}$) equals 1 when n is even and equals -1 when n is odd. Thus according to the index n, we further rewrite $x[n]$ as:

$$x[n] = \begin{cases} \frac{1}{N} \sum_{k'=0}^{\frac{N}{2}-1} (f[k'] + f[k' + \frac{N}{2}]) e^{j\frac{2\pi k' \times n}{N}} & n \text{ is even} \\ \frac{1}{N} \sum_{k'=0}^{\frac{N}{2}-1} (f[k'] - f[k' + \frac{N}{2}]) e^{j\frac{2\pi k' \times n}{N}} & n \text{ is odd} \end{cases} \tag{4}$$

Now, consider the exchange of positive and negative frequency components, which creates a new signal $\bar{x}[k], k = 0, \dots, N-1$, whose frequency components $\bar{f}$ satisfy:

$$\begin{aligned} \bar{f}[k'] &= f[k' + \frac{N}{2}], k' = 0, \dots, \frac{N}{2} - 1 \\ \bar{f}[k' + \frac{N}{2}] &= f[k'], k' = 0, \dots, \frac{N}{2} - 1 \end{aligned} \tag{5}$$

Substituting Equation 5 into Equation 4 shows the key conclusion that $\bar{x}[n]$ is equivalent to $x[n]$, when n is even and $\bar{x}[n]$ equals $-x[n]$ when n is odd.

$$\begin{aligned} \bar{x}[n] &= x[n] \quad \textit{n is even} \\ \bar{x}[n] &= -x[n] \quad \textit{n is odd} \end{aligned} \tag{6}$$

This proves that SC-FDMA will flip the QAM points with odd indices while leaving QAM points with even indices intact, so that LTE2B is able to pre-process the QAM points for accurately emulating the target ZigBee/BLE waveform. Note that the previous proof is based on the assumption that the DFT and IDFT have the same size, while the size of DFT is determined by the actual UE bandwidth and the IDFT size is fixed. Since the UE bandwidth is allocated by the LTE base station, the actual size of the DFT might be smaller than IDFT. As for this situation, the emulated waveform is downsampled from the ideal waveform, where Section 4 demonstrates LTE2B's reliable emulation from 1.08 MHz (smaller than the ZigBee's 2 MHz bandwidth) to 4.5 MHz.

□

REFERENCES

[1] *LTE2B supplementary material.* Available at https://github.com/liux4189/LTE2B.

[2] E. U. T. R. Access. 3gpp ts 36.322 v10. 0.0, dec. 2012. *LTE Advanced*.

[3] E. U. T. R. Access. Multiplexing and channel coding (release 8), 3gpp ts 36.212 v8. 7.0, 2009.

[4] F. Adib, S. Kumar, O. Aryan, S. Gollakota, and D. Katabi. Interference alignment by motion. In *MobiCom '13*, pages 279–290. ACM, 2013.

[5] M. Alliance. Multefire release 1.0 technical paper: A new way to wireless. *white paper, Jan*, 2017.

[6] P. Bahl, R. Chandra, T. Moscibroda, R. Murty, and M. Welsh. White space networking with wi-fi like connectivity. *ACM SIGCOMM Computer Communication Review*, 39(4):27–38, 2009.

[7] T. Bansal, B. Chen, P. Sinha, and K. Srinivasan. Symphony: Cooperative packet recovery over the wired backbone in enterprise wlans. In *Proceedings of the 19th annual international conference on Mobile computing & networking*, pages 351–362. ACM, 2013.

[8] E. Chai, K. Sundaresan, M. A. Khojastepour, and S. Rangarajan. Lte in unlicensed spectrum: are we there yet? In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, pages 135–148. ACM, 2016.

[9] K. Chebrolu and A. Dhekne. Esense: Communication through energy sensing. In *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, MobiCom '09, pages 85–96, 2009.

[10] K. Chebrolu and A. Dhekne. Esense: Communication through energy sensing. In *MobiCom '09*, pages 85–96. ACM, 2009.

