# ZigFi: Harnessing Channel State Information for Cross-Technology Communication

Xiuzhen Guo, *Student Member, IEEE,* Yuan He*, *Member, IEEE,* Xiaolong Zheng, *Member, IEEE,* Liangcheng Yu, *Student Member, IEEE,* and Omprakash Gnawali, *Member, IEEE*

***Abstract*—Cross-technology communication (CTC) is a technique that enables direct communication among different wireless technologies. Recent works in this area have made substantial progress, but CTC from ZigBee to WiFi remains an open problem. In this paper, we propose ZigFi, a novel CTC framework that enables communication from ZigBee to WiFi. ZigFi carefully overlaps ZigBee packets with WiFi packets. Through experiments we show that Channel State Information (CSI) of the overlapped packets can be used to convey data from ZigBee to WiFi. Based on this finding, we propose a receiver-initiated protocol and translate the decoding problem into a problem of CSI classification with Support Vector Machine. We further build a generic model through experiments, which describes the relationship between the Signal to Interference and Noise Ratio (SINR) and the symbol error rate (SER). Moreover, we extend ZigFi to multiple-to-one concurrent transmissions. We implement ZigFi on commercial-off-the-shelf WiFi and ZigBee devices. We evaluate the performance of ZigFi under different experimental settings. The results demonstrate that ZigFi achieves a throughput of 215.9bps, which is 18X faster than the state of the arts.**

***Index Terms*—Cross-technology, ZigBee to WiFi, Channel State Information**

## I. Introduction

Large-scale deployments of Internet of Things (IoT) have led to not only crowding of wireless spectrum but also heterogeneity in wireless technologies in devices and networks that are expected to work together [1], [2], [3]. Devices that use different wireless technologies (e.g. WiFi, ZigBee, and Bluetooth) have to share the unlicensed spectrum (e.g. ISM bands) when they coexist in the common space. Traditional approaches to manage this crowding and heterogeneity try to avoid, mitigate, or tolerate the wireless interference, and use multi-radio gateways. Whereas cross-technology communication (CTC) opens a new direction of direct communication among different wireless technologies [4] [5]. CTC avoids the unnecessary hardware cost and communication delay, compared to the indirect solution based on a multi-radio gateway [6]. Moreover, it becomes easier to coordinate heterogeneous wireless devices in a shared channel [7]. CTC is also an enabling technology for emerging IoT applications (e.g. industrial surveillance and smart home), where seamless data collection and interoperation are desired [8] [9] [10].

There has been some progress in CTC research. FreeBee [5] enables CTC by embedding symbols into beacons and shifting the beacon timings. Esense [11] applies energy sampling to realize data transmission from WiFi to ZigBee. WiZig [12] employs amplitude modulation and temporal modulation to optimize the throughput from WiFi to ZigBee over a noisy channel. $B^2W^2$ [13] designs the discrete amplitude and frequency shift keying (DAFSK) converter to convert the data stream from the upper layer of the BLE device into CTC symbols. By leveraging Channel State Information (CSI), the CTC symbols can be transmitted from BLE to WiFi.

Despite this progress, there is relatively little progress in CTC from ZigBee to WiFi. This problem is extremely challenging due to several asymmetries between the two technologies. First, there is a large difference in Tx power of ZigBee vs. WiFi. The maximum Tx power of WiFi is 100dBm, while the maximum Tx power of ZigBee is 0dBm. Second, the bandwidths of ZigBee and WiFi channels have a large difference. The channel bandwidth of WiFi is 20MHz, which is 10x of that of ZigBee (2MHz). The asymmetry in channel bandwidth also leads to apparent disharmony with regard to the encoding and decoding rates. As a result, from the view of a WiFi receiver, the ZigBee signals appear to be weak and susceptible to the noise. Simply increasing the Tx power of ZigBee will induce too much interference, not to mention the prohibitively high power consumption.

In this paper, we propose ZigFi, a receiver-initiated protocol for CTC from ZigBee to WiFi. The basic idea is to carefully piggy-back ZigBee packets over WiFi packets. By tracking the PHY-layer features of the received packets, a WiFi receiver is able to decode not only the WiFi packets sent by the WiFi sender, but also the data sent by the ZigBee sender. By using a machine learning approach for decoding, ZigFi can efficiently convey data from ZigBee to WiFi, even in noisy environments. The main contributions of this work are summarized as follows.

- We experimentally study how ZigBee and WiFi packets transmissions interact with each other from both transmitter and receiver perspective. We find that it is feasible to use Channel State Information (CSI) of the overlapped packets to convey data from ZigBee to WiFi. Based on this finding, we propose ZigFi, a framework that

Xiuzhen Guo, Yuan He are with the School of Software and BNRist, Tsinghua University, P.R. China. Xiaolong Zheng is from School of Computer Science, Beijing University of Posts and Telecommunications, P.R. China. Liangcheng Yu is from University of Pennsylvania, USA. Omprakash Gnawali is from University of Houston, USA.

E-mail: guoxz16@mails.tsinghua.edu.cn,
heyuan@mail.tsinghua.edu.cn,
zhengxiaolong@bupt.edu.cn,
liangcheng.yu46@gmail.com,
gnawali@cs.uh.edu

*Yuan He is the corresponding author.

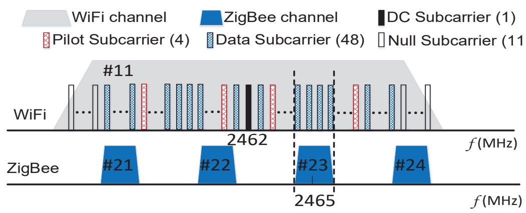



Fig. 1. The distribution of a WiFi channel and ZigBee channels

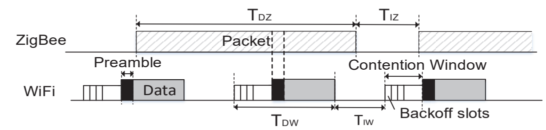
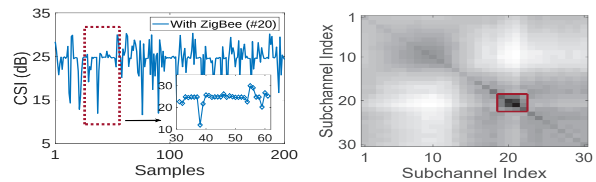



Fig. 2. Illustration of overlapping ZigBee and WiFi packets




(a) With ZigBee packets, subchannel=20

(b) Covariance between subchannels (darker is higher correlation)

Fig. 3. The CSI sequences with ZigBee packets of different subchannels

translates the decoding problem into a problem of CSI classification with Support Vector Machine (SVM).

- We design a receiver-initiated protocol for practical application of ZigFi. Using this protocol, a WiFi receiver can coordinate the communication settings (e.g. packet length and Tx power) with both the ZigBee sender and the WiFi sender. In this way, ZigFi achieves efficient and robust CTC even in noisy environments, minimizing the impact to ongoing WiFi transmissions.
- We implement and evaluate ZigFi on commercial WiFi devices and ZigBee motes. The results demonstrate that ZigFi achieves a throughput of 215.9bps, which is 18X faster than the state of the arts.

The rest of this paper is organized as follows. Section II discusses the related work. In Section III, we verify the feasibility and challenges of ZigFi. Section IV presents the design of ZigFi. In Section VI, we evaluate the performance of ZigFi. We conclude this work in Section VIII.

## II. Related Work

### A. Feasibility of ZigBee to WiFi CTC using CSI

**Collision avoidance and interference management.** These approaches propose to separate competing devices in the temporal [14] or the frequency domain [15]. WISE [16] enhances ZigBee throughput by harnessing the white spaces between WiFi transmissions. ZIMO [4] proposes a MIMO design for harmony coexistence of ZigBee and WiFi networks with the goal of protecting ZigBee data packets. ZiFi [17] utilizes low power ZigBee radio to detect the existence of WiFi hotspots, so that the standby energy consumption of WiFi devices can be significantly reduced. ZiSense [18] and Smoggy-Link [19] identify RSSI signatures of different wireless technology.

