APPROVAL SHEET

Title of Thesis: Monitoring Humans and Improving Wireless Network Performance with Heterogenous IoT Devices

Name of Candidate: Yan Li
Doctor of Philosophy, 2018

Thesis and Abstract Approved: _____

Ting Zhu
Associate Professor
Department of Computer Science and
Electrical Engineering

Date Approved: _____

ABSTRACT

Title of Thesis: Monitoring Humans and Improving Wireless Network Performance with Heterogenous IoT Devices

Yan Li, Doctor of Philosophy, 2018

Thesis directed by: Ting Zhu, P.h.D
Department of Computer Science and
Electrical Engineering

According to Gartner, the number of the internet of things (IoT) devices is growing exponentially to reach 26 billion by 2020. IoT devices are being designed to be used in smart building for vastly different applications such as automation, security, industrial controls, and life-saving health monitor. To be cost-effective and utilize existing infrastructure, these IoT devices must utilize the vast amount of existing radio frequency (RF) for human monitoring, movement tracking, and identification information. Moreover, these IoT devices use different radios and protocols to communicate due to different cost, data-rate, communication-range, frequency occupancy, and energy consumption requirements. Thus, these devices cannot directly communicate with each other while occupying the same frequency bands. Therefore, IoT networks face two challenges: privacy-preserving monitoring, tracking, and identification and efficient heterogeneous radio coexistence.

These challenges raise fundamental questions: 1) How can we use these IoT signals to monitor, track, and identify people in a privacy-preserving manner? 2) How can IoT devices that use different radios, frequencies, and modulation mechanisms (e.g., WiFi and ZigBee) communicate efficiently (increase throughput, lower energy usage, and lower latency) with each other?

The promising techniques to address these questions are to 1) perform channel state measurements between transmitter and receivers, 2) create hybrid WiFi-ZigBee

subcarriers on the overlapped channel, and 3) recycle signals by leveraging low power consumption backscatter radios. By sensing channel state information (CSI), WiFi radios can produce human monitoring and tracking signatures based on the Doppler Effect and multipath signals without attached devices and out of direct line-of-sight. Moreover, we determine that combination of the CSI and hybrid WiFi-ZigBee subcarriers allow for concurrent bidirectional ZigBee and WiFi communication. Leveraging the same WiFi-ZigBee hybrid subcarriers, devices can produce signals allowing for ultra-low power backscatter radios.

This thesis addresses these challenges by making the following contributions: Wobly allows for privacy-preserving tracking and positioning based on human gait using Wi-Fi CSI. Moreover, we can identify specific human body movements. Chiron enables concurrently transmitting (or receiving) 1 stream of WiFi data and up to 4 streams of ZigBee data to (or from) commodity WiFi and ZigBee devices as if there is no interference between these simultaneous connections due to CSI sensing. Passive-ZigBee demonstrates we can transform an existing productive WiFi signal into a ZigBee packet for a CoTS low-power consumption receiver. Moreover, this low power backscatter radio can bridge between the ZigBee and WiFi devices by relaying data allowing heterogenous radios to communicate with each other.

Our empirical evaluations show that i) Wobly correctly identifies at a rate of 87% and localizes rate of 90%. ii) Chiron's concurrent WiFi and ZigBee communication can achieve similar throughput as the sole WiFi or ZigBee communication. Chiron's spectrum utilization is more than 16 times better than a traditional IoT gateway. iii) Passive-ZigBee consumes 1,440 times lower power compared to traditional ZigBee while able to maintain maximum ZigBee standard network throughput. Passive-ZigBee also can relay data between WiFi and ZigBee networks.

Monitoring Humans and Improving Wireless Network Performance with Heterogenous IoT Devices

by
Yan Li

Thesis submitted to the Faculty of the Graduate School
of the University of Maryland in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2018

ACKNOWLEDGMENTS

I first want to thank my advisor, Dr. Ting Zhu, who taught me how to write concisely and clearly, think critically, and conduct relevant research. Dr. Ting Zhu has taught me how to write motivations and define research scope by thinking critically research strategies and proposals.

I want to thank my supporters at the Johns Hopkins Applied Physics Laboratory (APL). Specifically, Albert Tomko who taught about physics, communication, and propagation theories. My group supervisor, Mike Silberglit, who found funding for my travels and conference fees. Other people at APL includes James Sari, who provided theories and applications in physics, and Andrew Adams, who provided insight to machine learning algorithms.

I want to thank my wife, Alexis Li, for her support and love. She proofread a lot of my papers and was extremely patient with me while taking care of my daughter, Elliana Li.

I want to thank the students and coauthors who brainstormed and contributed to the papers. Specifically, I want to thank Zicheng Chi, Yao Yao, Xin Liu, Wei Wang, Tiantian Xie, Hongyu Sun, Zheng Lu, and Zhichuan Huang. Thank you for the brainstorming sessions that produced novel ideas.

I want to thank University of Maryland Baltimore County and their countless professors for the flexibility that allowed me to complete my degree with flexibility. Working full time and being on travel on the other side of the world required me to Skype into classes many times.

Yan Li

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

INTRODUCTION

1.1 Background and Motivation

The number of Internet-of-Things (IoT) devices will grow exponentially to reach 26 billion by 2020 and 1 trillion by 2025. Each person will touch or use 300 to 500 smart devices every day by 2032. Based on the Cisco Global Cloud Index, the data created by these devices will reach 42.3 ZB (i.e., 4.23×10^{22} bytes) per month and will be 49 times higher than total data center traffic by 2019. Thus, wireless communication and signal processing at the edge of the of the network must be efficient. To be efficient, these devices must 1) use existing productive signals for sensing and monitoring and 2) coexists together. However, because of the various applications, these devices use a variety of radios. The effects caused by these devices are that 1) they generate huge amount of radio frequency (RF) traffic that enable human tracking and activity sensing and 2) the heterogenous radios contain inefficiencies caused by the radios using different protocols.

1.1.1 IoTs Identifying, Tracking, and Sensing Human

Traditional human tracking systems employ image recognition through direct line-of-sight, thus requiring excess infrastructure for computer vision. Floor sensors,

wall attachments, and accelerometers (Guha et al. (2012)) are used to measure human activity. Devices like radio-frequency identification (RFID) (Ranjan, Juhi, & Yu (2013)), door sensors, and ultrasonic sensors (Hnat et al. (2012)) also track persons. These sensors are cumbersome, requiring installation or personal attachment. Micro-radars (Lyonnet (2010)) achieve tracking and localization by utilizing special signals that cause undesired interference.

To solve the issue of excess infrastructure, smart wireless or Internet of Things (IoT) and corresponding technologies devices have also been used to sense environment (Wei (2015) Zhu et al. (2015) Oppermann, Boano, & Römer (2014) Galstyan et al. (2004), humans Xiong (2015) Adib (2013) Adib (2015) Liu et al. (2014)), and movement (Chen (2015) Luong et al. (2015) Pu et al. (2013)). These sensing devices advance in two categories: 1) antenna and 2) signal processing designs. In the first category, the use of directional, horn antennas by IoT devices have gained popularity. These antennas are used in a variety of modern telecommunication systems. Previous research utilized directional antennas to improve localization accuracy by providing angular information in Wi-Fi networks (Varshney, Voigt, & Mottola (2013)) and improving throughput by directing and localizing energy. In the second category, researchers have applied advanced signal processing technologies on Wi-Fi-based IoT devices (Jayakumar et al. (2014)), which leverages Orthogonal frequency-division multiplexing (OFDM) for its ability to penetrate walls. For example CARM (Wang et al. (2015)) and WiTrack (Adib et al. (2014)) detect human activities and localize individuals behind walls using Radio Frequency (RF). However, these approaches cannot identify individual people. Different from previous approaches, we use angular and polarity features provided by a directional horn antenna to detect and identify humans and their activities behind a wall.

Therefore, the use of IoT's RF signals motivates the problem of tracking and

sensing humans without attached devices using existing deployed devices in a manner that preserves privacy.

1.1.2 IoTs Communication Protocols

Because of the large amount of data generated by IoT devices, we must process this data near the edge of the network rather than be transmitted to the data center. In edge computing, it is extremely important to efficiently collect the huge amount of data generated by these densely deployed IoT devices at the edge (e.g., gateway) of the network. Because most of these IoT devices are using the shared industrial, scientific, and medical (ISM) band, the ever-growing number of IoT devices and the huge amount of data generated by these devices will cause the ISM 2.4 GHz band extremely crowded. This issue is becoming worse at the gateway side because all the data from heterogeneous IoT networks needs to be sent to the gateway through the overlapped wireless channels. To avoid WiFi packets colliding with ZigBee and BLE packets at the gateway, traditional approaches use either carrier-sense multiple access (CSMA) or time division multiple access (TDMA). As shown in Figure 1.1, which is a waterfall figure obtained from a spectrum analyzer, ZigBee and WiFi devices are competing for the overlapped channel access. Since the ZigBee device uses only 2 MHz bandwidth (compared to 20 MHz bandwidth of WiFi), when the ZigBee device is transmitting (the red colored box in Figure 1.1), the WiFi device's transmissions have to stop (the black colored box in Figure 1.1) because of the CSMA scheme. Thus, when the ZigBee device is transmitting, the spectrum from 2.432 GHz to 2.447 GHz (highlighted in the white color dashed box in Figure 1.1) is wasted.

However, these approaches have two limitations: i) in the time domain, only one device is able to send the packets to the gateway at any given time. For example, if a ZigBee device is sending packets to the gateway, the WiFi HQ video camera needs

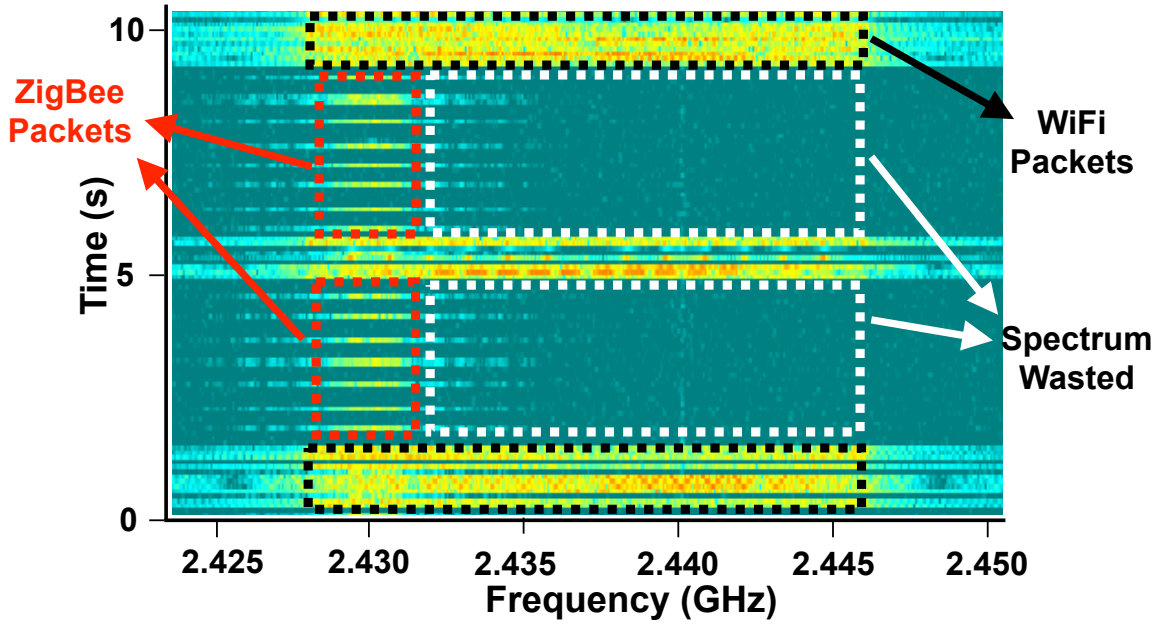


Fig. 1.1: A waterfall figure to demonstrate the low spectrum utilization among WiFi and ZigBee devices.

to wait. This will introduce a significant latency and an interruption to the real-time WiFi video traffic, especially when the number of ZigBee devices increases; ii) in the frequency domain, the transmission from a narrow-band ZigBee device will prevent the wide-band WiFi device's transmission. Therefore, the spectrum utilization is extremely low. For example, to avoid interference, when a ZigBee device is sending packets to the gateway using a 2 MHz channel (e.g., channel 19), the WiFi HQ video camera cannot use the whole 20 MHz WiFi channel 6 that is overlapped with ZigBee's channel 19. One may argue that the WiFi HQ video camera can use another WiFi channel. However, all the WiFi channels are overlapped with ZigBee channels. When the number of IoT devices exponentially increases, it is highly impossible to find a clear and designated channel that can only be used by WiFi devices.

Moreover, we argue that even Zigbee and WiFi packets can be transmitted simultaneously. The reason that both WiFi and ZigBee packets can be received by both

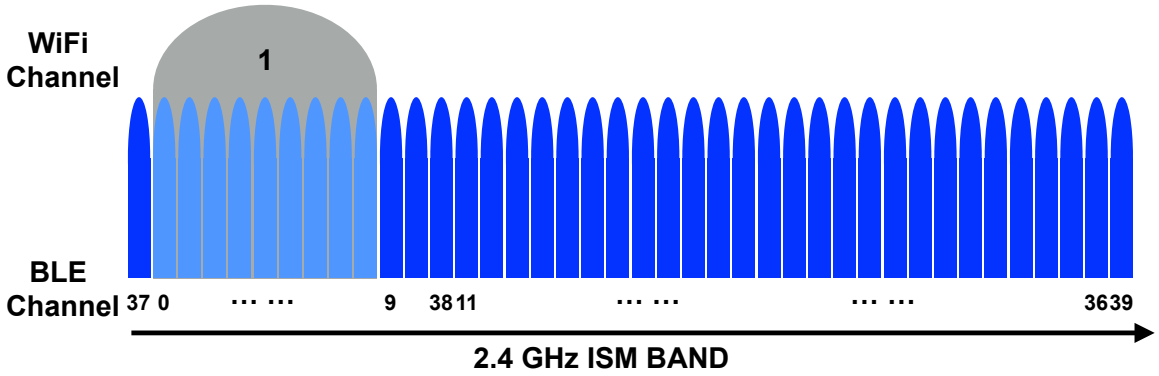


Fig. 1.2: Overlapped channels of ZigBee and WiFi

ZigBee and WiFi packets at full network throughput is based on the observation that ZigBee spreads its energy enabling it to be robust against WiFi's multi-tone signals. While the hybrid packet does introduce higher interference levels, we find that the robustness of WiFi and ZigBee standards can recover from the introduced noise.

Therefore, the goal design goal of densely high number of IoT devices radio protocol is to efficient communication communicate with multiple heterogenous devices.

1.1.3 Ultra-low Powered Backscatter Radio

The emergence of 1) implanted medical sensors and 2) wearable health-monitoring devices motivate the design of energy efficient radios. With the case of implanted sensors, the device will energy-harvest and be battery-free. Thus, ultra-low power radios must recycle signals from existing infrastructure (such as WiFi networks). Moreover, this recycling of signals must be efficient utilizing productive WiFi communication (meaning that WiFi communications should have minimal interference from backscatter radios). Productive wireless communication is compared to unproductive where a device generates a signal specific for the backscatter device that carries no data of value. With the case of the health-monitoring devices, these radios must also be energy efficient to allow for more than 10-year wearable battery

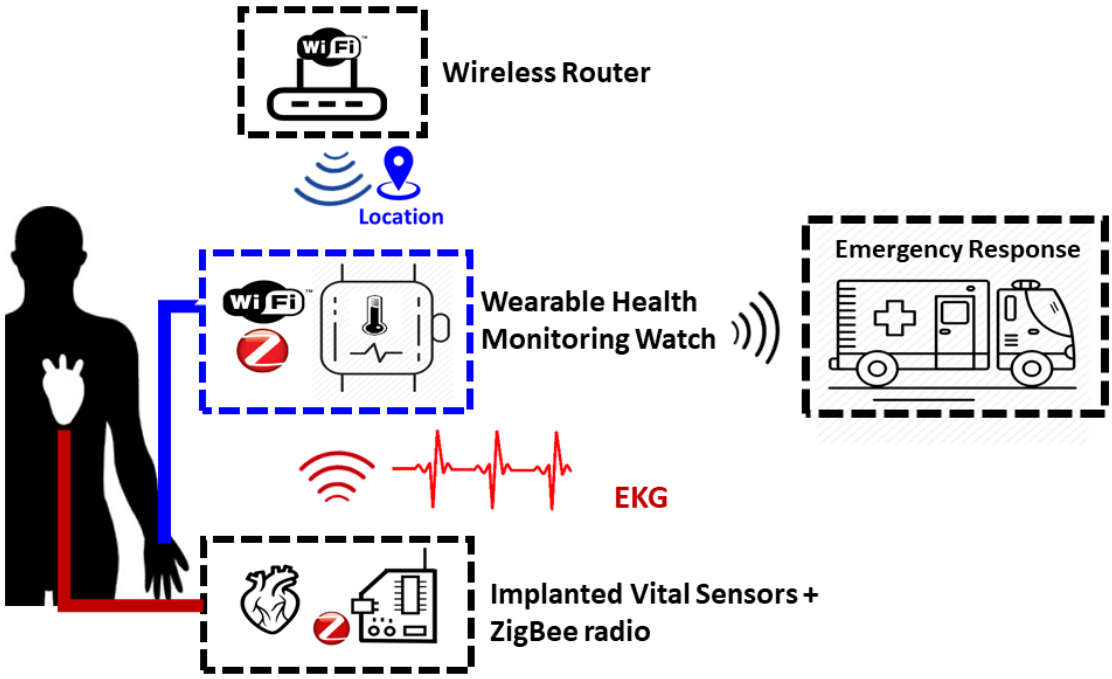


Fig. 1.3: Traditional Implanted Wireless and Monitor IoT Radios utilizing inefficient heterogenous radios

life and able to interface with existing IoT radios infrastructure.

To illustrate this energy-efficient heterogeneous IoT radio problem (Figure 1.3), an implanted cardiac sensor, that monitors for Atrial fibrillation by sending EKG data, requires a wireless link to a wearable smart health-monitoring watch. In the case of a critical cardiac event, the smart health-monitoring watch will send alerts to emergency responders with the location of the patient. This location information can be derived from in-door WiFi networks. Thus, heterogeneous radios (i.e WiFi and ZigBee radios) must be used in the traditional design.

Traditional implanted sensors and health monitoring devices would use ZigBee as a low power radio. To derive location data from indoor WiFi networks, the smart health-monitoring watch must also have a constantly active WiFi radio. The need for implanted battery-powered ZigBee radios and monitoring heterogeneous radios

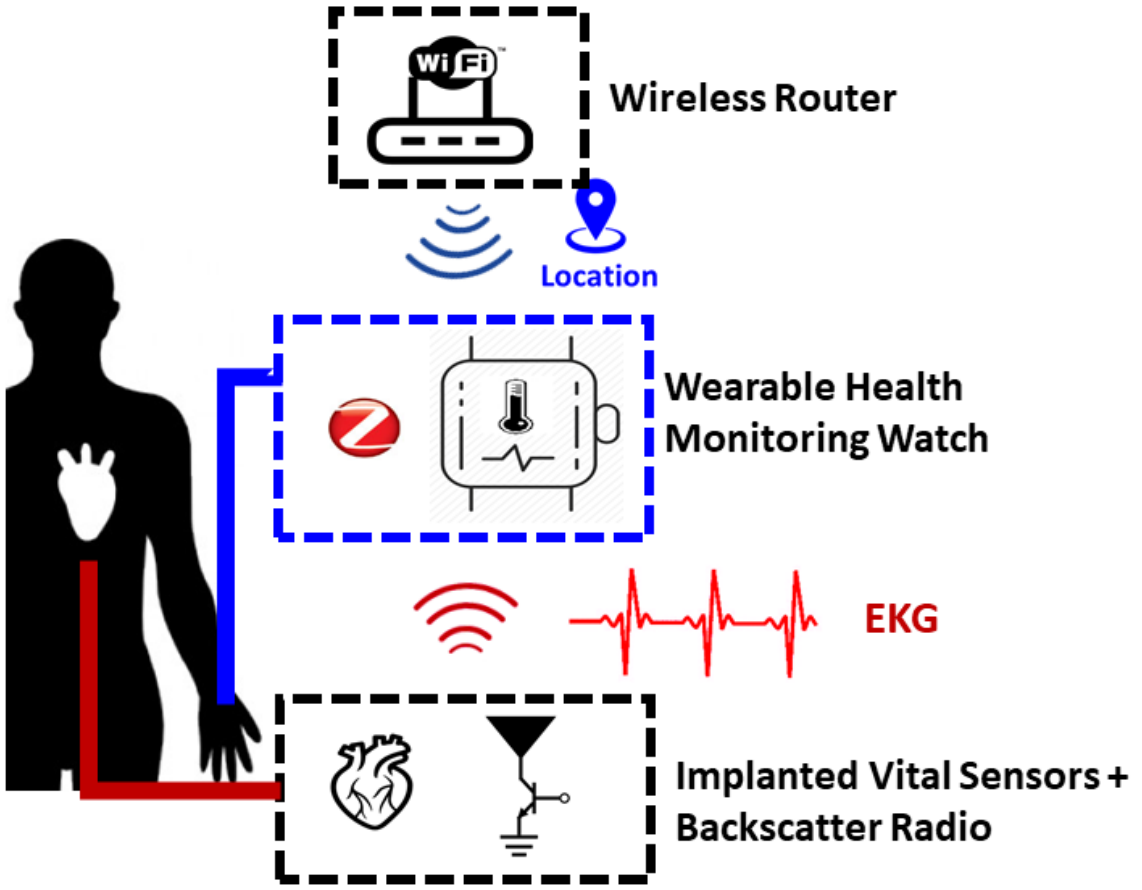


Fig. 1.4: Backscatter and CTC removes the need for WiFi radio in the wearable and consumes significantly less power in the sensor enabling implanted energy harvesting circuits.

increase the power consumption of the entire network.

Traditional ZigBee and WiFi radios consume 36mW and 210 mW respectively. Inspired by recently proposed backscatter designs that recycle signals, we seek to dramatically decrease the power consumption of the implanted sensor and the wearable monitor. Moreover, with the development of cross-technology communication radio, we seek to eliminate the WiFi radio on the wearable device (Figure 1.4).

1.2 Thesis Contribution

My thesis tackles these challenges and seeks to create ecosystems that enables IoTs to sense human activities and identities while allowing heterogenous radios to communicate efficently.

1.2.1 Contribution Summary

Overall, the key systems and contributions of this thesis are:

(a) Wobly - CSI based Biometric identification and tracking

Wobly allows for anonymous privacy preserving tracking and positioning based on human gait using Wi-Fi signals. This software defined radio (SDR), biometric, and localization system does not require attachment devices to persons and works in NLoS scenarios

(b) Chiron - Concurrent High Throughput Communication for IoT Devices

Chiron opens a promising direction for concurrent high throughput communication to heterogeneous IoT devices (e.g., wider-band WiFi and narrower-band ZigBee). Chiron enables concurrently transmitting (or receiving) 1 stream of WiFi data and up to 4 streams of ZigBee data to (or from) commodity WiFi and ZigBee devices as if there is no interference between these concurrent transmission.

(c) Passive-ZigBee - Enabling ZigBee Communication in IoT Networks with 1000X+ Less Power Consumption

Passive-ZigBee transforms an existing productive WiFi signal into a ZigBee packet for a CoTS low-power consumption receiver while consuming 1,440

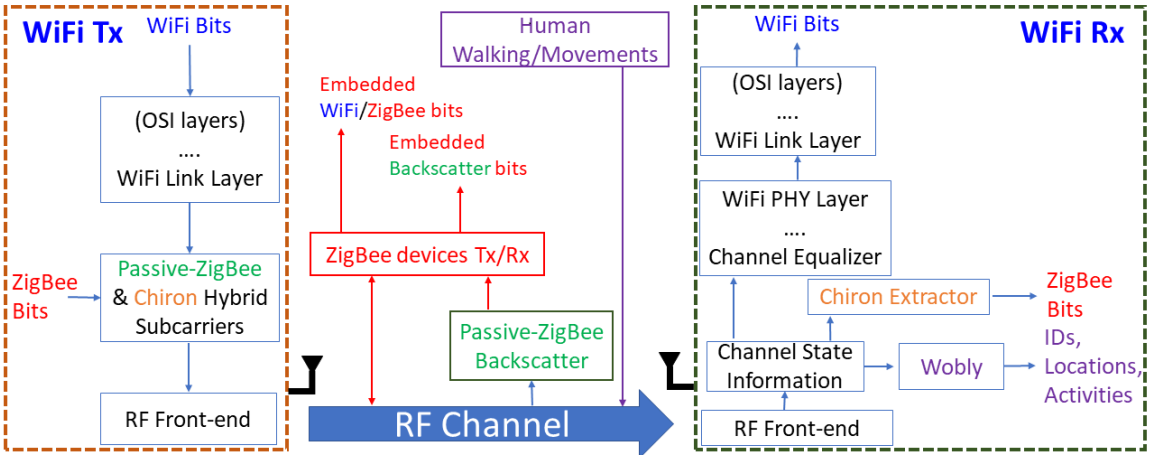


Fig. 1.5: Overall Thesis System Diagram

times lower power compared to traditional ZigBee. Moreover, this low power backscatter radio can bridge between the ZigBee and WiFi devices by relaying data allowing heterogenous radios to communicate with each other. Because Passive-ZigBee uses backscatter techniques, we also lower network latency.

1.3 Thesis Overview

Figure 1.5 shows an overview of the thesis. It includes three components to tackle the three key challenges of these systems. The first component is sensing human identity, activity, and movement using WiFi signals. The second component is to connect IoT devices with a heterogeneous gateway in the uplink and downlink using concurrent transmissions while sensing the channel state. The final component is to utilize ultra-low power backscatter for heterogenous radios.

Wobly - Exploiting WiFi CSI to track, monitor, and identify humans with privacy preservation In chapter 2, Wobly (Ting Zhu (2016) and Yan Li (a)) leverages Channel State Information (CSI), which is used to measure WiFi network performance at the application layer (such as SWAT Srinivasan, Maria A. Kazandjieva, &

Levis (2008)) and to avoid interference. By leveraging CSI, a directional antenna, extracted pilot tones, and correlated signals, specific features can be used to uniquely identify individuals and their activities (e.g., sitting and falling) while encoding the identity signature based on room configuration. In contrast to previous gait and body movement measuring techniques, our system (Wobly) does not require cameras, attached RFID tags, or ultrasound sensors. Moreover, Wobly passively acquires signals and thus does not interfere or require the production of special signals to identify and track individuals.

Chiron - Exploiting CSI for Heterogenous Gateway In chapter 3, Chiron (Li et al. (2018)) enables concurrent high throughput bidirectional communication in heterogeneous (i.e., wider-band WiFi and narrower-band ZigBee) IoT devices. Chiron allows for concurrent transmitions (or receiving) using 1 stream of WiFi data and upto 4 streams of ZigBee data to (or from) commodity WiF iand ZigBee devices. The result is the removal of interference between these concurrent transmissions. In a nut-shell, Chiron enables the concurrent high throughput communications by leveraging CSI to optimize transmission power and WiFi and ZigBee signals' unique difference – WiFi's low symbol rate (i.e., 312.5 Ksymbol/s) verses ZigBee's high chip rate (i.e., 2 Mchip/s). By doing this, we significantly increase the spectrum utilization and overall aggregated throughput among IoT devices.

Passive-ZigBee - Symbol level backscatter and CTC communications In chapter 4, Passive-ZigBee (Yan Li (b)) transforms an existing productive WiFi signal into a ZigBee packet for a CoTS low-power consumption receiver while consuming 1,440 times lower power compared to traditional ZigBee. Moreover, this low power backscatter radio can bridge between the ZigBee and WiFi devices by relaying data allowing heterogenous radios to communicate with each other.

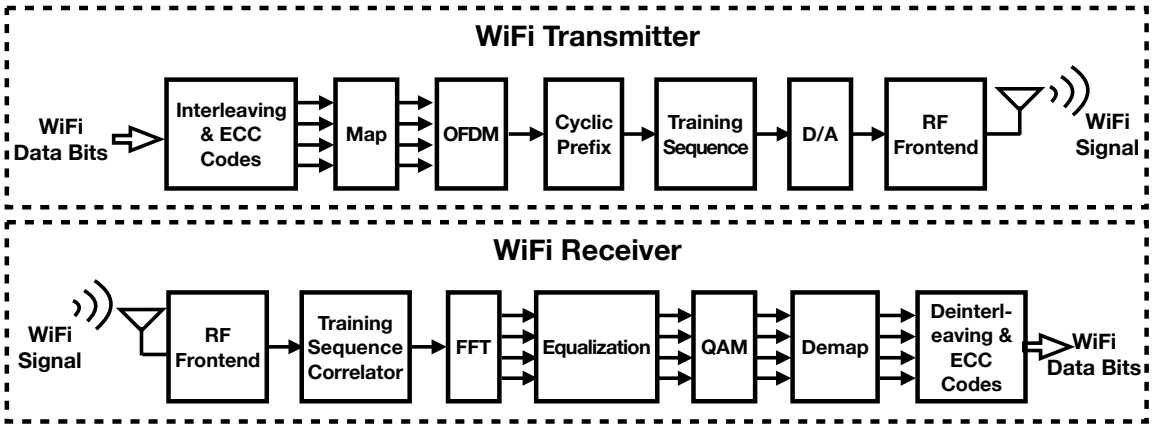


Fig. 1.6: The WiFi Transmitter and Receiver

1.4 Background

This thesis discusses how and why WiFi radios are able to generate wide band channel state information for 1) human activities monitoring with identification and 2) concurrent WiFi and ZigBee bidirectional communication. Moreover, based on the concurrent communication techniques, we also applied backscatter techniques to reduce energy consumption. This background section demonstrate why existing radios cannot communicate due to the differing protocols. We first introduce WiFi, ZigBee, and backscatter radios describing how they work. In the following chapters, we elaborate in more details and provide modifications to existing designs.

1.4.1 WiFi Radio

Figure 1.6 shows an WiFi system overview. A WiFi radio uses multiple sub-carriers to simultaneously transmit aggregate bits in a wider-band protocol. To perform this aggregate transmission: 1) The data payload is interleaved 2) The WiFi serial binary is parallelized and mapped into bits onto different channels. 3) On each channel, WiFi applies Quadrature Amplitude Modulation (QAM) to mapping bits to

different phases in sine waves. We define the various phase states of the signals as symbols. 4) Then, WiFi uses orthogonal frequency-division multiplexing (OFDM) to sum the sine waves. 5) Between each symbol duration, a cyclic prefix is appended to reduce inter-symbol interference. 6) Before the baseband WiFi signal, a training sequence allowing for sender and receiver discovery and synchronization is added. The output signal can be written as Equation 4.1.

$$W(t) = \sum_{n=0}^{N} \left[\left(I(t)\cos(2\pi f t_1) - Q(t)\sin(2\pi f t_1) \right) e^{2\pi j f_s n} \right] \tag{1.1}$$

Where there are N total WiFi subcarriers, and for each n subcarrier, we defined complex symbols states at the $I(t)$ and $Q(t)$ mapped by QAM. The duty cycle of each symbol is defined by f_1. We defined the subcarrier spacing frequency by f_s.

In the WiFi receiver, the system works in reverse mapping the aggregated sine waves back to bits. 1) A correlator and a phase synchronization (Phase Locked Loop) algorithm discover the training sequence and align the demodulator's initial phase state. 2) Using the reverse FFT algorithm, the receiver recovers the aggregated sine waves while accounting for the cyclic prefix. 3) A QAM demodulator maps the phase states of the sine waves to symbols and then to bits.

1.4.2 ZigBee Radio

The ZigBee transmitter and receiver is shown in Figure 4.5. In summary, ZigBee radios are low power narrow-band radio that spread its bits over a narrower frequency band. 1) ZigBee uses Direct Sequence Spread Spectrum (DSSS) to spread the signal into a wider band by multiplying with a higher rate (2 MHz) shared pseudorandom noise (PN) code. 2) After the spread spectrum process, the ZigBee modulator maps the bits to sine waves by Offset quadrature phase-shift keying (OQPSK) modulation

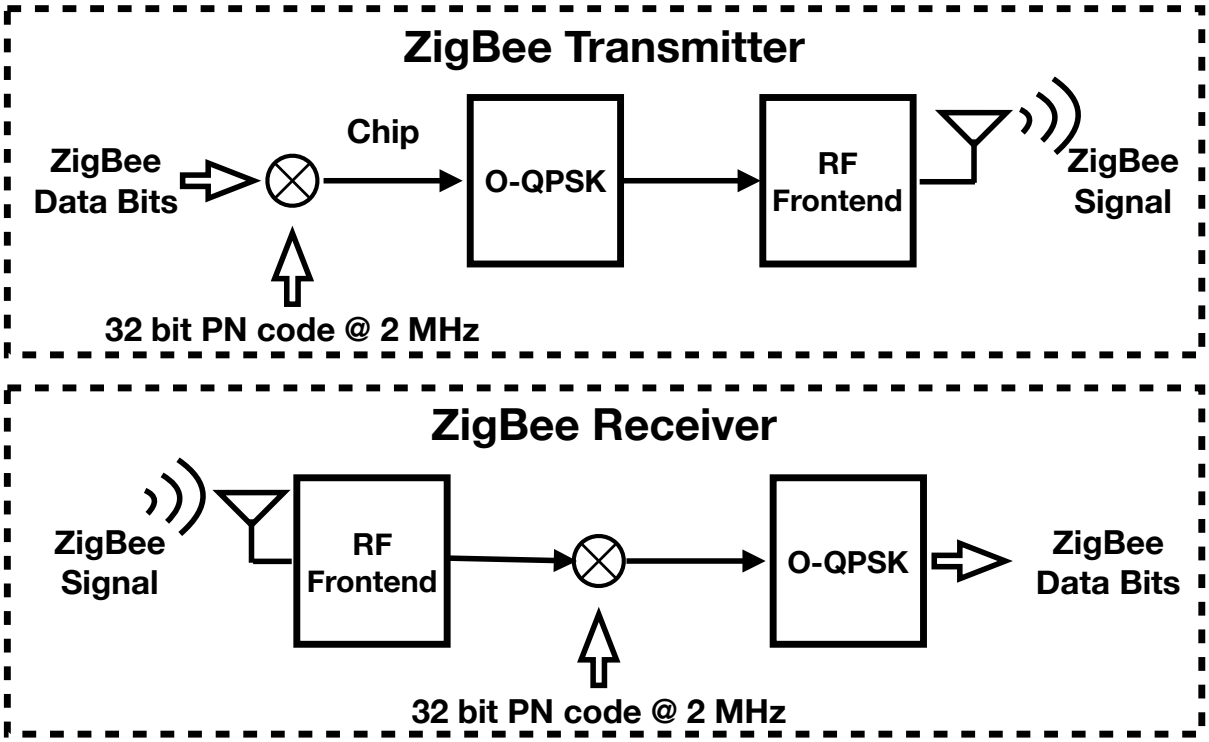


Fig. 1.7: The ZigBee Transmitter and Receiver

which reduces the dramatic phase shifts by offsetting the odd and even bits by a distinct period (Equation 4.2). These sine waves with 4 possible states are the ZigBee chips.

$$Z(t) = \frac{1}{\sqrt{2}} I(t) \cos(2\pi f t) - \frac{1}{\sqrt{2}} Q(t - T_s) \sin(2\pi f t) \tag{1.2}$$

Where there are 4 states for I and Q describing the information carrying sine waves, and T_s represent the period offset.

To receive a frame, 1) the ZigBee radio down-converts the received waveforms to baseband and digitalizes them into in-phase and quadrature (I/Q) samples using ADC. 2) The O-PQSK demodulates measure the changes in phase to symbols. 3). The baseband signal is multiplied by or correlated to a shared PN code which yields

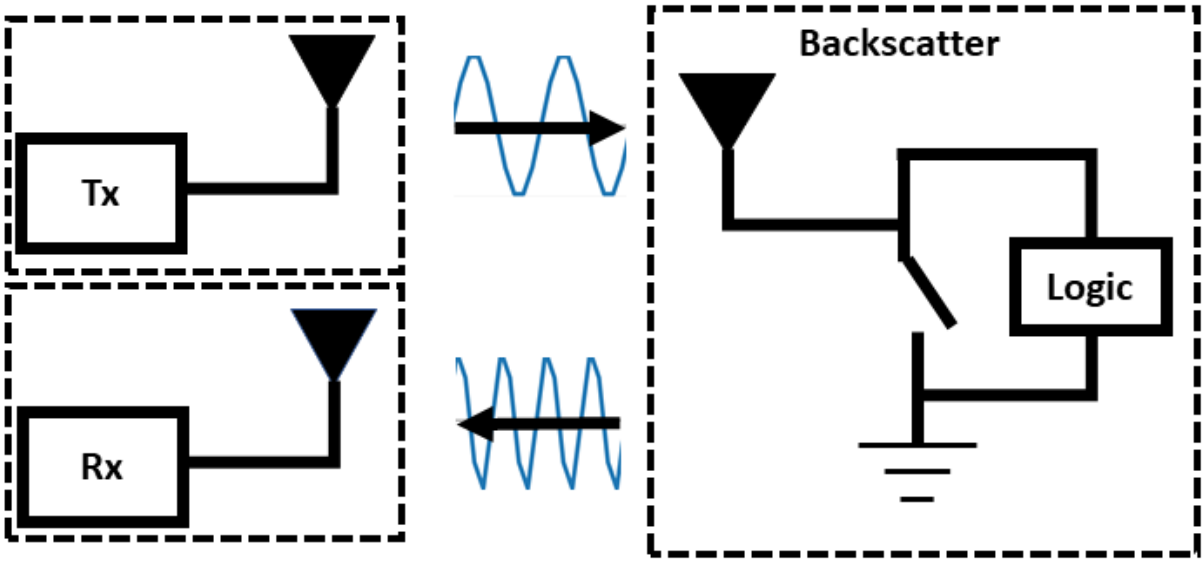


Fig. 1.8: An example of a backscatter radio

the encoded bits.

1.4.3 Backscatter Radio

Backscatter radios are designed to consume ultra-lower energy. Used in wearable with a small form factor, these circuits have the ability to convert to a DC current and stored as a energy. Shown in Figure 1.8, typically, a reader sends a carrier to excite the tag. While a portion of this carrier wave is harvested as energy, the signal is reflected with some modification performed by a logic circuit. The changed reflected signal contains the information that the tag wish to communicate. Because the backscatter uses existing signals, the energy usage is very efficient. Without the need for circuit warming, this reduces network latency.

1.4.4 Channel State

For wireless devices to communicate, radios must be able to sense and recover from interference introduced between the sender and receiver. In IoT devices, the typical interference is indoor and human movement multipath. Multipath is illustrated in Figure 1.9: the signal from the transmitter reaches the receiver via multiple propagation paths. The signal that propagates directly from the transmitter to the receiver takes the line-of-sight (LoS) path, P_l. The signal that is reflected by the static obstacle takes the non-line-of-sight (NLoS) path, P_{nl}. The signal bounced off the human body also creates a path, P_h. When the human is moving or performing activities, P_h would become P'_h, which has a different length comparing to P_h. Since paths P_l and P_{nl} are relatively stable, the human activities that cause the transition from P_h to P'_h can be derived based on measurable features of the received signal, such as amplitude, delay, and Doppler shift.