[11] B. Chen, Y. Qiao, O. Zhang, and K. Srinivasan. Airexpress: Enabling seamless in-band wireless multi-hop transmission. In *MobiCom '15*, pages 566–577. ACM, 2015.

[12] B. Chen, V. Yenamandra, and K. Srinivasan. Interference alignment using shadow channel. In *INFOCOM 2015*, pages 2128–2136. IEEE, 2015.

[13] L. Chen, R. Fan, K. Bian, M. Gerla, T. Wang, and X. Li. On heterogeneous neighbor discovery in wireless sensor networks. In *INFOCOM '15*, pages 693–701. IEEE, 2015.

[14] W. Du, J. C. Liando, H. Zhang, and M. Li. Pando: Fountain-enabled fast data dissemination with constructive interference. *IEEE/ACM Transactions on Networking*, 25(2):820–833, 2017.

[15] D. Evans. The internet of things how the next evolution of the internet is changing everything, 2011. http://www.cisco.com.

[16] S. Gollakota, S. D. Perli, and D. Katabi. Interference alignment and cancellation. In *ACM SIGCOMM Computer Communication Review*, volume 39, pages 159–170. ACM, 2009.

[17] X. Guo, Y. He, J. Zhang, and H. Jiang. Wide: Physical-level ctc via digital emulation. In *Proceedings of the 18th International Conference on Information Processing in Sensor Networks*, IPSN '19, pages 49–60, New York, NY, USA, 2019. ACM.

[18] T. Hao, R. Zhou, G. Xing, M. W. Mutka, and J. Chen. Wizsync: Exploiting wi-fi infrastructure for clock synchronization in wireless sensor networks. *IEEE Transactions on mobile computing*, 13(6):1379–1392, 2014.

[19] W. Jiang, S. M. Kim, Z. Li, and T. He. Achieving receiver-side cross-technology communication with cross-decoding. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, pages 639–652. ACM, 2018.

[20] W. Jiang, Z. Yin, R. Liu, Z. Li, S. M. Kim, and T. He. Bluebee: a 10,000x faster cross-technology communication via phy emulation. In *Sensys '17*. ACM, 2017.

[21] T. Jin, G. Noubir, and B. Sheng. Wizi-cloud: Application-transparent dual zigbee-wifi radios for low power internet access. In *INFOCOM, 2011 Proceedings IEEE*, pages 1593–1601. IEEE, 2011.

[22] S. M. Kim and T. He. Freebee: Cross-technology communication via free side-channel. In *The 21st Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2015.

[23] Z. Li and T. He. Webee: Physical-layer cross-technology communication via emulation. In *MobiCom '17*. ACM, 2017.

[24] C.-J. M. Liang, N. B. Priyantha, J. Liu, and A. Terzis. Surviving wi-fi interference in low power zigbee networks. In *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*, pages 309–322. ACM, 2010.

[25] R. Mahindra, H. Viswanathan, K. Sundaresan, M. Y. Arslan, and S. Rangarajan. A practical traffic management system for integrated lte-wifi networks. In *Proceedings of the 20th annual international conference on Mobile computing and networking*, pages 189–200. ACM, 2014.

[26] "MATLAB". Matlab lte system toolbox., 2018. https://www.mathworks.com/help/lte.

[27] multefire.org. MutleFire whitepapers. https://www.multefire.org/white-papers/, 2019.

[28] N. Nikaein, M. K. Marina, S. Manickam, A. Dawson, R. Knopp, and C. Bonnet. Openairinterface: A flexible platform for 5g research. *SIGCOMM Comput. Commun. Rev.*, 44(5):33–38, Oct. 2014.

[29] G. Nikolaidis, M. Handley, K. Jamieson, and B. Karp. Copa: cooperative power allocation for interfering wireless networks. In *Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies*, page 18. ACM, 2015.