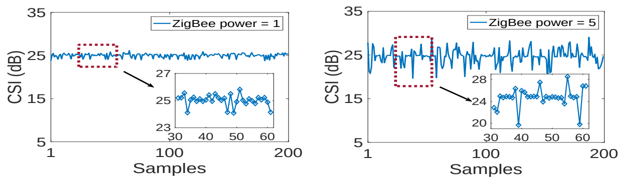
**Cross-technology Communication.** Packet-level CTC encodes data in either the temporal or the amplitude dimension. In the temporal dimension, FreeBee [5] embeds symbols into beacons by shifting their transmission timings. However, the throughput of FreeBee is bounded by the limited beacon frequency. DCTC [20] employs a similar technique with FreeBee while taking the application-layer data packets as targets to be shifted, which therefore has a similar limitation.

Esense [11] uses the power at which the packet is transmitted to encode data bits. HoWiEs [21] improves the Esense mechanism by modulating the packet length of WiFi. Gap Sense [22] leverages WiFi preamble to construct special energy pulses. The gap between the energy pulses is used to convey data. WiZig [12] employs modulation in both the amplitude and the temporal dimensions to optimize the throughput from WiFi to ZigBee. $B^2W^2$ [13] builds a CTC channel from BLE to WiFi by leveraging the CSI. C-Morse [23] uses the combination of the short ZigBee packets and the long ZigBee packets to construct the recognizable energy patterns at the WiFi receiver. EMF [9] modulates CTC symbols by shifting the packet order, which can form different packet occupancy ratios, to convey CTC messages.

Recent works propose physical-level CTC [24], [25]. WEBee [26] enables WiFi to ZigBee CTC by utilizing WiFi payload to emulate a ZigBee packet at the physical-layer. WEBee significantly improves the CTC throughput from WiFi to ZigBee. TwinBee [27] and LongBee [28] improve the performance of WEBee. BlueBee [29] modifies the payload of BLE to emulate the signal of ZigBee. XBee [30] realizes CTC from ZigBee to BLE based on cross-demapping.

## III. Observations

First, the overlapping on the frequency domain provides a theoretical support for using the CSI amplitude sequence (CSI mentioned later refers to the amplitude of the complex value) for CTC. The distribution of WiFi and ZigBee channels is shown in Fig. 1. A WiFi channel is divided into 64 different subcarriers and a ZigBee channel overlaps with several WiFi subcarriers. Second, CSI is generally used by WiFi to measure the channel status of each WiFi subcarrier [31] [32]. When the WiFi receiver receives a packet, it calculates the CSI values that include the phase deviation and amplitude variation caused by channel changes at the subcarrier level. ZigBee transmission results in constructive interference or destructive interference. When there is constructive interference, the strength of WiFi signal and the corresponding CSI amplitude increase. Conversely, the strength of WiFi signal and the corresponding CSI amplitude decrease when there is destructive interference. As shown in Fig. 2, if there are ZigBee packets during the transmission of WiFi packets, the ZigBee transmission will interfere with the WiFi preamble. So the CSI sequence affected by ZigBee has a higher variance. We introduce covariance. The calculation of covariance of the CSI sequences in different




(a) ZigBee power=1 (b) ZigBee power=5 (c) ZigBee power=30

Fig. 4. The CSI sequences with ZigBee packets of different Tx powers

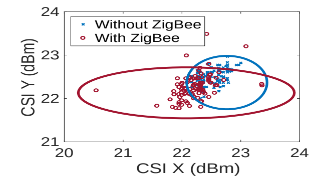



Fig. 5. The CSI pairs with/without ZigBee packets in two-dimension

subchannels is as follows. Given that $S_i$ and $S_j$ are two CSI sequences in subchannel $i$ and $j$, the covariance is

$$Cov(i,j) = \frac{\sum_{k=1}^{N} S_{ik} S_{jk}}{N} - \frac{\sum_{k=1}^{N} S_{ik}}{N} \frac{\sum_{k=1}^{N} S_{jk}}{N} \quad (1)$$

where $N$ is the number of points in each CSI sequence. It is noteworthy that when $i = j$, the covariance becomes the variance of a single subchannel.

### A. CSI sequence on different subchannels

We conduct experiments to observe the CSI sequences on different subchannels. The data rate of WiFi packet is 54Mbit/s with the modulation of 64QAM3/4. The WiFi sender to transmit 145-byte packets with 0.02ms on-air time on channel 11. The WiFi packet interval is 0.5ms. A TelosB node transmits 28-byte ZigBee packets on channel 23. The duration of a ZigBee packet is 0.9ms and the interval of ZigBee packets is 0.192ms. The distance between the WiFi transmitter and the WiFi receiver is 10m. The distance between the WiFi sender and the ZigBee transmitter is 7m, which is equal to the distance between the WiFi receiver and the ZigBee transmitter. The Tx power of ZigBee is power level 13 (-9dBm), which makes the variation of the CSI sequence distinctive and doesn't cause the CSMA of WiFi. The CSI sampling rate of WiFi is 2KHz. As shown in Fig. 3(a), the CSI sequence of subchannel 20 has a larger variation range when there are ZigBee packets. As shown in Fig. 3(b), the subchannels 19-22 have the largest variance over all subchannels. The center frequency of subchannel 20 is nearly equal to the ZigBee. So the CSI sequence of subchannel 20 is mostly distinctive from other subchannels.

### B. CSI sequences with different ZigBee packet lengths

We transmit long enough ZigBee packets to guarantee that one ZigBee packet overlaps with at least one WiFi packet preamble. Specifically, as shown in Fig. 2, the length of the ZigBee packet must satisfy:

$$T_{DZ} \geq T_{DW} + T_{IW} \quad (2)$$

where $T_{DZ}$ is the transmission time of the ZigBee packet. $T_{DW}$ and $T_{IW}$ are the transmission time of the WiFi packet and the transmission interval between two adjacent WiFi packets.

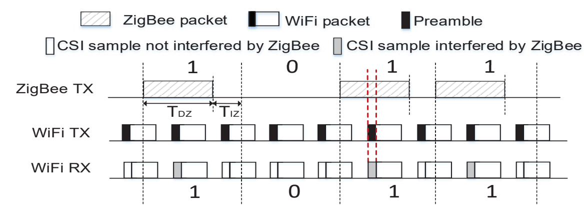



Fig. 6. The basic communication scheme of ZigFi

### C. CSI sequences with different ZigBee Tx power

We redo the experiment on channel 23 with ZigBee Tx power at levels 1, 5, and 30 (corresponding powers are -30dBm, -20dBm, and 0dBm), packet length at 28 bytes. As shown in Fig. 4(a), Fig. 4(b), and Fig. 4(c) respectively, as ZigBee power increases, the CSI sequence is more distinct. When ZigBee power is too high, the CSI sequence includes only a few peaks as shown in Fig. 4(c). This is because the WiFi sender can sense the interference from ZigBee transmission and backs off.

### D. On classifying CSI sequences

It is difficult to quantify the CSI variation because the channel is dynamic and noisy. As shown in the sub-figure of Fig. 3(a) or other figures, there are no simple rules to describe the variation of CSI values. We define a *CSI pair* as a pair of CSI values. The first value is interfered by ZigBee. The second value is obtained right after the first but is not necessarily interfered. We plot the CSI pairs obtained with and without ZigBee transmissions in two-dimension in Fig. 5. The two sets of CSI pair overlap with each other, making it difficult to identify the two cases (with and without ZigBee) with straightforward techniques (e.g. thresholding). As a result, we explore techiniques that help us classify these two different clusters at higher dimensional space.

**Summary:** First, frequency overlap is the prerequisite for CTC. In order to use the CSI sequence to enable ZigBee to WiFi CTC, some conditions need to be satisfied.

- The ZigBee packet must be large enough to make ZigBee packets overlap with WiFi packets in the time domain.
- We need to choose an appropriate ZigBee power to make the CSI sequence distinctive.