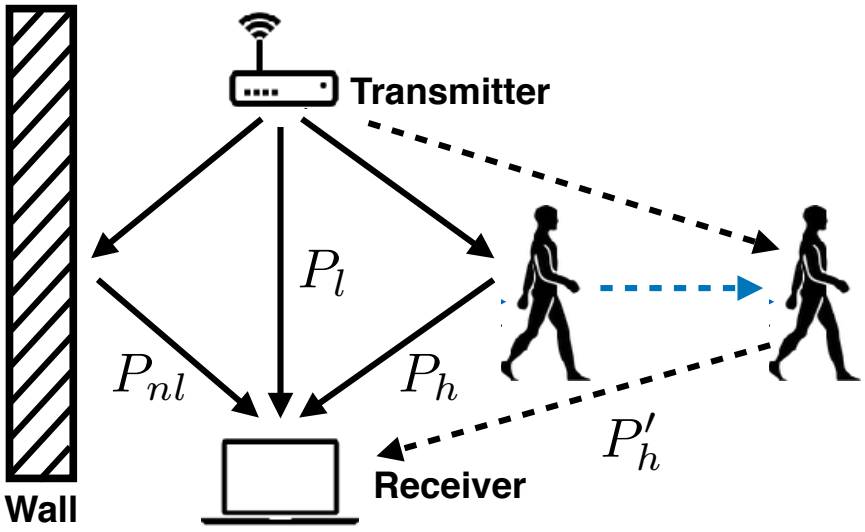


Fig. 1.9: Multipath effect caused by human motion

When the person moves, the received signal amplitude (i.e., RSS or CSI values)

fluctuates. Consequently, the RSS values collected from multiple receivers contains a unique pattern, which is the basis of RSS-based localization and tracking Zhang et al. (b). Through time-frequency analysis, the RSS sequence shows patterns that match the movement range and speed of human activities Ali et al.; Chi et al. (b), which enables the activity recognition.

When the person moves away from the transmitter and receiver, the signal bounced off the human body will take a longer path to reach the receiver. Since a longer path requires more propagation time, the delay of the received signal can also be used to conduct localization Gjengset et al. and tracking Xiong & Jamieson.

Doppler shift is introduced by the relative speed between the human body and the receiver Kim & Ling. Different human gestures introduce distinguishable patterns in the Doppler shift of RF signals, thus can be used for gesture recognition Pu et al..

Most of the RF based human motion sensing systems build on top of the measurements of RSS, delay, and Doppler shift. The changes in these three features can be represented by the complex value channel frequency response (CFR) Wang et al.. CFR can be denoted as $H(f,t)$, which can be calculated using the following

Equation:

$$H(f,t) = e^{-j2\pi\Delta f t} \sum_{k=1}^{N} a_k(f,t) e^{-j2\pi f \tau_k(t)} \tag{1.3}$$

where f is the frequency of a wireless channel, t is time. $a_k(f,t)$ is the amplitude attenuation. $\tau_k(t)$ is the delay. Δf is the Doppler shift. Given the transmitted signal $X(t)$, the received signal $Y(t)$ can be written as $Y(t) = H(f,t) \times X(t)$.

Chapter 2

WOBLY - EXPLOITING CSI TO TRACK, MONITOR, AND IDENTIFY HUMANS WITH PRIVACY PRESERVATION

2.1 Summary

Gait characterization and monitoring technologies are useful for the purposes of biometrics tracking and monitoring subjects (e.g., the elderly, at risk, and patients). Traditional techniques of measuring gait employ image processing or special sensors, which require either direct line of sight or physically attached sensors and thus, are cumbersome and costly. We propose Wobly that uses Wi-Fi signals to characterize multipath and Doppler Effect. Because of the physical property, the ubiquity, and the robustness of Wi-Fi signals, this type of sensing penetrates walls and does not require special signals or attachment of sensors to humans. In contrast to previous techniques, Wobly 1) extracts features that identify individuals by their intrinsic body movement during walking without attachments to the body; 2) addresses the need to conduct real-time monitoring of individuals and detecting events such as falling; 3) creates signatures by measuring Channel State Information (CSI), which provide high-fidelity location, movement, and identity information of human subjects; and 4)

preserve privacy by encoding gait signatures with room configurations. We implemented Wobly on a National Instruments (NI) Radio Frequency (RF) test-bed and conducted extensive experiments on six individuals at three locations. Our empirical results show that by applying a simple Naïve Bayes classifier on the extracted features, the correct identification rate was 87%. The correct localization rate was 90%. We demonstrated line-of-sight (LoS) and with non-line-of-sight (NLoS) scenarios.

2.2 Background

Gait characterization is based on the theory that all animals have neural networks that contribute to motion through cyclical patterns of feedback. The study of this phenomenon, known as Central Pattern Generators (CPG), was first credited to Graham Brown (Brown (1911)) who managed to reproduce patterns for stepping without commands from the cortex. Further research showed that special cells from the spinal cord utilized feedback to produce patterns. Because of the unique aspects of human bodies, such as size, leg length, walking cadence, and foot and ankle angles, we can generate classifiable signatures.

Understanding and monitoring humans' movements have further advanced the fields of biometrics and pathology. Biometrics uses gait analysis as forensics to identify and track individuals. Historical gait and location data aid the diagnosis of occupants in remote health monitoring applications (Kaye et al. (2011)). Patients' location histories and gait patterns form huge amount of data, which provides insightful trends that are useful for treatment.

Traditional human tracking systems employ image recognition through direct line-of-sight, thus requiring excess infrastructure for computer vision. Floor sensors, wall attachments, and accelerometers (Guha et al. (2012)) are used to measure human

activity. Devices like radio-frequency identification (RFID) (Ranjan, Juhi, & Yu (2013)), door sensors, and ultrasonic sensors (Hnat et al. (2012)) also track persons. These sensors are cumbersome, requiring installation or personal attachment. Micro-radars (Lyonnet (2010)) achieve tracking and localization by utilizing special signals that cause undesired interference.

To solve the issue of excess infrastructure, smart wireless or Internet of Things (IoT) and corresponding technologies devices have also been used to sense environment (Wei (2015) Zhu et al. (2015) Oppermann, Boano, & Römer (2014) Galstyan et al. (2004)), humans (Xiong (2015) Adib (2013) Adib (2015) Liu et al. (2014)), and movement (Chen (2015) Luong et al. (2015) Pu et al. (2013)). These sensing devices advance in two categories: 1) antenna and 2) signal processing designs. In the first category, the use of directional, horn antennas by IoT devices have gained popularity. These antennas are used in a variety of modern telecommunication systems. Previous research utilized directional antennas to improve localization accuracy by providing angular information in Wi-Fi networks (Varshney, Voigt, & Mottola (2013)) and improving throughput by directing and localizing energy. In the second category, researchers have applied advanced signal processing technologies on Wi-Fi-based IoT devices (Jayakumar et al. (2014)), which leverages Orthogonal frequency-division multiplexing (OFDM) for its ability to penetrate walls. For example (CARM Wang et al. (2015)) and (WiTrack Adib et al. (2014)) detect human activities and localize individuals behind walls using Radio Frequency (RF). However, these approaches cannot identify individual people. Different from previous approaches, we use angular and polarity features provided by a directional horn antenna to detect and identify humans and their activities behind a wall.

We also leverage Channel State Information (CSI), which is used to measure network performance at the application layer (such as SWAT Srinivasan, Maria

A. Kazandjieva, & Levis (2008)) and to avoid interference. By leveraging CSI, a directional antenna, extracted pilot tones, and correlated signals, specific features can be used to uniquely identify individuals and their activities (e.g., sitting and falling). Because of the Radio Frequency (RF) propagation, these privacy-preserving signatures can also be encoded by room configurations. In contrast to previous gait and body movement measuring techniques, our system (Wobly) does not require cameras, attached RFID tags, or ultrasound sensors. Moreover, Wobly passively acquires signals and thus does not interfere or require production of special signals to identify and track individuals. To summarize, the main contributions of this paper as follows:

- Wobly allows for identification and positioning of individuals based on human gait by using Wi-Fi signals. Our system senses human gait-based movement to generate signatures. Unlike previous gait-based systems, Wobly does not require physical attachment to human subjects and can work behind a wall.

- Wobly allows for anonymous privacy preserving tracking and positioning based on human gait using Wi-Fi signals. We produce signatures by encoding RF multipathing which is dependent on room configurations.

- Wobly uses standard Wi-Fi beacon signals to identify and track individuals. It also works passively to measure Doppler shift and multipathing to create unique human signatures. Unlike previous CSI studies, we demonstrate integration by demodulating Wi-Fi beacon signals for an equalization scheme. The deployment of Wobly followed modern Wi-Fi system architecture.

- We implemented Wobly and conducted extensive experiments with six individuals at three locations. Our empirical results show that by applying a simple Naïve Bayes classifier on the extracted feature, the identification and localiza-

tion rate was 87% and 90% correct respectively. We demonstrated sensing with line-of-sight (LoS) and NLoS with non-line-of-sight (NLoS) scenarios. We also demonstrate that people have different signatures when they stop walking and either sit or fall.

2.3 Motivation

This section discusses the needs and current technologies for monitoring systems in 1) smart clinics or hospitals and 2) homes of the elderly or disabled individuals. The information gained from these systems enables trend predication and detection of falls or pathological gait. Embedding such sensors in walls enables localization and health monitoring information. The Wobly's signatures provide high-fidelity localization and identification information.

2.3.1 Security Applications

With the increasing need of privacy protection and security from the rise in terrorism, it is critical to develop technologies and sensors to enhance physical security. Physical Intrusion Detection System (IDS) has the ability to tag, track, and identify individuals. Identification and location information are used in access control and behavior monitoring systems. To counter insider-threats, the need to monitor unusual behavior from internal personnel within buildings requires human sensing and localization. Current IDS technology utilizes cameras, RFIDs, IRIS scanners, human voice, infrared, and motion sensors. These sensors are used to protect homes, military and government installations, server farms, and other sensitive locations. By including gait as a hidden biometric, extra layer of restrictions provide additional security. The benefits of NLoS and standard signals with passive reception allows for

clandestine monitoring.

2.3.2 Localization Privacy in Smart Buildings

Preserving privacy in localization and tracking data is critical for smart government facilities, businesses offices, and homes. Tracking individuals in these settings enhances physical security and enable trend forecasting, such as: access control, customized directed marketing techniques, and personalized automation and preferences. Smart buildings that detect the location of individuals can lower energy consumption. With localization information, smart buildings and hospitals can enforce safety protocols and aid during emergency responses. People sensing enhances systems like Human Interactions Computer Interactions Hsu et al. (2010) and Building Operating System Services Dawson-Haggerty et al. (2013). However, current techniques require cameras with face recognition algorithms, attached devices, or smart phones, which all contain vulnerabilities. These techniques are intrusive, insecure, and easily violate privacy protection laws. Techniques used for protecting privacy include access control and microaggregation, which limits accuracy and access to information. The high fidelity localization signatures discussed in this paper provide anonymization using physical layer security, by encoding human gait and physical channels.

2.3.3 Preserving Privacy in Healthcare

Current use of accelerometers and attached devices such as smart phones allows for big data collection to detect trends in healthcare. With additional features, such as location and movement speed, these trends can provide insight on disease progression and causes (Figure 2.1). Storing such information in a health database helps predict trends and diagnosis. Monitoring the elderly and young individuals benefit healthcare automation, and thus lower costs. The data gathered from clinics are sensitive, as

diseases such as HIV carry stigma. Current technologies protect this data by access control, thus limiting data availability. These technologies contain vulnerabilities and may violate privacy laws. With the ability to penetrate walls and anonymization, Wobly enables human sensing without attached equipment and raises fewer privacy concerns.

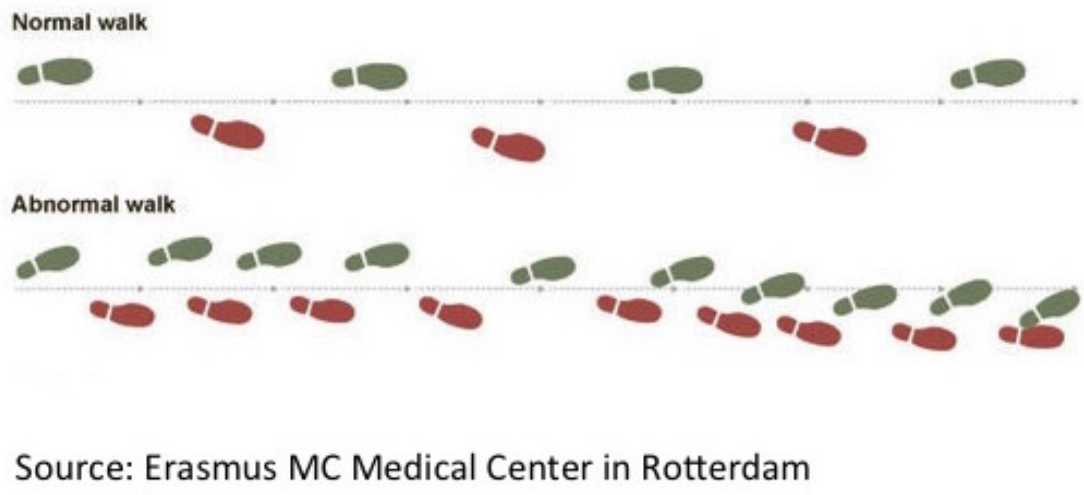


Fig. 2.1: Identify changes in gait caused by neurological disease Larsen (2012)

2.3.4 Monitoring of the Elderly or Disabled

Monitoring the elderly and disabled individuals enhances quality of life through automation and thus, lowers cost. Wobly has the ability to detect location and movement speed. Historical movement information can provide insight on disease progression and causes, and real-time monitoring provides faster response to falls. Monitoring gait trends enables early detection of stroke and neuro-degenerative disease like Parkinson, Alzheimer, and Huntington disease. Current use of accelerometers and attached devices (such as smart phones) detect fall, sense gait, and generate

trends. Storing such information in a health database helps predict trends and diagnosis. With the ability to penetrate walls, Wobly enables human gait sensing without attached equipment and raises fewer infrastructure concerns.

2.4 Threat Model

The threat for tracking systems is that adversaries may access the target's histories. Attackers may gain access to database services, sensors, or IoTs such as smart phones and wearables Cai, Machiraju, & Chen (2009). The access means are typically software code fallacies, eavesdropping, socially engineered techniques, or identity theft. Wobly trusts the facility and believe that no other identity recording systems are active.

Our assumptions are that adversaries, who may have access to signatures, do not have access to the room configuration and the targets simultaneously. For privacy, we also assume that identities are not associated with the signatures in any manner that exposes the sensitive information.

Because Wobly depends on physical layer channel encryption, we can utilize Wyner, Cheong, and Hellman's Wire-Tap Channel model (Figure 2.2) Leung-Yan-Cheong (1978). Wyner relaxed Shannon's model by adding noise to transmitted channel. In Wyner's wiretap modem, W is the message sent, $\hat{W}$ is the message received, and Z is the entropy of the message. Wyner defined the equivocation or the confusion in Equation 2.1 and perfect secrecy in Equation 2.2 for n channels.

$$\frac{1}{n} H\left(W|Z^n\right) \tag{2.1}$$

$$H\left(W|Z^n\right) \approx H(W) \tag{2.2}$$

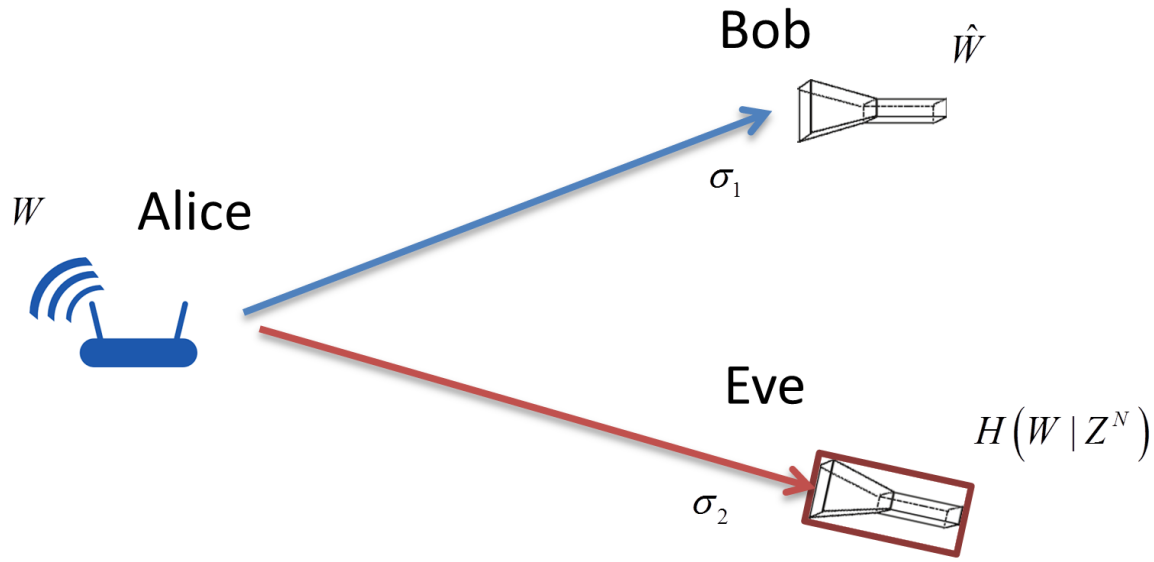


Fig. 2.2: Wyner described a wiretap channel, showing Alice communicating with Bob, with Eve as the eavesdropper.

Cheong and Hellma apply a statistical description of the channel and define channel secrecy in Equation 2.3.

$$C_s = \frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2+\sigma_2^2}\right) \tag{2.3}$$

Where σ_1 and σ_2 are receiver and eavesdropper channels, and P is the power level of the signature. Applying this to Wobly, Wyner theory suggests that the more the adversary's channel is different than the receiver's channel, the more secret Wobly will be. Therefore, we assume that the there are no adversaries' antennas placed close to Wobly's antenna.

2.5 Sensing the WiFi Signal

The main challenge is signal acquisition in real-world Wi-Fi networks to sense CSI values. To sense changes in the channel, we utilize a NI RF test bed designed for continuous signal acquisition. Section 2.5.1 intruduces how OFDM signals work. Section 2.5.2 presents channel interference caused by human gait. Section 2.5.3 explores reducing noise and improving Doppler and multipath signals. Section 2.5.4 presents the signatures detected.Section 2.5.5 explains measuring the human gait cycles. Section 2.5.7 outlines the techniques to identify human. Section 2.5.6 presents techniques to detect initial human movement. Section 2.5.7 discuss biometrics and identification. Section 2.5.8 describes a technique to localize.

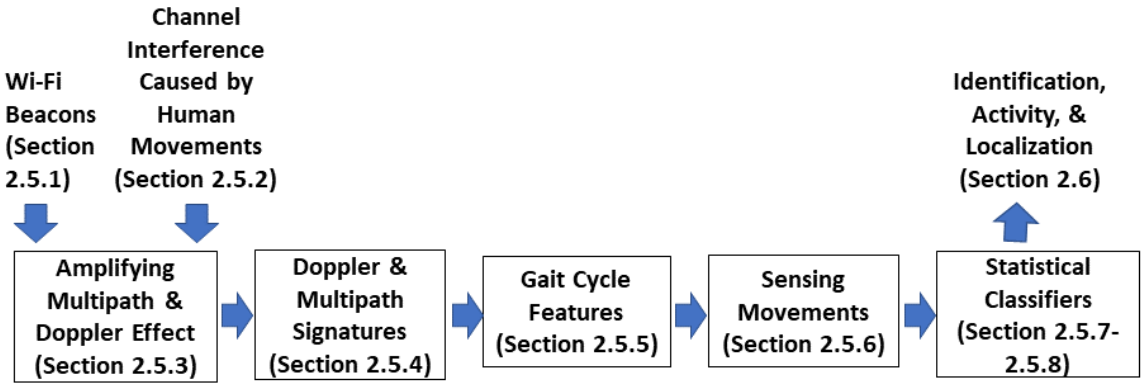


Fig. 2.3: The overall SDR System Architecture shows a Rx capable of sensing a Wi-Fi beacon and extract Doppler information.

To sense the small changes in frequencies, we addressed the following challenges: 1) modelling and detecting Doppler shifts and multipath effect to produce signatures; 2) acquiring Wi-Fi signals in homes and buildings to amplify Doppler Effect and multipathing; and 3) using classification algorithms to discriminate the signatures. We used a combination of antenna technologies, signal processing, and pattern recognition to monitor humans' activities from Wi-Fi signals (Figure 2.3). Because Wi-Fi signals

utilize OFDM, the demodulation scheme senses both Doppler Effect and multipath interference through CSI.

2.5.1 OFDM Signal Design

This section discusses the theories of generating a Wi-Fi beacon, which uses an OFDM BPSK modulation and a cyclic prefix. The challenges addressed in this section include leaveraging a Wi-Fi beacon with CSI estimating pilot tones and generating the industrial, scientific and medical (ISM) band signal. An OFDM signal is created by turning binary data into cyclical representations, usually taking the form of frequency, amplitude, or phase. In 802.11 standards for Wi-Fi beacons, this representation is Binary Phase Shift Key (BPSK). BPSK has two states representing 0 and 1.

$$S_n(t) = \sqrt{\frac{2E_b}{T_b}} \cos\left(2\pi f_c t + \pi\left(1-n\right)\right), n = 0, 1. \tag{2.4}$$

Where f_c is the center frequency. E_b and T_b are constants defining energy and duration per bit respectively. To minimize inter-symbol interference, the BPSK signal contained a cyclic prefix. The prefix is added to the beginning of the signal by copying portions of the end signal. This prefix added signal is the definition of a symbol, representing binary data.

$$s'_n[t-N] = \left[s_n\left[N-L+1\right] \ldots s_n[0] \ldots s_n[N-1]\right] \tag{2.5}$$

Where L is the length of the prefix. The reason why OFDM is such a popular encoding scheme is that multiple bits can be sent simultaneously (Figure 2.4) using multiple sub-carriers. With guard intervals, cyclic prefix, rate control, and equalization schemes these signals are resilient against Doppler, multipathing, and fading

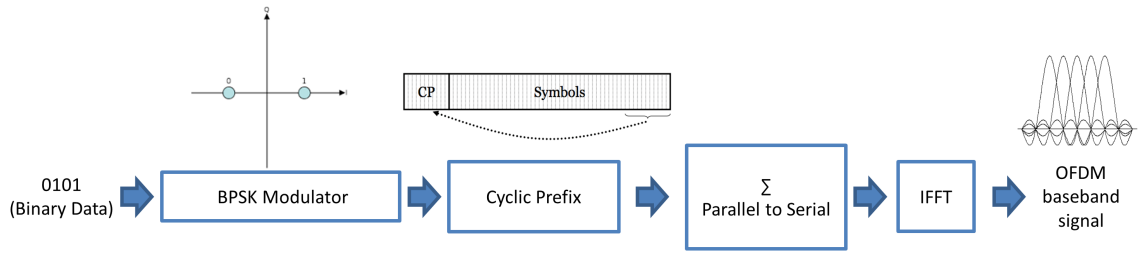


Fig. 2.4: Baseband OFDM BPSK modulated signal allows for multiple transmissions of multiple bits simultaneously.

interference. To simulate a beacon, the signal consisted of 20 MHz of bandwidth with 51 active subcarriers. The 51 carriers, derived from 51 bits, were summed together by the parallel to serial converter. OFDM utilizes the inverse Fast Fourier Transform (iFFT) to allow the subcarriers to be orthogonal, allowing for high spectral efficiency (shown in Figure 2.4). Modern communication systems define specific subcarriers as pilot tones, sent to perform channel estimation. To simulate this scheme, the NI system used an arbitrary wave generator (AWG) at baseband, up-converting the signal to 2.412 GHz, and sending pulsed OFDM signals at 1/3 duty cycle. This up-conversion process centers the baseband signal (Figure 2.7) to the desired transmit frequency by first up-sampling, then multiplying with a desired frequency sine wave, and finally high-pass filtering.

2.5.2 Channel Interference Model and Encoding Mechanism

The challenge addressed in this section is modelling interference caused by human movement. The two interferences that exist in Wi-Fi systems are Doppler frequency shifts and multipathing delays. By measuring these interference patterns over time, we form encoded human signatures that monitor human movements. Most human bodies move about 1 meter per second yielding about 10 Hz shifts. We note that

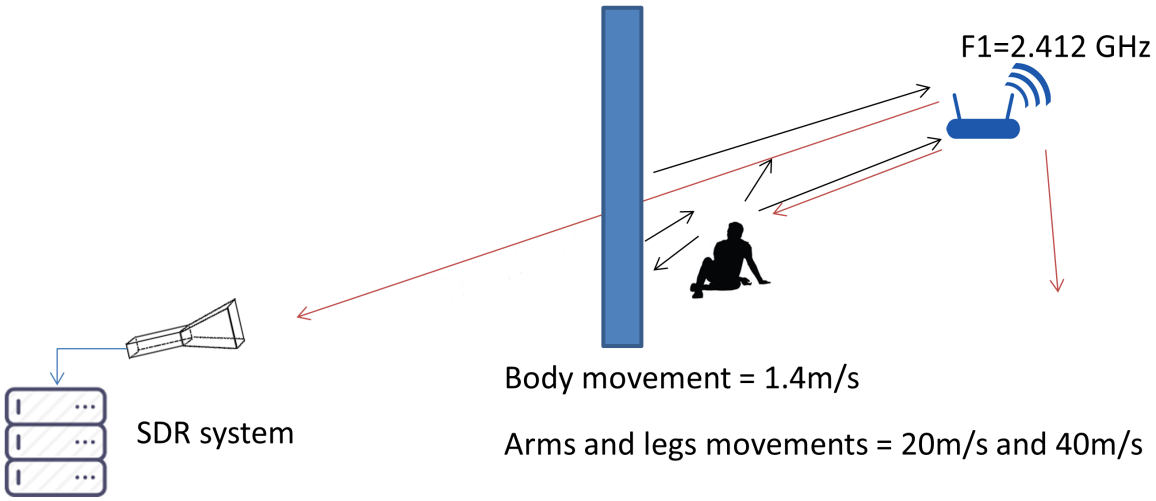


Fig. 2.5: Because of the moving person, the reflected signal contains frequency shifts (Doppler Effect). Both the velocity vector and the Doppler shift are broken into the vertical and horizontal components.

other papers have demonstrated that limbs create 300 Hz shifts, representing a falling body Lyonnet (2010) (shown in Figure 2.5). Modelling the limb and body reflected signals yields Equation 2.6.

$$f_{Dop} = \frac{\triangle\ limb}{c} f_{router} + \frac{\triangle\ body}{c} f_{router} + f_{router} \tag{2.6}$$

c is the speed of light. f_{Dop} is the combined Doppler shifts.

Delayed signals from electromagnetic waves' reflections and refractions cause polarity and power level changes. Multipath is defined in Equation 2.7. Multipathing is relatively stable in hallways and room where furniture remains unmoved (Figure 2.8). Thus by sensing these multipathing signals using a horn antenna and a high-speed digitizer, we can characterize human movement patterns which are encoded by the multipathing properties of the building.

$$\rho_0 e^{j2\pi f_{Dop}}\delta(0) + \rho_1 e^{j2\pi f_{Dop}}\delta(1) + ... + \rho_k e^{j2\pi f_{Dop}}\delta(k) \tag{2.7}$$

Where ρ represents power lost during multipath delay, $e^{jf_{Dop}}$ represents the Wi-Fi carrier signal, and $\delta(t)$ is the impulse function.

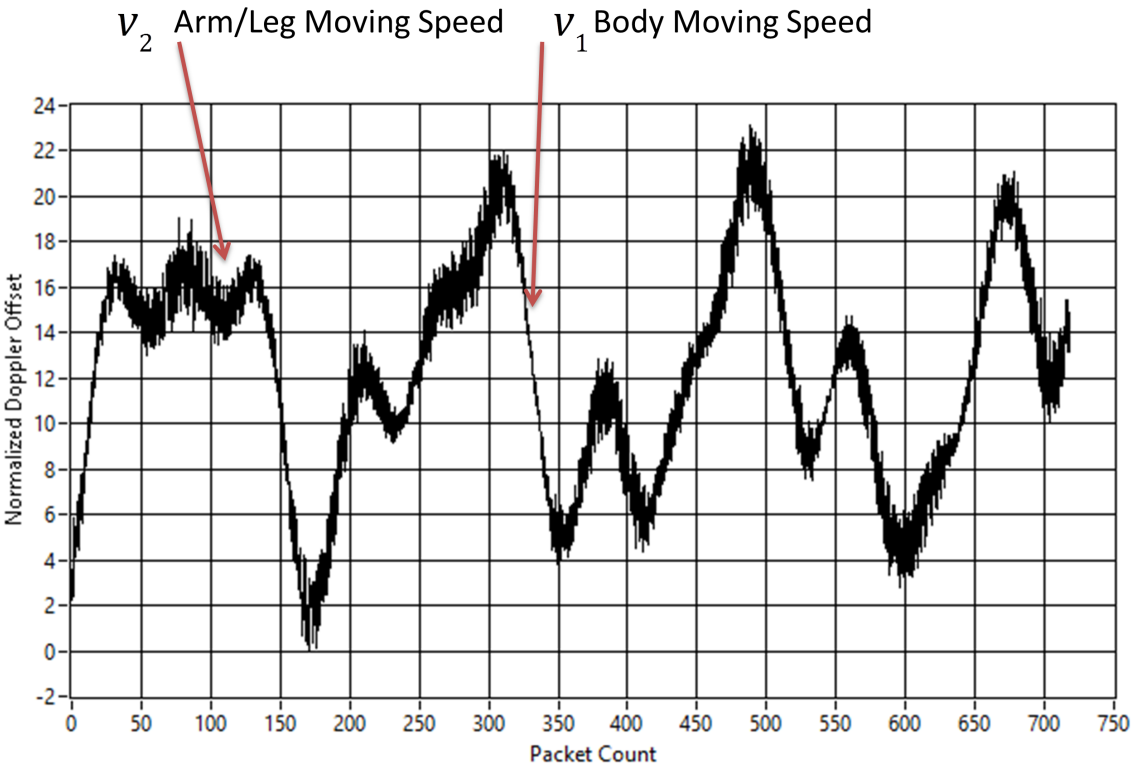


Fig. 2.6: This graph shows received pilot tones offsets with Doppler Effect caused by arm, leg, and body movements.

2.5.3 Amplifying Doppler Effect and Multipathing in CSI

The main challenge is capturing CSI values from 802.11 standard Wi-Fi signals and amplifying movement interference. The NI RF test bed must capture persons strolling through a hallway. During the capture, the two methods for removing noise

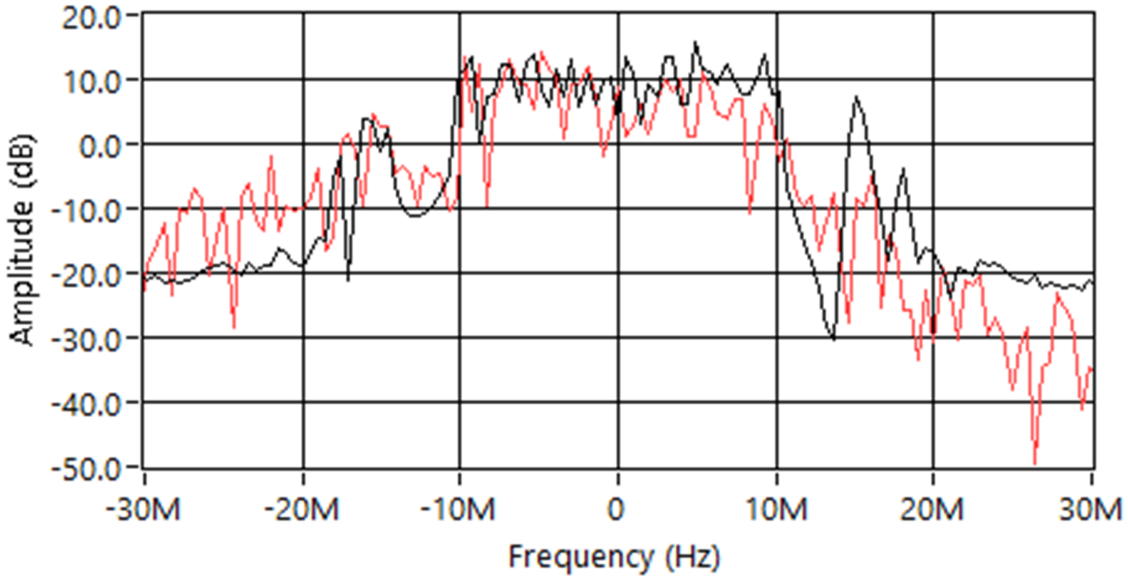


Fig. 2.7: Black is the magnitude of the baseband OFDM BPSK Modulated Signal Beacon Transmitted. Red line is the baseband signal received with channel effects.

and amplifying gait signature are antenna design and correlation. To characterize multipathing, a horn antenna sensed horizontal and vertically polarized signals. Transitions between the horizontal and vertical components occur when electromagnetic waves encounter human traffic. High gain and directionality provide increased movement signals and remove interference noise. Using multiplication, correlation increases the weak multipathed signal to provide a second signature through multiplication.

2.5.4 Signatures: Doppler Shifts and Multipath

Doppler shifts and multipathing occur in all mobile wireless systems. Therefore, all wireless receivers must compensate for carriers' frequencies shifts and delayed signals. In OFDM, an equalization scheme uses pilot tones to measure the channel interference. By measuring the equalization values, we form signatures to charac-

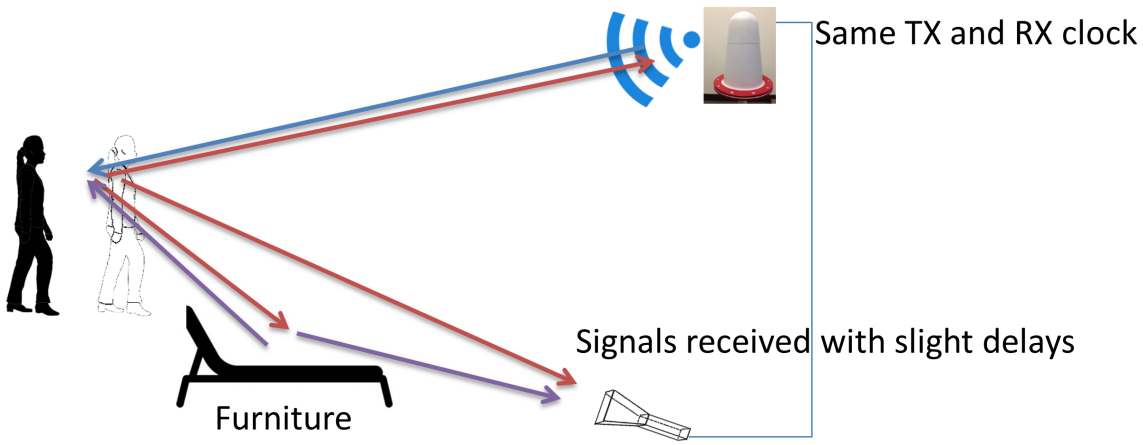


Fig. 2.8: As humans and room configuration change, the multipath signals also change. Because human gait is relatively consistent, we can encode a human signature using the physical channel, sensed by Wobly.

terize movement. To measure the shifted pilot tone levels, an OFDM demodulator uses a Fast Fourier Transform (FFT) to obtain carriers (Figure 2.7). The FFT also senses the amount of energy in each frequency bin. We measure the amount of shift by subtracting the sent and received demodulated signal (shown in Equation 2.8) (Figure 2.6).

$$S_1 = \sum_k \rho_k \kappa \sin(\pi f_{Dop} + f_{sent}) \sin(\pi f_{Dop} - f_{sent}) \delta\left(t - \tau_k\right) \tag{2.8}$$

Cross-correlation amplifies weak delayed signals. By multiplying received and sent signals, the values measure after the end of each pulse describes the multipath signals (Figure 2.9). Random noises do not correlate are minimized because of multiplication.

Let tx^* be the sent signal's conjugate, $rx(t)$ be the received pulse signal, and $\eta(t)$ be a Gaussian be the model of electromagnetic interference thermal noise.

$$\sum_t tx^*(k) rx(k+t) + tx^*(k)\eta(t) \tag{2.9}$$

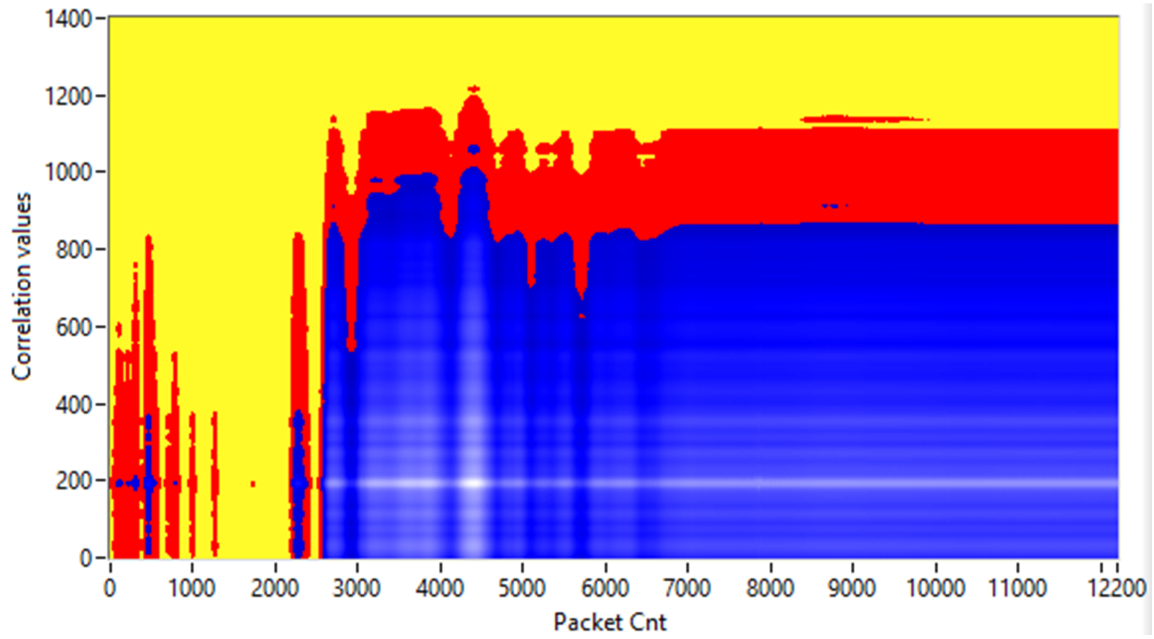


Fig. 2.9: Correlation between sent and received signals demonstrating multipath

The time domain correlation is defined in Equation 2.9 (Figure 2.10).

Because the non-correlative nature of the thermal noise, we can assume $x^*(k)\eta(t)$ is sufficiently small. We are able to measure the amount of delay, ρ_k, by measuring the distance between maximum and half of maximum point of correlation. Let $M_{\max}$ and $M_{\max/2}$ be the correlation maximum and half of the maximum values respectively. Let max and $\max_2$ be the index associated with those values respectively. Therefore we can define the distance of the correlation as $S_2(i) = \max_2 - \max$.