[30] B. Radunović, R. Chandra, and D. Gunawardena. Weeble: Enabling low-power nodes to coexist with high-power nodes in white space networks. In *Proceedings of the 8th international conference on Emerging networking experiments and technologies*, pages 205–216. ACM, 2012.

[31] S. Rathinakumar, B. Radunovic, and M. K. Marina. Cprecycle: Recycling cyclic prefix for versatile interference mitigation in ofdm based wireless systems. In *Proceedings of the 12th International on Conference on emerging Networking EXperiments and Technologies*, pages 67–81. ACM, 2016.

[32] T. Richardson and R. Urbanke. *Modern Coding Theory.* Cambridge University Press, New York, NY, USA, 2008.

[33] A. Saifullah, M. Rahman, D. Ismail, C. Lu, R. Chandra, and J. Liu. Snow: Sensor network over white spaces. In *SenSys '16*, 2016.

[34] A. Saifullah, M. Rahman, D. Ismail, C. Lu, J. Liu, and R. Chandra. Enabling reliable, asynchronous, and bidirectional communication in sensor networks over white spaces. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*, page 9. ACM, 2017.

[35] S. Sen, R. Roy Choudhury, and S. Nelakuditi. No time to countdown: Migrating backoff to the frequency domain. In *MobiCom '11*, pages 241–252. ACM, 2011.

[36] S. Sen, N. Santhapuri, R. R. Choudhury, and S. Nelakuditi. Successive interference cancellation: Carving out mac layer opportunities. *IEEE Transactions on Mobile Computing*, 12(2):346–357, 2013.

[37] K. Sundaresan, S. V. Krishnamurthy, X. Zhang, A. Khojastepour, S. Rangarajan, et al. Trinity: A practical transmitter cooperation framework to handle heterogeneous user profiles in wireless networks. In *MobiHoc '15*, pages 297–306. ACM, 2015.

[38] C. Vlachou, I. Pefkianakis, and K.-H. Kim. Lteradar: Towards lte-aware wi-fi access points. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 2(2):33, 2018.

[39] K. Wu, H. Tan, Y. Liu, J. Zhang, Q. Zhang, and L. M. Ni. Side channel: Bits over interference. *IEEE Transactions on Mobile Computing*, 11(8):1317–1330, 2012.

[40] Q. L. Yifan Zhang. Howies: A holistic approach to zigbee assisted wifi energy savings in mobile devices. In *Proceedings of the 32nd IEEE International Conference on Computer Communications (INFOCOM 2013)*, 2013.

[41] S. Yun and L. Qiu. Supporting wifi and lte co-existence. In *Computer Communications (INFOCOM), 2015 IEEE Conference on*, pages 810–818. IEEE, 2015.

[42] X. Zhang and K. G. Shin. Enabling coexistence of heterogeneous wireless systems: Case for zigbee and wifi. In *MobiHoc '11*, page 6. ACM, 2011.

[43] X. Zhang and K. G. Shin. Cooperative carrier signaling: Harmonizing coexisting wpan and wlan devices. *IEEE/ACM Transactions on Networking*, 21(2):426–439, 2013.

[44] X. Zhang and K. G. Shin. Gap sense: Lightweight coordination of heterogeneous wireless devices. In *INFOCOM, 2013 Proceedings IEEE*, pages 3094–3101. IEEE, 2013.

[45] R. Zhou, Y. Xiong, G. Xing, L. Sun, and J. Ma. Zifi: wireless lan discovery via zigbee interference signatures. In *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, pages 49–60. ACM, 2010.

[46] W. Zhou, T. Bansal, P. Sinha, and K. Srinivasan. Bbn: throughput scaling in dense enterprise wlans with bind beamforming and nulling. In *MobiCom '14*, pages 165–176. ACM, 2014.

[47] W. Zhou, T. Das, L. Chen, K. Srinivasan, and P. Sinha. Basic: backbone-assisted successive interference cancellation. In *MobiCom '16*, pages 149–161. ACM, 2016.