## IV. ZigFi Design

### A. Overview

ZigFi a novel CTC technique that enables communication from ZigBee to WiFi. Fig. 6 gives an overview of ZigFi: (1) In

TABLE I
FEATURES OF SVM

| | |
|---|---|
| $T_{var}$ | The variance of the CSI sequence within a window |
| $T_{range}$ | The difference between the maximum CSI and the minimum CSI within a window |
| $T_{min}$ | The minimum CSI within a window |
| $T_{mean}$ | The average value of CSI sequence within a window |
| $T_{max}$ | The maximum CSI within a window |
| $T_{mode}$ | The most frequently occurring CSI within a window |
| $F_1$ | The DC component of DFT within a window |
| $F_2$ | The first harmonic component of DFT within a window |
| $F_{var}$ | The variance of DFT within a window |
| $F_{min}$ | The minimum value of DFT within a window |
| $F_{mean}$ | The average value of DFT within a window |
| $F_{max}$ | The maximum value of DFT within a window |

our example, the ZigBee sender wants to send the bit sequence "1011" to the WiFi receiver. The ZigBee sender encodes "1"/"0" as the presence/absence of the ZigBee packet. Then the Zigbee sender transmits these packets or remains silent. (2) There is an existing WiFi sender transmitting packets. ZigBee packets overlap with WiFi packets in the air. (3) The WiFi receiver collects CSI sequences. SVM is used to classify the received CSI sequence as "0" or "1".

*1) The features extracted within a decoding window:* We set the window size is 10ms, which includes 20 CSI samples. We choose twelve features and conduct twelve groups of experiments. Each group has ten experiments. We increase the features of SVM classifier in order as Table I.

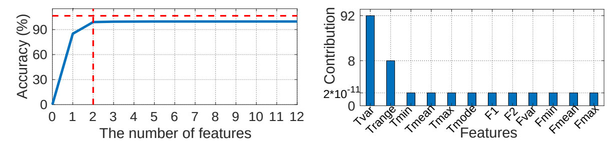
As shown in Fig. 7(a), the accuracy rate of SVM classifier can reach to 95%. The accuracy tends to be stable with the increase of the number of features. We analyze the variance contribution of each feature and the contribution rate result is shown in Fig. 7(b). The contribution rate of $T_{var}$ and $T_{range}$ have accumulated over 99%, which means that these two features are enough for SVM classifier.

In this way, we extract two features within a window. One is the variance of CSI values. The other is the difference between the maximum CSI and the minimum CSI.

## B. Decoding with a CSI classifier

*1) The window length of the SVM classifier:* We conduct several experiments to find the appropriate window length. The experiment result is shown in Fig. 8. We find that the accuracy of the SVM increases rapidly as we increase the window length. We suggest a window size of 4ms, which includes 8 CSI values. ZigFi achieves an accuracy above 0.9, as a good compromise between accuracy and data rate.

*2) Training the SVM classifier:* We conduct 120 experiments in four environments. We choose two different places, one is a 9m × 6m crowded office and another one is a 13m × 7m empty meeting room. We select the CSI sequences in these two places during the daytime and the night, respectively. In the daytime, there are twenty students in the office. These students can use WiFi to watch videos, surf the Internet, download files, and so on. There are five students in the meeting room. They are talking with each other and only surfing news site. Compared with the daytime environment, the office and the meeting room are relatively quiet at night.




(a) SVM accuracy with the increase of features (b) The contribution rate of twelve features

Fig. 7. Feature extraction of SVM

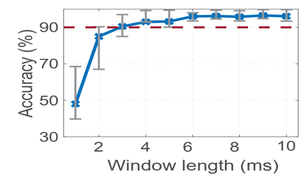



Fig. 8. The relationship between the accuracy and the window length

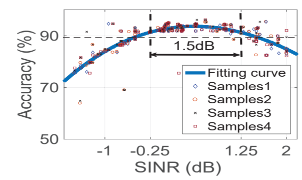



Fig. 9. The relationship between the accuracy and the SINR

As a result, these four environments are different in terms of background noise, multipath fading, human mobility, and interference. In each environment, we collect CSI sequences and label them as $-1$ or $+1$. A CSI sequence with only the WiFi transmission (not overlapped with ZigBee) is labeled $-1$. A CSI sequence with the overlapped transmissions from WiFi and ZigBee is labeled $+1$. Each experiment lasts for 30 seconds and the CSI sampling rate is 2KHz. The total CSI sequences are randomly divided into training and test datasets.

*3) The relationship between the Accuracy and the SINR:* We define a new metric SINR in ZigFi, which can be calculated by $SINR = 10lg\frac{S_Z}{I_W+N}$. Where $S_Z$ is the power of the received ZigBee packet, $I_W$ is the power of the received WiFi packet, and $N$ is the power of noise perceived by the WiFi receiver. In practice, it is difficult to quantify the CSI variation due to the channel dynamics. Thus we obtain an experimental model to describe the relationship between the SINR and the accuracy. We use the trained SVM to test the CSI sequences in the test dataset. Each CSI sequence corresponds to a SINR. Fig. 9 shows the test results and the polynomial fitting curve is $f(x) = p_1 * x^3 + p_2 * x^2 + p_3 * x + p_4$. Where $f(x)$ is the accuracy, $x$ is the SINR, and the coefficients are $p_1 = 0.2159, p_2 = -4.44, p_3 = 4.094, p_4 = 91.13$.

We find that with an increase in SINR, the CSI sequence becomes more distinct and the accuracy increases. But the accuracy decreases when the SINR exceeds a value, because too strong ZigBee transmission will make the WiFi sender back-off. Fig. 9 indicates that when the SINR is in the range $[-0.25, 1.25]$, the decoding accuracy is higher than 0.9.

Next, we analyze the energy cost on a ZigBee sender to participate in CTC using ZigFi. We assume that the energy cost of one ZigBee packet is $E_T$. there is a nonlinear relationship between $E_T$ and the Tx power $P_Z$, describe by $E_T = G(P_Z)$. Meanwhile, $S_Z$=$P_Z \times \eta$, where $\eta$ is the path loss factor and can be estimated online. We use $E$ to denote the expected energy cost on the ZigBee sender to send one ZigFi packet successfully. We have $E = \frac{E_T}{1-f(x)}$.

To minimize energy cost while achieving satisfactory decoding accuracy, we have:

$$\min\ E$$
$$s.t.\quad \begin{cases} E_T = G(P_Z) \\ th_l \le f(x) \le th_u, th_l = -0.25, th_u = 1.25 \\ f(x) = p_1 * x^3 + p_2 * x^2 + p_3 * x + p_4 \\ x = 10lg\frac{S_Z}{I_W+N} \\ S_Z = P_Z * \eta \end{cases} \tag{3}$$

The path loss can be measured by using the receiver-initiated mechanism, as described later. Solving the above equations yields the Tx power to be set at the ZigBee sender. SVM is used to decode the CTC symbols at the WiFi receiver. The method of SVM classification is general, however, the parameterization of the classifier needs to be updated in different environments. When ZigFi is implemented in a new environment, the SVM model needs to be retrained.

### C. The receiver-initiated mechanism

We design a receiver-initiated CTC mechanism to meet the following goals. First, the transmission of ZigFi relies on existing WiFi packet transmissions, so it is necessary to initiate or utilize packet transmissions between the WiFi sender and the WiFi receiver. Second, the Tx power of the ZigBee sender and the WiFi sender should be adjusted to achieve desired energy efficiency and decoding accuracy.

To send control information from the WiFi receiver to the ZigBee sender, multiple existing CTC techniques [12] [5] [11] can be used. We select the proposal in [12]. Specifically, the payload of a WiFi packet includes data from the WiFi receiver to the WiFi sender, while the packet-level modulation carries the data from the WiFi receiver to the ZigBee sender. The receiver-initiated mechanism is shown in Fig. 10. The specific process is as follows:

(1) The WiFi sender and the ZigBee sender listen to the channel. The following six parameters are determined by the WiFi receiver, before it sends the control packets: (a) the WiFi Tx power $P_W$, (b) the WiFi packet length $T_{DW}$, (c) the WiFi packet interval $T_{IW}$, (d) the ZigBee Tx power $P_Z$, (e) the ZigBee packet length $T_{DZ}$, and (f) the ZigBee packet interval $T_{IZ}$. These parameters have default values.