2.5.5 Detecting the Gait Cycle

The gait cycles are defined by points in the signatures where there are the fast change in frequency shifts and multipath delays. These points are the local minimums in the signatures. We measure the gait feature by measuring area under curve between these local minimums representing each step. Let G_k be the start and stop of each

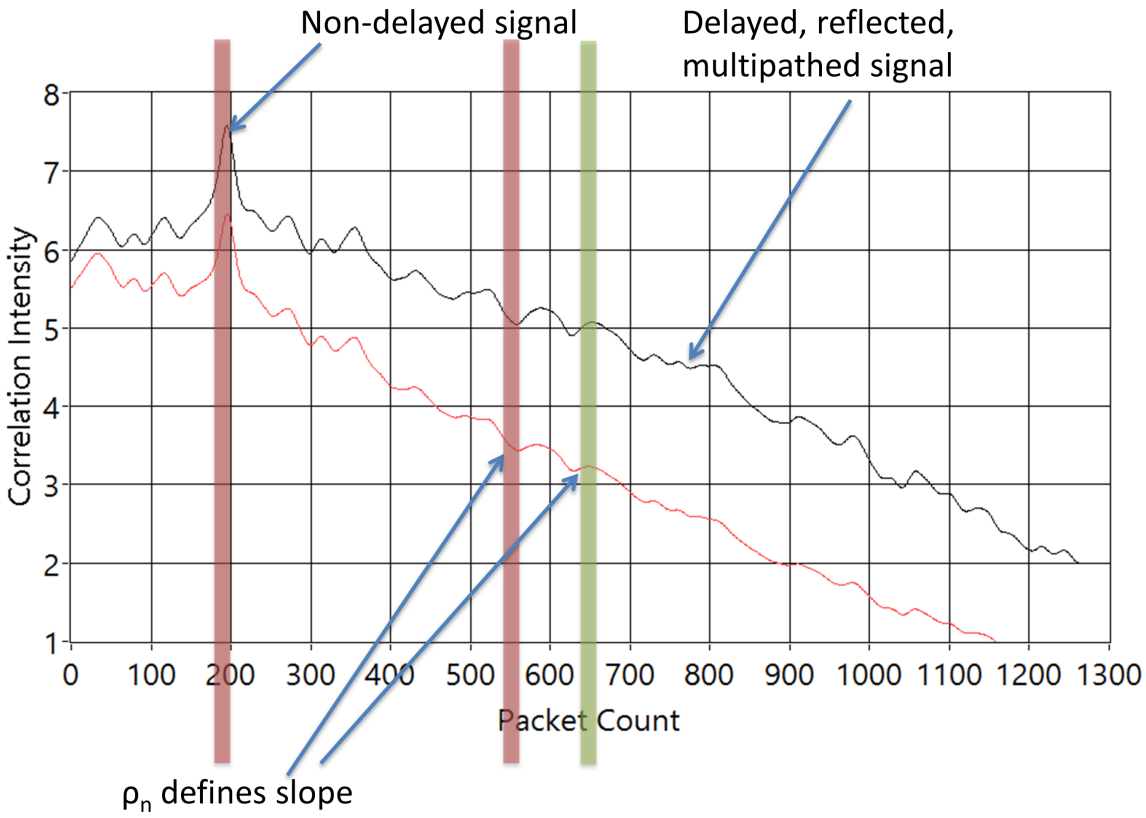


Fig. 2.10: This is correlation between a noisy and the original signal. Red and black lines represent two different time instances.

step. By using a wavelet transform, the algorithm finds the valleys in the features Adib et al. (2014). Let $G_k\,(j)$ be the m^{th} local minimum. For n local minimums, the feature gait vector can be defined in Equation 2.10.

$$f(j) = \left[\sum_{j=m}^{m+1} G_k(j), \sum_{j=m+1}^{m+2} G_k(j) \ldots \sum_{j=m+n-1}^{m+n} G_k(j)\right] \tag{2.10}$$

2.5.6 Sensing Movement

Human movement detection depends on thresholding the amount of Doppler shifts and Multipath offset. To perform human presence detection, the differential in

each feature set must exceed a calibrated constant M. The M is associated with the frequency shift of a falling body around 200 Hz. Therefore acquisition begins when $f(j) > M$.

2.5.7 Biometric Identification

This section describes how we used a Naïve Bayes classifier to distinguish identities and activities. First the data is filtered using a low pass smoothing and a threshold filter. The feature points that fall outside the 10% standard distribution are also removed, as they are artifacts. The Naïve Bayes used two fold cross validation as training data.

Let classes be I defining individuals (A_I); Multipath feature ($f_{mp}(k)$), Doppler Shift feature ($f_{ds}(k)$), and time ($f_{time}(k)$) are the observed features. Thus the Naïve Bayes classifier is defined in Equation 2.11, selecting the largest and closest probability given the observations.

$$\underset{k\in\{1,\ldots,I\}}{\arg\max}\, p\left(A_I\right) p\left(f_{mp}(k)|A_I\right) p(f_{ds}(k)|A_I) p\left(f_{time}(k)|A_I\right) \tag{2.11}$$

2.5.8 Localization

To locate individuals, we also used a Naïve Bayes classifier. Based on the observed Doppler frequency shifts, multipathing interference, and the time since human movement detection, the Naïve Bayes classifier determined locations. The locations points are discrete values measured in the room. Let classes be L defining discrete locations points (A_L); Multipath feature ($f_{mp}(k)$), Doppler Shift feature ($f_{ds}(k)$), and time ($f_{time}(k)$) are the observed features.

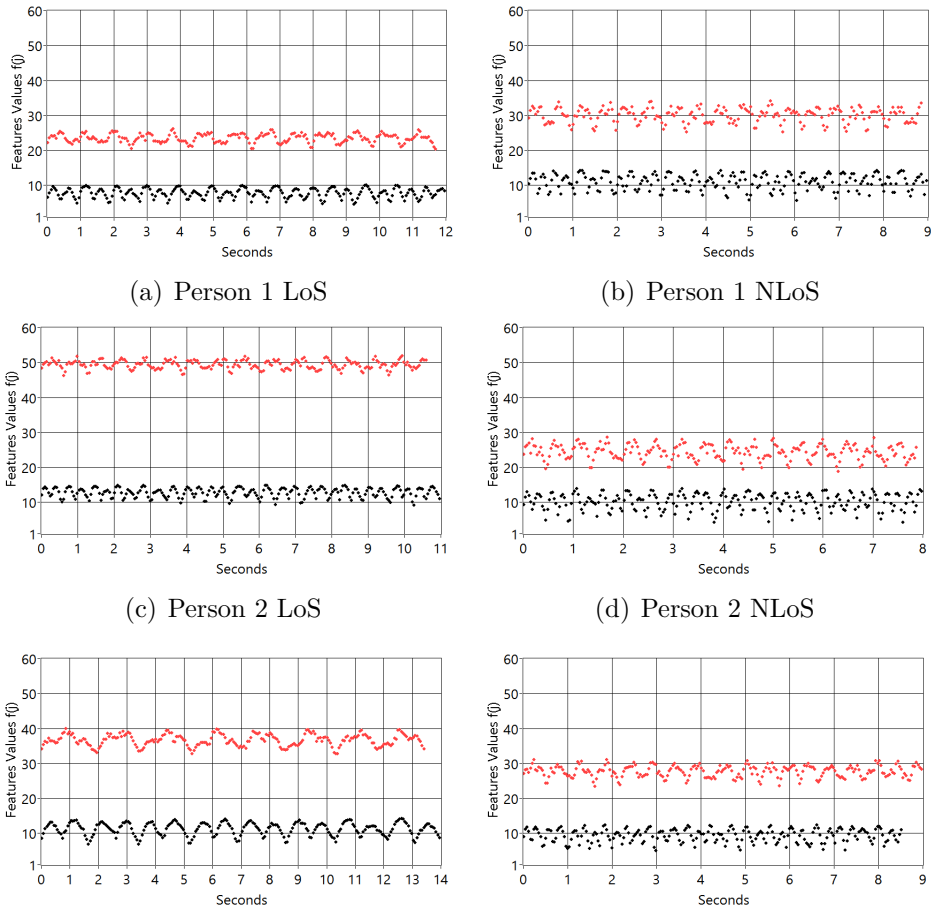
$$\underset{k\in\{1,\ldots,L\}}{\arg\max}\, p\left(A_L\right) p\left(f_{mp}(k)|A_L\right) p(f_{ds}(k)|A_L) p\left(f_{time}(k)|A_L\right) \tag{2.12}$$

2.6 Performance Evaluation

This section discusses the empirical implementation to sense humans and produce two features. The challenge addressed is demonstrating differentiation in a repeatable realistic test environment. A statistical model shows a description of the differentiation. Section 2.6.2 discusses the control or the baseline cases, showing noise rejection. Section 2.6.3 discusses the 12 signatures obtained from the experiment. Section 2.6.4 discusses signature sets during three human activities: sitting, falling, and dragging the leg. Section 2.6.5 demonstrates the signature as distinguishable and localization from features.

To emulate deployment in a clinic that serves individuals of different age ranges and sexes, we selected six different individuals. There were three males and three females with ages ranged from teens to 60s. The individuals walked in the middle hallway for about 12 meters, repeating this action several times (Figure 2.14). For the behind-the-wall case, the horn antenna was placed in a different room, 0.5 meters away from the wall. The broadcasting omnidirectional antenna was placed in the center of the hallway, and the receiving horn antenna was placed at an approximate height of 1.5 meters at the end of the hallway facing the test subjects. The test subjects were told to walk as naturally and consistently as possible. The Tx simulated a Wi-Fi deployment using a beacon transmitting using an omnidirectional antenna (Figure 2.15). The RF acquisition was aligned to the start and stop times, such that recorded time determined the location of the individuals.

Wi-Fi Signal Transmission We created a Wi-Fi beacon pulsing at an interval using the NI RF test bed. In 802.11 standards, modulation is Binary Phase Shift Key (BPSK). BPSK has two phase states representing 0 and 1. To minimize inter-symbol



(a) Person 1 LoS

(b) Person 1 NLoS

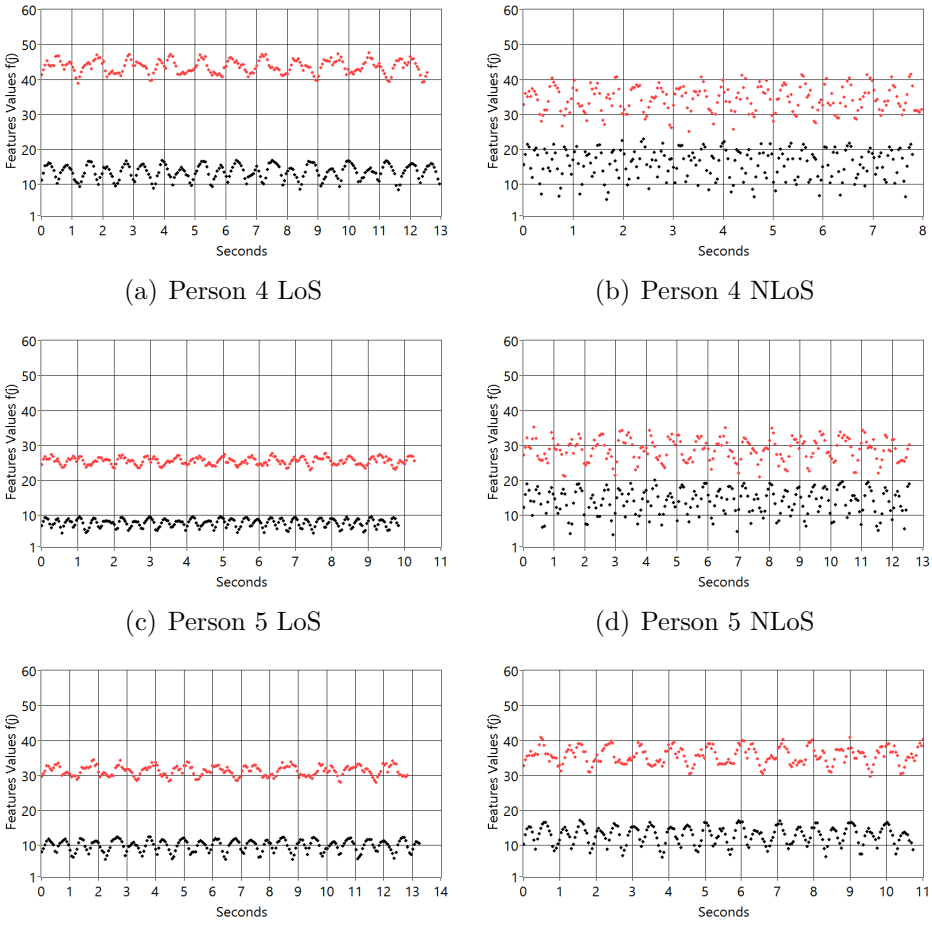
(c) Person 2 LoS

(d) Person 2 NLoS

(e) Person 3 LoS

(f) Person 3 NLoS

Fig. 2.11: Human signatures of first group of 3 individuals, who walked repeatedly, demonstrated stability and uniqueness. Red is the Doppler Effect gait feature, and black is the multipathing gait feature. Person 1 was male, age 29. Person 2 was female, age 26. Person 3 was male, age 49.



(a) Person 4 LoS

(b) Person 4 NLoS

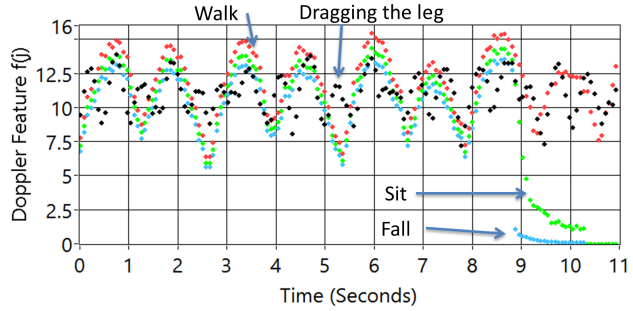
(c) Person 5 LoS

(d) Person 5 NLoS

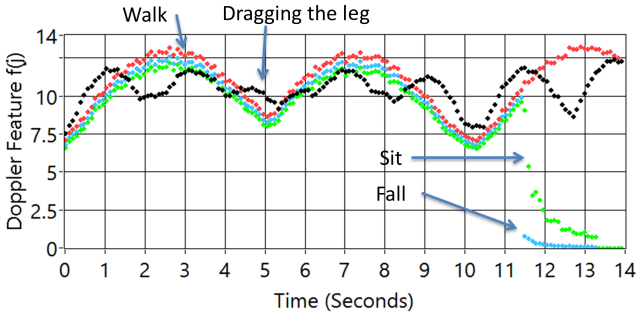
(e) Person 6 LoS

(f) Person 6 NLoS

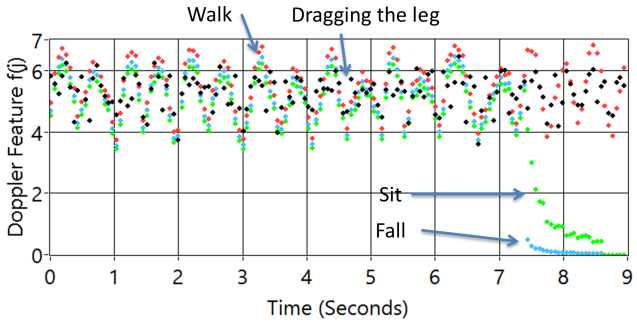
Fig. 2.12: Human signatures of 2nd group of 3 individuals, who walked repeatedly, demonstrated stability and uniqueness. Red is the Doppler Effect gait feature, and black is the multipathing gait feature. Person 4 was female, age 59. Person 5 was male, age 19. Person 6 was female, age 15. Each data point represents about 5 beacons or 500 milliseconds. The signatures were low pass filtered.



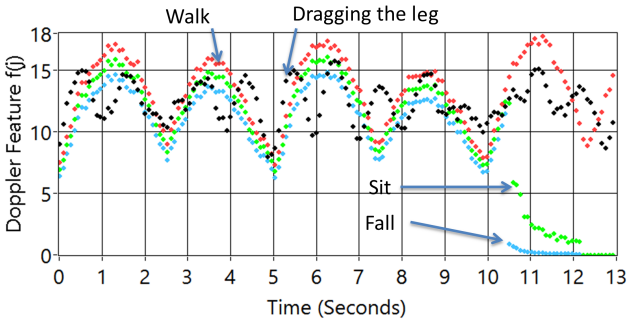
(a) Person 1



(b) Person 2



(c) Person 3



(d) Person 4

Fig. 2.13: Doppler Effect signatures of four individuals performing four actions: walking (red), sitting in chair (green), dragging a foot (black), and sitting on the ground (blue), demonstrated patient monitoring capabilities in fall detection, localization, and identification. The Doppler features had better activity detection features than the multipath feature. The signatures created biometric signatures for each individual.

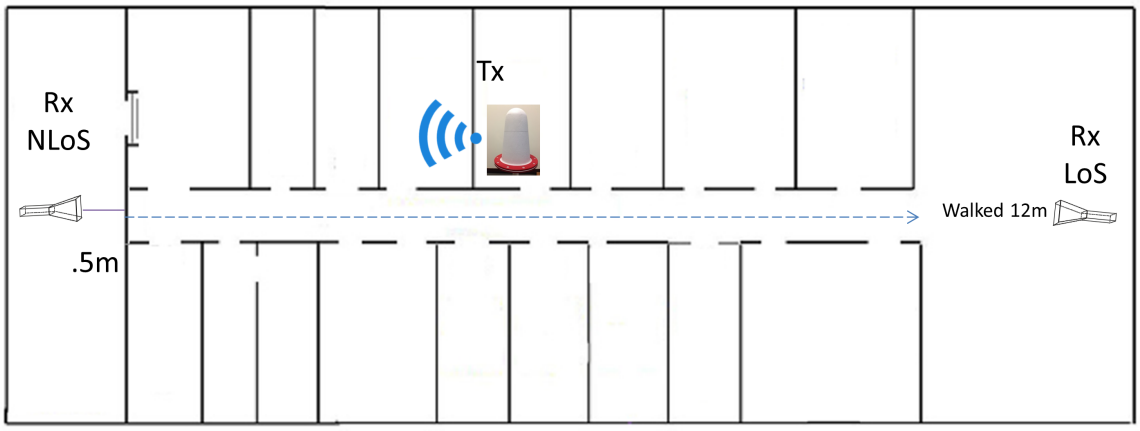


Fig. 2.14: Experimental setup showing multiple persons walked in a hallway repeatedly for 12 meters. Each person walked 10 times to provide training and classification data. The transmitting antenna (Tx) was placed in a middle hallway, and receiving antenna (Rx) was placed at the end of the hallway. Two different scenarios with line-of-sight and none-line-of-sight provided empirical data.

interference, the 802.11 standard require a cyclic prefix. The prefix is added to the beginning by copying portions of the end signal. Beacons consisted of 51 carriers, derived from 51 bits using 20 MHz of bandwidth. The carriers were summed together by the parallel to serial converter. An iFFT occurred on the signal to produce the Wi-Fi beacons.

Beacon Reception To receive the beacons and sense human activity, the NI RF test bed must sample the signal. To minimize noise, the signals were amplified right after the antenna and carried along RF over fiber system. RF-over-fiber systems are used in modern buildings to carry signal across great distances. We oversampled the data at 150 MS/s. The preamp amplified 10 dB from the ARA horn antenna. The horn antenna provided an additional 15 dB of directional gain in the main lobe. A transmitter (TX) and receiver (RX) pair operated on the same NI PXIE system providing the same clock. The RX digitized the baseband signal, streaming the

oversampled digitized values to the RAID (redundant array of independent disks) drive. An algorithm demodulated the OFDM signal and produced the CSI values.

2.6.1 Performance Insight

Based on the signatures, we noticed both the fast limb and the slow body movements. We noticed that people who have similar body shape do have similar features but are still distinguishable. When at rest on the ground or sitting on the chair, the Doppler features clearly showed different speed of action. Based on visual inspection, it was clear that features are different for someone dragging their legs. We utilized a simple Naïve Bayes to demonstrate that the features were classifiable. A more complex machine learning algorithm would produce better results.

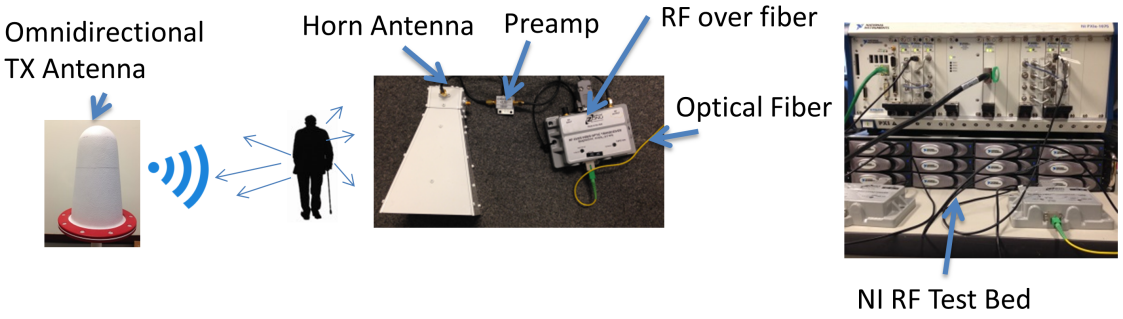
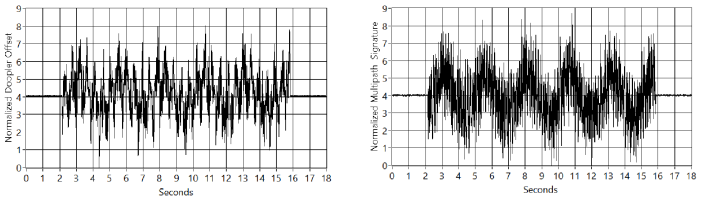


Fig. 2.15: The NI RF test bed consisted of signal acquisition (PXIe-562), signal generation (PXIe-5652), the down-converter (PXIe-5601), and the up-converter (PXIe-5450). To maintain high signal-to-noise ratio, we used a RF over fiber system.

2.6.2 Baseline: Control Case Signature

The challenge addressed in this section is the stability of the baseline signature with no movement and detecting human activity. The control case was a hallway of



(a) Baseline Doppler Effect feature (b) Baseline Multipath effect feature

Fig. 2.16: Doppler and multipath features demonstrated baseline and human activity. Baseline was when the area is devoid of movement.

an office devoid of movement. As expected, both signatures remained flat, because there was no movement to cause Doppler shift or multipathing (Figure 2.16). When a person strolled in the hallway, both Doppler and multipath feature changed. We observed both fast and slow changes in the signals representing the limb and body.

2.6.3 Repeatability and Uniqueness

The experiments demonstrated the uniqueness and repeatability of the signature. Six individuals walked the same area 10 times over. The feature graphs' multiple points, in each line-of-sight and none-line-of-sight scenarios, show that the structures to similar and stable (Figure 2.5.8).

Because each point represented 500 milliseconds from 10 trials, these feature graphs demonstrated that the signatures are unique for each person. Features are dependent on the antennas' locations and room configuration requiring recalibration. In most buildings, we can reasonably assume that furniture movement happens infrequently. We noticed that people with similar body sizes do produce similar features.

2.6.4 Detecting Events Like Falls and Abnormal Gait

Figure 2.13 shows unique features for individuals walking normally, sitting on a chair, sitting on the ground, and dragging a foot. We repeated each hallway walk experiment 10 times. The signatures were acquired in the hallway in NLoS. The antenna was placed at a two meters height and 0.5 meters away from the wall in an end of hallway room. Based on visual inspection, we can reasonably conclude that the feature can distinguish falls and abnormal gait.

2.6.5 Feature differentiability

The challenge addressed in this section is differentiation among the feature sets. We removed features that had little Doppler or multipath interference. The features that the Naïve Bayes classifier observed were Multipath, Doppler, and relative time of reception. The classes were persons identities, actions (sitting, falling, or dragging the leg), and location points. The simple Naïve Bayes classifier detected the right identity at about 92% rate (Table 2.2). The detection rates for dragging the leg, sitting on a chair, and falling to the ground were around 87%. Using location markers as classes, the average localization classification correct rates were around 80%.

2.7 Future Work

For Wobly to function in the real-world, it must sense multiple persons and adapt to room changes. WiTrack2.0 Adib (2015) has demonstrated sensing multiple persons and limbs. To adapt to room configuration changes, the two main methods are empirical-based machine learning and propagation scattering inversion. Machine learning depends on calibration, and scattering inversion require large numeric solutions to Maxwell equations. Both techniques should compensate for noise from

weather or other interferences. We recognize that limited non-diverse empirical testing, but Wobly extends existing developed gait-based biometric analysis.

2.8 Related Work

These sections describe previous studies that sense human movements and localized persons, addressing the challenges of monitoring humans. The following sections discuss previous works processing RF signals. All reviewed works have failed to identify and localize person based on intrinsic body movement.

Unlike previous works, this paper profiles the human gait to create signatures for biometrics, enabling tracking and tagging. This technique uses existing Wi-Fi signals utilizing only a receiver streaming system with through-wall penetration.

Using RF to sense human movements RF allows for NLoS and lower cost architecture. Recent works using human signals detected by RF sensors have provided the possibility of automation. Wobly produces human signatures based on the Doppler Effect and multipath signals Ting Zhu (2016). These systems have the ability to penetrate walls, track body parts, and sense multiple people's locations Oppermann, Boano, & Römer (2014). CARM, CSI (Channel State Information) Activity Recognition, quantifies correlations between CSI and human activity. CARM achieves 96% accuracy in detecting specific human activity using commercial Wi-Fi devices Wang et al. (2015). WiDraw uses Wi-Fi signals' Angle-of-Arrival to track hand trajectories to an error rate lower than 5 cm% Sun et al. (2015). By using inaudible sound pulses, AAMouse can turn a human hand into a mouse Yun (2015). WiSee enables whole home gesture recognition by measuring Doppler shifts Pu et al. (2013). Using Wi-Fi signals and MIMO interference nulling allow Wi-Vi to see behind walls and recognize gestures Adib (2013). Humantenna is an on-body sensing, which picks up

electromagnetic noise, to recognize body poses Cohn Gabe Morris (2012). WiTrack uses Time-of-Flight from multiple antennas to locate human through walls Adib et al. (2014), and WiTrack2.0 introduces Successive Silhouette Cancellation to localize multiple persons Adib (2015). Respiration rates can be sensed by measuring signal strength in single pair Kaltiokallio (2014) and network Luong et al. (2015). E-Gesture is an energy efficient gesture recognition system which uses motion sensing and smart phones Park et al. (2011). Using signal cancellation of 5 antennas, a SDR can identify keystrokes Chen (2015). These systems do not provide biometrics or specific person signature detection, but they are focused on localization and detecting movements.

RF Localization Tracking devices and individuals have been studied heavily using Signal Strength (SS), Time Difference of Arrival (TDoA), and Angle of Arrival (AoA) Lymberopoulos et al. (2015). These techniques always use some sort of statistical algorithm with geometry to determine location. Using TDOA and RSS, Cramer-Rao provides for indoor and outdoor localization Patwari et al. (2003). SpotOn uses CSI and applying algorithms to estimate the direction and triangulation from multiple Wi-Fi access points. SpotOn achieves accuracy of 0.6m in LoS and 1.5m in NLoS cases Kotaru et al. (2015). Tadar tracks moving objects using COTS RFID readers and tags in a 2D plane, converting RFIDs into antenna arrays for through-wall detection Yang et al. (2015). RFID receivers and transmitters placement optimization provides improved accuracy Wagner et al. (2012). Radio tomographic imaging (RTI) is able to track up to 4 targets based on SS sensing on multiple frequency bands Bocca et al. (2014). ToneTrack uses modern day smart devices, which operate on multiple frequency bands, increasing the effective bandwidth and also rely on TDoA Xiong (2015). Because of frequency hopping Bluetooth Low Energy (BTLE) and higher sampling rate, BTLE localization is more accurate Zhao et al. (2014). mTrack uti-

lizes highly direction 60 GHz millimeter wave radios to track a pen, within 8 mm precision based on AoA (beam-steering and phase shift) Wei (2015). FollowME uses geomagnetic field and natural walking patterns from previous users for navigation in both in-door and semi-outdoor scenarios Shu et al. (2015).

Indoor localization has also been done using smart phone internal sensors, such as accelerometers and contextual knowledge Parnandi et al. (2010). Detecting NLoS conditions enable better distance estimations Xiao et al. (2015). Ring Overlapping bases on Comparison of Received Signal Strength Indicator (ROCRSSI) uses a range free localization method Liu, Wu, & He (2004). Similarly, a range free anchor free Monte Carlo localization algorithm improves accuracy and processing time Baggio & Langendoen (2008). APIT is also a range free solution for random nodes with irregular radio patterns He et al. (2003). RFIDs have been used for sensor calibration dynamic environments for Wi-Fi localization systems Chen et al. (2005). SpinLoc is able to provide precise indoor localization using Doppler Effect Chang et al. (2008). A distributed online learning algorithm is able to converge on the location using a wireless sensor network Galstyan et al. (2004). Sequenced based localization proves fewer geometric nodes are required in a multipath fading RF channel Yedavalli & Krishnamachari (2008). When FM and Wi-Fi signatures are combined together, improved localization is able to overcome channel interference Chen et al. (2013).

2.9 Summary

In this paper, we introduced a novel gait-based activity monitoring system (i.e. Wobly), which can identify and track individuals and their corresponding activities by using Wi-Fi signals. In contrast to traditional approaches, this technique penetrates walls and does not require additional attached devices or special signals. Different

from other Wi-Fi based human activity recognition systems (e.g., CARMWang et al. (2015) and WiTrackAdib et al. (2014)), our system can identify individuals based on their unique gaits. Specifically, we presented 1) methods of identifying and tracking individuals in LoS and NLoS, showing uniqueness of signatures, which is encoded by gaits; 2) integration with existing modern Wi-Fi infrastructure by using demodulation and correlation of OFDM signals; and 3) empirical analysis to differentiate human subjects walking and detections of different activities (walking, sitting on a chair, falling to the ground, and dragging a leg) in LoS and NLoS. Using wavelets, Wobly characterizes the signatures and provides feature vectors for a simple Naïve Bayes classifiers, which can identify and locate with 87% correctness and 90% correctness respectively.

Table 2.1: Confusion matrix for LoS (Top) and NLoS (Bottom) with Male (M), Female (F), sitting, and dragging leg cases

LOS NLOS	P1 M	P2 M	P3 M	P4 F	P5 F	P6 F	Sitting Ground	Sitting Chair	Dragging Leg
P1	924	11	9	14	13	12	11	13	14
M	832	13	16	18	17	13	12	11	12
P2	12	913	16	12	11	16	13	17	18
M	14	861	13	14	15	11	12	20	15
P3	16	11	895	12	14	12	11	17	15
M	18	14	851	13	12	20	16	12	13
P4	18	16	18	988	15	13	17	16	12
F	16	13	14	870	19	18	12	20	15
P5	18	13	21	17	895	14	19	18	20
F	14	12	13	16	854	17	22	21	19
P6	16	16	16	12	14	951	17	16	12
F	13	17	14	16	16	474	22	12	17
Sitting	16	18	18	21	14	16	891	18	22
Ground	13	17	14	16	16	24	882	12	11
Sitting	18	18	17	21	18	16	18	891	12
Chair	17	17	14	18	16	14	17	862	18
Dragging	16	16	15	22	17	17	12	17	892
Leg	13	17	14	16	16	18	21	19	871

Table 2.2: Naïve Bayes classifying features sets for positioning of individuals

LOS NLOS	1M	3M	6M	9M	12M
1M	899	21	23	21	24
	833	25	28	17	19
3M	23	893	18	20	21
	26	788	25	19	23
6M	16	21	895	21	24
	18	24	871	31	29
9M	17	20	19	858	25
	21	19	23	790	28
12M	21	19	22	19	895
	24	27	31	26	814

Chapter 3

CHIRON: CONCURRENT HIGH THROUGHPUT COMMUNICATION FOR IOT DEVICES

3.1 Overview

The exponentially increasing number of heterogeneous Internet of Things (IoT) devices motivate us to explore more efficient and higher throughput communication, especially at the bottleneck (i.e., edge) of the IoT networks. Our work, named Chiron, opens a promising direction for Physical (PHY) layer concurrent high throughput communication to heterogeneous IoT devices (e.g., wider-band WiFi and narrower-band ZigBee). Specifically, at the PHY layer, Chiron enables concurrently transmitting (or receiving) 1 stream of WiFi data and up to 4 streams of ZigBee data to (or from) commodity WiFi and ZigBee devices as if there is no interference between these simultaneous connections. We extensively evaluate our system under different real-world settings. Results show that Chiron's concurrent WiFi and ZigBee communication can achieve similar throughput as the sole WiFi or ZigBee communication. Chiron's spectrum utilization is more than 16 times better than the traditional gateway.

3.2 Introduction

Internet-of-Thing (IoT) devices use different radios and modulation mechanisms (e.g., WiFi, ZigBee, and Bluetooth). Therefore, they cannot directly communicate with each other. Traditionally, communication between different wireless technologies is achieved indirectly via gateways equipped with multiple radio interfaces. The gateway will become a bottleneck when the exponentially increasing number of heterogeneous IoT devices are deployed. For example, in Figure 3.1, when the WiFi device is transmitting packets to the gateway, the ZigBee device has to back-off to avoid the collision. Similarly, when the ZigBee device is transmitting to the gateway, the WiFi device needs to back-off. Since WiFi's bandwidth (20 MHz) is much higher than ZigBee's bandwidth (2 MHz), when ZigBee is transmitting, WiFi's 18 MHz spectrum that is not overlapped with ZigBee is wasted (shown in Figure 3.1).

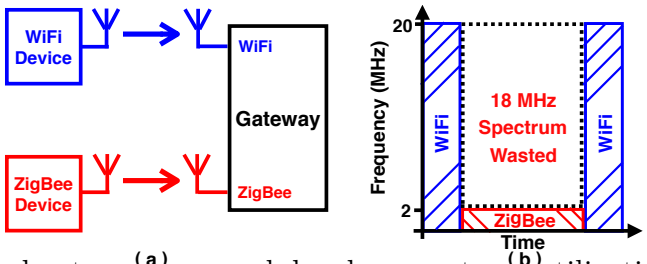


Fig. 3.1: Traditional gateway approach has low spectrum utilization, which results in low aggregated throughput.

Moreover, we argue that even ZigBee's 2 MHz spectrum may not be fully utilized, because ZigBee's maximum throughput is only 250 kbps, which results in 0.125 bit/s/Hz spectrum utilization. On the other hand, WiFi's spectrum utilization is much higher. For example, with 20 MHz bandwidth, 802.11n can achieve up to 288.8 Mbps throughput 802, which results in 14.4 bit/s/Hz. Therefore, we argue that we should explore a more spectrum efficient and higher throughput communication

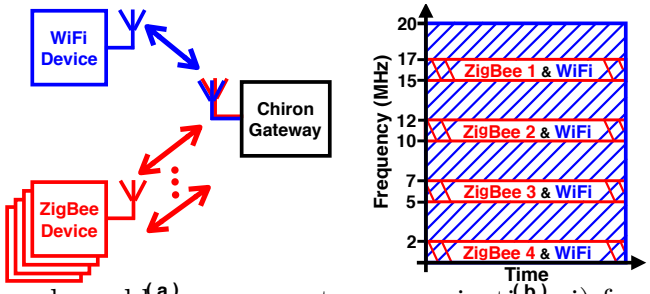


Fig. 3.2: Our approach enables concurrent communications i) from commodity WiFi and ZigBee devices to the gateway; and ii) from the gateway to commodity WiFi and ZigBee devices. Therefore, the spectrum utilization is significantly increased.

technique in ZigBee and WiFi coexisted environment.

In this paper, we introduce a new direction for PHY layer concurrent high throughput communication from (or to) heterogeneous (i.e., wider-band WiFi and narrower-band ZigBee) IoT devices. As shown in Figure 3.2, our work (named Chiron) enables concurrently transmitting (or receiving) 1 stream of WiFi data and up to 4 streams of ZigBee data to (or from) commodity WiFi and ZigBee devices as if there is no interference between these concurrent transmissions. In a nut-shell, Chiron enables the concurrent high throughput communications at the PHY layer by leveraging WiFi and ZigBee signals' unique difference – WiFi's low symbol rate (i.e., 250 Ksymbol/s) verses ZigBee's high chip rate (i.e., 2 Mchip/s). By doing this, we significantly increase the spectrum utilization and overall aggregated throughput among IoT devices.

The main contributions of our work are as follows:

• To the best of our knowledge, this is the first work that enables concurrent high throughput communication i) from the gateway to heterogeneous commodity IoT devices; and ii) from IoT devices to the gateway. Our new gateway design naturally fits at the edge of the IoT networks and can significantly increase the spectrum utilization and overall aggregated throughput.

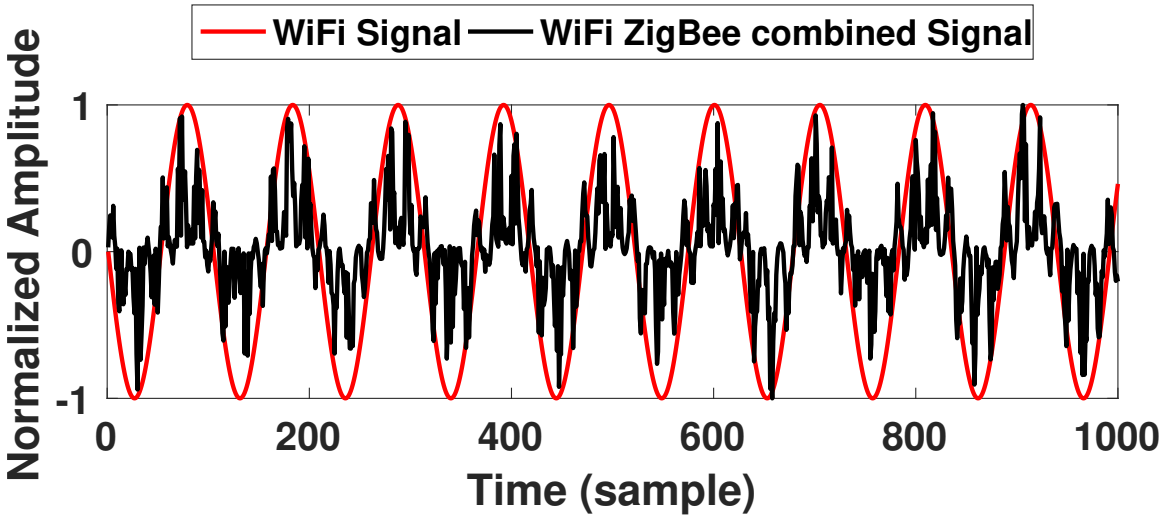


Fig. 3.3: Combined WiFi and ZigBee Signals

• To enable the concurrent communication, we addressed several unique challenges, which include i) how to detect and separate the concurrently received WiFi (e.g., IEEE 802.11 g/n) and ZigBee (e.g., IEEE 802.15.4) signals at the gateway; and ii) how to concurrently send out the combined WiFi and ZigBee signals, which can be demodulated by both commodity WiFi devices and commodity ZigBee devices.

• We implemented Chiron on i) commodity WiFi devices; ii) commodity ZigBee devices; and iii) USRP devices. Then, we extensively evaluated our system under four real-world scenarios (i.e., line-of-sight, none-line-of-sight, human in the middle, and wearable). Results demonstrate that Chiron's spectrum utilization is more than 16 times more than the traditional gateway.

3.3 Observation and Motivation

The design of Chiron is motivated by the following observation:

Observation: Although WiFi and ZigBee communicate at the overlapped radio fre-

quency, WiFi's symbol rate and ZigBee's chip rate [1] are significant different that WiFi's symbol rate is 250 Ksymbols/s while ZigBee's chip rate is 2 Mchips/s.

This observation serves as the foundation of our design. Figure 3.3 shows the combined WiFi and ZigBee signal (the black line) in time domain. The red line is the original WiFi signal. From Figure 3.3, one can tell that WiFi signal's amplitude changes much slower than ZigBee signal's amplitude. Therefore, it is possible to design a gateway that can send (or receive) the combined WiFi and ZigBee signal which contains both WiFi data and ZigBee data to (or from) commodity WiFi and ZigBee devices. By doing this, the spectrum utilization and throughput can be significantly increased.

