# Poster Abstract: Physical-layer Cross-Technology Communication with Narrow-Band Decoding

Lingang Li*, Yongrui Chen* and Zhijun Li†,
*University of Chinese Academy of Sciences †Harbin Institute of Technology
lilingang17@mails.ucas.edu.cn, chenyr@ucas.ac.cn, lizhijun.hit@gmail.com

***Abstract*—Recent advances on physical-layer Cross-Technology Communication (PHY-CTC) achieve high throughput direct communication across different wireless technologies, by emulating the standard waveform of the receiver. However, this signal emulation method faces the challenges of inherent unreliability due to the imperfect emulation. Therefore, it's not suitable to achieve PHY-CTC from WiFi to BLE, since a BLE receiver can not tolerate any bit error in preamble checking when receiving a BLE frame. We present NBee, the first WiFi to BLE physical-level CTC. The key insight lies in Narrow-Band Decoding, i.e., 22MHz bandwidth WiFi (802.11b) signal can be correctly decoded at the BLE RF front-end with only 1MHz bandwidth, if the WiFi payload bits are selected by a specific pattern. More specifically, NBee leverages the unique signatures in the WiFi signal distorted by 1MHz Low Pass Filter (LPF) at BLE to extract information. Evaluation results on commodity BLE chips show NBee can achieve 1Mbps CTC with 95% packet reception rate (PRR), 3400x faster than the state-of-art CTC from WiFi to BLE.**

## I. Introduction

Recently, the rapid development of the Internet of Things (IoT) has led to the emergence of Cross-Technology Communication (CTC) [1], which enables direct communication across heterogeneous devices. As a new technique, CTC can bring many benefits to IoT applications, including: (i) saving the deployment cost of gateway. (ii) exploring the potential of cross-technology collaboration among heterogeneous technologies. (iii) reducing cross-technology interference and improving spectrum utilization by explicit channel coordination.

Recent advances on physical-layer CTC (PHY-CTC) achieves high throughput via signal emulation [1], [2], which closely emulate the receiver signal by selecting appropriate payload bits at the sender. However, it is not suitable for a receiver which requires accurate emulation (e.g., BLE). Due to standard and hardware restrictions, the OFDM-based emulation can be easily distorted by intrinsic errors such as Cyclic Prefixing (CP) related errors [1]. While for a BLE receiver, it can not bear any bit error in its preamble checking, thus will lost the whole emulated frame if any emulation error happens in its preamble. Therefore, WiFi-to-BLE physical-layer CTC has not be achieved yet with today's signal emulation method.

As shown in [3], when a wide band signal (e.g., 22MHz 802.11b signal) passes through a narrow-band filter (e.g., 1MHz BLE LPF), it could leave some traceable signatures which enable the receiver to extract original information. This observation, called as Narrow-Band Decoding [3], can be leveraged to achieve CTC from WiFi to commodity BLE chips. Specially, we find that although the filter will significantly distort the waveform of 802.11b WiFi symbols, the sign (i.e., positive or negative) of a phase shift caused by a symbol transition remains the same. Since the phase shift is used to decode BLE bit at GFSK demodulator, we can reversely select WiFi symbols to generate the desired symbol transitions and corresponding bits at BLE receiver. Also, as many WiFi control frames such as beacon, ACK and RTS/CTS are generated by 802.11b, we can easily embed CTC information in these WiFi control frames to deliver messages to BLE devices.

In all, the advantages of NBee are three folds: (1) Transparent: NBee requires neither hardware nor firmware changes in commodity chips, only carefully choosing the payload of a WiFi frame. As a comparison, some other CTCs (e.g., DopplerFi [4], G-Bee [3]) need to modify at least the firmware of WiFi or BLE. (2) High throughput: since a BLE receives NBee frames as standard BLE frames, the bit rate of NBee can reach 1Mbps, which is 3400x faster than the state-of-art [4] CTC from WiFi to BLE. (3) Reliable: without signal emulation, the intrinsic emulation errors are avoided. Therefore, the reliability of NBee is much higher than emulation based CTC (i.e., 95% PRR of NBee vs. 60% PRR of WEBee [1]).

## II. NBee Desgin

**Narrow-Band Decoding.** According to 802.11b DSSS standard, the chip sequence of data bit '1' is 10110111000 (Barker code), and bit '0' is 01001000111. Note that these two sequences are complement to each other, their waveforms are shown in Fig. 1. Then, after passing through the 1MHz filter at the BLE receiver, some patterns can be observed in the output signals. More specifically, when WiFi bit is '1', the amplitude of output signal always keep positive, no matter how the former bit and latter bit influence the shape of its waveform. The reason is: i) the LPF has an effect of averaging the signal; ii) the average amplitude of bit '1' is positive because the number of chip 1 is one more than that of chip 0. Therefore the amplitude of bit '1' remains positive after filtering. Similarly, for bit '0', the amplitude keeps negative. Therefore, after filtering, the symbol will remain at the same quadrant in the constellation (see Fig. 1). On the other hand, the GFSK demodulator performs a phase shift calculation to decode one bit every microsecond ($1\mu$s), which is exactly the same duration of a WiFi symbol. The decoded BLE bit is 0 if

Yongrui Chen* and Zhijun Li† are the corresponding authors.

978-1-7281-2700-2/19/$31.00 2019 © IEEE

the sign of phase shift is negative, or 1 if positive. Therefore, if we carefully choose the WiFi symbols, the desired phase shift sequence for correct GFSK decoding is generated.