(2) The WiFi receiver conducts the channel estimation and detects whether there is an incoming WiFi packet. If there is an existing WiFi link, the ZigFi transmission will piggy-back on an existing WiFi packet transmissions. Specifically, the WiFi receiver sends the probe packets to the ZigBee sender. The length of the WiFi probe packet is longer than the sleeping period of the ZigBee sender. The ZigBee device listens to the channel and conducts CCA based on the RSSI. The ZigBee device adopts the scheme of RSSI fingerprinting [18] to detect the incoming WiFi packet. The ZigBee device extracts features of the received RSSI values (such as on-air time, average value, peak value, and peak to average ratio). When detecting the active WiFi sender based on the method of RSSI fingerprinting, the ZigBee device will wake up. Using this method, the ZigBee sender can efficiently identify the device that is transmitting. Accordingly, it can identify the right cases when the ZigFi communication should be initiated. The energy efficiency will be preserved in this way.

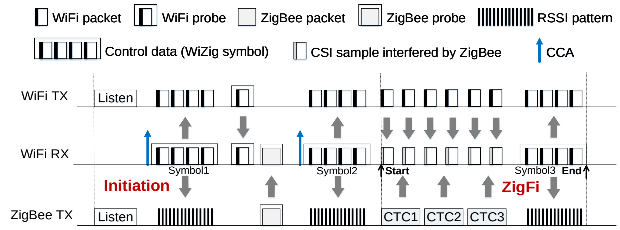



Fig. 10. The process of receiver-initiated mechanism

(3) If there is no incoming WiFi packet, the WiFi receiver needs to trigger the packet transmissions from both the WiFi sender and ZigBee sender by using *Symbol1*. On receiving the control packets, the WiFi sender and the ZigBee sender send a probe to the WiFi receiver, using the Tx powers specified in the control packets. For the WiFi sender, any normal packet is regarded as a probe. For the ZigBee sender, the probe is a sequence of ZigBee packets with specific length.

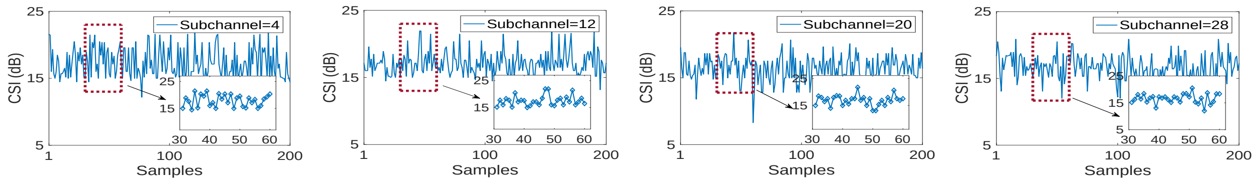
(4) On receiving the probes, the WiFi receiver updates the parameters related to the channel condition (e.g. the path loss). Then the WiFi receiver returns them to the WiFi sender and the ZigBee sender, denoted by *Symbol2*.

(5) On receiving *Symbol2*, the ZigFi transmission starts. Meanwhile, the WiFi receiver can send a control packet *Symbol3* to end the ZigFi transmission, when needed.

We analyze the duration of our receiver-initiated mechanism. *Symbol1*, *Symbol2*, and *Symbol3* are used to transmit control messages from the WiFi receiver to the WiFi sender and the ZigBee sender. These symbols leverage the energy of WiFi packets to transmit CTC messages from WiFi to ZigBee. For the WiFi to ZigBee CTC, the WiFi receiver can actively transmit packets with a fixed packet length. WiFi uses the absence/presence of WiFi packets to represent the control symbol 0/1 [12]. In order to achieve the synchronization between WiFi and ZigBee, a customized preamble, which includes four WiFi to ZigBee symbols {1,0,1,0}, is transmitted first. After detecting the preamble, the ZigBee device starts to decode the control message that follows the preamble. When the duration of a WiFi packet is 0.02ms and the WiFi packet interval is 0.5ms, one CTC bit from WiFi to ZigBe takes 0.52ms. The duration of *Symbol1* (*Symbol2*, *Symbol3*) including ten CTC bits is about 5.2ms. The WiFi/ZigBee probe is the WiFi/ZigBee packet. A ZigBee packet lasts 0.9ms and the interval of ZigBee packets is 0.192ms. After adding the transmission time of ZigFi which depends on the WiFi packet length and interval, our receiver-initiated mechanism needs about 20ms.

### D. The justification of the ZigFi overhead

We discuss the overhead of ZigFi and explain its justification. First, ZigFi relies on a WiFi link to obtain the CSI sequence. The overhead depends on the existence of WiFi traffic. If there are enough ongoing WiFi packets sent to the ZigFi receiver, transmission of these existing packets doesn't introduces new WiFi traffic but can provide CSI sequence for




(a) Subchannel=4 (b) Subchannel=12 (c) Subchannel=20 (d) Subchannel=28

Fig. 11. The CSI sequences of different subchannels when ZigBee transmits packets on channel 21, 22, 23, and 24 respectively

ZigFi. When there are no existing WiFi packets to the ZigFi receiver in the environment, we need to inject WiFi packets to build a ZigFi link. 2KHz is the highest CSI sample rate of the commercial device. And the highest transmission rate of WiFi packet is also 2K packet/s. In practice, it is not necessary for ZigFi to always use that highest rate. The ZigFi transmission is on demand. When the required CTC symbol rate of ZigFi is relatively small, we may reduce the transmission rate of WiFi packets. Therefore, the overhead of WiFi packet can be controlled.

Second, in order to guarantee that one ZigBee packet overlaps with at least one WiFi packet, the ZigBee packet length needs to satisfy the Eq. (2). The duration of 97% WiFi packets is less than 380us [23] and the interval of WiFi packets is about 200us [33]. The duration of a typical ZigBee packet with length of 30 bytes is about 1ms, which is enough to overlap with a WiFi packet.

Considering the dynamics of WiFi packet length, the length of ZigBee packets can be fixed at a sufficiently large value, so as to ensure that (in the time domain) ZigBee packets can overlap WiFi packets of different lengths. The maximum length of a WiFi packet is 1024 bytes and the minimum rate is 6Mbps with the modulation of BPSK1/2. Under this condition, the maximum duration of a WiFi packet is 1.36ms. Meanwhile, the WiFi packet interval is about 200us [33]. Accordingly, we may fix the ZigBee packet length at 60 bytes and the duration of the ZigBee packet will be 1.92ms, which is long enough to overlap with a WiFi packet. Dynamic changes of WiFi packet length may affect the number of collected CSI samples within a time window. The SVM classifier classifies the CSI sequence based on the statistical features of the CSI sequence. Two features are used: the variance of CSI values, the difference between the maximum CSI and the minimum CSI within a window. Therefore, provided that the number of CSI samples is varied, the decoding mechanism using the SVM classifier remains effective.

Third, ZigFi manipulates the CSI of WiFi packets (by overlapping ZigBee packets on them) rather than producing collisions. The ZigBee device disables CSMA to enable deliberate overlapping. The WiFi device doesn't disable CSMA. The power adjustment in ZigFi ensures that when the ZigBee device transmits, the WiFi sender won't backoff. When there is another WiFi transmitter transmitting at the hidden side, the WiFi sender will backoff. The WiFi receiver-initiated mechanism of ZigFi can deal with this situation. The WiFi receiver first transmits control packets to wake up the WiFi sender and the ZigBee sender. These control packets will make the other WiFi transmitter (including the hidden one) backoff. The WiFi receiver plays the function of reserving channel. When the WiFi sender starts to send, the hidden WiFi transmitter will not interfere with it. The WiFi receiver-initiated mechanismis ensures that WiFi packets can be prior to ZigBee packets.

The operational scenario of ZigFi involves a WiFi sender, a WiFi receiver and a ZigBee sender. When a WiFi sender is transmitting packets to a WiFi receiver, a ZigBee sender can piggy-back its packets on this WiFi link to deliver CTC symbols. For a pair of the WiFi sender and the ZigBee sender, the power adjustment matches the power of them to satisfy the SINR requirement of the WiFi receiver. In the scenarios including multiple WiFi senders and one ZigBee sender, or one WiFi sender and multiple ZigBee senders of the same channel, there are multiple pairs of WiFi sender and ZigBee sender. Our power adjustment doesn't guarantee satisfying SINR range requirement of the WiFi receiver.