3.4 Design Overview and Challenges

Based on our observation, the design goal of Chiron is to maximize the spectrum utilization when the gateway receives (or transmits) data from (to) commodity WiFi and ZigBee devices. Figure 3.6 shows Chiron's system architecture. For clarity purpose, we divide the whole system into two parts: i) Chiron Receiver and ii) Chiron Sender.

- Chiron Receiver (Figure 3.6(a)): There are two main challenges in Chiron receiver's design. The first challenge is how to incorporate different traffic patterns of wireless traffic generated by commodity WiFi and ZigBee devices at the gateway. To address this challenge, we design a customized WiFi & ZigBee signals detector, which can detect whether the received signal is a sole WiFi, sole ZigBee or a WiFi and ZigBee overlapped signal. The output goes to i) a

[1] ZigBee protocol uses Direct Sequence Spread Spectrum (DSSS) technique, in which, a chip is the smallest unit of a rectangular pulse. Similar to WiFi's symbol rate, ZigBee's chip rate reveals the signal varying speed.

WiFi demodulator when sole WiFi signals are detected; ii) a ZigBee demodulator when sole ZigBee signals are detected; or iii) a signal separator when the WiFi and ZigBee overlapped signal are detected. The second challenge is how to separate the overlapped signal. To address this challenge, we developed a signal separator by leveraging our observation that the WiFi's symbol rate and ZigBee's chip rate are significantly different. The detailed design is described in Section 3.6.1.

- Chiron Sender (Figure 3.6(b)): The main challenge in Chiron sender's design is how to combine the ZigBee signal with WiFi signal so that the combined signal can be demodulated at both the commodity ZigBee and WiFi receivers' side. To address this challenge, we developed WiFi & ZigBee Signals combiner with a linear optimization algorithm that generates the combined signals and ensures the signal distortion is within the tolerance range of commodity WiFi and ZigBee devices' modulation schemes. The detailed design is described in Section 3.6.2.

3.5 Background

To explain Chiron, it is necessary to first understand how WiFi and ZigBee radios work. Although our description is specific, our design has the potential to be applied to other heterogeneous radios that share the same frequency band.

3.5.1 How WiFi transmitter & receiver work

WiFi Transmitter: Figure 3.4(a) illustrates how the WiFi device transmits information in following steps:

Step 1: The WiFi data goes into a serial to parallel converter which allocates the bits

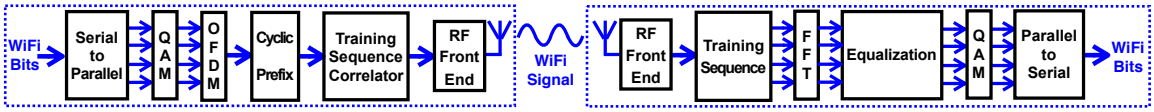


Fig. 3.4: The WiFi Transmitter and Receiver

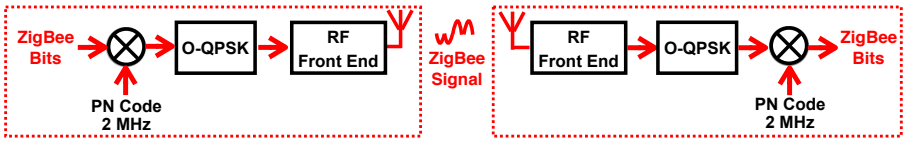


Fig. 3.5: The ZigBee Transmitter and Receiver

on different subcarriers.

Step 2: On each subcarrier, WiFi modulates information using Quadrature Amplitude Modulation (QAM) by mapping bits to different phases in sine waves.

Step 3: To combine the sine waves efficiently, WiFi adopts orthogonal frequency-division multiplexing (OFDM) by utilizing an inverse fast Fourier transform (IFFT), expressed in Equation 4.5. The duty cycle that the IFFT operates defines the symbol duration.

$$C_m(t) = \sum_{n=0}^{N} \left[(I(t)\cos(2\pi f t_1) - Q(t)\sin(2\pi f t_1))\, e^{2\pi j k n} \right] \tag{3.1}$$

Where there are N total WiFi subcarriers, and for each n subcarrier, we defined complex symbols states at the $I(t)$ and $Q(t)$ mapped by QAM. The duty cycle of each symbol is defined by f. We defined the subcarrier spacing frequency by k. Thus, $C_m(t)$ is the combined sine waves for mth bits.

Step 4: Between each symbol duration, a cyclic prefix is appended to reduce inter-symbol interference. The added cyclic prefix signal is defined as the baseband WiFi

signal.

Step 5: Before the baseband WiFi signal, a training sequence allowing for sender and receiver discovery and synchronization is added. Thus, in a conventional WiFi sender, the baseband and training sequence signals are then up-converter to the desired transmit frequency, amplified, filtered, and radiated by the RF front-end.

WiFi Receiver: Figure 3.4(b) shows how a WiFi receiver works in following steps:

Step 1: The radio down-converts the WiFi signal to baseband frequencies.

Step 2: The radio attempts to correlate for the training sequence. If the training sequence correlation exceeds the detection threshold, the signal goes to next step.

Step 3: The WiFi receiver will apply a standard FFT to the signal to separate the subcarriers.

Step 4: Multiple QAM subcarriers demodulators map the sine waves' phase states to each symbol state and bit combination.

Step 5: The demodulated bits on each subcarrier are combined by a parallel to serial convertor.

3.5.2 How ZigBee transmitter & receiver work

ZigBee Transmitter: Figure 4.5(a) illustrates how a ZigBee transmitter works in two steps:

Step 1: To compensate for channel interference and reduce the transmission power, ZigBee uses Direct Sequence Spread Spectrum (DSSS) to spread the signal into a wider band by multiplying with a higher rate (2 MHz) pseudorandom noise (PN) code. This PN code is shared between the sender and receiver.

Step 2: After the spread spectrum process, the ZigBee modulator maps the bits to sine waves by Offset Quadrature Phase-shift Keying (OQPSK) modulation which reduces

the dramatic phase shifts by offsetting the odd and even bits by a distinct period of time. The output of the OQPSK signal is the ZigBee baseband signal described in Equation 3.2. The output of the modulators is transmitted in the same manner as the WiFi.

$$Z(t) = \sqrt{\frac{2E}{T}} \cos\left(2\pi f t + (2n_z - 1)\frac{\pi}{4}\right), n_z = 1, 2, 3, 4 \tag{3.2}$$

Where E is energy per symbol, and T is the symbol duration. The symbol frequency is defined as f with 4 states defined by n_z.

ZigBee Receiver: Figure 4.5(b) shows how a ZigBee receiver works described in three steps:

Step 1: The radio down-converts the signal to the ZigBee baseband.

Step 2: The baseband signal is multiplied by or correlated to a shared PN code.

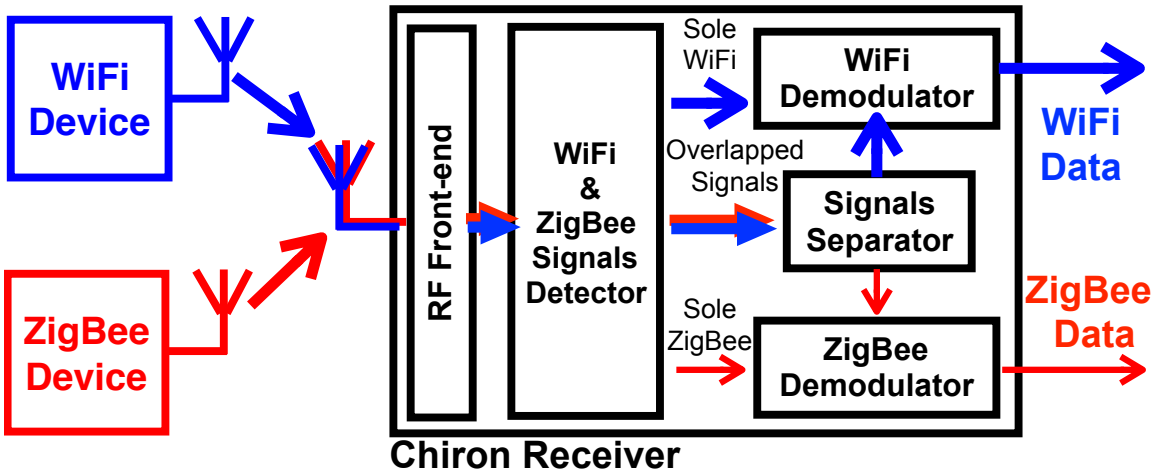
Step 3: If the PN code correlation exceeds the detection threshold, an O-QPSK demodulator maps the sine waves' phase states to each symbol and bit combination.

3.6 Design of Chiron

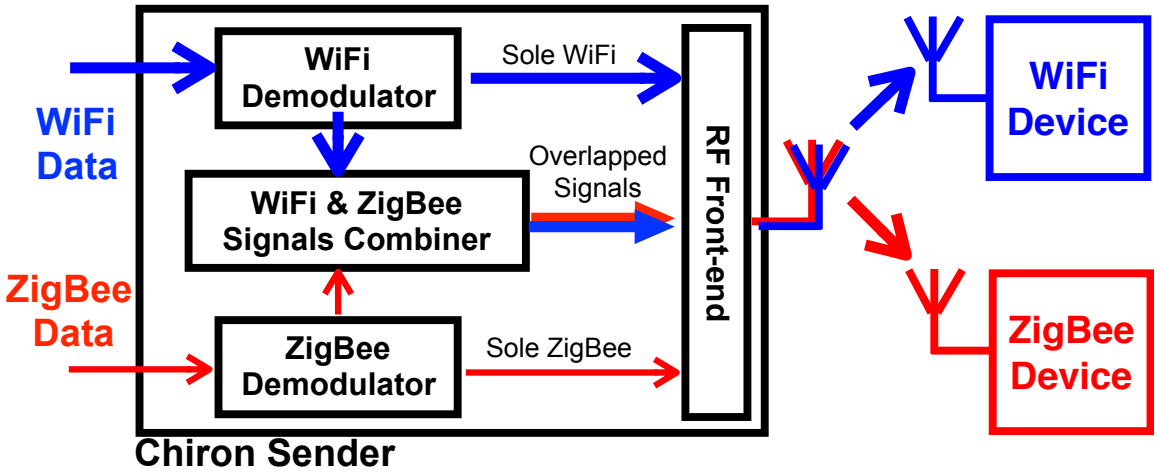
In this section, we describe the design of Chiron, which includes the receiver and sender parts.

3.6.1 Receiver

The objective of Chiron receiver is to disentangle the overlapped WiFi and ZigBee signals. However, before this disentanglement happens, the receiver must determine if and when the overlapped signal presents. To determine if and when this signal presents, we utilize i) WiFi training sequence and ZigBee PN code correlation; and ii) WiFi Channel State Information (CSI). When the overlapped signal is detected,



(a) Chiron Receiver



(b) Chiron Sender

Fig. 3.6: System Architecture

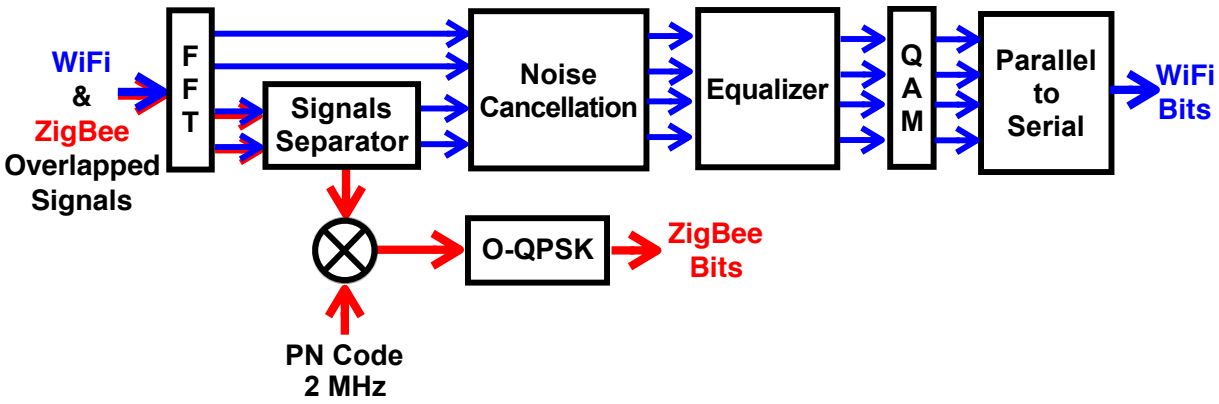


Fig. 3.7: The Demodulation of Overlapped WiFi & ZigBee Signals

we use noise cancellation and the native WiFi and ZigBee interference correction mechanism to recover the transmitted data. The following sections detail the i) WiFi & ZigBee signals detection and ii) overlapped WiFi and ZigBee signal receiving.

WiFi & ZigBee Signals Detection To ensure Chiron works with COTS WiFi and ZigBee devices, Chiron has to be backward compatible with normal WiFi and ZigBee signals. Thus, Chiron must be able to demodulate both the sole WiFi (i.e., a WiFi device is communicating with Chiron gateway without concurrent ZigBee transmission) or ZigBee packets (i.e., a ZigBee device is communicating with Chiron gateway without concurrent WiFi transmission). The first step is to determine whether the incoming signal is WiFi signal, ZigBee signal, or WiFi and ZigBee overlapped signal. This is based on WiFi training sequence ($WiFi\_taining\_seq$ and ZigBee PN code ($ZigBee\_PN$) correlation. To do this, we designed Algorithm 1 as follows. Where acq_signal is the incoming signal. W_t and Z_t are the correlation threshold of WiFi training sequence and ZigBee PN code, respectively. First, we calculate the cross-correlation between incoming signal acq_signal and WiFi training sequence $WiFi\_taining\_seq$ (Line 1). Second, we calculate the cross-correlation

between incoming signal acq_signal and ZigBee PN code $ZigBee\_PN$ (Line 2). Finally, we compare the results with the two thresholds W_t and Z_t to determine the signal type (Lines 3-9).

Algorithm 1 WiFi & ZigBee Signals Detection

Input: acq_signal, $WiFi\_taining\_seq$, $ZigBee\_PN$, W_t, and Z_t.
Output: $Type\_signal$.

1: $T_w \leftarrow \int_{-\infty}^{+\infty} acq\_signal * WiFi\_taining\_seq$
2: $T_z \leftarrow \int_{-\infty}^{+\infty} acq\_signal * ZigBee\_PN$
3: if $T_w > W_t$ & $T_z < Z_t$ then
4: $\quad Type\_signal = WiFi$
5: else if $T_w < W_t$ & $T_z > Z_t$ then
6: $\quad Type\_signal = ZigBee$
7: else
8: $\quad Type\_signal = WiFi + ZigBee$
9: end if

If the incoming signal is sole WiFi or ZigBee, the signal feeds into normal WiFi or ZigBee demodulator, respectively. If the signal is determined as overlapped signal, Chiron needs to separate then demodulate it.

Overlapped WiFi and ZigBee Signal After the WiFi and ZigBee overlapped signal is detected, we must separate and demodulate the signal then apply error correcting mechanism to the distorted signals. For a WiFi and ZigBee overlapped signal (as shown in Figure 3.7), the ZigBee signal overlaps only portion (7 subcarriers) of the wider frequency-band WiFi signal (consisting of at least 64 subcarriers). Therefore, even when ZigBee signal overlaps with WiFi during the initial training sequence, the training sequence correlation will still exceed the detection threshold. After the training sequence detection, the WiFi carriers are separated by the FFT, the overlapped subcarrier will experience distortions. These distortions are sensed by

CSI and pilot tones, identifying the affected subcarriers. The identified ZigBee channel are then down-converted with the WiFi distortions. To recover from the WiFi distortions, we implemented filters that remove the slower WiFi subcarriers signals from the faster-changing ZigBee chips. After the high-pass filters operating at WiFi subcarriers frequencies, the ZigBee signal is decoded using the normal demodulator (as we mentioned in Section 3.5.2) which yields the ZigBee symbols and bits.

As an overview to recover the WiFi bits (shown in Figure 3.7), first, from the received WiFi signal, we subtract out portions of interfering ZigBee signals. Then, we apply an equalization method on the remaining WiFi signals using a channel sensing technique. Finally, after the signals are demodulated into bits, we apply an error correcting code to the bits associated those equalized and denoised WiFi subcarriers that are overlapped with ZigBee channels. To recover the distorted WiFi signal, we designed four steps shown below:

Step 1: ZigBee Signal Removal: Our ZigBee interference removal functions by removing the higher frequency ZigBee Chips (2 MHz) and leaving the slower WiFi symbol (250 KHz). This is done by a bandpass filter that allows the WiFi signals to proceed and suppressing the ZigBee signal. Thus, this filtering process only occurs on the portion of WiFi subcarriers that are overlapped by the ZigBee signal.

Step 2: Environmental Noise cancellation: Chiron must correct phase noise from ZigBee signal filter and environmental noise (such as human, transmitter, and receiver movements). Because of human movements and objects that reflect RF signals, the WiFi channel can experience strong frequency selective fades. Moreover, Chiron's concurrent communication also causes distortions within specific frequency bands. To remove the frequency and phase distortions, we utilize pilot tones that are sine waves agreed upon by the transmitter and receiver. Therefore, pilot tones estimate

the channel interference, and then Chiron corrects the interference as follows:

First, the receiver measures the received pilot tone sine wave represented in complex format. Then, the receiver computes the offset between the agreed upon expected sine wave expressed in Equation 3.3. Finally, by computing the correction factor a and b, the receiver applies a correction to all the subcarriers around pilot tone's frequency.

$$a \cdot I(t)\cos(2\pi ft) - b \cdot Q(t)\sin(2\pi ft) \tag{3.3}$$

Where, $I(t)$ and $Q(t)$ represent the complex sine wave of a pilot tone, and a and b represent interference added to the pilot tones and the correction factor.

Step 3: WiFi Demodulation: These equalized quadrature signals are sent to the normal WiFi OFDM demodulation systems and the original WiFi bits are recovered (as we introduced in Section 3.5.1).

Step 4: Forward Error Correction: After the WiFi bits are demodulated from each WiFi subcarrier, we note that the ZigBee overlapped subcarriers have a higher bit error rate. Moreover, the overlapped ZigBee packets also have a higher probability of error. By appending Forward Error Correcting (FEC) to the data stream during concurrent communication, we can also increase the probability of correct reception. Because the corruption in the WiFi bitstream can be expected, as ZigBee packets are transmitted within a fixed frequency band, we can append extra FEC to non-affected bits. We utilize a fast linear FEC Low-density parity-check code (LDPC) to be compatible with modern 802.11 standards. By utilizing LDPC's sparse parity matrix, Chiron spread the parity information across the payload frame. To be compatible with commodity devices, we increased the convolutional coding FEC rate. Additionally, interleaving bits during formation of the FEC increases the likelihood of packet

reception.

3.6.2 Sender

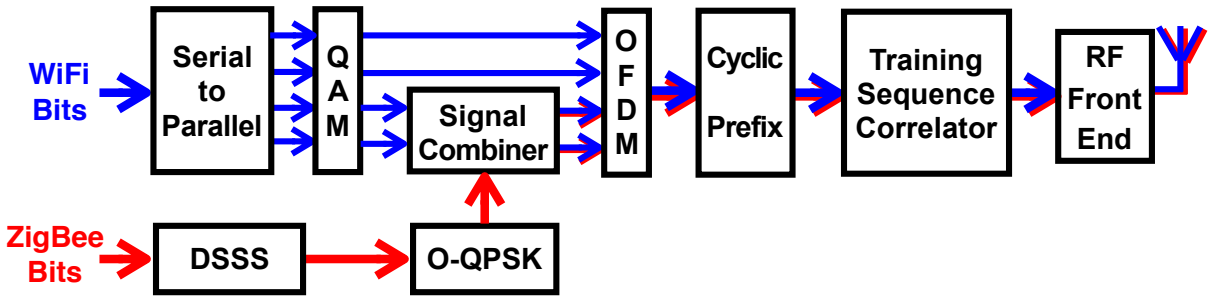


Fig. 3.8: WiFi & ZigBee Signals Combiner

Figure 3.8 shows an overview of the Chiron sender. 1) First, the WiFi signals are parallelized and mapped by QAM, and the ZigBee bits are modulated by DSSS and O-PQSK (detailed in Section 3.5). 2) The overlapped WiFi subcarriers are combined with ZigBee sine waves. 3) Both the overlapped and the regular WiFi subcarriers are efficiently combined using OFDM. 4) Finally, a cyclic prefix and training sequence is appended to the signal and sent to the RF frontend.

To transmit the signals concurrently, the output of the wider-band WiFi signal must contain similar signals as the output of the ZigBee and desired WiFi. Thus, a portion of the signals from the WiFi QAM modulator will contain distorted signals. The distortion must not exceed the interference tolerance of WiFi's OFDM and ZigBee DSSS modulation schemes. We describe a linear optimization algorithm that combines both WiFi subcarriers to contain both WiFi and ZigBee signals. This combination is possible because the chip rate and the symbol rate of WiFi and ZigBee are significantly different. To combine the ZigBee and WiFi signal, we recognize that 7 WiFi subcarriers overlap a single ZigBee channel. Thus, the overlapping WiFi

subcarriers, which operates with 312.5 KHz offsets, must contain both the higher 2 MHz frequency ZigBee chips rate and the lower 250 WiFi KHz symbol rate. To create this combined signal, we use linear programming with weights.

We set up the linear programming model as a maximization model. Chiron adds WiFi subcarrier sample instant with a weighted ZigBee sample instant expressed in Equation 3.4. The maximizing constraint is the matching of the combined output signal to both the original ZigBee and WiFi signals (Equation 3.5). To measure how well the combined signals matches, we use cross-correlation. Therefore, the maximizing constraints are cross-correlation between the combined sub-carriers and 1) the original WiFi sub-carriers and 2) the spread signal ZigBee signal.

To achieve this maximizing objective, we solve for optimal weights that are added to WiFi subcarrier, expressed in equations 3.4 and 3.5. Where n to d index of the overlapping WiFi subcarriers, C_m is the WiFi QAM modulated sine wave, $Z(l)$ is the ZigBee signal, and w is the weight applied per ZigBee sine wave. The subcarriers are efficiently combined using an IFFT, expressed by the equation $e^{e\pi jkt}$. By solving the weights using a linear optimization technique, we efficiently combine the WiFi subcarriers without having to resort to multiple subcarriers down and up conversions and filtering. The optimal resulting weights represent the higher frequency distortion factors added to each WiFi subcarrier. Thus, this linear programming results yields an efficiently combined WiFi and ZigBee signal.

$$\begin{array}{c} Max \\ w \in R \end{array} \left[\begin{array}{l} \sum\limits_{t=0} B^* \left(w(t_1)\right) \cdot C \left(t_1 + n\right), \\ \sum\limits_{t=0} B^* \left(w(t_2)\right) \cdot Z \left(t_2 + n\right) \end{array} \right] \tag{3.4}$$

subject to

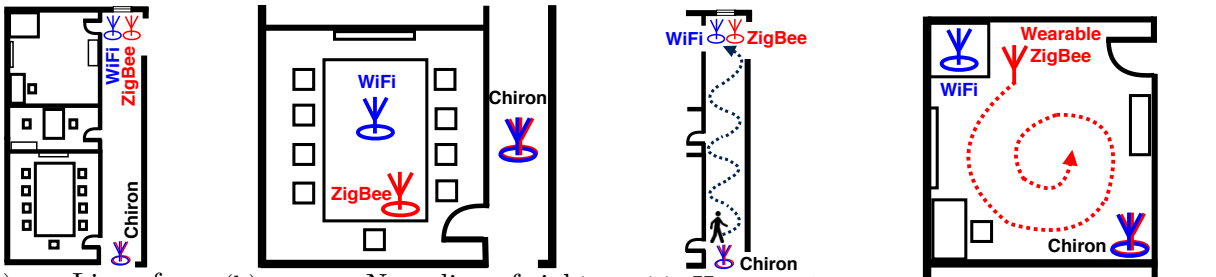
$$B(w\left(t\right)) = \sum_{n=0}^{N} \left(C_m(t) + w(t) \cdot Z(t)\right) e^{2\pi jkn} \tag{3.5}$$

In the combined WiFi and ZigBee signal, the ZigBee signal is typically longer than the WiFi packet. To solve this problem of different packet length, we leverage nulling out the WiFi signals expressed in Equation 3.5. C_m is zero, and the ZigBee signal $Z(t)$ with the weight w is left. Therefore, the overlapping subcarriers are left with only the ZigBee signals when the ZigBee is longer than the WiFi packet.

3.7 Experimental Evaluation

In this section, we introduce our evaluation of Chiron with different metrics (i.e., spectrum utilization, throughput, bit error rate and packet recaption ratio) in four real-world scenarios.

3.7.1 Experimental Setup



(a) Line-of-sight (LoS) (b) None-line-of-sight (NLoS) (c) Human in the Middle (d) Wearable Scenario

Fig. 3.9: Four Experimental Scenarios

We evaluated our Chiron system in an engineering building, which has a lot of other WiFi access points, Bluetooth devices, and ZigBee devices that create interference. We conducted experiments under four scenarios (shown in Figure 3.9):

• Line-of-sight (LoS): The Chiron gateway and WiFi/ZigBee devices are in Line-of-sight (shown in Figure 3.9(a)).

• None-line-of-sight (NLoS): The Chiron gateway and WiFi/ZigBee devices are placed in different rooms (shown in Figure 3.9(b)).

• Human in the Middle: During human in the middle scenario, a person walks in the trajectory shown in the black dashed line (shown in Figure 3.9(c)).

• Wearable Scenario: In the wearable scenario, a person carries a ZigBee device and walks in the trajectory. As described in the white paper from ZigBee Alliance [3], ZigBee radios are used in wearable applications, such as chronic disease management, health, and wellness (shown in Figure 3.9(d)).

In the LoS, NLoS and human in the middle scenarios, we vary the communication distance between Chiron gateway and the WiFi/ZigBee devices. Note that the distance between the WiFi and ZigBee is fixed because the gateway-to-WiFi's communication distance does not impact the communication from the gateway to ZigBee and vice versa.

In our experiment, the design of Chiron gateway (described in Section 4.5) is implemented on a USRP. We used a commodity DELL XPS 9550 laptop's WiFi card and TelosB tel as the WiFi and ZigBee devices, respectively, to communicate with Chiron gateway for evaluation. Since Chiron technique focuses on physical layer concurrent communications while the application profile may affect the measured benefit of Chiron, in this evaluation we focused entirely on the physical layer to explore the advantages of Chiron.

For each data point, we transmitted and received around 5 million bits. The following metrics are used to evaluate the Chiron system:

• Throughput: successfully received bits divide by the transmission time.

• Bit Error Rate (BER): the number of successfully received bits divided by the number of transmitted bits.

• Packet Reception Ratio (PRR): the number of successfully received packets divided by the number of transmitted packets.

• Spectrum Utilization: throughput per second per hertz at the receiver side.

To compare with Chiron which can conduct concurrent communications between WiFi and ZigBee, we also implemented the following schemes:

• Sole WiFi-to-Gateway or Sole Gateway-to-WiFi: In these two schemes, a WiFi device is transmitting (or receiving) packets to (or from) our gateway without the concurrent transmission of ZigBee devices. These two schemes serve as the upper bound of the achievable throughput for WiFi communication in real-world settings. We note that there exists the interference from the other IoT devices' wireless traffic inside the building.

• WiFi-to-Gateway with ZigBee traffic or ZigBee-to-Gateway with WiFi traffic: These two schemes represent the traditional gateway's performance in real-world scenarios, in which WiFi devices are competing with ZigBee devices for sending the packets to our gateway. This serves as the baseline.

• Sole ZigBee-to-Gateway or Sole Gateway-to-ZigBee: In these two schemes, one or multiple ZigBee devices are transmitting/receiving packets to/from the gateway without concurrent WiFi transmission. When we evaluate ZigBee communication, these two schemes serve as the upper bound of the achievable throughput.

• Gateway-to-ZigBee with WiFi traffic or Gateway-to-WiFi with ZigBee traffic: These two schemes represent the traditional gateway's performance while sending in real-world scenarios, in which WiFi packets and ZigBee packets are allocated to different time slots to avoid collision. This serves as the baseline.

3.7.2 Overall Performance

In this section, we evaluate the overall performance, which includes spectrum utilization and throughput of Chiron. In this experiment, we set one COTS WiFi device and multiple COTS ZigBee devices communicating with the gateway. For traditional multi-radio gateway approach, these devices communicate in a TDMA manner because concurrent communications are not allowed. For Chiron, these devices conduct concurrent communications as stated in Section 4.5.

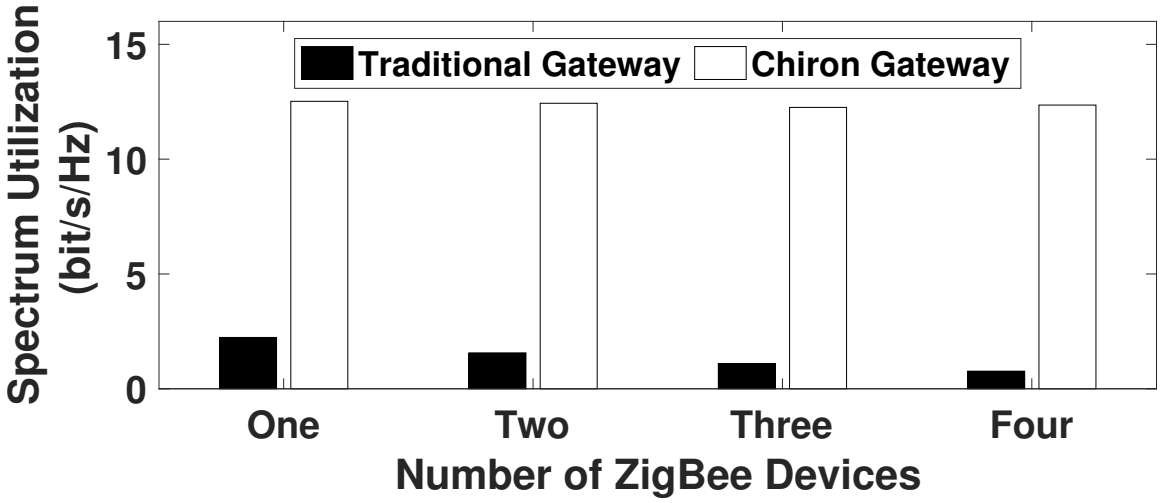


Fig. 3.10: Spectrum Utilization: since Chiron can concurrently communicate to both the WiFi and ZigBee devices, Chiron gateway's spectrum utilization is 16X better than that of the traditional gateway when the number of ZigBee devices is 4.

Spectrum Utilization To show the significant benefit of Chiron, we first evaluate the spectrum utilization in heterogenous networks (WiFi and ZigBee devices coexist). Figure 3.10 shows the comparison between traditional multi-radio gateway and Chiron gateway. In traditional multi-radio gateway approach, the gateway has to allocate ZigBee and WiFi packets into different time slot, which yields a very low spectrum utilization of 2.34 bit/s/Hz and 0.767 bit/s/Hz when there are one and four ZigBee

senders.

For Chiron, since it can concurrently communicate with both the WiFi and ZigBee devices, the spectrum utilization is much higher than traditional multi-radio gateway. When the number of ZigBee is four, the spectrum utilization of Chiron gateway can achieve 12.355 bit/s/Hz which is more than 16X better than traditional Gateway.

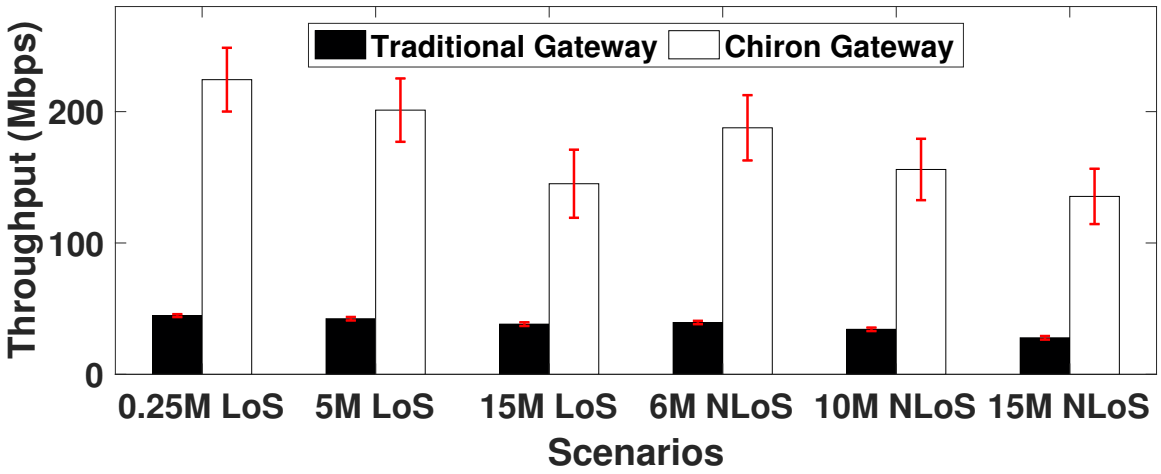


Fig. 3.11: Overall Throughput: across all the communication distances for both the LoS and NLoS scenarios, the throughput of Chiron (up to 224.34 Mbps) is higher than traditional gateway.

Overall Throughput We show the overall throughput of Chiron comparing with multi-radio gateway. The overall throughput includes both the WiFi and ZigBee parts. As shown in Figure 3.11, across all the communication distances for both the LoS and NLoS scenarios, Chiron features the higher throughput than the traditional gateway. When the distance is 0.25 meters in LoS, the overall throughput of Chiron is 224.34 Mbps which shows more than 4X higher than of traditional gateway. The reason is Chiron can conduct concurrent WiFi and ZigBee communications (as described in previous sections) while the traditional scheme only allow one type communication

(with either WiFi or ZigBee) at a time.

Throughput in Multiple WiFi and ZigBee This section demonstrates Chiron can communicate with multiple WiFi and ZigBee devices. Figure 3.14(a) shows the throughput across four different WiFi devices. Since all of the four WiFi devices work on the same frequency band, they share the 20 MHz bandwidth in terms of frequency and transmit (or receive) at different time to avoid collision. The aggregated throughput of Chiron gateway is around 200 Mbps which is similar to the single WiFi communication as shown in Figure 3.11. Compared with the traditional gateway approach, the aggregated throughput of Chiron is more than two times higher because the communications between WiFi and gateway are not interrupted by the ZigBee communication. Figure 3.14(b) shows the throughput across four different ZigBee devices. For Chiron gateway, we observed that all of the four ZigBee devices can achieve a high throughput (up to two times better than the traditional gateway approach) because the 20MHz WiFi channel is overlapped with up to four ZigBee channels. Therefore, the Chiron gateway can communicate with four ZigBee devices on four different channels and have negligible impact to the concurrent communication between the Chiron gateway and WiFi devices.

3.7.3 Receiver Evaluation

In this section, we introduce the performance of Chiron receiver in which both the COTS WiFi and ZigBee devices transmit to the Chiron gateway.

ZigBee-to-Gateway Communication Throughput: To illustrate the effectiveness of Chiron on ZigBee-to-Gateway link, we first compare its throughput with sole ZigBee-to-Gateway (i.e., communications between COTS ZigBee device and COTS multi-radio gateway by using normal ZigBee protocol). The results are shown in

Figure 3.15. In Figure 3.15(a), one ZigBee device communicates with either one ZigBee gateway (native ZigBee-to-Gateway) or the Chiron gateway (Chiron ZigBee-to-Gateway). We can observe that the throughput of Chiron ZigBee-to-Gateway (the mean value is 223.97 Kbps at 0.25 meter) is very close to sole ZigBee-to-Gateway on different communication distances and approaching the cap of theoretical ZigBee protocol's throughput. Also, the performance is stable on different communication distances (the mean value is 220.32 Kbps at 15 meters). Further, while comparing Chiron ZigBee-to-Gateway with ZigBee-to-Gateway with WiFi traffic (the grey bar), Chiron ZigBee-to-Gateway is about 2.3 times of ZigBee-to-Gateway with WiFi traffic because Chiron gateway can concurrently receive from both the WiFi and ZigBee receivers.

Since one WiFi channel can overlap with up to four ZigBee channels, we evaluated four ZigBee devices communicating with either another four ZigBee devices (sole ZigBee-to-Gateway) or the Chiron gateway (Chiron ZigBee-to-Gateway) and show the aggregated throughput in Figure 3.15(b). By looking at the results, the performance is still stable across all of the communication distances. The difference between native ZigBee-to-Gateway and Chiron ZigBee-to-Gateway is very small even at 15 meters. However, when WiFi traffic exists, Chiron ZigBee-to-Gateway shows big advantage comparing with native ZigBee-to-Gateway with WiFi.

The reasons Chiron can achieve comparable throughput of ZigBee protocol even under WiFi interference are: i) the Chiron gateway can demodulate original OQPSK signal (modulation scheme adopted by ZigBee protocol); and ii) Chiron can demodulate ZigBee signal along with overlapped WiFi signal as introduced in Section 4.5.

Bit Error Rate: Figure 3.16 shows the Bit error rate (BER) of Chiron ZigBee-to-

Gateway link. Though ZigBee signal is overlapped with WiFi signal at Chiron gateway side, our technique (introduced in Section 4.5) is still able to differentiate them and demodulate them. Thus, the ZigBee-to-Gateway link BER still follow the characteristic of OQPSK (ZigBee's modulation scheme). Figure 3.16(a) shows the BER in LoS scenario, we can observe that all of the BERs are lower than 0.5%. In NLoS scenario (Figure 3.16(b)), all of the BERs are still lower than 0.5% but the average is higher than in LoS scenario. This is because the direct path is blocked and the multipath effect is more complicated in NLoS scenario.

Packet Reception Ratio: The Chiron gateway is able to demodulate ZigBee and WiFi overlapped packet. To confirm the effectiveness, we conducted experiments to evaluate the Packet Reception Ratio (PRR). Figure 3.17 shows the PRR of Chiron ZigBee-to-Gateway link. In LoS scenarios (Figure 3.17(a)), when the communication distance is short (at 0.25 meter), the PRR can achieve 95%. When the communication distance increases, the PRR drops and reaches 70.4% when the distance is 15 meters. In NLoS scenarios (Figure 3.17(b)), because of rich multipath effects and propagation loss, the PRR drops a little bit. The value is 84.4% at 6 meters. This experiments validated the ZigBee-to-Gateway communication along with WiFi communication in Chiron.