In power adjustment mechanism, the WiFi receiver detects the channel and measures the SINR every 2s. When the SINR is not in the suitable range in Fig. 9, the WiFi receiver transmits control messages to inform the ZigBee sender to adjust power. The overhead during the online adjustment mainly comes from the SINR measurement and the communication from WiFi to ZigBee. The overhead of SINR measurement is negligible because the WiFi device has powerful computing capability. The overhead of transmission from WiFi to ZigBee depends on how often the ZigBee sender adjusts the Tx power. When the SINR changes very quickly, the WiFi receiver informs the ZigBee sender to adjust the Tx power. We select the method of WiZig [12], which leverages the energy of WiFi packets to transmit control messages from WiFi to ZigBee. In practice, it takes tens of WiFi packets to complete the ZigBee Tx power adjustment.

## V. Extension to multiple-to-one concurrent transmissions

The design of ZigFi can be extended to multiple-to-one concurrent transmissions. One WiFi channel overlaps with four ZigBee channels and each ZigBee channel overlaps with four different WiFi subchannels. For each one-to-one CTC, we choose the subchannel with higher CSI variance to achieve the ZigBee to WiFi CTC. Multiple ZigBee senders with different channels can simultaneously transmit to a common WiFi receiver. For example, the WiFi channel 11 overlaps with four different ZigBee channels 21, 22, 23, and 24 (as shown in Fig. 1). ZigBee channel 23 overlaps with WiFi four subchannels 18,

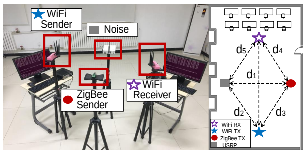
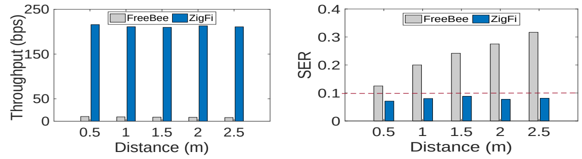



Fig. 12. The devices and the network used in the experimental evaluation




(a) Throughput

(b) SER

Fig. 13. Performance comparison of FreeBee and ZigFi

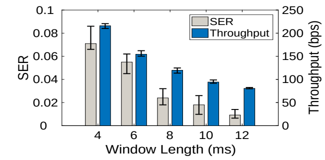
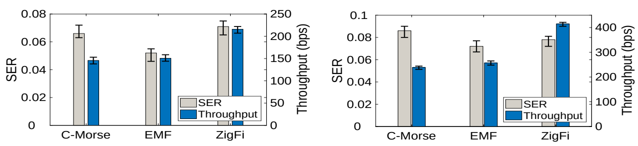



Fig. 14. ZigFi performance with different decoding window lengths




(a) Single transmission

(b) Multiple transmissions

Fig. 15. Performance comparison of C-Morse, EMF, and ZigFi

19, 20, 21 and the CSI sequence in subchannel 20 has a higher variance. So we chhoose subchannel 20 to achieve the CTC from ZigBee channel 23 to WiFi channel 11. Similarly, we choose subcahnnel 4, 12, 28 to realize the CTC from ZigBee channel 21, 22, 24 to WiFi channel 11 respectively.

We configure four TelosB nodes to transmit ZigBee packets on channel 21, 22, 23, and 24, respectively. At the receiver, we observe CSI sequences on the subchannel 4, 12, 20, and 28, which are shown in Fig. 11(a), Fig. 11(b), Fig. 11(c), and Fig. 11(d). Those CSI sequences of four subchannels all have a larger variation range. So multiple ZigBee senders can concurrently transmit to a common WiFi receiver as long as the center frequency of ZigBee is aligned with the center frequency of the corresponding WiFi subchannel.

## VI. Evaluation

### A. Implementation

We implement ZigFi on commercial WiFi devices (Intel 5300) and TelosB motes, as shown in Fig. 12. The CSITool software platform is installed on the WiFi devices and used to collect CSI readings. Configuration of WiFi and ZigBee is same with the experiments in Section III. The experiment is carried out in a real office environment and we use a USRP to generate noise on demand. The performance metrics mainly include throughput (measured by the successfully decoded bits per second) and SER (ZigFi symbol error rate). We can reduce SER by increasing decoding window length with more ZigBee packets to deliver one ZigFi symbol.

### B. Overall performance comparison

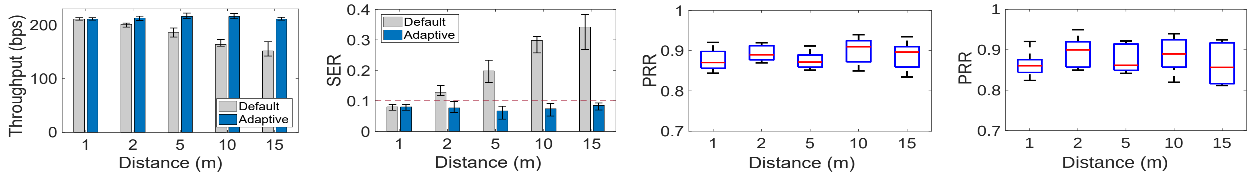
*1) Performance comparison with FreeBee:* We compare ZigFi with FreeBee [5] as shown in Fig. 13(a) and Fig. 13(b). ZigFi shows significant enhancement over FreeBee in terms of throughput and SER. For example, when the distance is 0.5m, the throughput of FreeBee and ZigFi are 10.5bps and 215.9bps, respectively. The SER of FreeBee and ZigFi are 0.125 and 0.071.

The decoding window length affects ZigFi performance. As shown in Fig. 14, when the decoding window length is 4ms, the throughput of ZigFi is 215.9bps and the SER of 0.071. When the decoding window length is 12ms, the SER decreases to 0.0092 (below 1%) and the throughput also decreases to 80.6bps. The adjustment of the decoding window length aims at a tradeoff between the SER and the throughput.

*2) Performance comparison with C-Morse and EMF:* We further compare ZigFi performance with C-Morse [23] and EMF [9]. C-Morse uses the combination of the short ZigBee packets {dot, dot, dash} and the long ZigBee packets {dash, dot, dot} to construct the recognizable energy patterns at the WiFi receiver. We set the duration of a dot at 1ms and the duration of a dash at 2ms. The decoding window length of WiFi receiver is 6ms. EMF modulates CTC symbols by shifting the packet order to form different packet occupancy ratios. We set the duration of ZigBee packet denoting "1" at 2ms and the duration of ZigBee packet denoting "0" at 1ms. The decoding window length of WiFi receiver is 6ms. The evaluation result is shown in Fig. 15(a). The throughput of C-Morse, EMF, and ZigFi are 145.8bps, 150.6bps and 211.6bps respectively, the SER of C-Morse, EMF, and ZigFi are 0.066, 0.052, and 0.074 respectively. For one-to-one transmission, the performance of C-Morse is worse than EMF. The performance of ZigFi is better than C-Morse and EMF.

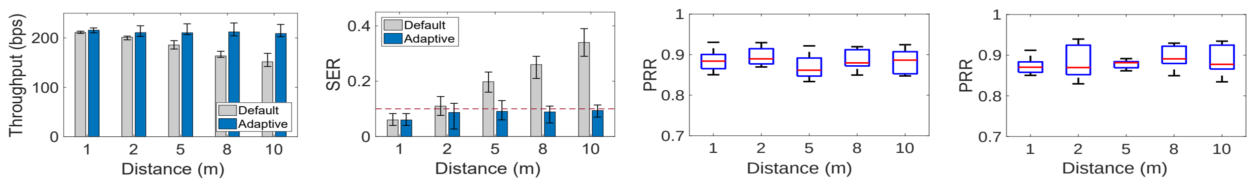
We conduct experiments to compare the spectrum efficiency of these works. C-Morse supports many-to-one (many ZigBee senders to one WiFi receiver) transmission based on timing multiplexing. We turn on two ZigBee senders one by one and they transmit to one WiFi receiver in different time slots. EMF supports one-to-many (one ZigBee sender to many WiFi receivers) transmission. Two types of ZigBee packets with the duration of 1ms and 2ms are used to generate different packet occupancy ratios. The decoding window lengths of two WiFi senders are 5ms and 10ms. ZigFi supports the many-to-one (many ZigBee senders to one WiFi receiver) transmission based on subchannel multiplexing. We control two ZigBee devices to transmit ZigBee packets on channel 21 and 23. The decoding subchannels of WiFi are subchannel 4 and 20. As shown in Fig. 15(b), the aggregated throughput of C-Morse is 238.6bps with the SER of 0.086. The aggregated throughput of EMF is 256.8bps and the SER is 0.072. The aggregated throughput of ZigFi is 414.6bps and the SER is 0.077.

We discuss the three works in the following three aspects. First, the communication range of ZigFi is larger than C-Morse and EMF. These three works propose two different CTC methods. C-Morse and EMF are functioned by utilizing RSSI, while ZigFi leverages CSI to realize CTC. Due to



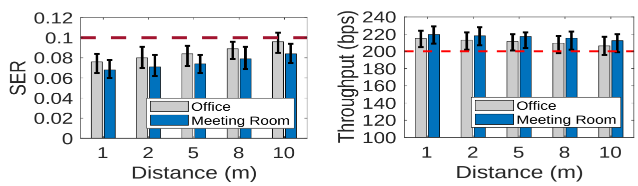

(a) ZigFi Throughput (b) ZigFi SER (c) WiFi PRR without ZigBee (d) WiFi PRR with ZigBee

Fig. 16. ZigFi under different distance between the ZigBee sender and the WiFi receiver




(a) ZigFi Throughput (b) ZigFi SER (c) WiFi PRR without ZigBee (d) WiFi PRR with ZigBee

Fig. 17. ZigFi performance under different distance between the ZigBee sender and the WiFi receiver in the NLOS scenario




(a) SER (b) Throughput

Fig. 18. ZigFi performance in different environments

the relatively weak Tx power of ZigBee and low receiving sensitivity of WiFi, RSSI-based CTC can only work in very limited range. Compared with RSSI, the CSI of the WiFi receiver is more sensitive to ZigBee signals, thus increases the achievable communication range from ZigBee to WiFi. Second, ZigFi is complementary to C-Morse and EMF in the application scenarios. C-Morse and EMF require the ZigBee sender exclusively occupy the channel. Otherwise, other devices coexisting in the channel will may affect the RSSI received at the WiFi receiver. That is to say, when C-Morse or EMF is used, WiFi and ZigBee transmitters can't transmit at the same time. Differing from this scenario, ZigFi leverages an existing WiFi link. The ZigBee sender transmits packets to overlap with the WiFi packets in the air. Third, in terms of performance, ZigFi is also better than C-Morse and EMF. The throughput of ZigFi in our paper is measured by goodput, which takes the SER into consideration. From the evaluation results, the goodput of ZigFi is respectively 45% and 41% higher than that of C-Morse and EMF. Moreover, with the increase of the number of concurrent ZigBee senders, the performance gain of ZigFi will be more remarkable.

### C. Performance under different settings

In the following experiments, the default mode doesn't have the power adjustment, so the ZigBee sender transmits packets with a predefined power. In our experiment, the default ZigBee Tx power level is 13 (-9dBm). In the adaptive power mode, ZigBee sender transmits with an adaptive power.

**Performance with different distance between the ZigBee sender and the WiFi receiver.** We change the distance between the ZigBee sender and the WiFi receiver $d_4$ from 1m to 15m. Fig. 16(a) and Fig. 16(b) plot the results. In the default mode, the SER increases and the throughput decreases with the increase of the distance. In the adaptive mode, we adjust the Tx power and the performance of the ZigFi close to 210bps across all distances. When the distance is 15m, the default mode and the adaptive mode achieve a throughput of 151.7bps and 211.4bps. The SER of CTC symbols of ZigFi is 0.085 in the adaptive mode. We will discuss the imapct of distance on the PRR of WiFi packets in Section VI-D.

**The performance of ZigFi in the Non-Line-of-Sight (NLoS) Scenario.** We place an obstacle between the ZigBee sender and the WiFi receiver to block the line-of-sight transmission. As shown in Fig. 17(a) and Fig. 17(b), ZigFi in the default mode is susceptible to signals' NLOS propagation. ZigFi in the adaptive power mode is robust under similar conditions. When $d_4$ is 10m, the throughput in the adaptive power mode is 208.9bps and the SER is 0.094. As shown in Fig. 17(c) and Fig. 17(d), the PRR of WiFi is larger than 0.85 under all settings. When the distance is 10m, the WiFi PRR is 0.878 and 0.862 with and without ZigBee.

### D. The impact on existing WiFi communication

In ZigFi, we adjust the Tx power of ZigBee to make the variation of the CSI sequence distinctive and doesn't cause the CSMA of WiFi. In the previous four groups of experiments, we also measure the PRR of the WiFi link with/without ZigBee transmissions. Overall, the ZigBee transmission has minimal impact on the PRR of the WiFi link. As an example, in the experiments corresponding to Fig. 16(c) and Fig. 16(d), the PRR of WiFi packets with and without ZigBee transmissions are 0.864 and 0.868.

Although WiFi CSI readings have been affected by ZigBee packets, the WiFi packets from the WiFi sender can be suc-

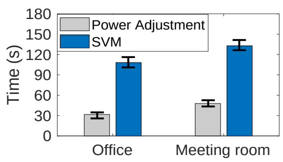



Fig. 19. The effective duration of power adjustment and SVM training

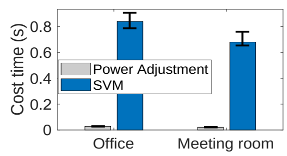



Fig. 20. The time cost of power adjustment and SVM training

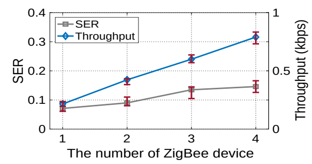



Fig. 23. The SER and throughput of multiple-to-one concurrent transmissions

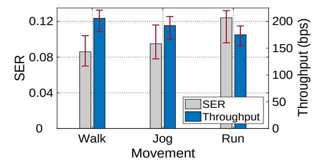



Fig. 24. ZigFi performance under mobility

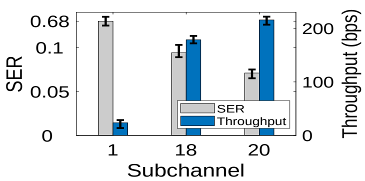



Fig. 21. ZigFi performance in different subchannels

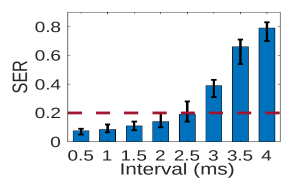



Fig. 22. The SER of ZigFi with different WiFi packet interval

cessfully decoded by the WiFi receiver with high probability because WiFi employs equalization and bit error correcting techniques to tolerate modest errors. There will not be two WiFi to WiFi links simultaneously transmitting since the CSMA on the ZigFi enabled WiFi device is kept enabled. Even though the ZigBee sender disables CSMA, it will not cause interference to the normal WiFi to WiFi communication. The impact caused by ZigBee-to-WiFi interference actually doesn't happen with ZigFi.

### *E. ZigFi performance in different noisy environments*

We conduct experiments to evaluate the performance of ZigFi in two different noisy environments, an office and a meeting room. There are twenty students in the office. These students watch videos, surf the Internet, down load files, and conduct other daily activities. There are five students in the meeting room and they are at a remote video conferencing. These two environments are different in terms of channel noise/interference. The distance between the ZigBee sender and the WiFi receiver varies from 1m to 10m. We compare the SER and the throughput of ZigFi in these two environments.

Fig. 18 shows the experiment results. The SER of ZigFi is lower than 0.1 and the throughput of ZigFi is higher than 200bps, no matter in the office or in the meeting room. When the distance between the ZigBee sender and the WiFi receiver is 10m, the SER of ZigFi in the office and in the meeting room is 0.096 and 0.084 respectively. The throughput of ZigFi in the office and in the meeting room is 206.1bps and 212.4bps respectively. The performance of ZigFi in the meeting room is better than in the office. This is because the environment of the office is more complex and the noise is more uncontrollable.