WiFi-to-Gateway Communication In this section, we evaluate the WiFi-to-Gateway link of Chiron. To do this, we first compare the performance of sole WiFi-to-Gateway (i.e., a WiFi device communicates with a COTS multi-radio gateway without ZigBee traffic) with Chiron WiFi-to-Gateway (i.e., concurrent transmission with ZigBee-to-Gateway link). We conducted the experiments with either one ZigBee device or four ZigBee devices because one 20 MHz WiFi channel can overlap with up to four ZigBee channels. The results are shown in Figure 4.22, we ob-

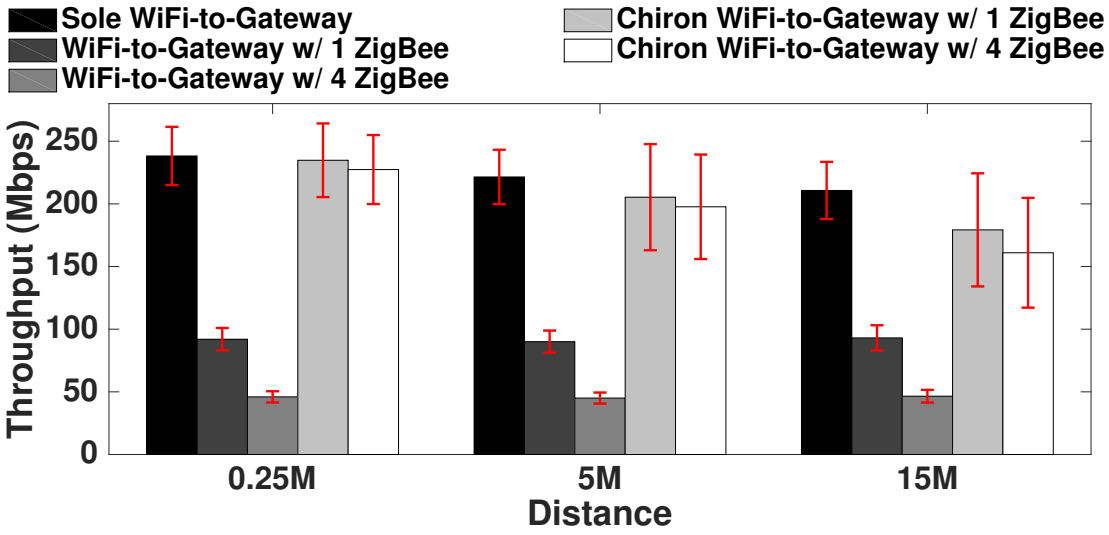


Fig. 3.12: Throughput of WiFi-to-Gateway Link: Chiron shows similar throughput to sole WiFi-to-Gateway but almost 4 times of traditional gateway approach when four ZigBee devices exist.

serve that the throughput of Chiron WiFi-to-Gateway can achieve similar level of sole WiFi-to-Gateway. When the distance is close (i.e., at 0.25 meter LoS), Chiron WiFi-to-Gateway with one ZigBee and four ZigBee only show 1.4% and 4% difference comparing with native WiFi-to-Gateway, respectively. When the distance is long, the difference increases because at the gateway side, Chiron encounters interference from either one or four ZigBee devices. However, by resolving the interference (as stated in Section 4.5), the Chiron WiFi-to-Gateway throughput with one ZigBee and four ZigBee are only 7.3% and 15% lower than native WiFi-to-Gateway, respectively, at 15 meters.

Then, we compare the throughput while ZigBee traffic exists. At 0.25 meter, Chiron WiFi-to-Gateway is 1.55X and 3.94X times high the normal WiFi-to-Gateway while one or 4 ZigBee devices are communicating with the gateway, respectively. At

15 meters, we also observe similar increases. The reason is that different normal multi-radio gateway, Chiron gateway is able to disentangle and demodulate WiFi and ZigBee signals concurrently.

Mobile Scenarios To extensively evaluate the robustness of Chiron, we conducted an experiments with a designated person walking in the middle of sender and receiver (as shown in Figure 3.9(c)). Moreover, to evaluate the wearable applications (such as health and wellness monitoring zig), we also asked the participant wearing the ZigBee device (in pocket or on wrist) and performing daily activities (shown in Figure 3.9(d)).

ZigBee-to-Gateway: Figure 3.18(a) shows the ZigBee-to-Gateway link throughput with humans walking in the middle. The throughput is relatively stable because the native ZigBee modulation scheme is well adopted in Chiron that the OQPSK-DSSS scheme is robust to environment noise. Comparing with direct LoS scenario (Figure 3.15(a)), the performance only drops 2% when the communication distance is short. When the communication distance increases to 20 meters, the throughput drops 6.4%.

Figure 3.18(b) shows four wearable scenarios: i) person walks away from the Chiron gateway with ZigBee sender in pocket; ii) person walks towards from the Chiron gateway with ZigBee sender in pocket; iii) person walks around the meeting room with ZigBee sender in pocket; and iv) person walks around the meeting room with ZigBee attached to the wrist. We can observe the fluctuation across the four wearable scenarios. However, overall, the performance is stable. The lowest throughput still can achieve 190 Kbps when the person walks around the meeting room with ZigBee sender in pocket.

WiFi-to-Gateway: Figure 3.19 shows the WiFi-to-Gateway link throughput. In human in the middle (Figure 3.19(a)), the WiFi-to-Gateway link maintains up to 226.2

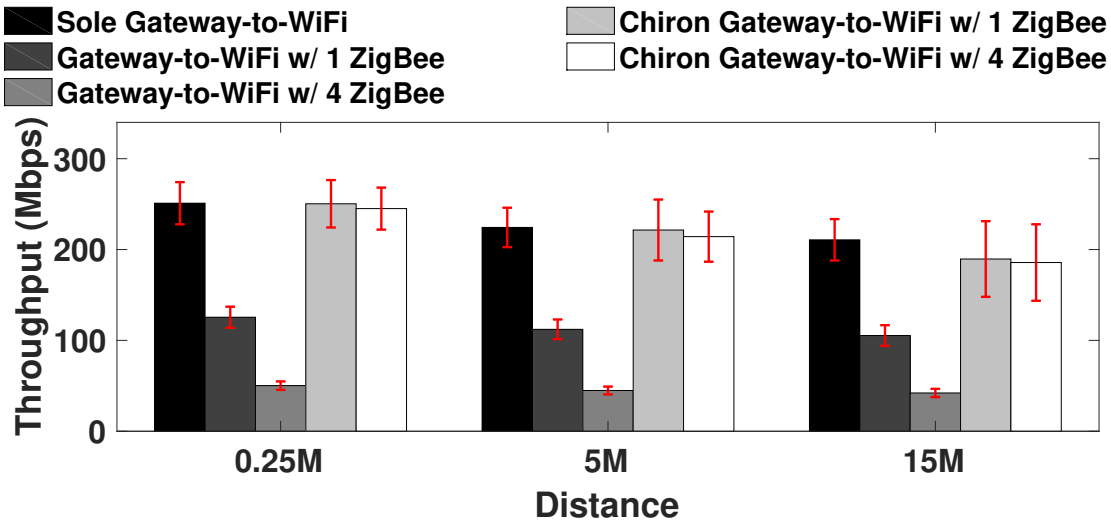
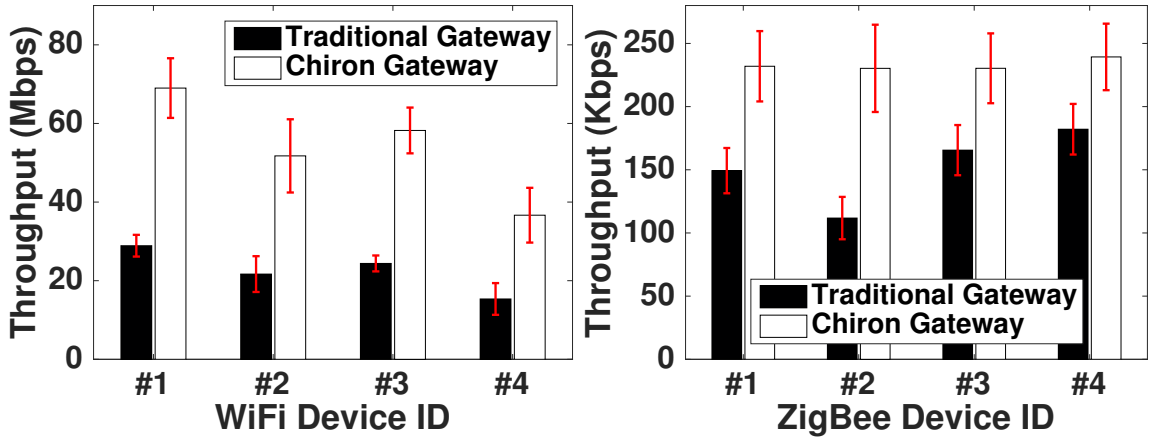


Fig. 3.13: Throughput of Gateway-to-WiFi Link: Chiron shows about 5 times of the traditional gateway approach when transmitting to four ZigBee devices concurrently.

Mbps. However, different from ZigBee-to-Gateway link, the performance drops relatively quickly because the sophisticated modulation scheme (which adopts by WiFi protocol) suffers more degradation in multipath rich environment. In wearable scenario (Figure 3.19(b)), the red error bar (which indicates the standard deviation) has an average value of 25%, which means the WiFi-to-Gateway links fluctuates due to the advanced modulation scheme defined by WiFi standard.

3.7.4 Sender Evaluation

In this section, we evaluate the performance of Chiron sender in which the Chiron gateway concurrently transmit to both the COTS WiFi and ZigBee devices. To illustrate the robustness of Chiron, we extensively evaluate it in multiple stationary and mobile scenarios.

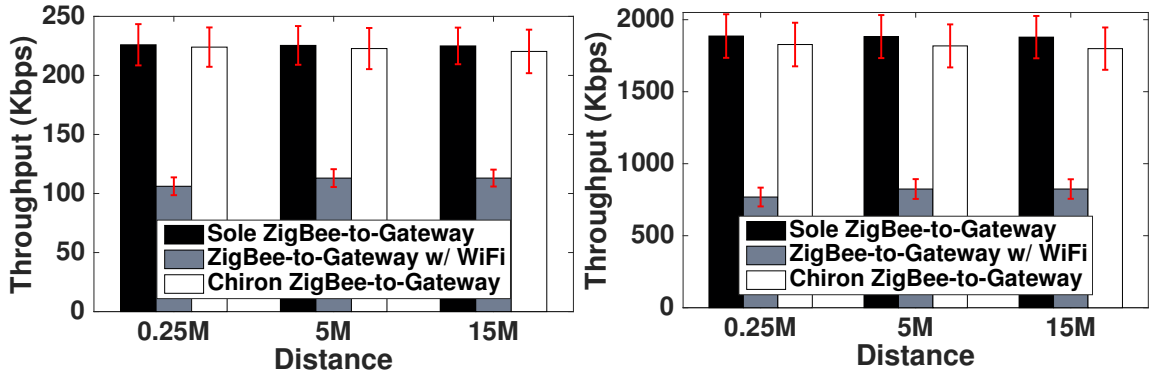


(a) WiFi (b) ZigBee

Fig. 3.14: Multiple WiFi and ZigBee Devices Communicate with Chiron Gateway: Chiron gateway can concurrently communicate with four different ZigBee devices (which are on different ZigBee channels) while communicating with different WiFi devices alternatively.

Gateway-to-ZigBee Communication Throughput: Figure 3.20 shows the comparison among sole Gateway-to-ZigBee (i.e., COTS multi-radio gateway communicates with ZigBee device without WiFi traffic), Gateway-to-ZigBee with WiFi traffic (i.e., COTS multi-radio gateway communicates with both ZigBee and WiFi devices), and Chiron Gateway-to-ZigBee (i.e., concurrently sending to both ZigBee and WiFi devices). Figure 3.20(a) shows the result of the gateway communicating with either one ZigBee device. In which the throughput of Chiron Gateway-to-ZigBee is almost the same with sole Gateway-to-ZigBee on different communication distances and approaching the cap of theoretical ZigBee protocol's throughput (250 Kbps). However, while WiFi messages exist, the multi-radio approach (the bar labeled with Gateway-to-ZigBee w/ WiFi in Figure 3.20(a)) is half of our Chiron approach because Chiron features concurrent transmissions to both ZigBee and WiFi.

As we mentioned in Section 3.7.3, one WiFi channel is able to overlap with up to four ZigBee channels. Therefore, we also evaluated four multi-radio gateways (sole



(a) One ZigBee

(b) Four ZigBee

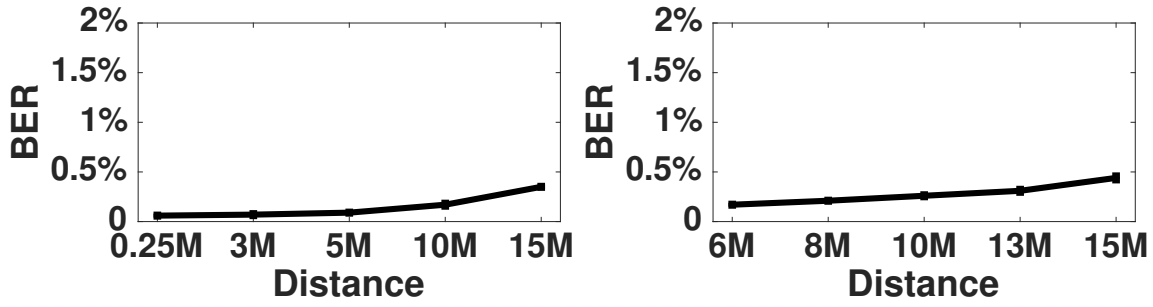
Fig. 3.15: Throughput of ZigBee-to-Gateway Link: When WiFi traffic exists, the throughput of Chiron ZigBee-to-Gateway is about 2.3 times higher than traditional gateway approach. Besides, Chiron ZigBee-to-Gateway is similar to sole ZigBee-to-Gateway which does not have WiFi traffic interference.

Gateway-to-ZigBee) or the Chiron gateway (Chiron Gateway-to-ZigBee) communicating with four ZigBee devices. The aggregated throughput is shown in Figure 3.20(b). By looking at the figure, we can also conclude the throughput of Chiron Gateway-to-ZigBee is two times of the normal multi-radio approach when WiFi traffic exists.

The reason Chiron can double the throughput when communicates with both WiFi and ZigBee devices is that at Chiron gateway, it is able to combine the WiFi and ZigBee signals together, but the signal can be demodulated at COTS WiFi and ZigBee receivers' side.

Bit Error Rate: Figure 3.21 shows the BER of Gateway-to-ZigBee link in both the LoS. The average BER are all lower than 0.5% at different distance (even at 15 meters) because the DSSS (direct-sequence spread spectrum) is inherited (from ZigBee protocol) in Chiron Gateway-to-ZigBee Link.

Packet Reception Ratio: The Chiron gateway is able to send ZigBee and WiFi combined packet. To confirm the effectiveness, we conducted experiments to evaluate the

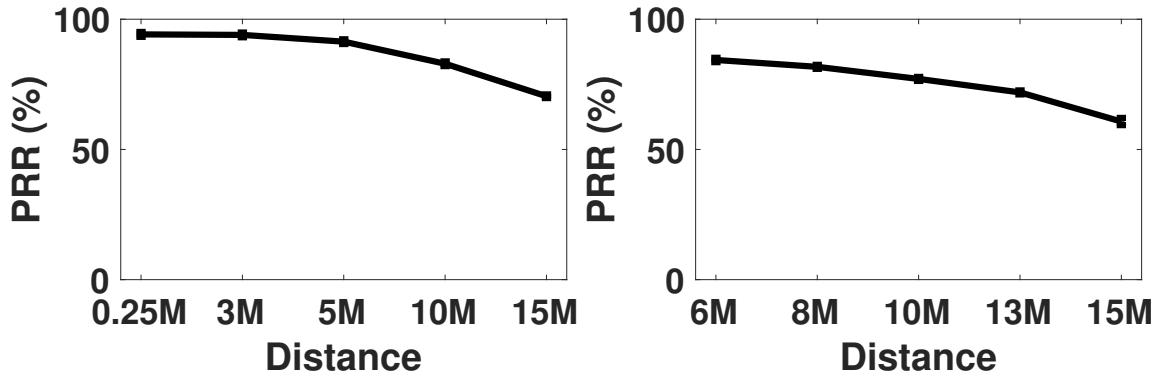


(a) LoS (b) NLoS

Fig. 3.16: Bit Error Rate of ZigBee-to-Gateway Link: Chiron ZigBee-to-Gateway link's BERs are lower than 0.5% across different distances in both LoS and NLoS scenarios.

Packet Reception Ratio (PRR) in this section. Figure 3.22 shows the PRR of Chiron Gateway-to-ZigBee link. In LoS scenarios (Figure 3.22(a)), when the communication distance is short (at 0.25 meter), the PRR is around 93.2%. When the communication distance increases, the PRR drops and reaches 69.7% when the distance is 15 meters. In NLoS scenarios (Figure 3.22(b)), because of rich multipath effects and propagation loss, the PRR is a little bit lower comparing with in LoS scenario. The value is 79.4% at 6 meters. This experiments validated the Gateway-to-ZigBee communication along with WiFi communication in Chiron.

Gateway-to-WiFi Communication To show the concurrent sending capacity of Chiron, we compare the performance of sole Gateway-to-WiFi (no ZigBee traffic) and Gateway-to-WiFi with ZigBee traffic with Chiron Gateway-to-WiFi (results are shown in Figure 3.13). When there is no ZigBee message to send we observe that the throughput of Chiron Gateway-to-WiFi can achieve similar level of sole Gateway-to-WiFi. If the gateway has ZigBee message, our Chiron design shows huge benefit. When the gateway needs to communicate with one ZigBee, Chiron Gateway-to-WiFi shows two times better performance comparing with the normal multi-radio gateway



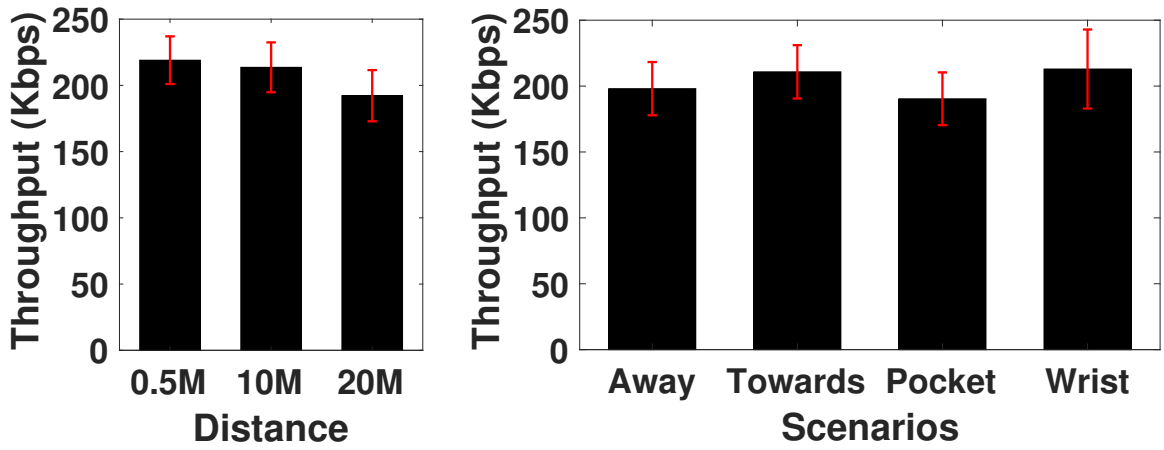
(a) LoS (b) NLoS

Fig. 3.17: Packet Reception Ratio of ZigBee-to-Gateway Link: Chiron ZigBee-to-Gateway link achieve an up to 95% PRR, even when the distance increases to 15 meters, the PPR can still reach 70.4%.

approach. Furthermore, when communicating with four ZigBee devices, Chiron shows almost four times better performance comparing with the normal multi-radio gateway approach. The reason is that Chiron can better utilizes the spectrum to embed ZigBee signal into WiFi signal. Since one 20 MHz WiFi channel is overlapped with up to four ZigBee channels, the Chiron gateway is able to communicate with four ZigBee receivers along with one WiFi receiver.

Mobile Scenarios To fit Chiron in mobility applications, we also evaluated it in human in the middle (as shown in Figure 3.9(c)) and wearable scenarios (as shown in Figure 3.9(d)).

Gateway-to-ZigBee: Figure 3.23(a) shows the Gateway-to-ZigBee link throughput with humans walking in the middle. The throughput is relatively stable because the native ZigBee modulation scheme is well adopted in Chiron that the OQPSK-DSSS scheme is robust to environment noise. Comparing with direct LoS scenario (Figure 3.20(a)), the performance only drops 3% when the communication distance is short.



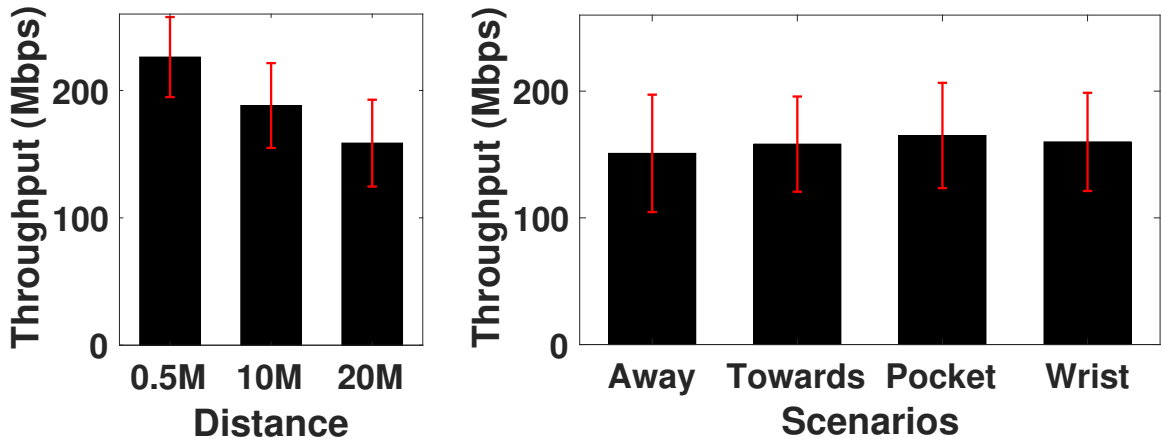
(a) Human in the Middle (b) Wearable Scenarios

Fig. 3.18: ZigBee-to-Gateway Throughput in Mobile Scenarios: The performance is stable in different mobile scenarios.

When the communication distance increases to 20 meters, the throughput drops 7.6%.

Figure 3.23(b) shows four wearable scenarios: i) person walks away from the Chiron gateway with ZigBee sender in pocket; ii) person walks towards from the Chiron gateway with ZigBee sender in pocket; iii) person walks around the meeting room with ZigBee sender in pocket; and iv) person walks around the meeting room with ZigBee attached to the wrist. We can observe the fluctuation across the four wearable scenarios. However, overall, the performance is stable. The lowest throughput still can achieve 188.07 Kbps when the person walks around the meeting room with ZigBee sender in pocket.

Gateway-to-WiFi: Figure 3.24 shows the throughput of the Gateway-to-WiFi link. In human in the middle (see Figure 3.24(a)) scenario, the Gateway-to-WiFi link's throughput can be up to 245.07 Mbps. Even when the distance increases to 20 meters, its throughput is still more than 165 Mbps. This indicates that our design is reliable over a long distance. In different wearable scenarios (see Figure 3.24(b)), our approach maintains similar throughput. This demonstrates that our design can



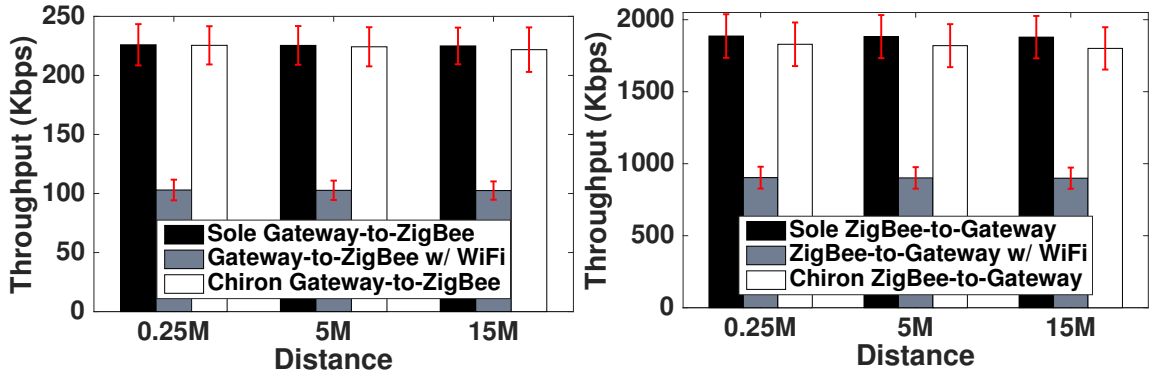
(a) Human in the Middle (b) Wearable Scenarios

Fig. 3.19: WiFi-to-Gateway Throughput in Mobile Scenarios: Results shows Chiron is robust in different real-world setup.

support different types wearable applications.

3.8 Related Works

To improve the performance of wireless communication, researchers have proposed various interference mitigate techniques Prasad, Arslan, & Rangarajan; Das et al.; Gummadi et al.; Salimi et al.; Singh et al.; Sahai et al. (2013); Sen et al. (2013) and collision avoidance solutions Shi et al.; Sen, Choudhury, & Nelakuditi (2012); Nandagopal et al.; Singh et al.; Merz et al. (2004). To further improve the spectrum utilization, different methods Panchal, Yates, & Buddhikot (2013); Premnath et al.; Yun, Kim, & Qiu; Tan et al.; Zhang et al. (a); Khan et al.; Lee et al.; Sun, Sen, & Koutsonikolas; Kumar et al.; Deek et al.; Chintalapudi et al. have been proposed. Instead of improving spectrum utilization within the same protocol (i.e., WiFi or ZigBee), our work takes a new approach by exploring the possibility of increasing the spectrum utilization when heterogeneous radios with different protocols are communicating concurrently. Specifically, our approach enables the bi-directional concurrent



(a) One ZigBee

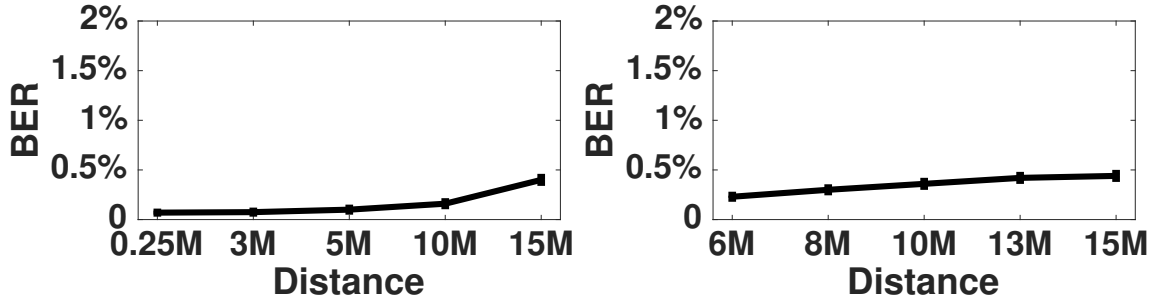
(b) Four ZigBee

Fig. 3.20: Throughput of Gateway-to-ZigBee Link: When WiFi presents, Chiron is able to double the throughput comparing with the traditional gateway approach because Chiron can concurrently transmit to both the WiFi and up to four ZigBee device.

communication of WiFi and ZigBee.

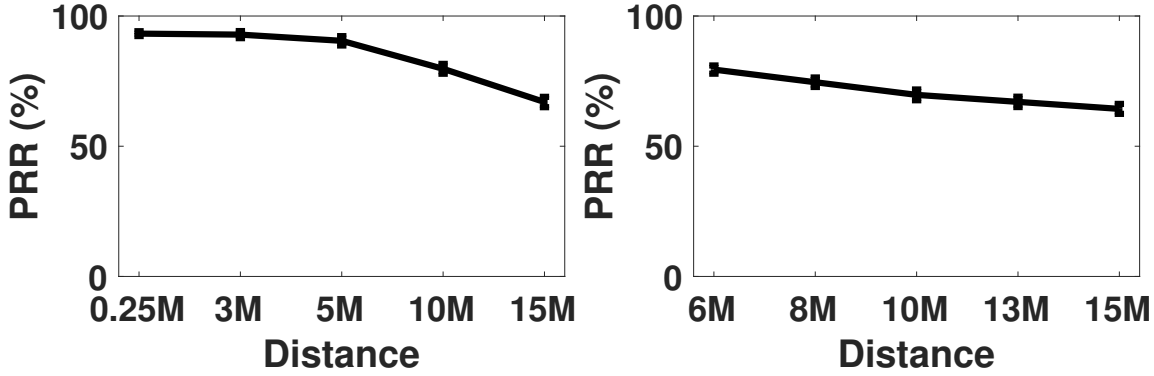
Several cross-technology communication systems Chebrolu & Dhekne; Zhang & Li; Kim & He; Zhang & Shin; Chi et al. (a); Z. Chi, Z. Huang, Y. Yao, T. Xie, H. Sun, and T. Zhu (2016); Yin et al. (2017); Jiang et al. (2017); Guo, Zheng, & He (2017); Wenchao Jiang, Roufeng Liu, Zhimeng Yin, Song Min Kim and T. He (2017) have been introduced, to utilize the coexistent features of different wireless technologies within the same frequency band.

Esense Chebrolu & Dhekne and HoWiES Zhang & Li enable WiFi to ZigBee communication by sensing the packet length of WiFi packets. GSense Zhang & Shin uses special preamble to coordinate heterogeneous devices. FreeBee Kim & He achieved communication among WiFi, ZigBee and Bluetooth by modulating periodical beacons. EMF Z. Chi, Z. Huang, Y. Yao, T. Xie, H. Sun, and T. Zhu (2016), C-MORSE Yin et al. (2017), DCTC Jiang et al. (2017), and WiZig Guo, Zheng, & He (2017) convey cross-technology data at the packet level (i.e., packet length or transmission power). This packet level modulation results a low network performance (i.e., the



(a) LoS (b) NLoS

Fig. 3.21: Bit Error Rate of Gateway-to-ZigBee Link: The BER remains low (less than 0.5%) even in NLoS scenario.

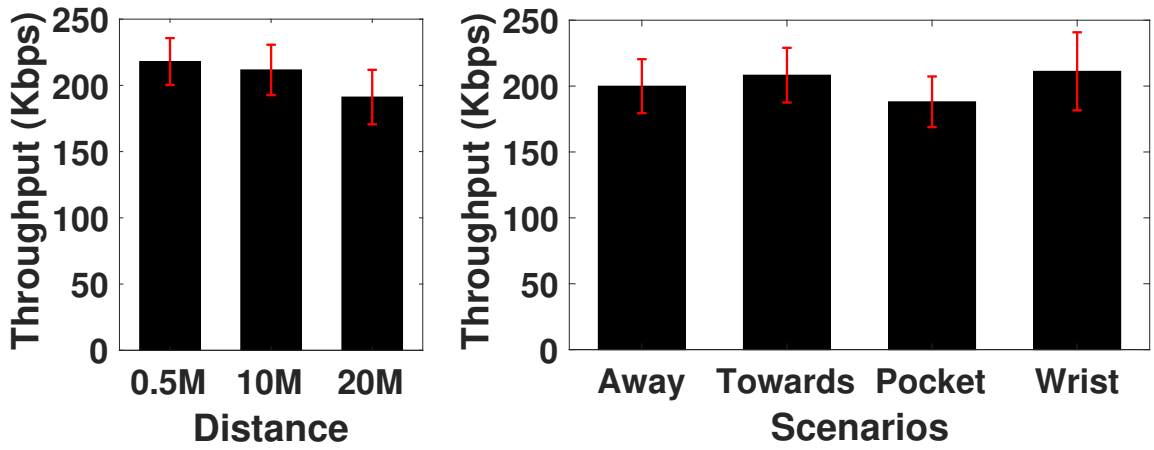


(a) LoS (b) NLoS

Fig. 3.22: Packet Reception Ratio of Gateway-to-ZigBee Link: When transmitting to both the WiFi and ZigBee devices, the PRR still achieves up to 93.2%.

throughput is at tens or hundreds of bps level). B^2W^2 Chi et al. (a) enables BLE to WiFi transmission by using CSI of WiFi system. WEBee Z. Li and T. He (2017) and PMC Z. Chi, Y. Li, Y. Yao, and T. Zhu (2017) use WiFi signal to emulate ZigBee signal at the physical layer.

Although WEBee can achieve relatively high CTC throughput, its spectrum utilization is extremely low. This is because when WEBee uses WiFi packets to emulate ZigBee packets, the original payload in the WiFi packets are changed and cannot be used to send out the WiFi data. A single WiFi transmission occupies

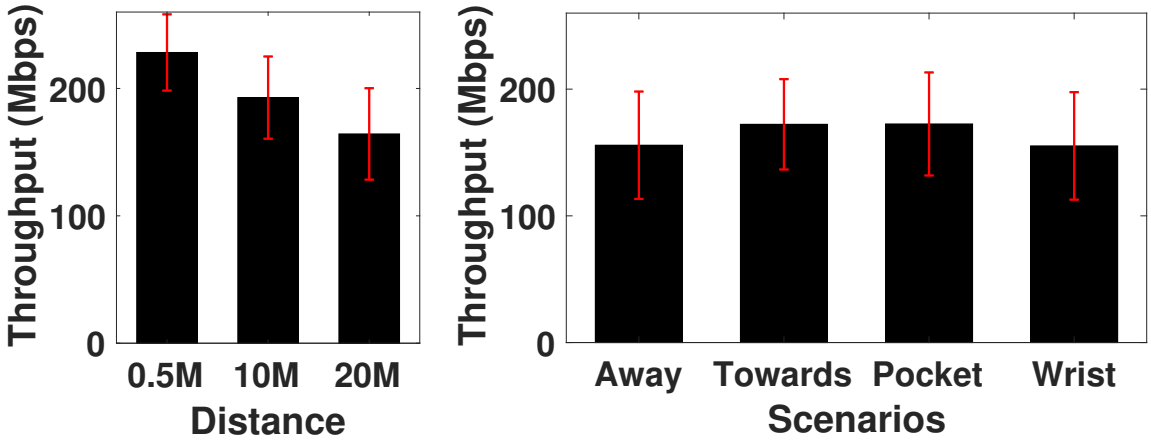


(a) Human in the Middle (b) Wearable Scenarios

Fig. 3.23: Gateway-to-ZigBee Throughput in Mobile Scenarios: The throughput is very close to that in LoS scenario, which validate the robustness of Chiron.

a 20 MHz channel, while ZigBee receivers only obtain information within a 2MHz-wide ZigBee channel. Since WiFi has more advanced modulation schemes, WiFi can use its 20 MHz channel to transmit WiFi packets at hundreds of Mb/s. By using WEBee, WiFi can only emulate ZigBee packets at 126 Kbps. Therefore, WEBee's spectrum utilization is much lower than original WiFi communication. Similarly, BlueBee Wenchao Jiang, Roufeng Liu, Zhimeng Yin, Song Min Kim and T. He (2017) also has very low spectrum efficiency, because it uses high throughput Bluetooth signal to emulate low throughput ZigBee signal. Moreover, WEBee, PMC, and BlueBee only provide the communication from one direction (i.e., WiFi or Bluetooth to ZigBee).

Different from the above approaches, our approach enables the concurrent communication from both WiFi and ZigBee devices to the gateway and the reverse direction. By combining or separating the WiFi and ZigBee signal at the bit level, Chiron is able to achieve the similar performance as if in sole WiFi to WiFi or ZigBee to ZigBee communications. Our experimental results demonstrate that our approach's spectrum utilization is more than 16 times higher than traditional approaches.



(a) Human in the Middle (b) Wearable Scenarios

Fig. 3.24: Gateway-to-WiFi Throughput in Mobile Scenarios: In human in the middle scenario, the Gateway-to-WiFi link's throughput can be up to 245.07 Mbps. In different wearable scenarios, our approach maintains similar throughput. This demonstrates that our design can support different types wearable applications.

3.9 Discussion and Future Work

In this section, we discuss the potential opportunities of Chiron.

3.9.1 Chiron under Different WiFi Standards

WiFi standard includes a variety of generations (from IEEE 802.11 to IEEE 802.11ah and so on). Since Chiron solves the spectrum waste problem while WiFi coexists with ZigBee, we only consider the standard works within 2.4GHz band. As long as the WiFi standard uses OFDM based modulation scheme, such as IEEE 802.11 g/n/ac, Chiron is compatible. That is because the OFDM based modulation scheme chops a wide band (i.e., 20MHz) into small pieces (i.e., 312.5 KHz), which yields a slow symbol rate as we discovered in the motivation section. It is possible that Chiron can support the 40MHz WiFi channel defined by IEEE 802.11n. And more interesting, up to 8 ZigBee channels are overlapped with a 40 MHz WiFi channel. This means that by using Chiron technique, the gateway is able to concurrently communicate

with one WiFi device and up to 8 ZigBee devices. In this scenario, the spectrum utilization can be further improved. We will investigate it in our future work.

Multiple-input and multiple-output (MIMO) technique is introduced to WiFi system since IEEE 802.11n. Basically, the MIMO technique increases throughput by spacial multiplexing (i.e, using multiple antennas at both the sender and receiver sides to multiply the channel capacity). For a MIMO enabled WiFi system (e.g., with IEEE 802.11n, a WiFi sender with two antennas and a WiFi receiver with two antennas consist a 2×2 MIMO system), it is possible to enable Chiron technique because the Chiron gateway only needs to transmit one spacial stream to ZigBee device.

3.9.2 Generality of Chiron

Our Chiron technique explores the possibility to combine WiFi and ZigBee signals. Potentially, Chiron technique can be applied to other wireless communications as long as two communication protocols: i) work on the overlapped frequency bands; and ii) have distinct symbol rates. By having these two properties, it is possible that Chiron can utilize the tolerance of wireless communication to combine two signals with different modulation schemes. However, due to the varieties of different modulation schemes, more future works are needed to investigate different combinations.

3.9.3 Supports for Upper Layers

With the exponentially increasing number of IoT devices, the traditional multi-radio gateway (e.g., a gateway equipped with both WiFi and ZigBee radios) introduces a spectrum utilization bottleneck, which is caused by the competition between WiFi and ZigBee communications (shown in Figure 3.1 in the introduction section). Our Chiron technique utilizes the unique properties of WiFi's and ZigBee's physical

layers to significantly improve the spectrum utilization. Since Chiron technique does not require any hardware modification on ZigBee device, the original functionalities at upper layers should not be affected, but we have not evaluated that. To further evaluate whether Chiron technique affects the original upper layers' design, we plan to investigate the application profiles such as ZigBee Home Automation (HA), ZigBee Light Link (LL), and building automation in the future. We also plan to investigate how to leverage the Chiron technique for further performance improvements in existing upper layer MAC Zhou & Zhu (2007, 2008a,b), routing Zhu & Towsley (2011); Gu, Zhu, & He (2009); Zhu & Yu (2006b,a); Malvankar, Yu, & Zhu (2006), and flooding protocols Zhu et al. (2010); Guo et al. (2011); Zhu et al. (2013).

3.10 Summary

With the exponentially increasing number of IoT devices, there is a pressing need to more efficiently utilize the spectrum in the crowded ISM band, especially at the edge (i.e., gateway) of the IoT network. In this paper, we explore a new direction – concurrent communication for a gateway to (or from) commodity WiFi and ZigBee devices. Our extensive experimental results indicate that Chiron achieves reliable performance under different settings (i.e., LoS, NLoS, mobile, and wearable). Chiron's concurrent WiFi and ZigBee communication can achieve similar throughput as the sole WiFi or ZigBee communication.

The design principle of Chiron is generic and has the potential to be applied to other frequency band that coexists radios with different symbol rates. The design of Chiron fits naturally at the edge of IoT networks to support commodity WiFi and ZigBee devices. By simply changing the gateway, the spectrum utilization can be increased by more than 16 times.