We also evaluate the effective duration of power adjustment and SVM training. The effective duration is defined as the duration between two times of operations (power adjustment or training of SVM). As shown in Fig. 19, the average effective duration of a power adjustment in the office is 31.6s, which is shorter than that in the meeting room. This is because the environment of the office is more dynamic than meeting room. The average effective duration of a SVM training in the office and the meeting room is 108.2s and 132.8s, respectively. At the same time, we also provide the time cost to perform a power adjustment and training, respectively. As shown in Fig. 20, the time costs of power adjustment in the office and the meeting room are 42.8ms and 31.6ms. Training SVM model including training CSI collection takes 0.84s in the office and 0.72s in the meeting room.

### *F. ZigFi performance in different subchannels*

The center frequency of subchannel 20 is the closest to the ZigBee channel 23 and subchannel 18 overlaps with the edge of ZigBee channel 23. The center frequency of subchannel 1 is the farthest from the center frequency of ZigBee. As shown in Fig. 21, the throughput of ZigFi in subchannel 20 and 18 are 215.9bps and 178.6bps respectively. The SER of ZigFi in subchannel 1 increases to 0.68 since that subchannel 1 doesn't overlap with ZigBee channel 23. So subchannel 1 can't be used to achieve CTC from ZigBee channel 23 to WiFi channel 11. Therefore, frequency overlap is the prerequisite for ZigFi.

### *G. ZigFi performance with different WiFi packet intervals*

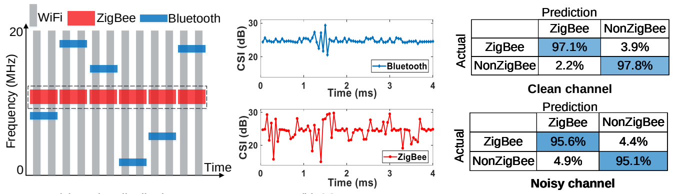
We increase the WiFi packet interval from 0.5ms to 4ms. The ZigBee sender transmits packets continuously with the interval of 0.192ms. The SER of ZigFi is shown in Fig. 22. With the increase of the WiFi packet interval, the SER is stable firstly and then decreases sharply. The is because the decoding window can tolerate the reduction of the number of CSI values. Whereas, when the WiFi packet interval exceeds 3ms, the number of CSI values within a decoding window is too few to be decoded at the WiFi receiver.

### *H. Extension to multiple-to-one concurrent transmissions*

First, we only control a TelosB node to transmit ZigBee packets on channel 23. Second, another TelosB node opetrating on channel 21 joins the concurrent transmission. Third, we control another ZigBee node to transmit packets on channel 24. Finally, another ZigBee node transmits packets on channel 22. As a result, there is a four-to-one concurrent transmission to achieve the CTC from ZigBee to WiFi. As shown in Fig. 23, both the throughput and the SER increase with the number of ZigBee senders devices. When all the four overlapping channels are used, the aggregated goodput is 790.1bps.

### *I. ZigFi performance under mobility*

In this experiment, a student carrying a ZigBee node walks, jogs, and runs with the speed of 1m/s, 2m/s, and 4m/s,




(a) Packet distribution (b) CSI sequence (c) Evaluation result

Fig. 25. Characteristics of WiFi, ZigBee, and Bluetooth packets. (a) Packet distribution of WiFi, ZigBee, and Bluetooth. (b) CSI sequences affected by ZigBee and by Bluetooth. (c) The SVM classification result.

respectively. We adjust the Tx power of the WiFi sender and the ZigBee sender to ensure the SINR at the WiFi receiver in the suitable range. As shwon in Fig. 24, when the movement speeds are 1m/s, 2m/s, and 4m/s, the SER are 0.086, 0.095, and 0.124, the throughputs are 205.7bps, 192.3bps, and 175.2bps. ZigFi works well under mobility. But in some high-speed mobile scenarios, the SINR variation caused by mobility is faster than the Tx power adjustment, the performance of ZigFi may reach the "default" value, where the ZigBee sender transmits packets with a predefined power.

## VII. Discussion

There are a lot of other wireless devices on the 2.4GHz ISM band, such as WiFi, Bluetooth, cordless phone and baby monitor. The anti-interference methods in the wireless network can be used in ZigFi. The WiFi communication used by ZigFi and the other interfering links won't transmit at the same time, because they both enable CSMA. Therefore, unless there are hidden terminals, the suspected interference between ZigFi transmission and the normal ZigBee/WiFi communication doesn't happen.

The classification problem in ZigFi is to distinguish ZigBee-affected CSI from other CSI, rather than to distinguish CSI affected by different interfering signal sources. Note that ZigFi uses the SVM classifier to decode CTC symbols. If the CSI sequence is affected by ZigBee, the CTC symbol is "1". Otherwise, the CTC symbol is "0". When there are other signals, the SVM needs to distinguish the CSI sequence affected by ZigBee signal from the CSI sequence affected by other non-ZigBee signals, such as Bluetooth, cordless phone or baby monitor. So this is a SVM classification problem, which can be solved by training SVM classifier. We conduct experiments to evaluate the SVM classification result in two different environments. In one of them, there are five students in the meeting room, talking to each other. The WiFi sender transmits packets on WiFi Channel 11 and the ZigBee sender transmits packets on ZigBee Channel 23. The WiFi receiver receives packets and obtains the CSI sequence of its subchannel 20. The distance between the WiFi sender and the WiFi receiver is 10m. The distance between the WiFi sender and the ZigBee sender is 7m, which is equal to the distance between the WiFi receiver and the ZigBee sender. There are no other Bluetooth devices here. In the other setting, the experiment is conducted in the same meeting room with the same ZigFi settings. Whereas, five students in the room continuously kept listening to music with the Bluetooth headset and sending photos via the Bluetooth connection, using their smartphones. In this way, there are Bluetooth signals throughout the experiments. The SVM classification result is shown in Fig. 25(c). We find that the accuracy of SVM classifier is higher than 95% in two environments. So the SVM classifier can distinguish the CSI sequence affected by ZigBee signals from the CSI sequence affected by other non-Zigbee signals, such as Bluetooth.

We explain the above experimental results as follows. CSI characterizes the channel changes of different WiFi subcarriers. Fig. 25(a) shows the spectrum and time-domain characteristics of WiFi, ZigBee and Bluetooth packets. Bluetooth adopts channel hopping and overlaps with different WiFi subchannels at different times. The probability that the CSI sequence of a WiFi subchannel is continuously affected by Bluetooth signals within a time window is very low. ZigBee doesn't have the channel hopping mechanism, so the overlap between ZigBee and WiFi packets appears always on the same WiFi subcarrier. Within a time window, the CSI sequence of this subchannel will be continuously affected. We conduct experiments to observe and compare the WiFi CSI sequences affected by ZigBee and by Bluetooth. The WiFi sender transmits WiFi packets on WiFi Channel 11. The ZigBee sender transmits ZigBee packets on ZigBee Channel 23, which overlaps WiFi packets on WiFi subchannel 20. The Bluetooth sender transmits Bluetooth packets with channel hopping. Fig. 25(b) plots the CSI sequence of WiFi subchannel 20 affected by Bluetooth packets and by ZigBee packets respectively. These two curves are very different in terms of variance and the difference between the maximum CSI and the minimum CSI within a window. Based on this fact, the SVM classifier can distinguish different CSI sequences affected by ZigBee and by Bluetooth.

## VIII. Conclusion

In this paper, we tackle the problem of CTC from ZigBee to WiFi. Our study reveals that CSI of the overlapped packets can be utilized to convey data across different wireless technologies. We design a receiver-initiated protocol and translate the decoding problem into a problem of CSI classification with SVM. The implementation and experiments demonstrate that ZigFi achieves ZigBee to WiFi CTC with minimal impact on existing WiFi traffic in the network.