Chapter 4

PASSIVE-ZIGBEE: ENABLING ZIGBEE COMMUNICATION IN IOT NETWORKS WITH 1000X+ LESS POWER CONSUMPTION

4.1 Overview

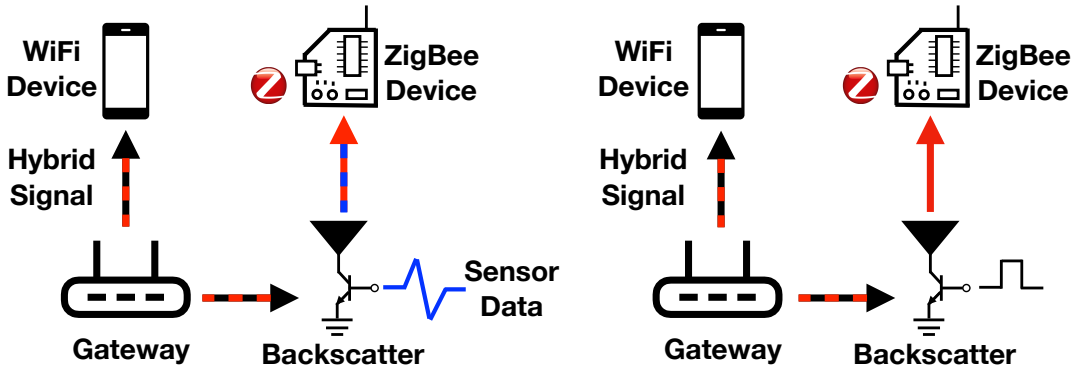
Within heterogenous IoT sensor networks, users of ZigBee devices expect long-lasting battery usage due to its ultra-low power and duty cycle. In IoT networks, to demonstrate even further ultra-low power consumption, we introduce Passive-ZigBee that demonstrates we can transform an existing productive WiFi signal into a ZigBee packet for a CoTS low-power consumption receiver while consuming 1,440 times lower power compared to traditional ZigBee. Moreover, this low power backscatter radio can bridge between the ZigBee and WiFi devices by relaying data allowing heterogenous radios to communicate with each other. We built a hardware prototype and implement these devices on a commodity ZigBee, WiFi, and an FPGA platform. Our experimental evaluation demonstrates the backscattered WiFi packets can be decoded by CoTS ZigBee receivers over a distance of 55 meters in none-line-of-sight and with human movements. Our Passive-ZigBee can consume only $25\mu W$ when transferring sensor data and relay ZigBee and WiFi data compared to traditional ZigBee (36mW).

Our FPGA synthesis tool demonstrated the extremely low power consumption.

4.2 Introduction

Gartner predicts that the Internet of Things (IoT) devices will increase to 20 billion by 2020 connecting all those devices (implanted or wearable health monitors, security locks, human trackers, etc) to the internet and each other. For these connected devices' battery to last more than 10 years or use energy harvesting technology, they must consume ultra-low power. Based on the low-power consumption needs of the IoT devices and widely-deployed existing WiFi radios infrastructure, we seek to ask: can we produce ultra-low power backscatter ZigBee devices that harvest energy from the deployed WiFi infrastructure? Traditional ZigBee offers a promising solution by consuming far less power than WiFi radios (36mW and 210 mW respectively). However, inspired by recently proposed backscatter designs, we seek to dramatically decrease power consumption. Unlike previous works, Passive-ZigBee is the first to achieve maximum standard-based network-throughput communication while harvesting energy from productive WiFi communication packets and thus consuming ultra-low energy.

We propose Passive-ZigBee, a novel backscatter communication that produces productive WiFi packets and transforms that packet to a commodity-compliant ZigBee packet instantaneously. Passive-ZigBee concurrently produces fully-compliant 802.11n WiFi and 802.15.4 ZigBee packets. We observe that WiFi devices are the most ubiquitous, dense, and powerful compared to other IoT devices. We argue that Passive-Zigee's devices require significantly lower power consumption due to 1) productive WiFi packets, 2) ultra-low power, simple, and inexpensive backscatter tags, and 3) low-power ZigBee listeners. Passive-ZigBee reuses existing WiFi and ZigBee



(a) Sensor (b) Relay

Fig. 4.1: System Overview

devices thus encourages backscatter adoption. The resulting radios enable significantly longer battery life and energy harvesting devices in the sensor networks compared to a traditional ZigBee. Moreover, because of the simplistic tag design, these tags require a smaller footprint on the sensor's integrated chip. Thus, Passive-ZigBee provides a novel design for a lower-energy consumption sensor network.

Fig. 4.2: A health-monitoring application where WiFi router provides localization data and control messages relayed by Passive-ZigBee's tag. This tag also sends glucose, oxygen saturation, and ECG data. The listener is a long-battery-life wearable ZigBee health monitoring and medicine delivery device.

In a nutshell, Passive-ZigBee 1) creates a hybrid ZigBee WiFi packet and 2) leverages backscatter to communicate to a listening ZigBee device operating in any of the industrial, scientific and medical (ISM) band. More specifically, as shown

in figure 4.1, Passive-ZigBee operates in two modes: 1) utilizing productive WiFi to WiFi packets, low-power consumption backscatter radios transmit sensor data to listening ZigBee devices, and 2) enabling concurrent WiFi to WiFi and WiFi to ZigBee communications through a backscatter radio relay. The reason that Passive-ZigBee packets can be received by both ZigBee and WiFi devices at full network throughput is based on the observation that ZigBee spreads its energy enabling it to be robust against WiFi's multi-tone signals. While the hybrid packet does introduce higher interference levels, we find that the robustness of WiFi and ZigBee standards can recover from the introduced noise. Specifically, we make the following technical contributions:

- We design a novel Gateway to produce hybrid signals that contain concurrent ZigBee and WiFi symbols. We leverage the facts that 1) WiFi and ZigBee use vastly different Symbol and Chip rates (250 KHz and 2 MHz), and 2) 802.11n WiFi signal contains enough subcarriers such that all possible ZigBee symbols can be contained in a single WiFi packet. Thus this hybrid WiFi packet enables productive Gateway to commodity WiFi communications.

- We design a low-power and small-footprint backscatter radio that 1) receives the Gateway's hybrid packet and 2) backscatters the signal to a listening ZigBee device. We achieve this design by using a multiplier that shifts the incoming Gateway signal to different frequencies at the ZigBee symbol rate. By mapping and frequency-shifting the ZigBee symbols embedded in the wide-band WiFi, the backscatter can transmit sensor data in a customized packet to a commodity ZigBee device.

- We enable low-power consumption bridging in WiFi and ZigBee networks by embedding ZigBee to WiFi data in the hybrid gateway's packet for the backscat-

ter to relay. We achieve this design by leveraging the inherent interference robustness built into the ZigBee and WiFi communication protocols.

- Through prototyping the hybrid gateway on both a software defined radio and a commodity radio and backscatter on an FPGA, Passive-ZigBee consumes 1,440 times less energy than traditional ZigBee transmitters according to our FPGA synthesis tool.

4.3 Motivation

The increase of more than 20 billion mobile connects IoT devices that range from home automation controls to life-saving health-monitoring devices create demands for efficient energy usage. Thus, the goal of low-energy consumption, 10+ year battery life, and energy harvesting sensors and controller motivate our design to communicate to ZigBee devices. A sample application includes energy-harvesting ECG (Electrocardiogram), glucose, and Pulse-Oximetry sensors embedded in patients transmitting data to a wearable long-battery-life operated health monitor and drug delivery device which needs location and control data from a cloud server (Figure 4.2). The health device will only deliver drug at specific locations with certain vital sign levels and control information. Due to high-power and ubiquitous availability WiFi network, these WiFi signals are an ideal target for energy harvest in backscatter sensors and control information access.

Limitation of Traditional ZigBee: Current ZigBee devices operate by the generation of transmitting RF signals through a self-contained integrated chip and analog RF component with an attached battery. While these ZigBee devices are small and considered low-power, they still draw mA of current during transmission Dementyev et al. (2013). The highest energy consumptions components are the amplifiers and

baseband generating digital logic. Moreover, traditional ZigBee radios were not designed to interact with existing WiFi devices in a heterogeneous network.

Limitation of gateways: In the ever-crowding and denser wireless networks, the main limitation of the gateways is the energy and device costs to bridge the heterogenous radios. The traditional gateway translates between the WiFi and ZigBee protocols by 1) receiving a data packet from the WiFi device and 2) then retransmitting that data using ZigBee protocols. Examining the case with multiple ZigBees sensors and control devices operating simultaneously on different channels, the gateway would need multiple additional ZigBee radios. In the case where ZigBee sensors operate on the same band, the WiFi using carrier-sense multiple access (CSMA) will back-off due to interference caused by the physical proximity of the collocated ZigBee and WiFi radios on the gateway. Thus, the 1) additional radios, 2) repetitive overhead packets, and 3) gateway deployment increases the energy consumption of the WiFi devices requiring additional infrastructure. With the case that ZigBee and WiFi operating on the same frequency bands, the WiFi must back-off due to CSMA, degrading network throughput. Additionally, the translation between WiFi and ZigBee protocols also introduces additional latency.

Advantages of Passive-ZigBee: By leveraging productive WiFi networks, Passive-ZigBee removes the need for the amplifiers and RF generation and therefore, consumes μW power enabling communication between pairs of a backscatter tag and a single ZigBee receiver. Moreover, Passive-ZigBee enables WiFi and ZigBee to communicate. Because of the ultra-low current draws, Passive-ZigBee significantly improves battery and provides a framework toward battery-free energy-harvesting sensors.

4.4 Design Overview and Challenges

Our design has two main players: a modified WiFi Gateway and Passive-Zigbee tags. The gateway is a router that coordinates between heterogenous IoT devices (WiFi, ZigBee, and backscatter tags). Specifically, the active wider-band gateway operating on the WiFi network's frequency has the ability to concurrently transmit WiFi and ZigBee signals. The low-power narrower-band ZigBee operate on separate frequencies to avoid Carrier-sense multiple access (CSMA) back-off. The Passive-ZigBee tag backscatters the gateway signal to 1) carry sensor data and 2) relay messages to ZigBee devices. The signals produced by both devices are able to be decoded by commodity WiFi and ZigBee devices.

The rest of the section describes an overview of WiFi and ZigBee devices. We then explain how to transmit and receive hybrid WiFi and ZigBee signals. After producing these hybrid signals, we provide a theoretical design of a low-power tag which will backscatter the signals. We demonstrate how these tags can 1) send the tag's sensor data and 2) relay packets between the ZigBee and WiFi devices.

- How does the gateway produce signals for WiFi devices and the backscatter tags simultaneously? The design challenge for the hybrid gateway is to perform productive communication to WiFi devices and relay mode for backscatter devices. This is done by modifying the wider-band WiFi signal (described in Section 4.6.1).

- How does the backscatter tag send sensor data to a listening ZigBee? The design challenge of the backscatter tag is to reflect the WiFi Gateway signal to transmit sensor data while achieving full ZigBee network throughput and maintaining ultra-low power utilization for both the tag transmitter and receiver. This process is done by modifying the frequency of the hybrid gateway signal that

contains ZigBee symbols (described in Section 4.7).

- How does the backscatter create custom ZigBee frames for a commodity device? The backscatter reflects various groups of the wider-band WiFi subcarriers that contain embedded ZigBee symbols. By selecting and reflecting specific portions of WiFi signals, the tags form customized ZigBee frames achieving full ZigBee network throughput (described in Section 4.7.2).

- How does the backscatter tag relay WiFi data to the ZigBee Network? The design challenge of the backscatter tag is to relay and bridge the WiFi gateway to ZigBee networks utilizing ultra-low energy. The tag reflects portions of the WiFi signals that contain ZigBee information to a ZigBee listener (described in Section 4.7.3).

- How does a commodity WiFi device act as a hybrid WiFi ZigBee Gateway? By embedding messages in the WiFi payload, the CoTS WiFi devices can emulate ZigBee frames in the subcarriers. With coordinated backscatter tags, we can achieve low power transmission and reception using listening CoTS ZigBee devices (described in Section 4.8.1).

4.5 Background

First, we introduce the WiFi and ZigBee communication protocols.

4.5.1 WiFi Radio

Figure 4.3 shows a WiFi system overview. A WiFi radio uses multiple subcarriers to simultaneously transmit aggregate bits in a wider-band protocol. To perform this aggregate transmission: 1) The data payload is interleaved; 2) The WiFi

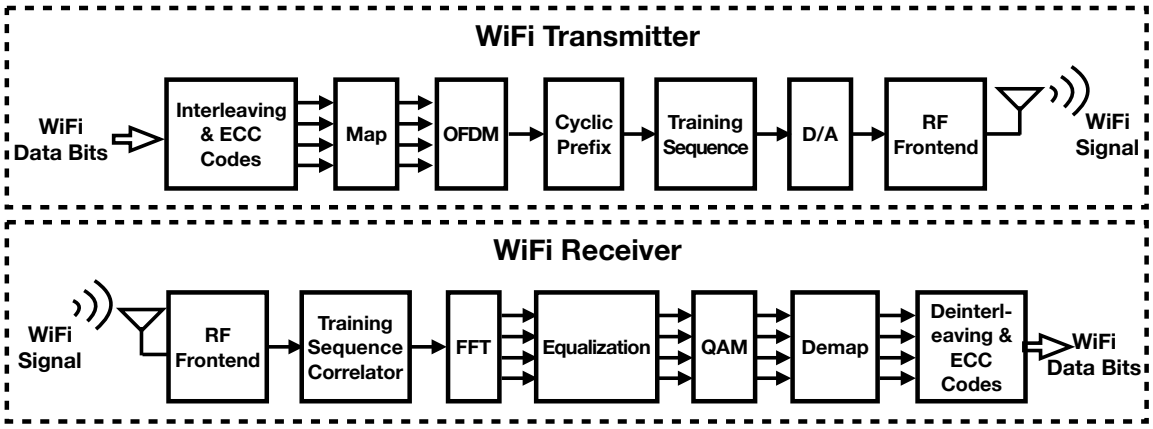


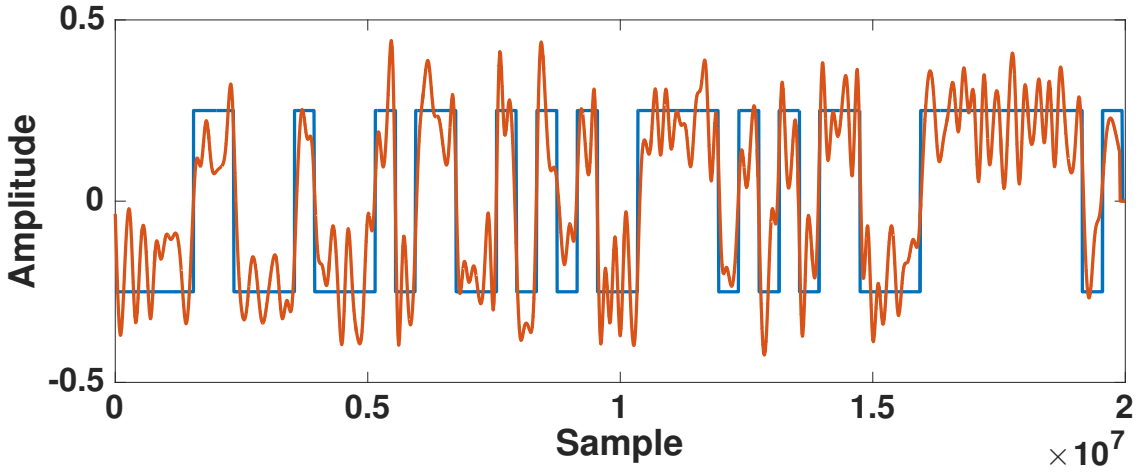
Fig. 4.3: The WiFi Transmitter and Receiver

serial binary is parallelized and mapped into bits onto different channels; 3) On each channel, WiFi applies Quadrature Amplitude Modulation (QAM) to mapping bits to different phases in sine waves. We define the various phase states of the signals as symbols. 4) Then, WiFi uses orthogonal frequency-division multiplexing (OFDM) to sum the sine waves. 5) Between each symbol duration, a cyclic prefix is appended to reduce inter-symbol interference. 6) Before the baseband WiFi signal, a training sequence allowing for sender and receiver discovery and synchronization is added. The output signal can be written as Equation 4.1.

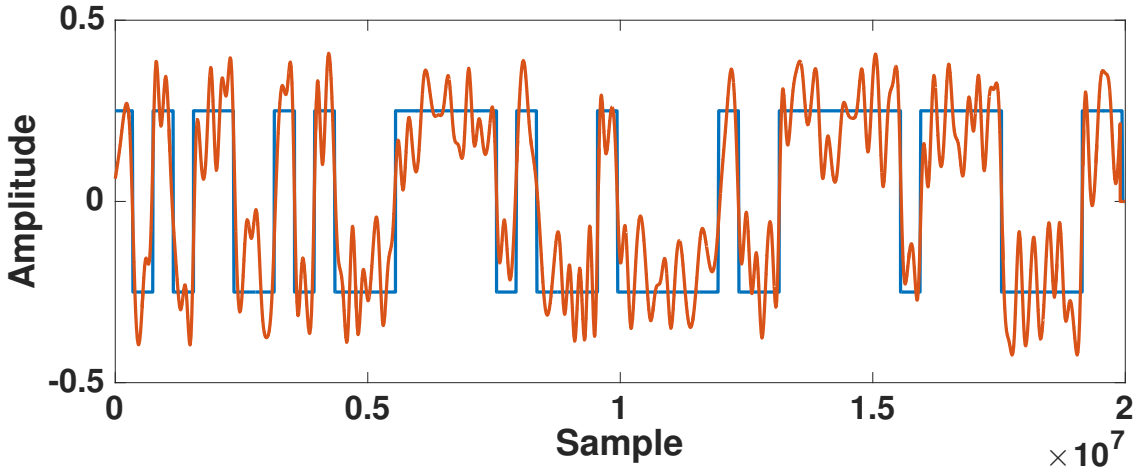
$$W(t) = \sum_{n=0}^{N} \left[\left(I(t)\cos(2\pi f t_1) - Q(t)\sin(2\pi f t_1) \right) e^{2\pi j f_s n} \right] \tag{4.1}$$

Where there are N total WiFi subcarriers, and for each n subcarrier, we defined complex symbol states at the $I(t)$ and $Q(t)$ mapped by QAM. The duty cycle of each symbol is defined by ft_1. We defined the subcarrier spacing frequency by f_s.

In the WiFi receiver, the system reverses the mapped and aggregated sine waves back to bits. 1) A correlator and a phase synchronization (Phase Locked Loop) algorithm discover the training sequence and align the demodulator's initial phase



(a) In-phase



(b) Quadrature

Fig. 4.4: A hybrid WiFi subcarrier containing added ZigBee signals

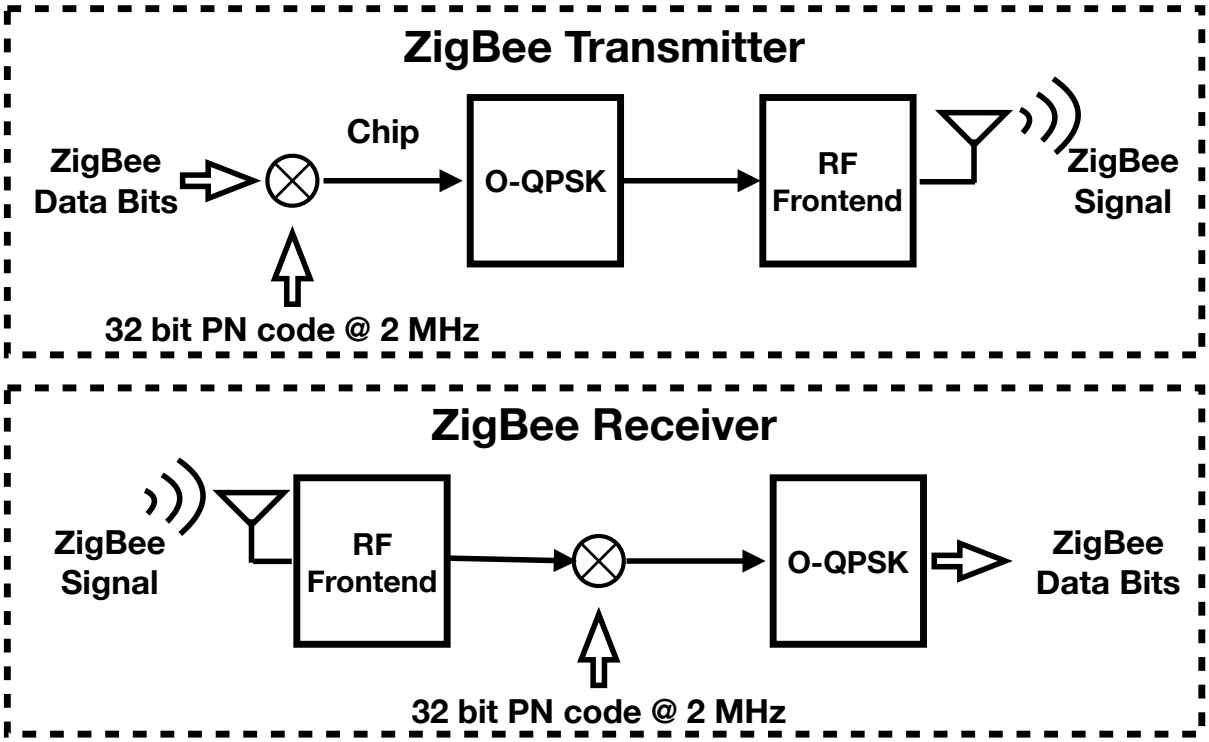


Fig. 4.5: The ZigBee Transmitter and Receiver

state. 2) Using the inverse FFT algorithm, the receiver recovers the aggregated sine waves while accounting for the cyclic prefix. 3) A QAM demodulator maps the phase states of the sine waves to symbols and then to bits.

4.5.2 ZigBee Radio

Passive-ZigBee reflects WiFi packets to commodity ZigBee. The ZigBee transmitter and receiver is shown in Figure 4.5. In summary, ZigBee radios are low power narrow-band radio that spread its bits over a narrower frequency band. 1) ZigBee uses Direct Sequence Spread Spectrum (DSSS) to spread the signal into a wider band by multiplying with a higher rate (2 MHz) shared pseudorandom noise (PN) code. 2) After the spread spectrum process, the ZigBee modulator maps the bits to sine

waves by offset quadrature phase-shift keying (OQPSK) modulation which reduces the dramatic phase shifts by offsetting the odd and even bits by a distinct period (Equation 4.2). These sine waves with 4 possible states are the ZigBee chips.

$$Z(t) = \frac{1}{\sqrt{2}} I(t) \cos(2\pi f t) - \frac{1}{\sqrt{2}} Q(t - T_s) \sin(2\pi f t) \tag{4.2}$$

Where there are 4 states for I and Q describing the information carrying sine waves, and T_s represents the period offset.

To receive a frame, 1) the ZigBee radio down-converts the received waveforms to baseband and digitalizes them into in-phase and quadrature (I/Q) samples using an analog-to-digital converter (ADC). 2) The O-PQSK demodulator measures the changes in phase to symbols. 3). The baseband signal is multiplied by or correlated to a shared PN code which yields the encoded bits. Due to satisfying the statistical randomness property, the PN ensure that interference such as Doppler frequency shifts and multipathing can be recovered from correlations by allowing for some chip errors.

4.6 Passive-ZigBee

The objective of Passive-ZigBee is to 1) generate a hybrid ZigBee WiFi signal that enables commodity WiFi communication and 2) using a backscatter sensor device, reflect portions of the hybrid signal to a listening commodity Zigbee device. This system enables 1) backscatter sensor to ZigBee communication and 2) relay the WiFi data to the ZigBee networks that operate on differing channels.

4.6.1 Hybrid WiFi ZigBee Gateway

Figure 4.4 shows an example of a single hybrid WiFi and ZigBee subcarrier that can concurrently transmit WiFi and ZigBee signals. The design of a hybrid WiFi and ZigBee signal is possible due to the observations that 1) ZigBee chip and WiFi symbol rates operate on distinct frequencies (2 MHz and 250 KHz) and 2) 7 WiFi subcarriers overlap a ZigBee signal. The intuition is that WiFi subcarriers and ZigBee chips change its phase and amplitude states at different times with different bandwidths. This design is a form of channel sharing using different times similar to CDMA (Code Division Multiple Access). Because of filters that commodity ZigBee and WiFi radio employ, the hybrid packets can be demodulated by both devices.

To achieve the Passive-ZigBee's objective of communicating to ZigBee devices while still maintaining productive WiFi to WiFi communication, we utilize a Software Defined Radio (SDR) to produce a hybrid concurrent WiFi and ZigBee signal. The advantage of an SDR design is the custom gateway can simultaneously communicate with WiFi devices while producing all combinations of ZigBee symbols for the backscatter to reflect. This hybrid signal is achieved by solving for weights added to WiFi baseband QAM signals.

Tx a Hybrid Signal Figure 4.6 shows the objective of the hybrid gateway is to embed in the wide-band WiFi subcarriers the combination of the ZigBee symbol states, such that a backscatter can choose which symbol to reflect. Thus, a combined hybrid WiFi and ZigBee frames can be received by unmodified WiFi and ZigBee devices. To transmit the signals concurrently, the output of the hybrid gateway must contain a mixture of ZigBee and desired WiFi signals. This mixture is compared to the two baseline signals: normal WiFi signal and WeBee's emulated ZigBee signal. To generate this hybrid signal, we utilize an optimization search algorithm resulting

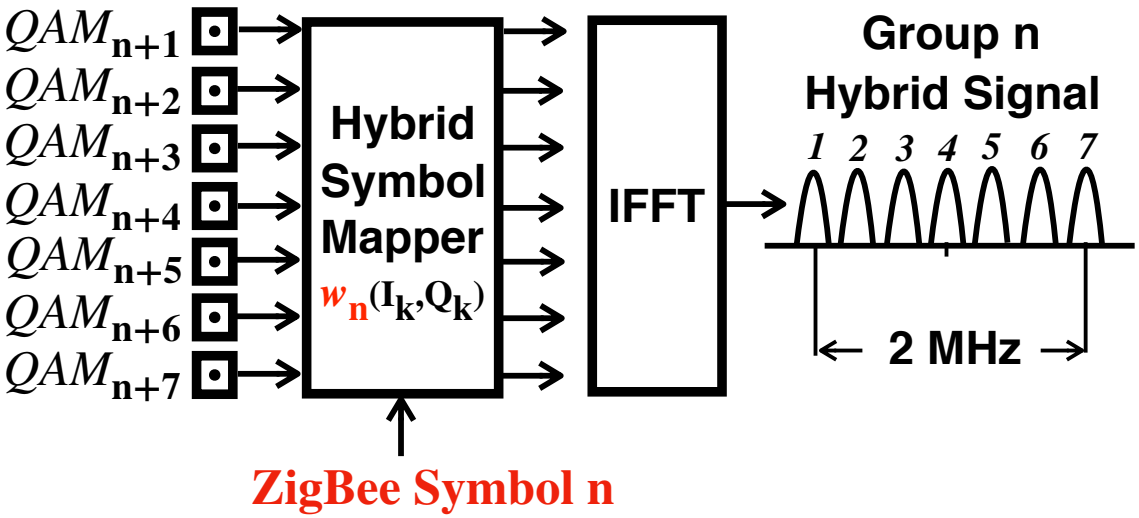


Fig. 4.6: Hybrid Process

in a linear look-up table. The size of the table is based on the number of the QAM states that matches the 4 OQPSK states. With 7 subcarriers per ZigBee chip, this is a combinatorics problem with 4 objects selecting 7 samples allowing for replacements yielding 120 entries. Due to the WiFi router infrastructure, we don't expect the memory requirements from the look-up table to be an issue.

To combine the ZigBee and WiFi hybrid signal, we recognize that seven WiFi subcarriers contain a single ZigBee channel. Thus, the seven WiFi subcarriers, which operates with 312.5 KHz frequency offsets, must contain both the higher 2 MHz frequency ZigBee chips rate and the lower 250 WiFi KHz symbol rate. To combine these signals, we utilize a look-up table defined by an optimization search algorithm.

We define this optimization algorithm as a search for weights to add to while combining the WiFi subcarriers and ZigBee signals. Minimizing the output's Error Vector Magnitude (EVM) of WiFi and ZigBee symbols. EVM measures the error distance between the desired phase states of both ZigBee and WiFi symbols.

We define the cost function in Equation 4.3 where I_{ref} and Q_{ref} are the reference or expected phase states. The I_{Meas} and Q_{Meas} are the measured or recovered phase states.

$$C = \sqrt{(I_{ref} - I_{Meas})^2 + (Q_{ref} - Q_{Meas})^2} \tag{4.3}$$

Minimize C_{WiFi} and C_{ZigBee} where to w_1 and $w_2 \in R$ subjected to

$$\begin{aligned} I_{Meas} &= (I_n(t_1) + w_1 \cdot Z_I(t_2)) \cos(2\pi f t) \\ Q_{Meas} &= (Q_n(t_1) + w_2 \cdot Z_Q(t_2)) \sin(2\pi f t) \end{aligned} \tag{4.4}$$

Where I_n and Q_n represent WiFi symbols, and w_1 and w_2 are searchable weights to scale the ZigBee symbols Z_I and Z_Q.

The inputs to the look-up table are a WiFi QAM phase signal and a ZigBee DSSS O-PQSK symbol, and the output is a hybrid combined ZigBee WiFi signal.

The output of the hybrid gateway will be

$$\sum_{n=0}^{N} \left[((I(t) + w_i) \cos(2\pi f t_1) - (Q(t) + w_q) \sin(2\pi f t_1)) \, e^{2\pi j f_s n} \right] \tag{4.5}$$

Because of the ZigBee 4 O-PQSK states, there are $2^4 = 16$ possible ZigBee chip states. Thus, the WiFi subcarriers must have all 16 possible ZigBee states embedded in the wide-band signal. Since 7 WiFi subcarriers overlap a single ZigBee symbol, we need $7\dot{k}$ WiFi subcarriers to carry all the possible k ZigBee states.

The modifications to the WiFi subcarriers include the cyclic prefix, the repetitive portions of the WiFi signal to decrease intersymbol interference. Thus, the weights are different for the repetitive portions of the WiFi subcarriers, but the modification from the must not remove all the guard interval. Again mixture is moderated by the optimization algorithms. Due to satisfying the statistical randomness property, the 32-PN codes per symbol scheme ensures that interference such as Doppler frequency

shifts and multipathing can be recovered from correlations.

To illustrate this process, Figure 4.9 demonstrates embedding the ZigBee and WiFi signals together. 1) The ZigBee symbols are spread using a shared PN code. 2) The selected ZigBee and WiFi symbols are mapped using the look-up table generating the hybrid sine waves. 3) The hybrid sine waves are spread using the IFFT algorithms. 4) The rest of the transmission scheme is the same as the standard WiFi protocol described in Section 4.5.1.

4.7 Backscatter

Figure 4.1 shows an overview of our system. A WiFi radio transmits a custom packet, and the backscatter reflects the packet to a ZigBee receiver while modulating the narrowband information. When the tag backscatters the packet, it shifts the frequency of the reflected signals to select the desired ZigBee symbol. The ZigBee receiver listens on the normal ZigBee channel, receives the reflected packet, and decodes the packet using the normal ZigBee decoding mechanism. Next, we discuss the key components of our system which enable this capability, first 1) embedding sensor data on the reflecting signal, 2) bridging between the ZigBee and WiFi network operating on different frequency bands, and 3) synchronization.

4.7.1 Backscatter Coding

As shown in Equation 4.6 and 4.7, backscatter tags operate on the principles of reflecting existing signals with modifications in the amplitude, phase, and frequency. 1) A transmitter excites electrons and sends a signal. 2) The excited electrons from a transmitter are induced from an antenna onto the receiver because of the potential difference between the ground and the antenna. 3) The radio modifies the signal and

re-excites transmitting the electrons.

$$\begin{aligned} S_{out} &= S_{in} \times S_{tag} \\ &= \sin(2\pi f_{in}t) \times [D + \frac{2}{\pi}\sum_{I=1}^{\infty}\frac{sin(n\pi D)}{n}cos(2\pi f_{tag}nt)] \\ &= S_{DC} + S_{shift} \end{aligned} \tag{4.6}$$

$$\begin{aligned} S_{shift} &= \sin(2\pi f_{in}t) \times \frac{2}{\pi}\sum_{n=1}^{\infty}\frac{sin(n\pi D)}{n}\cos(2\pi f_{tag}nt)] \\ &= \sum_{n=1}^{\infty}\frac{2sin(n\pi D)}{n\pi}[\sin(2\pi f_{in}t) \times \cos(2\pi f_{tag}nt)] \\ &= \sum_{n=1}^{\infty}\frac{sin(n\pi D)}{n\pi}\{\sin[2\pi(f_{in} - f_{tag}n)t] \\ &+ \sin[2\pi(f_{in} + f_{tag}n)t]\} \\ &= S_{left} + S_{right} \end{aligned} \tag{4.7}$$

$$S_{right} = \sum_{n=1}^{\infty}\frac{sin(n\pi D)}{n\pi}\sin[2\pi(f_{in} + f_{tag}n)t] \tag{4.8}$$

Thus, backscatter tags are extremely efficient. Because backscatter tags do not need to generate an active carrier wave, these tags require far less power. These tags reduce latency because the radio does not need for the circuits to be warm.

4.7.2 Sensor Data to Commodity ZigBee

Utilizing the hybrid ZigBee WiFi gateway, the backscatter's objective is to shift the desired symbol states embedded in the wide-band hybrid signals to the channel that the ZigBee device listens.

As shown in figure 4.7, the objective of the backscatter is to select which group of ZigBee symbols embedded in the wideband WiFi signal to reflect using

Algorithm 2 Algorithm on the backscatter

Input: $WZ\_Sym\_Freq[K]$, ZB_Listen_Freq, $BS\_Bits[N]$
Output: BS_Sig.

1: for $i = 1; 4 * i < N; i = i + 1$ do
2: $\quad Symbol[i] = BS\_Bits[(1, 2, 3, 4) + i)]$
3: end for
4: if $4 * i = N$ then
5: $\quad Symbol\ Number:\ M = i - 1$
6: else
7: $\quad M = i$
8: $\quad Symbol[i + 1] = BS_Bits[N + 4 - 4 * i] \mid 0000$
9: end if
10: for $i = 0; i < M; i = i + 1$ do
11: $\quad Frequency\ Offset:\ F$
12: $\quad F \rightarrow MAP(WZ\_Sym\_Freq[K],\ Symbol[i])$
13: $\quad BS\_Sig \rightarrow Mix(F, ZB\_Listen\_Freq)$
14: end for

frequency shifting to a listening ZigBee receiver expressed in algorithm 2. The array $WZ\_Sym\_Freq[K]$ defines the frequencies in the wide-band WiFi signal that contain the ZigBee symbols. ZB_Listen_Freq defines the frequency of the listening ZigBee radio. The array $BS\_Bits[N]$ are the array of N bits acquired from the sensor to be transmitted. The intuition is by shifting and reflecting the desired combination of ZigBee symbols embedded in the wideband hybrid gateway signal, the backscatter communicates to a listening commodity ZigBee device at full 802.15.4 standard throughput. To understand this WiFi subcarrier selecting and frequency shifting process expressed in the function Mix, we explain heterodyning.

Heterodyning is the process of changing the original signal frequency to another frequency by mixing the two signals together. The mathematical principle behind

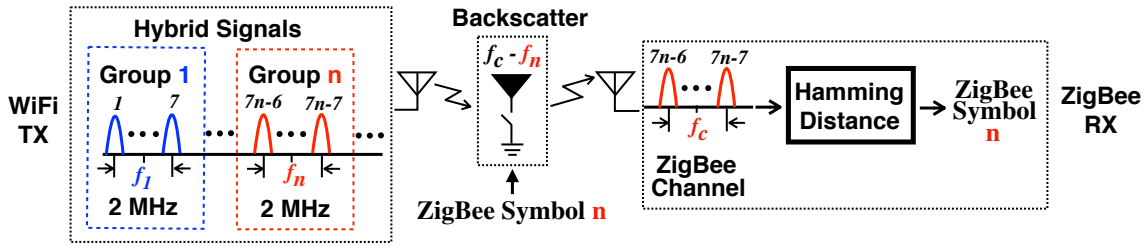


Fig. 4.7: 7 WiFi Subcarriers carrying concurrent WiFi and ZigBee Data

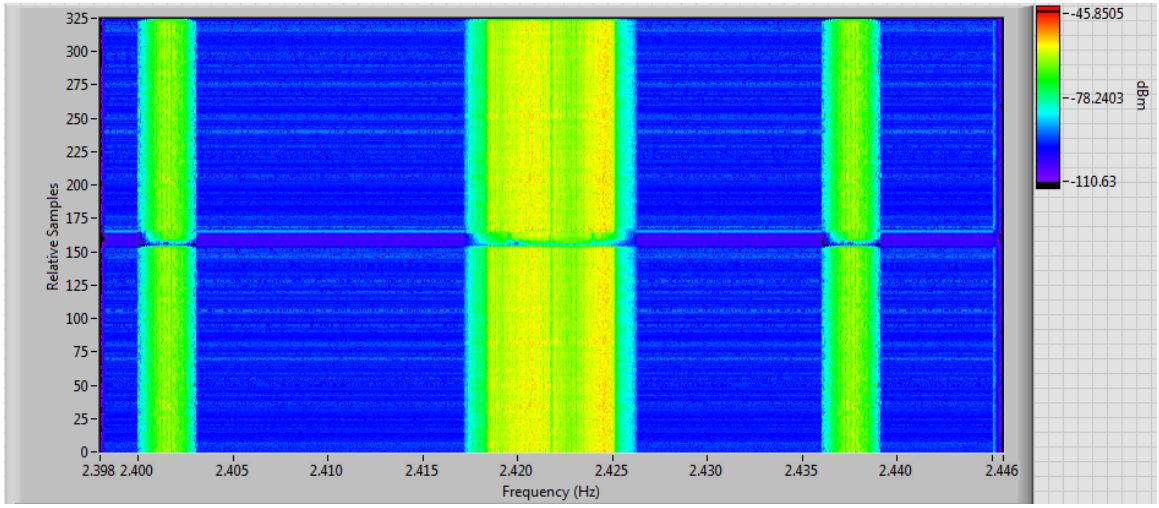


Fig. 4.8: Reflected WiFi Hybrid signal

this process is a trigonometric identity, expressed in Equation 4.9.

$$\begin{aligned} &\sin(2\pi f_1 t)\sin(2\pi f_{i2} t) \\ &= \tfrac{1}{2}\left[\cos\left(2\pi\left(f_1 - f_{i2}\right)t\right) - \cos\left(2\pi\left(f_1 + f_{i2}\right)t\right)\right] \end{aligned} \tag{4.9}$$

Where f_1 is the frequency of hybrid Gateway signal, and f_{i2} is the carrier frequency of the tag's clock at symbol instance i. Therefore, after the multiplication, there is a frequency shift $f_1 + f_{i2}$ and a phase shift as shown in figure 4.8. Thus, the backscatter is able to change the incoming signals' frequency to the listening receiver. Here, we ignore the DC component. We could use an existing technique to cancel

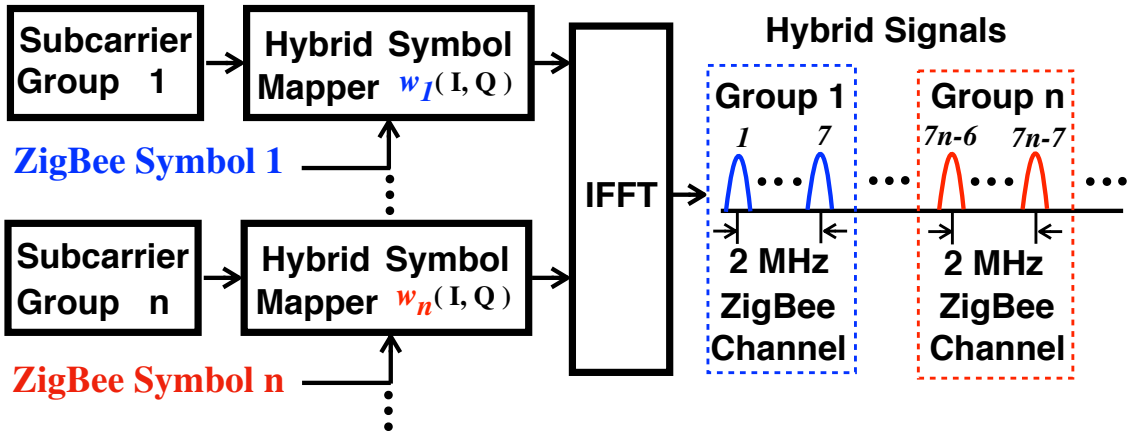


Fig. 4.9: The Hybrid ZigBee WiFi Gateway

one of the sidebands, such as S_{left}, and keep S_{right} left.

Between each ZigBee symbol rate, the tag must change f_{i2} to the center location of each group of the 7 WiFi subcarriers that each contain a possible ZigBee symbol state. Because there are 4 symbol states in O-QPSK signal, there is a total of $2^4 = 32$ combinations. To change the tag's carrier frequency f_{i2}, the clock would need to perform dynamic frequency scaling by varying the voltage level expressed in Equation 4.10. P is the power consumed; C is the clock capacitance; V is the voltage; f_{i2} is the tag's clock frequency.

$$P = C \cdot V^2 \cdot f_{i2} \tag{4.10}$$

Figure 4.9 demonstrates this process. 1) The WiFi gateway embeds possible ZigBee symbols in 7 subcarriers that covers ZigBee frequency band. 2) Multiple groups of the 7 WiFi subcarriers produce differing ZigBee symbols. These subcarriers contain concurrent WiFi and ZigBee data that commodity WiFi and ZigBee devices can demodulate due to the vastly differing symbol and chip rate. 3) The backscatter selects and shifts these groups of 7 subcarriers to the center frequency of the listening

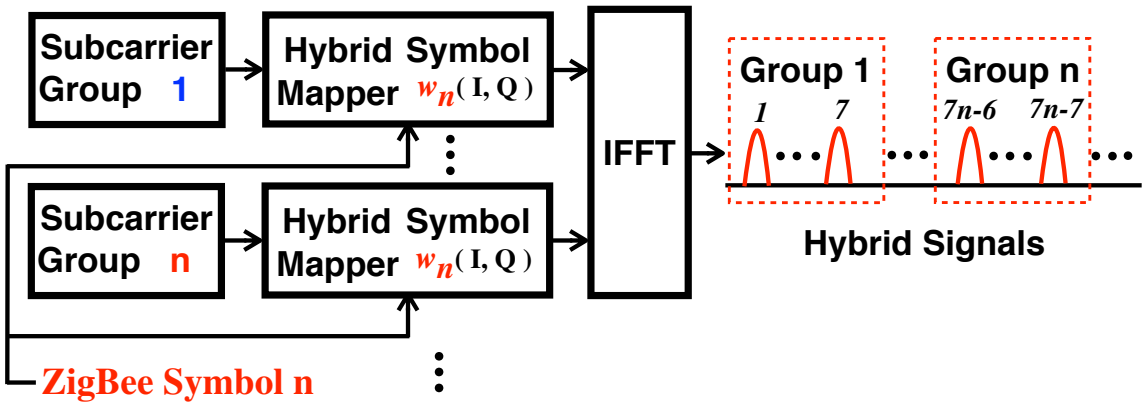


Fig. 4.10: The Hybrid ZigBee WiFi Gateway for relay

ZigBee radio. Figure 4.10 shows the hybrid process of backscatter relay.

4.7.3 Relay WiFi data to ZigBee Network

The objective of the tag is to relay WiFi data to ZigBee networks that are operating outside of the WiFi network's frequency. As an example, the hybrid gateway transmits a packet to a WiFi receiver. Embedded in that same packet, the gateway embeds ZigBee data using portions of the WiFi packet. In the relay mode, each subcarrier groups contain changing ZigBee symbols that allow the backscatter to relay and bridge to a ZigBee network operating out of the WiFi frequency band.

Figure 4.10 demonstrates this relaying and bridging process. 1) The gateway embeds the WiFi to ZigBee data in all the groups of 7 subcarriers that covers ZigBee frequency band as before. 2) Multiple groups of the 7 WiFi subcarriers contain the ZigBee symbols that change in respect to the ZigBee symbol duration. Unlike the backscatter sensor data mode, the symbols remain the same for all the groups of

subcarriers. 3) The backscatter relays the gateway's message to the listening ZigBee.

4.7.4 Symbol Level Synchonization

In order for the backscatter tag to shift at the rate of each symbol period, the tag must have the knowledge from the hybrid WiFi ZigBee packets symbol period. To achieve this synchronization, we leverage WiFi's training sequence. This training sequence allows for fine timing and frequency synchronization using a specialized BPSK modulation. We utilize a sliding cross-correlation on the signal envelope to seek for this marker for the beginning of symbols. This sliding cross-correlation produces spikes that a simple threshold will provide the phase alignment information. The reason why the correlation to the preamble envelope works for detecting the start is that the preamble has a much greater power level compared the data payload and the preamble is standard for every WiFi packet.

4.7.5 Channel Access

Both WiFi and ZigBee protocols adopt Carrier-sense multiple access with collision avoidance (CSMA/CA) to reduce the probability of packets' collisions among different transmitters. Basically, CSMA/CA senses the channel before transmitting. If the channel is busy, the transmitter backs off and senses again until the channel is free. To sense a particular channel, an energy consuming ADC and a bandpass filter is needed. However, as an ultra low power device, the PassiveZigBee tag is not able to power these two modules. To conduct channel sensing, we offload the sensing task to the gateway side. Specifically, the gateway senses not only the WiFi channel but the targeted ZigBee channel (i.e., the channel which PassiveZigBee shifts to) as well before transmitting the hybrid signal. By doing this, the PassiveZigBee can shift the hybrid signal without backoff.

For example, assuming the gateway communicates with a WiFi device on WiFi channel 1 and the PassiveZigBee transmits to a commodity ZigBee receiver on ZigBee channel 16 (by shifting the hybrid signal from gateway). Before transmitting, the gateway senses the both the WiFi channel 1 and ZigBee channel 16 to avoid collisions on these two channels.

4.8 Implementation

We built Passive-ZigBee using off-the-shelf components utilizing a Virtex 5 FPGA to provide a clock and multiplier as the backscatter. We utilized a standard Software Defined Radio (SDR) and a commodity WiFi and ZigBee devices to prototype the design.

4.8.1 Using CoTS WiFi Devices as the hybrid transmitter

The objective of Passive-ZigBee is to transmit ZigBee symbols frames in wideband WiFi packets allowing a backscatter to select the frames and communicate with a commodity ZigBee. To achieve this objective, we can use a commodity WiFi device to emulate ZigBee symbols by embedding specific bits in the data payload. We formulate the searching of the string of bits to produce the terms of a search problem.

Emulating a ZigBee Signal We leverage WeBee's technical contribution that was able to emulate ZigBee in WiFi packets. To emulate possible ZigBee frames, we need to first define the output of a WiFi payload in terms of a signal S_w. Let the data load be defined as arrays of bits as $WiFi_Payload$. We first define the possible ZigBee frames in equation 4.11. Where I_k, Q_k is the WiFi symbols for n subcarriers. Since 7 WiFi subcarriers overlap a signal ZigBee frame, we consider the combining the subcarriers as the emulated ZigBee signal. Our search is to find a set of WiFi

symbols I_k, Q_k that matches the ZigBee signal $z(N)$ (Equation 4.11).

$$w_i\left(I_k, Q_k\right) = \sum_{n}^{n+7}\left[I_k \cos\left(2\pi f t\right) - Q_k \sin(2\pi f t)\right] e^{2\pi j f_2 n}$$
$$\max\left\{\begin{array}{c} \arg\max \\ \left(I_k, Q_k\right) \in S \end{array} \left[w_i\left(I_k, Q_k\right) * z(N)\right]\right\} \tag{4.11}$$

The emulation procedure is that 1) the desired ZigBee frames are mapped to a set of WiFi symbols (I_k and Q_k). 2) The I_k and Q_k WiFi symbols are then mapped into WiFi bits. 3) Finally, 4) the correct position for the bits are mapped into the packet based on the WiFi devices convolutional interleaving function, such that the WiFi subcarriers produce the respective QAM states that emulate the ZigBee signal. Because of imperfections of emulating ZigBee signal due factors such as repetitive cyclic prefix, the ZigBee's demodulation frame correlation threshold has to be decreased.

4.8.2 Software Defined Hybrid WiFi ZigBee Gateway

The objective of the gateway was to transmit and receive combined and separate ZigBee and WiFi packets. We utilize National Instruments FPGA with 802.11 core to build a custom hybrid WiFi ZigBee gateway. Utilizing a multi-rate design, we synthesized a prototype compatible OFDM QAM design with embedded DSSS O-PQSK signals to transmit to commodity Zigbee and WiFi development receivers (XBee and UP Squared Grove).

4.8.3 Backscatter Tag

The objective of the backscatter tag is to reflect existing signals to the ZigBee listener. We prototyped the backscatter tag design on a National Instruments (NI) FlexRio. The design was a simple mixer that shifted frequencies from the operating

frequency of ZigBee and WiFi networks. In a practical implementation, we must sense the WiFi signal through correlation threshold on the WiFi training sequence and remove the interference produced by the mixing process described in Section 4.7.2 as to reduce interference from non-relevant WiFi subcarriers. Otherwise, these reflected subcarriers may interfere with other ZigBee channels.

Removing WiFi Subcarrier with active components To achieve the optional removal of reflected subcarrier interference, we must achieve the objective of the removing the extra interference signal in the backscatter signal. While removing this interference does not affect the listening ZigBee, interference may occur with other IoT devices depending on the network setup including the strength of the router signal and distance between the tag and other IoT devices. This optional process requires more active components include a low-noise-amplifier and an output band-pass filter must be used. This filter is centered around the ZigBee listener with a bandwidth of 2 MHz matching the ZigBee devices. The amplifier ensures that the signal loss from the filter does not compromise signal integrity. We prototype this design on the NI Flexrio board.

4.9 Evaluation

We describe the evaluation of the performance of Passive-ZigBee in achieving uplink backscatter up to 55m in none-line-of-sight and mobility scenarios (Section 4.9.2). Our experiments demonstrate the following

Our Passive-ZigBee prototype achieves an uplink backscatter of 55m in non-of-sight scenarios (NLOS). This distance performance is due to the fact that WiFi routers output higher power than standard ZigBee. In mobility scenarios, we achieve the full 15m distance in hallways in our academic building as our signals need to pass

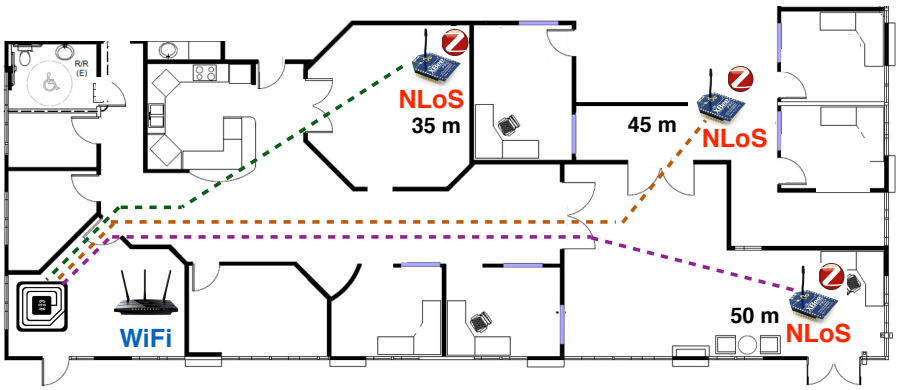


Fig. 4.11: The evaluation plan for NLoS and mobility

through several (2+) human bodies that are made of mostly water that stops RF signals.

Our system is able to achieve the close to full 250 Kbps throughput in close range (under around 30m) in non-line-of-sight from the from the tag to the commodity ZigBee listener. With human bodies and movement, the ZigBee achieved around 200 Kbps.

The operational range of our WiFi ZigBee hybrid router to tag is more than 10m. Our commodity WiFi receiver is able to receive 802.11n packets at 25m.

Lastly, we show that our simple, low-power tag only consumes around 25 μW while shifting the router signal to another frequency band. Through this shifting, we remove carrier interference caused by the all the radios thus decreasing interference. Because the receives are all commodity devices, we show that our system is compatible with existing IoT infrastructure.

We benchmark Passive-ZigBee's range using three metrics: throughput, bit error rate (BER), and received signal strength indicator (RSSI). For a baseline, we controlled the interfering signals by shielding using a Faraday cage that offered -90 dB signal isolation; we placed the router, tag, and ZigBee receiver in the Faraday cage.

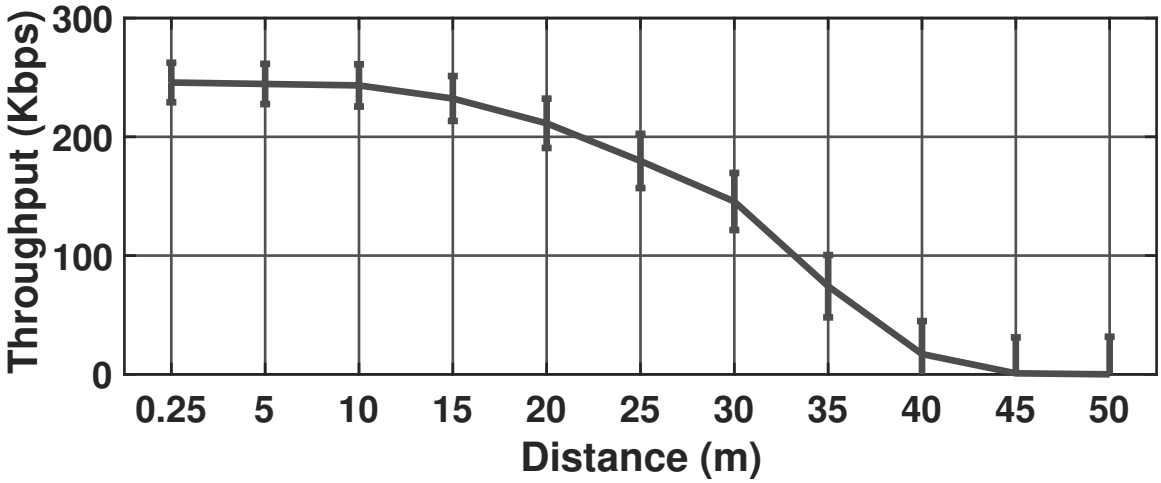


Fig. 4.12: Backscatter to ZigBee throughput in NLoS Passive-ZigBee has stable throughput over communication distance in NLoS scenario.

In our NLOS deployment, the WiFi ZigBee transmitter and the tag were placed in a room while the ZigBee device was operating in the hallway separated by a door and one or two drywall. In mobility scenarios, we attached the ZigBee receiver to the human body and received messages while moving. We moved the ZigBee and receiver away increasing from the tag and measured throughput, BER, and RSSI. Then we also move the ZigBee listener away from the tag and measured throughput, BER, and RSSI.

We evaluate Passive-ZigBee with the hybrid gateway at 2.422 GHz at 40 MHz with 108 subcarriers. Our ZigBee receivers operated at 2.405 to 2.480 GHz.

4.9.1 NLoS Performance

In this section, we evaluate the backscatter to ZigBee throughput over communication distance. Figure 4.12 shows the results. At 0.25 meter, the throughput achieves around 230 Kbps (note that 250 Kbps is the maximum throughput defined by ZigBee's protocol). When the communication distance increases to 10 meters,

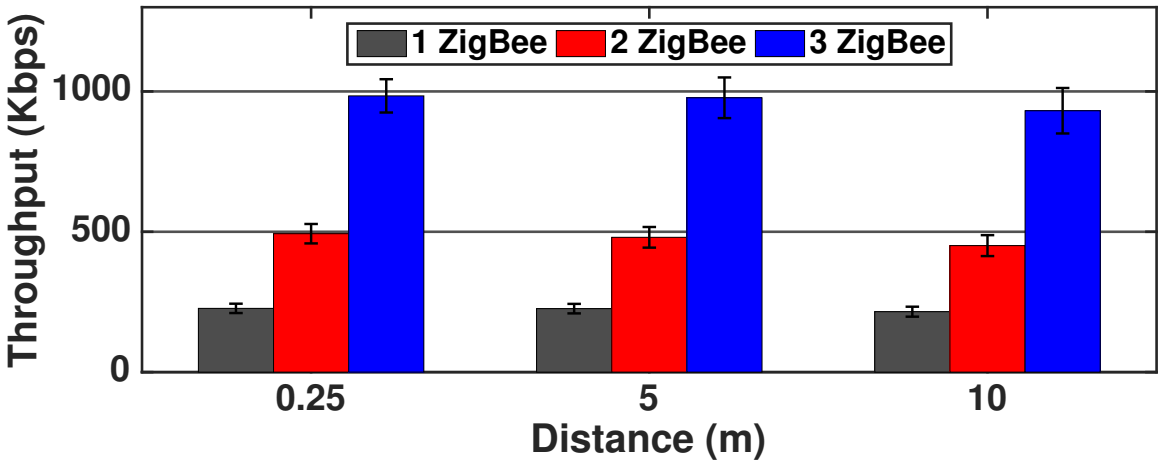


Fig. 4.13: Backscatter to ZigBee throughput in Mobile Scenario. Passive-ZigBee has stable throughput over communication distance.

the throughput of backscatter to ZigBee communication is very stable (around 225 Kbps). We further evaluated the throughput at longer distances. At 35 meters, it still maintains around 80 Kbps. The reason is that Passive-ZigBee has simple design at the backscatter side that the low power device only needs to select the incoming signal to modulate OQPSK signal.

Takeaway: Passive-ZigBee is able to achieve low power and long-range communication.

4.9.2 Mobility Performance

Since Passive-ZigBee is designed for low power sensors, potentially, it can be deployed on human bodies for medical or fitness applications. To investigate the performance of Passive-ZigBee on the human body, we asked up to three participants to wear the Passive-ZigBee tags in their pockets and walked around the office. Figure 4.13 shows the aggregated throughput across one, two, or three tags over different communication distances. Overall, for one tag, the throughput is stable when the

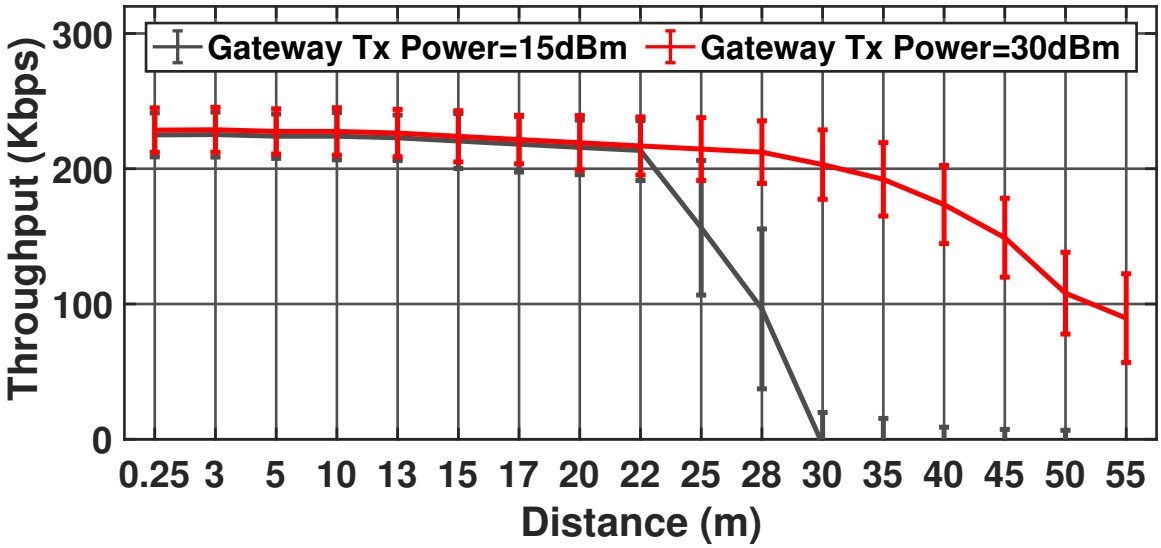


Fig. 4.14: Backscatter to ZigBee Throughput under different Gateway Transmission Power

communication distance increases from 0.25 meter to 10 meters (the results only show a slight decrease from 227Kbps to 215Kbps). The reason is that the tag shifted the signal to out-of-band ZigBee receiver. Thus, it is not affected by the original in-band WiFi signal. For two and three tags, the throughput linearly increases because the Passive-ZigBee tags can reflect the hybrid signal to different frequency channels that they do not impact with each other.

Takeaway: Passive-ZigBee shows stable throughput even attached to a human body and in mobile scenarios.

4.9.3 Impact of Gateway Transmission Power

In this section, we test how the gateway transmission power impacts the backscatter to ZigBee throughput over communication distance. Figure 4.14 shows the results. When the communication distance is relatively short (less than 22 meters), the throughput under 15 dBm and 30 dBm are similar and maintains around 220 Kbps.

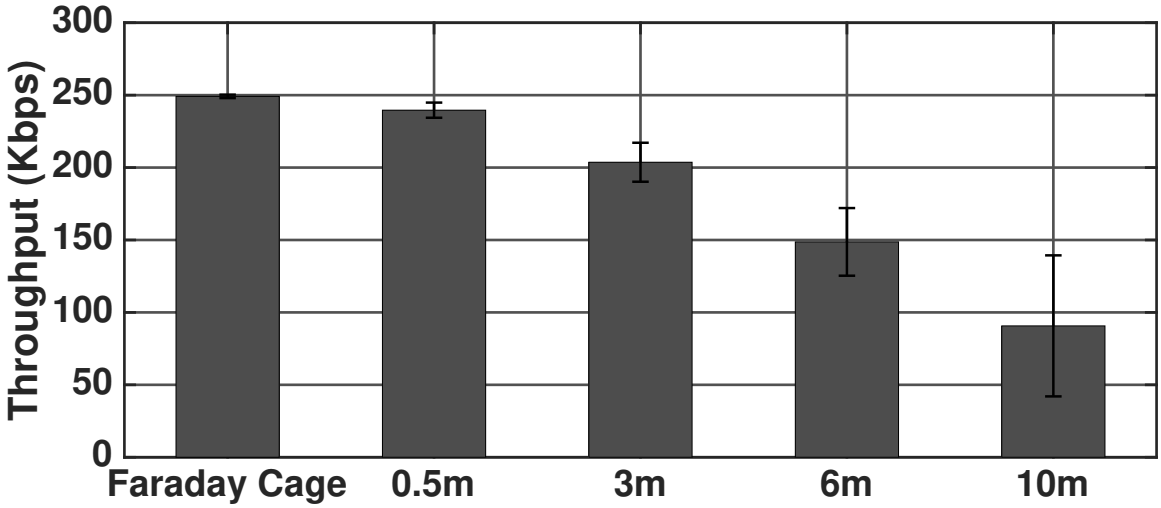


Fig. 4.15: The throughput of Backscatter to ZigBee in NLoS

After 22 meters, the throughput under 15 dBm transmission power drops exponentially as the SNR decreases. Thus, the commodity ZigBee throughput under -30 dBm transmission power is still stable. Even at 55 meters, the throughput under -90 dBm transmission power achieves up to 88 Kbps throughput. The receiver will drop the packet when incorrect DSSS chips exceed the threshold of the demodulator.
Takeaway: When the communication range is within 22 meters, the gateway transmission power does not impact too much on Passive-ZigBee's throughput. When the communication is longer than 22 meters, the gateway transmission power shows a positive impact on Passive-ZigBee's performance.

Impact of Transmitter-Tag Distance Figure 4.15 shows the impact of increasing tag to ZigBee receiver distance to throughput, and Figure 4.16 shows the impact respect to BER. Our experiment demonstrates successful reception at over 10 meters non-line-of-sight. At close distances, we achieved near maximum ZigBee standard throughput (250 Kbps). The backscatter tag does significantly decrease the reflected

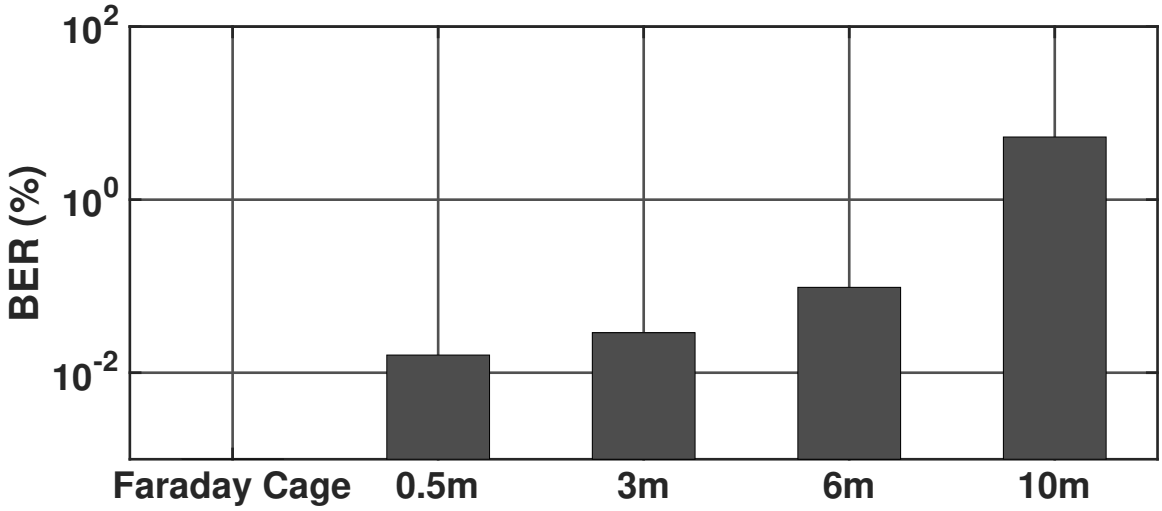


Fig. 4.16: BER of Backscatter to ZigBee in NLoS

power; but due to the robustness of ZigBee spread spectrum protocols, our experiment demonstrates more than 10 meter of reception. The exponential increase of BER is expected with DSSS and QPSK.

4.9.4 Latency

To demonstrate latency in bridging WiFi and ZigBee networks, we experimented in IoT networks comparing Gateway and Passive-ZigBee backscatter approaches. We modeled the time between when data was given to the transmitting radio to when the RF signal is received. We measured the collisions and CSMA backoff with commodity ZigBee and WiFi devices using lossless National Instruments RF recording system. In all the cases, we experimented with ZigBee receivers that operate in both WiFi in-band and out-band networks. As shown in Figure 4.17, due to CSMA back-off, in-band ZigBee devices experience heavy latency (53 ms). Without out-of-band band ZigBee devices, latency (15 ms) is primarily caused by the translation between the WiFi and ZigBee protocols. The cause of low latency (6 ms) in Passive-ZigBee is the

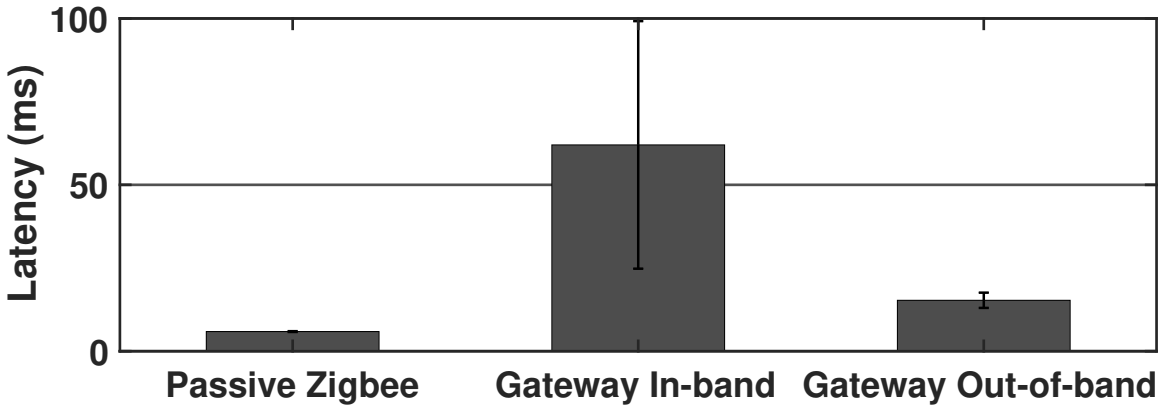


Fig. 4.17: Latency

decoding logic in ZigBee receiver due to instantaneous frequency shifting method of Passive-ZigBee without having to wait for baseband generating circuits to warm. Takeaway: Passive-ZigBee shows much lower latency compared with traditional ZigBee devices.

4.9.5 Use of Commodity WiFi Gateway

To demonstrate that we can use commodity WiFi to emulate ZigBee signals, we used an Atheros QCA9880 802.11ac chipset due to the ability to inject packets and to fix scramble seeds. We also operated in 5 GHz with 80 MHz in increase number available subcarriers. Because of the ability to directly inject packets and monitor the signal produced, we could determine how the bits were interleaved into the FFT outputs by demodulating using a Keysight Vector Signal Analyzer. In our experiment, we were only able to synthesize 10 simultaneous ZigBee symbols due to pilot tones and firmware compatibility. Thus this limited our throughput. This limitation can be removed with newer devices and firmware. Our experiment demonstrates the framework that 180 MHz 802.11ac can generate all the possible symbol combinations. We also lowered the correlation threshold in MICAz ZigBee

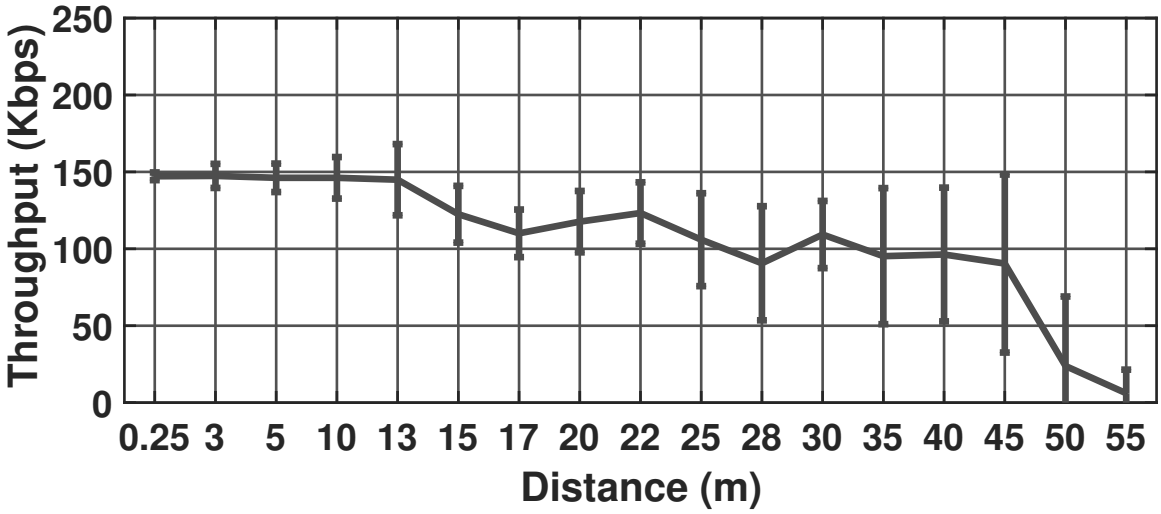


Fig. 4.18: Throughput of Backscattering COTS WiFi to ZigBee in NLoS.

listener to adapt to the emulated signals. The results in Figure 4.18 demonstrate that at 0.5 meter, 35 meters, and 50 meters communication distance, the throughput achieves around 150 Kbps, 100 Kbps, and 25 Kbps, respectively.

Takeaway: Passive-ZigBee can use a commodity WiFi as a sender to communicate with ZigBee devices.

4.9.6 BER

In this section, we show the results of Bit error rate (BER) at different received signal strength. Figure 4.19 shows the results for different WiFi modulation schemes (including 16, 64, and 256 QAM). We can observe that with lower rank modulation scheme (i.e., 16 QAM), the BER is lower and the BER is relatively high with higher rank modulation schemes (i.e. 64 and 256 QAM). The reason is that the hybrid signal needs to emulate both ZigBee and WiFi signal. Since lower higher rank modulation scheme is sensitive to SNR, the optimization scheme (introduced in Section 4.6.1) adds more weight on WiFi signal. Thus at ZigBee receiver side, the BER is relatively

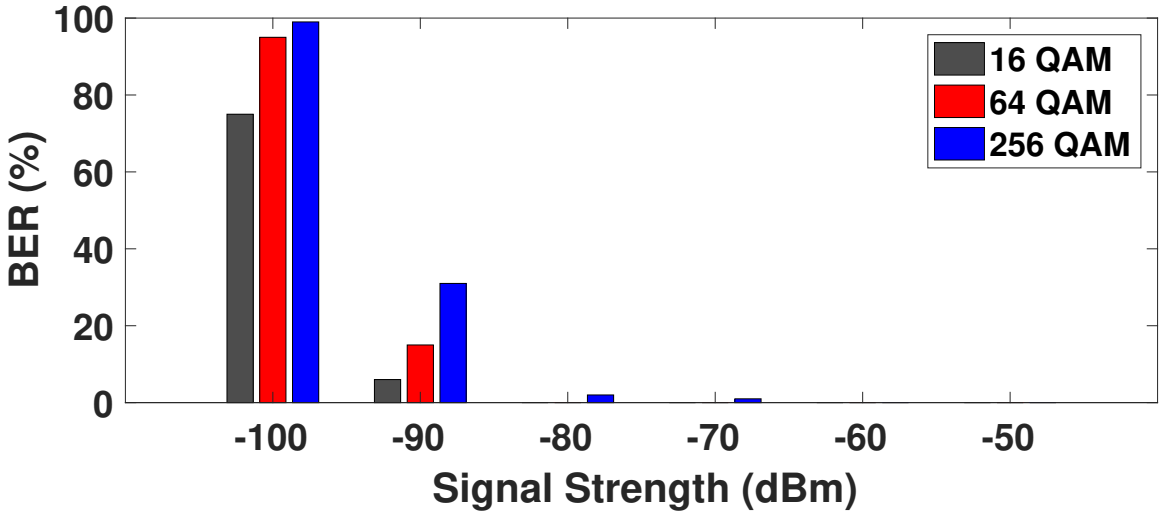


Fig. 4.19: Bit error rate (BER) at ZigBee Receiver Side

high compared with the lower rank modulation scheme. The results show that the BER is approaching 0 when the received signal strength is higher than -80 dBm. This ensures the backscatter to ZigBee communication at a high throughput.

Takeaway: Passive-ZigBee shows low BER when the signal strength is higher than -90 dBm regardless of the WiFi modulation scheme.

4.9.7 RSS @ the ZigBee Receiver

We measured the received signal strength (RSS) at ZigBee receiver side and show the results in Figure 4.20. The figure shows the RSS with different gateway transmission power (15 and 30 dBm). Overall, we can observe that the overall RSS decreases along with the communication distance increases; this is the major reason that the throughput decreases and BER increases over distance. The received signal strength for 15 dBm (black solid curve) is lower than 30 dBm (red dashed curve). The results have some fluctuation caused by the multipath effect. We also experimented on mobility scenario measuring the RSSI levels measuring the distance between a person

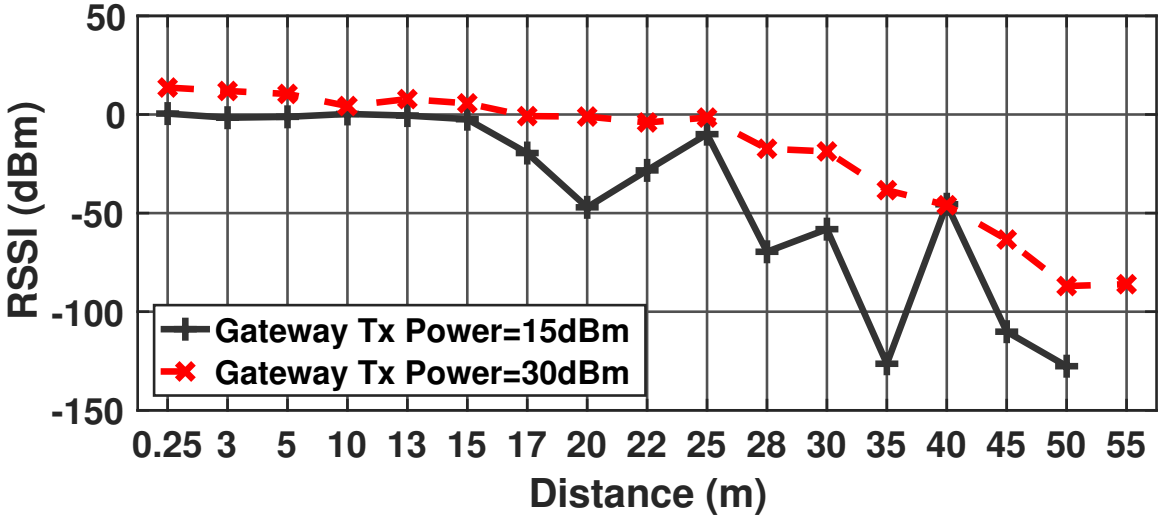


Fig. 4.20: RSS @ ZigBee Receiver Side

walking with tag and stationary ZigBee receiver. The RSSI levels demonstrate that the ZigBee receiver was able to receive messages beyond 10 meters distance at -70 dBm.

4.9.8 The impact to On-going WiFi Communications

In this section, we evaluate the impact of 1) backscatter to on-going WiFi traffic and 2) hybrid WiFi ZigBee signal. Figure 4.22 shows that regardless of whether backscatter presents or not, the throughput of WiFi communication decreases along with communication distance increases because the SNR decreases while communication distance increases. By comparing the scenarios with or without backscatter at the same communication distance (for example 35 meters), the results did not show an obvious difference. It is because that the backscatter shifts the WiFi signal to another channel which is far (in terms of frequency) from the original WiFi channel.

Compared to the original WiFi router, the hybrid WiFi ZigBee decreased throughput by about 10% due to interference created to the original WiFi signals.

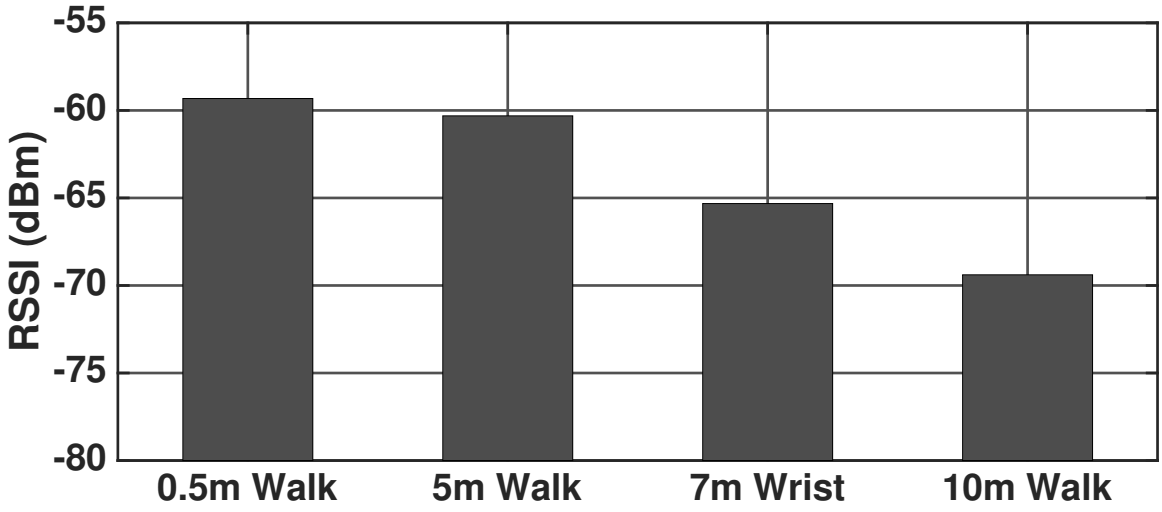


Fig. 4.21: Mobility RSSI

	Clock	Logic
Energy Consumption (uW)	11	6

Table 4.1: Energy Consumption for Each Component

This is due to our increase in overhead bits using WiFi's native convolutional forward error correcting codes.