## Acknowledgment

This work was supported by National Key R&D Program of China No. 2017YFB1003000, National Basic Research Program (973 program) under Grant of No. 2014CB347800. National Nature Science Foundation of China No. 61772306 and No. 61672320, and China Postdoctoral Science Foundation No. 2016M601034.

## References

[1] Z. Zhou, C. Wu, Z. Yang, and Y. Liu, "Sensorless sensing with wifi," *Tsinghua Science and Technology*, vol. 20, no. 1, pp. 1–6, 2015.

[2] M. Doddavenkatappa, M. C. Chan, and B. Leong, "Splash: fast data dissemination with constructive interference in wireless sensor networks," in *Proceedings of USENIX NSDI*, 2013.

[3] B. Bloessl, S. Joerer, F. Mauroner, and F. Dressler, "Low-cost interferer detection and classification using telosb sensor motes," in *Proceedings of ACM MobiCom*, 2012.

[4] Y. Yan, P. Yang, X. Li, T. Yue, Z. Lan, and L. You, "Zimo: building cross-technology mimo to harmonize zigbee smog with wifi flash without intervention," in *Proceedings of ACM MobiCom*, 2013.

[5] S. M. Kim and T. He, "Freebee: Cross-technology communication via free side-channel," in *Proceedings of ACM MobiCom*, 2015.

[6] T. Zachariah, N. Klugman, B. Campbell, J. Adkins, N. Jackson, and P. Dutta, "The internet of things has a gateway problem," in *Proceedings of ACM HotMobile*, 2015.

[7] Z. Yin, Z. Li, S. Min Kim, and T. He, "Explicit channel coordination via cross-technology communication," in *Proceedings of ACM MobiSys*, 2018.

[8] J. Han, H. Ding, C. Qian, W. Xi, Z. Wang, Z. Jiang, L. Shangguan, and J. Zhao, "Cbid: A customer behavior identification system using passive tags," *IEEE/ACM Transactions on Networking*, vol. 24, no. 5, pp. 2885–2898, 2016.

[9] Z. Chi, Z. Huang, Y. Yao, T. Xie, H. Sun, and T. Zhu, "Emf: Embedding multiple flows of information in existing traffic for concurren communication among heterogeneous iot devices," in *Proceedings of IEEE INFOCOM*, 2017.

[10] Y. Jiang, Z. Li, and J. Wang, "Ptrack: Enhancing the applicability of pedestrian tracking with wearables," in *Proceedings of IEEE ICDCS*, 2017.

[11] K. Chebrolu and A. Dhekne, "Esense: communication through energy sensing," in *Proceedings of ACM MobiCom*, 2009.

[12] X. Guo, X. Zheng, and Y. He, "Wizig: Cross-technology energy communication over a noisy channel," in *Proceedings of IEEE INFOCOM*, 2017.

[13] Z. Chi, Y. Li, H. Sun, Y. Yao, Z. Lu, and T. Zhu, "B2w2: N-way concurrent communication for iot devices," in *Proceedings of ACM SenSys*, 2016.

[14] S. Sen, R. R. Choudhury, and S. Nelakuditi, "Csma/cn: carrier sense multiple access with collision notification," in *Proceedings of ACM MobiCom*, 2010.

[15] A. Gonga, O. Landsiedel, P. Soldati, and M. Johansson, "Multi-channel communication vs. adaptive routing for reliable communication in wsns," in *Proceedings of IEEE/ACM IPSN*, 2012.

[16] J. Huang, G. Xing, G. Zhou, and R. Zhou, "Beyond co-existence: Exploiting wifi white space for zigbee performance assurance," in *Proceedings of IEEE ICNP*, 2011.

[17] R. Zhou, Y. Xiong, G. Xing, L. Sun, and J. Ma, "Zifi: wireless lan discovery via zigbee interference signatures," in *Proceedings of ACM MobiCom*, 2010.

[18] X. Zheng, Z. Cao, J. Wang, Y. He, and Y. Liu, "Zisense: towards interference resilient duty cycling in wireless sensor networks," in *Proceedings of ACM SenSys*, 2014.

[19] M. Jin, Y. He, X. Zheng, D. Fang, D. Xu, T. Xing, and X. Chen, "Smoggy-link: Fingerprinting interference for predictable wireless concurrency," in *Proceedings of IEEE ICNP*, 2016.

[20] W. Jiang, Z. Yin, S. M. Kim, and T. He, "Transparent cross-technology communication over data traffic," in *Proceedings of IEEE INFOCOM*, 2017.

[21] Y. Zhang and Q. Li, "Howies: A holistic approach to zigbee assisted wifi energy savings in mobile devices," in *Proceedings of IEEE INFOCOM*, 2013.

[22] X. Zhang and K. G. Shin, "Gap sense: Lightweight coordination of heterogeneous wireless devices," in *Proceedings of IEEE INFOCOM*, 2013.

[23] Z. Yin, W. Jiang, S. M. Kim, and T. He, "C-morse: Cross-technology communication with transparent morse coding," in *Proceedings of IEEE INFOCOM*, 2017.

[24] Z. Chi, Y. Li, Y. Yao, and T. Zhu, "Pmc: Parallel multi-protocol communication to heterogeneous iot radios within a single wifi channel," in *"Proceedings of IEEE ICNP"*, 2017.

[25] Y. Li, Z. Chi, X. Liu, and T. Zhu, "Chiron: Concurrent high throughput communication for iot devices," in *Proceedings of ACM MobiSys*, 2018.

[26] Z. Li and T. He, "Webee: Physical-layer cross-technology communication via emulation," in *Proceedings of ACM MobiCom*, 2017.

[27] Y. Chen, Z. Li, and T. He, "Twinbee: Relable physical-layer cross-technology communication with symbol-level coding," in *Proceedings of IEEE INFOCOM*, 2018.

[28] Z. Li and T. He, "Longbee: Enabling long-range cross-technology communication," in *Proceedings of IEEE INFOCOM*, 2018.

[29] Z. Li, W. Jiang, and T. He, "Bluebee: Physical-layer cross-technology communication via emulation," in *Proceedings of ACM SenSys*, 2017.

[30] W. Jiang, S. Min Kim, Z. Li, and T. He, "Achieving receiver-side cross-technology communication with cross-decoding," in *Proceedings of ACM MobiCom*, 2018.

[31] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: gathering 802.11n traces with channel state information," *ACM Sigcomm Computer Communication Review*, vol. 41, no. 1, pp. 53–53, 2011.

[32] Z. Li, Y. Xie, M. Li, and K. Jamieson, "Recitation: Rehearsing wireless packet reception in software," in *Proceedings of ACM MobiCom*, 2015.

[33] F. Hermans, O. Rensfelt, T. Voigt, E. Ngai, and P. Gunningberg, "Sonic: classifying interference in 802.15.4 sensor networks," in *Proceedings of ACM IPSN*, ACM, 2013.


**Xiuzhen Guo** is currently a Ph.D. student in Tsinghua University. She received the B.E. degree in the School of Electronic and Information Engineering from Southwest University in 2016. Her research interests include Internet of Things and wireless networks.

**Yuan He** is an associate professor in the School of Software and TNLIST of Tsinghua University. He received his B.E. degree in the University of Science and Technology of China, his M.E. degree in the Institute of Software, Chinese Academy of Sciences, and his PhD degree in Hong Kong University of Science and Technology. His research interests include wireless networks, Internet of Things, pervasive and mobile computing. He is a member of the IEEE and ACM.

**Xiaolong Zheng** is currently an associate researcher with the School of Computer Science, Beijing University of Posts and Telecommunications, China. He received his B.E. degree from the Dalian University of Technology, China, in 2011, and his Ph.D. degree from the Hong Kong University of Science and Technology, China, in 2015. His research interests include the Internet of Things, wireless networks, and ubiquitous computing.

**Liangcheng Yu** received the B.E. degree in Automation from Zhejiang University, China. He is currently a Ph.D. student at the University of Pennsylvania. He is mainly interested in computer systems and networking.

**Omprakash Gnawali** is an associate professor at the Computer Science Department of the University of Houston, USA. He does research in wireless networks, cybersecurity, and related technologies and contributed research articles, open source software, and industry standards. He received his SB and MEng from MIT, PhD from USC, and was a postdoc at Stanford.