Takeaway: Passive-ZigBee does not make an impact to on-going WiFi traffic because it is able to shift the signal to out-of-band ZigBee channel.

4.9.9 Energy Consumption

Table 4.1 shows the breakdown of the components of Passive-ZigBee. Our results are based on Xilinx Power Estimator tool. The clock does consume variable power depending desired clock speed but averages out to 11 μW. The mapping logic can be synthesized using selective NAND gates using 6 μW. Our FPGA synthesis tool shows that the critical transmitting components use around 25 μW of power. The power produced from energy harvesting devices produce around 100 μw from indoor

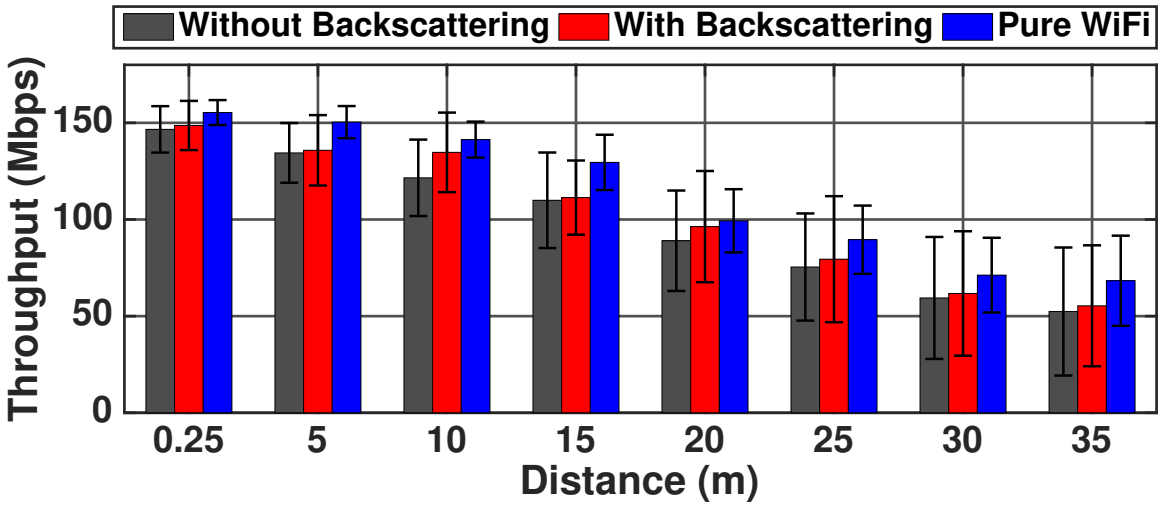


Fig. 4.22: The impact to On-going WiFi Communications

lights and temperature supporting Passive-ZigBee.

We experimented up to 15 links of backscatter to ZigBee communications as well as traditional ZigBee to ZigBee communications and estimating the energy consumption at the sender sides (backscatter or ZigBee sender). From the results shown in Figure 4.23 (note that the y-axis is in log scale), we observe that the average energy consumption of backscatter is 1,440 times lower than the traditional ZigBee communications while providing similar throughput.

Takeaway: Comparing to traditional ZigBee, Passive-ZigBee saves 1,440 times energy to transmit a packet.

4.10 Related Works

The related works are divided into two categories:

Backscatter: Backscatter techniques enable a promising way for extremely low power sensing and computing devices due to the removal of carrier and symbols generators. Recent research demonstrates these backscatter systems, such as TV backscatter Liu

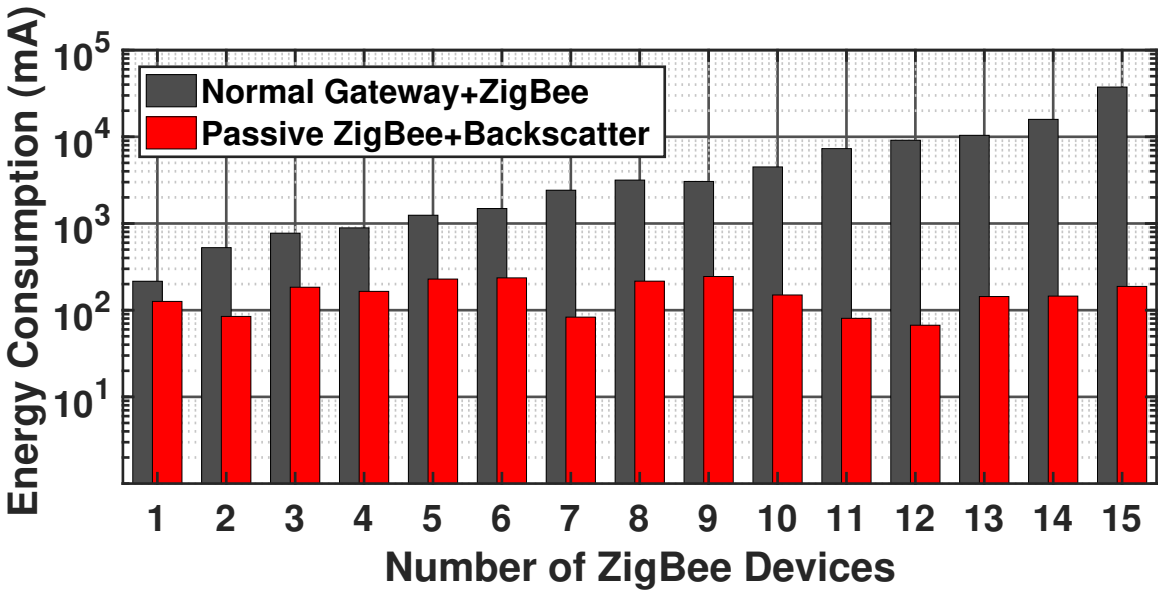


Fig. 4.23: Energy Consumption (the y-axis is in log scale)

et al., full-duplex backscatter Liu, Talla, & Gollakota, turbocharing backscatter Parks et al., LoRa backscatter Talla et al. (2017) which works on 900 MHz to achieve longer communication distances.

Interesting works include Kellogg et al. (2014); Bharadia et al. (2015); Kellogg et al. (2016); ZHANG et al. (2016b); Iyer et al. (2016); Zhang et al. (2016a, 2017) which utilize the ambient signals on the ISM 2.4 GHz band to enable communications between low power backscatters and pervasive receivers (e.g., WiFi, ZigBee, and Bluetooth devices). Specifically, the WiFi backscatter Kellogg et al. (2014) piggybacks backscatter's data on existing WiFi signal and receives it on a cell phone using CSI (Channel States Information). Backfi Bharadia et al. (2015) utilizes full-duplex technique on the WiFi receiver side to separate the WiFi and backscattered signal, which boosts the backscatter-to-receiver throughput. Passive WiFi Kellogg et al. (2016) and FS-Backscatter ZHANG et al. (2016b) shift the backscattered signal to out-of-band to achieve higher SNR for demodulation. Interscatter Iyer et al. (2016)

reflects the Bluetooth signal to commodity WiFi devices for medical applications. Hitchhike ZHANG et al. (2016b) uses a coding scheme to remove additional carriers so that backscatter can reflect between 802.11b compatible WiFi devices. Freerider Zhang et al. (2017) further improves the system in Hitchhike so that it works with 802.11g WiFi, ZigBee, and Bluetooth devices.

Different from current backscatter works, our PassiveZigBee achieves both productive WiFi 802.11n communications while maintaining extremely low power consumption to i) communicate with ZigBee networks; and ii) bridge WiFi networks and ZigBee networks. Meanwhile, it generates minimal impact to existing WiFi communication and achieves maximum ZigBee standard throughput.

Cross Technology Communication (CTC): In this category, the researchers both mitigate and utilize the interference among different wireless communication techniques (e.g., WiFi, ZigBee, and Bluetooth). Esense Chebrolu & Dhekne and Gsense Zhang & Shin utilize special timing features of packet length and gap duration, respectively. FreeBee Kim & He, EMF Chi et al. (2017a), C-morse Yin et al. (2017) and DCTC Jiang et al. (2017) use packet level modulation to improve the CTC performance. B^2W^2 Chi et al. (a) demodulates the BLE data by using the CSI at WiFi side. In WEBee Li & He (2017), they propose to manipulate the WiFi payload for ZigBee signal emulation. Other proposals that demonstrated symbol level modification for CTC include PMC Chi et al. (2017b) and Chiron Li et al. (2018). Reducing latency under concurrent communcation, ECT Wei Wang & Zhu. (2017) changes node prioirties through network protocals.

Different from above CTC papers, our goal is to enable ultra-low power sensor which can not only communicate with ZigBee devices but forward messages from WiFi device to ZigBee device as well.

Passive-ZigBee is a novel backscatter low power radio that leverages existing

commodity WiFi and ZigBee infrastructure by transforming productive WiFi packets into ZigBee packets. The backscatter uses 1,440 times lower power compared to a traditional ZigBee transmitter. Moreover, the backscatter also is capable of relaying data between WiFi to ZigBee devices. To perform the reverse communication path, we could use existing techniques such as Chiron Li et al. (2018).

4.11 Summary

Passive-ZigBee is a novel backscatter low power radio that leverages existing commodity WiFi and ZigBee infrastructure by transforming productive WiFi packets into ZigBee packets. The backscatter uses 1,440 times lower power compared to a traditional ZigBee transmitter. Moreover, the backscatter is also capable of relaying data between WiFi to ZigBee devices.

Chapter 5

CONCLUSION AND FUTURE WORK

5.1 Thesis Summary

This thesis explores fundamental factors that leverage the WiFi 1) CSI to preserve privacy while sensing humans, 2) subcarriers to enhance better coexistence between heterogeneous IoT radios, and 3) backscatter to dramatically reduce energy consumption. Preserving privacy while sensing and tracking humans, we measured CSI observed from WiFi beacons. Improving spectral utilization, we leveraged CSI and hybrid WiFi-ZigBee packets to improve IoT network performance. Reducing energy consumption, we leveraged hybrid WiFi-ZigBee packets and backscatter that enable implantable energy-harvesting sensors to interface with existing WiFi and ZigBee infrastructure.

We proposed a novel privacy preserving CSI encoding system, Wobly, that allows sensing tracking humans activities while encoding a person's identity. Specifically, we characterize multipath and Doppler Effect that encoded gait signatures with room configurations. Wolby 1) extracts features that identify individuals by their intrinsic body movement during walking without attachments to the body and 2) addresses the need to conduct real-time monitoring of individuals and detecting events such as falling.

We proposed Chiron a promising direction for Physical (PHY) layer concurrent high throughput communication to heterogeneous IoT devices (e.g., wider-band WiFi and narrower-band ZigBee). Specifically, at the PHY layer, Chiron enables concurrently hybrid transmitting (or receiving) 1 stream of WiFi data and up to 4 streams of ZigBee data to (or from) commodity WiFi and ZigBee devices as if there is no interference between these simultaneous connections.

Finally, we proposed Passive-ZigBee that included a backscatter radio and transformed a productive WiFi signal into a packet for a low-power ZigBee receiver while consuming 1,440 times lower power compared to traditional ZigBee transmitters. Additionally, this low power backscatter tag can relay between the ZigBee and WiFi devices allowing heterogenous radios to communicate with each other.

5.2 Future Work

I would like to continue to explore with regard to 1) efficient communication, 2) physical wireless security, and 3) sensing human movements. Adoption of sensor fusion in healthcare and smart buildings will require privacy and security techniques. I would like to explore the utilization of backscatter technique involving other signals. Application of machine learning algorithms to fuse, classify, and predict data from multiple sensors and models will enhance sensor system adoptions.

Appendix A

APPENDIX: THE IOT CHANNEL MODEL

A.1 Traditional Shared Channel

CSMA and TDMA assume two devices cannot simultaneously transmit and receive due to interference. Multiple devices sharing the same band impact 1) SNR, 2) data rate, and 2) spectrum efficiency. In traditional CSMA and TDMA, the other users' signals are treated as noise sources. In contrast, the Chiron concurrently transmit hybrid packets and receive concurrent packets that are aware of other interfering signals through channel state sensing.

Shannon-Hartley theorem provides the maximum possible transmission rate C at a given Signal to Noise Ratio (SNR) and users density. With devices, S_i competing in same bandwidth, B, we can define the theorem as equation A.1.

$$C = B \cdot \log_2 \left(1 + \frac{S_1}{\sum_{i=2}^{n} S_i + N} \right) \tag{A.1}$$

We statistically model efficiency of a CSMA, as the performance of the network, depends on the density of the number of devices operating in the same band. The probability of back-off is defined in Equation A.2, where S is the noise threshold, and

T_n and T_N are the density of winning transmitter and active transmitters respectively.

$$P(T_n, S) \triangleq 1 - \frac{T_n}{T_N} \tag{A.2}$$

We also define an exponential back-off in equation A.3, where c is number of collision and a is the back-off factor.

$$W(c) = a^c - 1 \tag{A.3}$$

We therefore can define the rate (bits/s) of the transmission in a given bandwidth as

$$R_{csma} \triangleq \sum T_n \cdot W\left(1 - P(T_n, S)\right) \cdot B \cdot \log_2\left(1 + SN \cdot D\right) \tag{A.4}$$

Let B is the bandwidth, SN is the SNR, and D is the distance between the transmitter and the receiver. We can also define spectrum efficiency in terms of user density by equation A.5, where N is the number of users, P is the length of the packet, I is the interval between packets, and B is the bandwidth.

$$R_{csma} \propto \frac{N \cdot P}{I \cdot B} \tag{A.5}$$

A.2 Cross-Technology Sensing

The challenge of cross-technology communication is that radios use various methods of modulation, clocks, and sampling rates. Comparing traditional CSMA/TDMA (described in the previous section), we recognize the era of software-defined radios (SDR) enables flexible sensing and transmission schemes. For different standards to sample each other, we need to demonstrate that under-sampling another standard's enables communication. Based on Nyquist-Shannon's sampling theorem, the sam-

pling rate for two standards defined in Equation A.6.

$$f_s \geq \frac{(packets/\sec)}{2} \tag{A.6}$$

In concurrent transmission, we sample messages from different technologies through collided and delayed packets. To demonstrate this type of sensing, we examine sensing between ZigBee and Wi-Fi. Under 802.15.4 standard, the minimum sampling rate is 2 MS/sec 484 (2009). With short guard intervals with a minimum of 64 us, the WiFi packets rate is around 15,000/sec, which is far less than the minimum sampling rate of ZigBee. Therefore we can conclude that a ZigBee device can sense all Wi-Fi packets.

A.3 Concurrent Transmission's Channel Model

Through cross technology signals sensing, described in previous section, Chiron's controlled packet collisions can improve network throughput through noise cancellation, equalization, and error correcting codes. We can improve the SNR due to the fact the receiver has knowledge of the interfering signal. In concurrent transmission, the threshold for noise is reduced significantly because cognitive devices will adjust transmission power and output simultaneous signals. Also, the perceived device's density function approaches to a single pair device because a the lack of exponential back-off (Equation A.7).

$$\lim_{T_n \to 0} 1 - \frac{T_n}{T_N} = 1 \tag{A.7}$$

However the SNR and device distance function increase in complexity. The complexity requires the transmitters to be aware of power ranges that are functions of distances, estimated in the handshake protocal. Therefore, we can model the rate (bit/s) in

Equation A.8. Where SNR is the propagation function in relationship to the distance, D, of the transmitter and receiver.

$$R_{concurrent} \triangleq \sum B \cdot \log_2 (1 + SNR(D)) \tag{A.8}$$

Most back-off schemes act on sensed conflict using exponential delays schemes. We thus hypothesize that concurrent transmission rate is exponentially faster, as there is no probability of back off. The exponential function, $W(c)$, does not exists in concurrent equation A.8 compared to CSMA's rate equation A.4.

A.4 The Multiuser Channel Model

The objective the combined ZigBee and WiFi signal is for multiple users to jointly use channel simultaneously while using differing modulations. Because of the differing modulations, the different signals do interfere with each other. Moreover, system and channel noise also create interference for the receivers. To theoretically analyze the performance of this shared frame, we must formulate the signal to interference plus noise ratio (SINR).

Because the joint signal was created based on a minimization optimization problem, the SINR analysis provides the amount of interference introduce. We define SINR in Equation A.9. We define SINR with respective to the BLE and WiFi receivers.

$$\frac{P}{I + N} \tag{A.9}$$

.

We define P as power and I as the interference in respect to the receiver and N is the channel added to the transmitter's and receiver's systems noise factors. For

the ZigBee receiver example, the P is the power of the ZigBee signal embedded in the WiFi signal and I is the WiFi signal. In the WiFi receiver context, the opposite is true, where P is the power WiFi signal and I is the added ZigBee signal.

Due to the optimization method of combing the signals, each combination of different symbols produces different SINR. Normally, P, I, and N are expressed in terms of power, defined in terms of Voltage V^2 and a resistance constant. We express the P and I terms in the amount of correlation to the intended signal without the constant r.

Let c (Equation A.10) be the correlation of the BLE and WiFi modulation signal $K(t)$ and the unmodified signal $S(t)$. This unmodified signal is original BLE or WiFi signal. Let w be the correlation between the unmodified ZigBee or WiFi signal to itself. The length is signal is a symbol.

$$c = \sum K^*(t) * S(t) \tag{A.10}$$

$$w = \sum S^*(t) * S(t) \tag{A.11}$$

We therefore can define SINR in equation A.12.

$$\frac{c}{(w - c) + N} \tag{A.12}$$

Bibliography

2009. Ieee standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (wpans) amendment 3: Alternative physical layer extension to support the japanese 950 mhz bands. IEEE Std 802.15.4d-2009 (Amendment to IEEE Std 802.15.4-2006) c1–27.

https://en.wikipedia.org/wiki/IEEE_802.11n-2009.

Adib; Fadel, K.; Zach, K.; Dina, M.; and C, R. 2014. 3d tracking via body radio reflections. NSDI.

Adib, K. 2013. See through walls with wi-fi! SIGCOMM.

Adib, Kabelac, K. 2015. Multi-person localization via rf body reflections. NSDI.

Ali, K.; Liu, A. X.; Wang, W.; and Shahzad, M. Keystroke recognition using wifi signals. In MobiCom, 2015.

Baggio, A., and Langendoen, K. 2008. Monte carlo localization for mobile wireless sensor networks. MSN 6(5):718–733.

Bharadia, D.; Joshi, K. R.; Kotaru, M.; and Katti, S. 2015. Backfi: High throughput wifi backscatter. SIGCOMM Comput. Commun. Rev. 45(4):283–296.

Bocca, M.; Kaltiokallio, O.; Patwari, N.; and Venkatasubramanian, S. 2014. Multiple target tracking with rf sensor networks. TMC 13(8):1787–1800.

Brown. 1911. The intrinsic factors in the act of progression in the mammal. PRSLBS.

Cai, L.; Machiraju, S.; and Chen, H. 2009. Defending against sensor-sniffing attacks on mobile phones. In Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds, 31–36. ACM.

Chang, H.-l.; Tian, J.-b.; Lai, T.-T.; Chu, H.-H.; and Huang, P. 2008. Spinning beacons for precise indoor localization. In SenSys.

Chebrolu, K., and Dhekne, A. Esense: Communication through energy sensing. In MobiCom, 2009.

Chen, Y.-C.; Chiang, J.-R.; Chu, H.-h.; Huang, P.; and Tsui, A. W. 2005. Sensor-assisted wi-fi indoor location system for adapting to environmental dynamics. In MSWiM, 118–125. ACM.

Chen, Y.; Lymberopoulos, D.; Liu, J.; and Priyantha, B. 2013. Indoor localization using fm signals. TMC 12(8):1502–1517.

Chen, Yenamandra, S. 2015. Tracking keystrokes using wireless signals. MobiSys.

Chi, Z.; Li, Y.; Sun, H.; Yao, Y.; Lu, Z.; and Zhu, T. B2w2: N-way parallel communication for iot devices. In Sensys, 2016.

Chi, Z.; Yao, Y.; Xie, T.; Huang, Z.; Hammond, M.; and Zhu, T. Harmony: Exploiting coarse-grained received signal strength from iot devices for human activity recognition. In ICNP, 2016.

Chi, Z.; Huang, Z.; Yao, Y.; Xie, T.; Sun, H.; and Zhu, T. 2017a. Emf: Embedding multiple flows of information in existing traffic for concurrent communication among heterogeneous iot devices. In IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, 1–9.

Chi, Z.; Li, Y.; Yao, Y.; and Zhu, T. 2017b. Pmc: Parallel multi-protocol communication to heterogeneous iot radios within a single wifi channel. In Network Protocols (ICNP), 2017 IEEE 25th International Conference on, 1–10. IEEE.

Chintalapudi, K.; Radunovic, B.; Balan, V.; Buettener, M.; Yerramalli, S.; Navda, V.; and Ramjee, R. Wifi-nc: Wifi over narrow channels. In NSDI, 2012.

Cohn Gabe Morris, Daniel Patel. Shwetak Tan, D. 2012. Humantenna: Using the body as an antenna for real-time whole-body interaction. CHI.

Das, S. M.; Koutsonikolas, D.; Hu, Y. C.; and Peroulis, D. Characterizing multi-way interference in wireless mesh networks. In WiNTECH, 2016.

Dawson-Haggerty, S.; Krioukov, A.; Taneja, J.; Karandikar, S.; Fierro, G.; Kitaev, N.; and Culler, D. E. 2013. Boss: Building operating system services. In NSDI, volume 13, 443–458.

Deek, L.; Garcia-Villegas, E.; Belding, E.; Lee, S.-J.; and Almeroth, K. The impact of channel bonding on 802.11n network management. In CoNEXT, 2011.

Dementyev, A.; Hodges, S.; Taylor, S.; and Smith, J. 2013. Power consumption analysis of bluetooth low energy, zigbee and ant sensor nodes in a cyclic sleep scenario. In Wireless Symposium (IWS), 2013 IEEE International, 1–4. IEEE.

Galstyan, A.; Krishnamachari, B.; Lerman, K.; and Pattem, S. 2004. Distributed online localization in sensor networks using a moving target. In IPSN.

Gjengset, J.; Xiong, J.; McPhillips, G.; and Jamieson, K. Phaser: Enabling phased array signal processing on commodity wifi access points. In MobiCom 2014.

Gu, Y.; Zhu, T.; and He, T. 2009. Esc: Energy synchronized communication in sustainable sensor networks. In 2009 17th IEEE International Conference on Network Protocols, 52–62.

Guha, S.; Plarre, K.; Lissner, D.; Mitra, S.; Krishna, B.; Dutta, P.; and Kumar, S. 2012. Autowitness: locating and tracking stolen property while tolerating gps and radio outages. TOSN 8(4):31.

Gummadi, R.; Wetherall, D.; Greenstein, B.; and Seshan, S. Understanding and mitigating the impact of rf interference on 802.11 networks. In SIGCOMM, 2007.

Guo, S.; Kim, S. M.; Zhu, T.; Gu, Y.; and He, T. 2011. Correlated flooding in low-duty-cycle wireless sensor networks. In 2011 19th IEEE International Conference on Network Protocols, 383–392.

Guo, X.; Zheng, X.; and He, Y. 2017. Wizig: Cross-technology energy communication over a noisy channel. In IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, 1–9.

He, T.; Huang, C.; Blum, B. M.; Stankovic, J. A.; and Abdelzaher, T. 2003. Range-free localization schemes for large scale sensor networks. In MobiCom.

Hnat; Timothy W, Griffiths, E.; Dawson; and Ray, Whitehouse, K. 2012. Doorjamb: unobtrusive room-level tracking of people in homes using doorway sensors. SenSys 309–322.

Hsu, J.; Mohan, P.; Jiang, X.; Ortiz, J.; Shankar, S.; Dawson-Haggerty, S.; and

Culler, D. 2010. Hbci: human-building-computer interaction. In BuildSys, 55–60. ACM.

Iyer, V.; Talla, V.; Kellogg, B.; Gollakota, S.; and Smith, J. 2016. Inter-technology backscatter: Towards internet connectivity for implanted devices. In Proceedings of the 2016 Conference on ACM SIGCOMM 2016 Conference, SIGCOMM '16, 356–369. New York, NY, USA: ACM.

Jayakumar, H.; Lee, K.; Lee, W. S.; Raha, A.; Kim, Y.; and Raghunathan, V. 2014. Powering the internet of things. In ISLPED.

Jiang, W.; Yin, Z.; Kim, S. M.; and He, T. 2017. Transparent cross-technology communication over data traffic. In IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, 1–9.

Kaltiokallio, Yigitler, J. 2014. Non-invasive respiration rate monitoring using a single cots tx-rx pair. IPSN.

Kaye, J. A.; Maxwell, S. A.; Mattek, N.; Hayes, T. L.; Dodge, H.; Pavel, M.; Jimison, H. B.; Wild, K.; Boise, L.; and Zitzelberger, T. A. 2011. Intelligent systems for assessing aging changes: home-based, unobtrusive, and continuous assessment of aging. The Journals of Gerontology Series B: Psychological Sciences and Social Sciences.

Kellogg, B.; Parks, A.; Gollakota, S.; Smith, J. R.; and Wetherall, D. 2014. Wi-fi backscatter: Internet connectivity for rf-powered devices. In Proceedings of the 2014 ACM Conference on SIGCOMM, SIGCOMM '14, 607–618. New York, NY, USA: ACM.

Kellogg, B.; Talla, V.; Gollakota, S.; and Smith, J. R. 2016. Passive wi-fi: Bringing low power to wi-fi transmissions. In 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), 151–164. Santa Clara, CA: USENIX Association.

Khan, M.; Bhartia, A.; Qiu, L.; and Lin, K. C.-J. Smart retransmission and rate adaptation in wifi. In ICNP, 2015.

Kim, S. M., and He, T. Freebee: Cross-technology communication via free side-channel. In MobiCom 2015.

Kim, Y., and Ling, H. Human activity classification based on micro-doppler signatures using a support vector machine. In IEEE TGRS, 2009.

Kotaru, M.; Joshi, K.; Bharadia, D.; and Katti, S. 2015. Spoton: Indoor localization using commercial off-the-shelf wifi nics. IPSN.

Kumar, S.; Cifuentes, D.; Gollakota, S.; and Katabi, D. Bringing cross-layer mimo to today's wireless lans. In SIGCOMM, 2013.

Larsen. 2012. Lost that skip in your step? gait is linked to cognitive decline and alzheimer's.

Lee, O.; Sun, W.; Kim, J.; Lee, H.; Ryu, B.; Lee, J.; and Choi, S. Chaser: Channel-aware symbol error reduction for high-performance wifi systems in dynamic channel environment. In INFOCOM, 2015.

Leung-Yan-Cheong, H. 1978. The gaussian wire-tap channel. IEEE Transactions on Information Theory 24:451–456.

Li, Z., and He, T. 2017. Webee: Physical-layer cross-technology communication via emulation. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking, MobiCom '17, 2–14. New York, NY, USA: ACM.

Li, Y.; Chi, Z.; Liu, X.; and Zhu, T. 2018. Chiron: Concurrent high throughput communication for iot devices. In Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services, 204–216. ACM.

Liu, V.; Parks, A.; Talla, V.; Gollakota, S.; Wetherall, D.; and Smith, J. R. Ambient backscatter: Wireless communication out of thin air. In SIGCOMM 2013.

Liu, K.; Chen, C.; Jafari, R.; and Kehtarnavaz, N. 2014. Multi-hmm classification for hand gesture recognition using two differing modality sensors. In DCAS, 1–4.

Liu, V.; Talla, V.; and Gollakota, S. Enabling instantaneous feedback with full-duplex backscatter. In MobiCom 2014.

Liu, C.; Wu, K.; and He, T. 2004. Sensor localization with ring overlapping based on comparison of received signal strength indicator. In MASS, 516–518. IEEE.

Luong, A.; Madsen, S.; Empey, M.; and Patwari, N. 2015. Rubreathing: non-contact real time respiratory rate monitoring system. In IPSN.

Lymberopoulos, D.; Liu, J.; Yang, X.; Choudhury, R. R.; Handziski, V.; and Sen, S. 2015. A realistic evaluation and comparison of indoor location technologies: experiences and lessons learned. In IPSN.

Lyonnet, Ioana, A. 2010. Human gait classification using microdoppler time-frequency signal representations. IIRF.

Malvankar, A.; Yu, M.; and Zhu, T. 2006. An availability-based link qos routing for mobile ad hoc networks. In 2006 IEEE Sarnoff Symposium, 1–4.

Merz, R.; Widmer, J.; Le Boudec, J.-Y.; and Radunovic, B. 2004. A Joint PHY/MAC Architecture for Low-Radiated Power TH-UWB Wireless Ad Hoc Networks. Technical report.

Nandagopal, T.; Kim, T.-E.; Gao, X.; and Bharghavan, V. Achieving mac layer fairness in wireless packet networks. In MobiCom, 2010.

Oppermann, F. J.; Boano, C. A.; and Römer, K. 2014. A decade of wireless sensing applications: Survey and taxonomy. In The Art of Wireless Sensor Networks. Springer. 11–50.

Panchal, J. S.; Yates, R. D.; and Buddhikot, M. M. 2013. Mobile network resource sharing options: Performance comparisons. IEEE Transactions on Wireless Communications 12(9):4470–4482.

Park, T.; Lee, J.; Hwang, I.; Yoo, C.; Nachman, L.; and Song, J. 2011. E-gesture: a collaborative architecture for energy-efficient gesture recognition with hand-worn sensor and mobile devices. In SenSys.

Parks, A. N.; Liu, A.; Gollakota, S.; and Smith, J. R. Turbocharging ambient backscatter communication. In SIGCOMM2014.

Parnandi, A.; Le, K.; Vaghela, P.; Kolli, A.; Dantu, K.; Poduri, S.; and Sukhatme, G. S. 2010. Coarse in-building localization with smartphones. In MobiCASE. Springer. 343–354.

Patwari, N.; Hero III, A. O.; Perkins, M.; Correal, N. S.; and O'dea, R. J. 2003. Relative location estimation in wireless sensor networks. ITSP 51(8):2137.

Prasad, N.; Arslan, M.; and Rangarajan, S. Enhanced interference management in heterogeneous cellular networks. In ISIT, 2014.

Premnath, S. N.; Wasden, D.; Kasera, S. K.; Farhang-Boroujeny, B.; and Patwari, N. Beyond ofdm: Best-effort dynamic spectrum access using filterbank multicarrier. In COMSNETS, 2012.

Pu, Q.; Gupta, S.; Gollakota, S.; and Patel, S. Whole-home gesture recognition using wireless signals. In MobiCom, 2013.

Pu; Qifan, G.; Sidhant, G.; Shyamnath, P.; and Shwetak. 2013. Whole-home gesture recognition using wireless signals. MobiCom.

Ranjan; Juhi, Y.; and Yu, Whitehouse, K. 2013. An rf doormat for tracking people's room locations. UbiComp.

Sahai, A.; Aggarwal, V.; Yuksel, M.; and Sabharwal, A. 2013. Capacity of all nine models of channel output feedback for the two-user interference channel. IEEE Transactions on Information Theory 59(11):6957–6979.

Salimi, S.; Jorswieck, E. A.; Skoglund, M.; and Papadimitratos, P. Key agreement over an interference channel with noiseless feedback: Achievable region distributed allocation. In CNS, 2015.

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

Sen, S.; Choudhury, R. R.; and Nelakuditi, S. 2012. Csma/cn: Carrier sense multiple access with collision notification. IEEE/ACM Trans. Netw. 20(2):544–556.

Shi, J.; Aryafar, E.; Salonidis, T.; and Knightly, E. W. Synchronized csma contention: Model, implementation and evaluation. In INFOCOM, 2009.

Shu; Yuanchao, S.; Kang G, H.; Tian, C.; and Jiming. 2015. Last-mile navigation using smartphones. MobiCom.

Singh, N.; Gunawardena, D.; Proutiere, A.; Radunovi, B.; Balan, H. V.; and Key, P. Efficient and fair mac for wireless networks with self-interference cancellation. In WiOpt, 2011.

Srinivasan; Maria A. Kazandjieva, Jain, E. K.; and Levis, P. 2008. Swat: enabling wireless network measurements. In SenSys. ACM.

Sun, L.; Sen, S.; Koutsonikolas, D.; and Kim, K.-H. 2015. Widraw: Enabling hands-free drawing in the air on commodity wifi devices. MobiCom.

Sun, L.; Sen, S.; and Koutsonikolas, D. Bringing mobility-awareness to wlans using phy layer information. In CoNEXT, 2014.

Talla, V.; Hessar, M.; Kellogg, B.; Najafi, A.; Smith, J. R.; and Gollakota, S. 2017. Lora backscatter: Enabling the vision of ubiquitous connectivity. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 1(3):105:1–105:24.

Tan, K.; Shen, H.; Zhang, J.; and Zhang, Y. Enable flexible spectrum access with spectrum virtualization. In DySpan, 2012.

http://www.memsic.com/userfiles/files/DataSheets/WSN/telosb_datasheet.pdf.

Ting Zhu, Y. L. 2016. Gait-based wi-fi signatures for privacy-preserving. ASIACCS.

Varshney, A.; Voigt, T.; and Mottola, L. 2013. Directional transmissions and receptions for high throughput burst forwarding. In SenSys.

Wagner, S.; Handte, M.; Zuniga, M.; and Marrón, P. J. 2012. On optimal tag placement for indoor localization. In PerCom, 162–170. IEEE.

Wang, W.; Liu, A. X.; Shahzad, M.; Ling, K.; and Lu, S. Understanding and modeling of wifi signal based human activity recognition. In MobiCom, 2015.

Wang, W.; Liu, A. X.; Shahzad, M.; Ling, K.; and Lu, S. 2015. Understanding and modeling of wifi signal based human activity recognition. MobiCom.

Wei Wang, Tiantian Xie, X. L., and Zhu., T. 2017. Ect: Exploiting cross-technology concurrent transmission for reducing packet delivery delay in iot networks. In Network Protocols (ICNP), 2017 IEEE 25th International Conference on. IEEE.

Wei, Z. 2015. mtrack: High-precision passive tracking using millimeter wave radios. MobiCom.

Wenchao Jiang, Roufeng Liu, Zhimeng Yin, Song Min Kim and T. He. 2017. Bluebee: a 10,000x faster cross-technology communication. In SenSys.

Xiao, Z.; Wen, H.; Markham, A.; Trigoni, N.; Blunsom, P.; and Frolik, J. 2015. Non-line-of-sight identification and mitigation using received signal strength. TWC 14(3):1689–1702.

Xiong, J., and Jamieson, K. Arraytrack: A fine-grained indoor location system. In NSDI 2013.

Xiong, Sundaresan, J. 2015. Tonetrack: Leveraging frequency-agile radios for time-based indoor wireless localizatio. MobiCom.

Yan Li, T. Z. Using wi-fi signals to characterize human gait for identification and activity monitoring. In Chase 2016.

Yan Li, Zicheng Chi, X. L. T. Z. Passive-zigbee: Enabling zigbee communication in iot networks with 1000x+ less power consumption. In Sensys 2018.

Yang, L.; Lin, Q.; Li, X.; Liu, T.; and Liu, Y. 2015. See through walls with cots rfid system! MobiCom.

Yedavalli, K., and Krishnamachari, B. 2008. Sequence-based localization in wireless sensor networks. TMC 7(1):81–94.

Yin, Z.; Jiang, W.; Kim, S. M.; and He, T. 2017. C-morse: Cross-technology communication with transparent morse coding. In IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, 1–9.

Yun, S.; Kim, D.; and Qiu, L. Fine-grained spectrum adaptation in wifi networks. In MobiCom, 2013.

Yun, Chen, Q. 2015. Turning a mobile device into a mouse in the air. Mobisys.

Z. Chi, Y. Li, Y. Yao, and T. Zhu. 2017. PMC: Parallel Multi-protocol Communication to Heterogeneous IoT Radios within a Single WiFi Channel. In ICNP.

Z. Chi, Z. Huang, Y. Yao, T. Xie, H. Sun, and T. Zhu. 2016. EMF: Embedding Multiple Flows of Information in Existing Traffic for Concurrent Communication among Heterogeneous IoT Devices. In INFOCOM.

Z. Li and T. He. 2017. Webee: Physical-layer cross-technology communication via emulation. In MobiCom.

Zhang, Y., and Li, Q. Howies: A holistic approach to zigbee assisted wifi energy savings in mobile devices. In INFOCOM, 2013.

Zhang, X., and Shin, K. G. Gap sense: Lightweight coordination of heterogeneous wireless devices. In INFOCOM, 2013.

Zhang, J.; Shen, H.; Tan, K.; Chandra, R.; Zhang, Y.; and Zhang, Q. Frame retransmissions considered harmful: Improving spectrum efficiency using micro-acks. In MobiCom, 2012.

Zhang, Q.; Xu, W.; Huang, Z.; Zhou, Z.; Yi, P.; Zhu, T.; and Xiao, S. Context-centric target localization with optimal anchor deployments. In ICNP, 2015.

Zhang, P.; Bharadia, D.; Joshi, K.; and Katti, S. 2016a. Hitchhike: Practical backscatter using commodity wifi. In Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM, SenSys '16, 259–271. New York, NY, USA: ACM.

ZHANG, P.; Rostami, M.; Hu, P.; and Ganesan, D. 2016b. Enabling practical backscatter communication for on-body sensors. In Proceedings of the 2016 ACM SIGCOMM Conference, SIGCOMM '16, 370–383. New York, NY, USA: ACM.

Zhang, P.; Josephson, C.; Bharadia, D.; and Katti, S. 2017. Freerider: Backscatter communication using commodity radios. In Proceedings of the 13th International Conference on Emerging Networking EXperiments and Technologies, CoNEXT '17, 389–401. New York, NY, USA: ACM.

Zhao, X.; Xiao, Z.; Markham, A.; Trigoni, N.; and Ren, Y. 2014. Does btle measure up against wifi? a comparison of indoor location performance. In EW, 1–6. VDE.

Zhou, C., and Zhu, T. 2007. Highly spatial reusable mac for wireless sensor networks. In IEEE WiCOM.

Zhou, C., and Zhu, T. 2008a. A spatial reusable mac protocol for stable wireless sensor networks. In IEEE WiCOM.

Zhou, C., and Zhu, T. 2008b. Thorough analysis of mac protocols in wireless sensor networks. In IEEE WiCOM.

Zhu, T., and Towsley, D. 2011. E2r: Energy efficient routing for multi-hop green wireless networks. In 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 265–270.

Zhu, T., and Yu, M. 2006a. A dynamic secure qos routing protocol for wireless ad hoc networks. In 2006 IEEE Sarnoff Symposium, 1–4.

Zhu, T., and Yu, M. 2006b. Nis02-4: A secure quality of service routing protocol for wireless ad hoc networks. In IEEE Globecom 2006, 1–6.

Zhu, T.; Zhong, Z.; He, T.; and Zhang, Z.-L. 2010. Exploring link correlation for efficient flooding in wireless sensor networks. In Proceedings of the 7th USENIX Conference on Networked Systems Design and Implementation, NSDI'10, 4–4. Berkeley, CA, USA: USENIX Association.

Zhu, T.; Zhong, Z.; He, T.; and Zhang, Z. L. 2013. Achieving efficient flooding by utilizing link correlation in wireless sensor networks. IEEE/ACM Transactions on Networking 21(1):121–134.

Zhu, Y.; Zhu, Y.; Zhao, B. Y.; and Zheng, H. 2015. Reusing 60ghz radios for mobile radar imaging. MobiCom.

http://www.zigbee.org/zigbee-for-developers/applicationstandards/zigbee-health-care/.