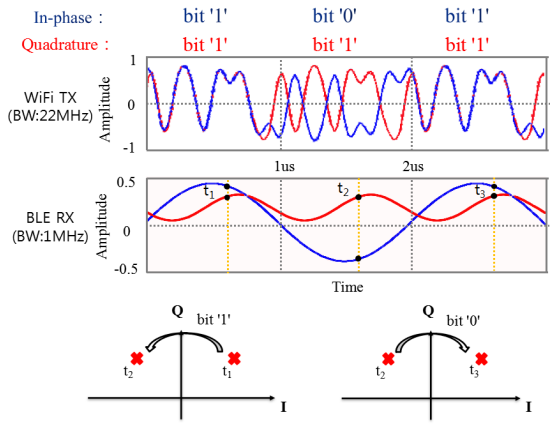


Fig. 1. The waveforms are the DQPSK signal transmitted by WiFi sender and the filtered signal at BLE receiver respectively. The phase shifts of symbols after filtering are shown in the constellation diagram.

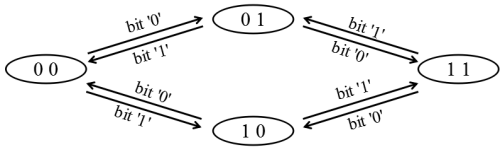


Fig. 2. The data in the ellipses are the WiFi QPSK symbols, and the arrow shows the decoded bits at BLE caused by WiFi symbols transitions.

**WiFi Payload Selection.** As shown in Fig.1, WiFi sends bits '1,0,1' in In-phase and '1,1,1' in Quadrature. After passing through the 1MHz filter, the samples at $t_1$ and $t_2$ are in the first and second quadrant respectively, according to the signs of I and Q values. Therefore, the phase shift from $t_1$ to $t_2$ is greater than $\pi/2$ but less than $\pi$, and the BLE receiver will decode it as bit '1'. Similarly, the phase shift from $t_2$ to $t_3$ is greater than $-\pi$ but less than $-\pi/2$, and the receiver will decode a bit '0' . To produce a desired BLE frame at BLE side, we set the first symbol as '11' in WiFi payload. Then we determine the following WiFi symbols based on the decoding map illustrated in Fig. 2. For example, if the next bit of BLE frame is '1', the following WiFi symbol should be '01'.

**Multi-Channel Communication.** There may be a deviation between the center frequency of a WiFi channel and a BLE channel (e.g., 2437MHz for 6-th WiFi channel vs. 2436MHz for 15-th BLE channel). However, even the carrier frequency deviation exists, WiFi signals can still be decoded by BLE receiver. The reason is as follows. For the received signals, its sampled values $s[n]$ can be expressed as [3]:

$$s[n] = (w(nT_s)e^{j2\pi(f_w - f_B)nT_s}) * h[n] \quad (1)$$

Here, $s[n]$ is $n$-th sample which is used to calculate the phase shift at the BLE receiver. $w(t)$ is the baseband analog waveform at WiFi transmitter, $f_w$ is WiFi carrier frequency and $f_B$ is BLE carrier frequency. $T_s$ is the sampling interval ($1\mu$s). $*$ indicates convolution, while $h[n]$ is the impulse response of LPF with 1MHz bandwidth. Since the carrier frequency difference between WiFi and BLE (i.e.,$f_w$-$f_B$) is either 0 or an integer multiple of 1MHz, the value of $2\pi(f_w$-$f_B)nT_s$ will be either 0 or an integer multiple of $2\pi$, and the phase of sample remains unchanged because it is added by an integer multiple of $2\pi$. Therefore the decoding results will not be affected since they depend on phase shift calculation. In this way, NBee can achieve cross-technology Multi-Channel Communication, i.e., a WiFi device can concurrently communicate with multiple BLE devices at different channels.

## III. Evaluation

We implement NBee in USRP N210 (with 802.11b PHY) and TI CC2540 BLE chip, and evaluate the performance in different scenarios.

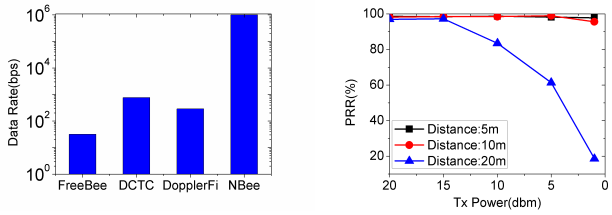


Fig. 3. (a) Comparison of throughput between NBee and state-of-arts CTCs from WiFi to BLE. (b) The effects of transmit power and transmission distance on packet reception rate (PRR).

Fig. 3a compares the throughput between NBee and other WiFi to BLE CTC schemes. From the figure we can see that NBee outperforms other schemes by over 3400x because all others are packet-level CTC, which are quite inefficient since only several bits can be modulate into one packet through packet length, beacon interval, CSI etc. Fig. 3b shows the impact of distance and transmission power on packet reception rate (PRR). When the distance is within 10m, the change in Tx power does not have much influence on PRR (which is always over 95%). When the distance reaches 20m, the PRR will decrease as the Tx power drops. Usually, the Tx power of a commodity WiFi card is greater than 10dBm, the PRR of NBee is over 80% even at a distance of 20m.


## Acknowledgements

This work was supported by the NSF China 61672196 and UCAS Cooperation Funding with Institutions Y55201QY00.


## References


[1] Zhijun Li and Tian He. Webee: Physical-layer cross-technology communication via emulation. In *MobiCom '17*. ACM, 2017.

[2] Wenchao Jiang, Zhimeng Yin, Ruofeng Liu, Zhijun Li, Song Min Kim, and Tian He. Bluebee: a 10,000 x faster cross-technology communication via phy emulation. In *Sensys*. ACM, 2017.

[3] Yoon Chae, Shuai Wang, and Song Min Kim. Exploiting wifi guard band for safeguarded zigbee. In *Sensys*, pages 172–184. ACM, 2018.

[4] Wei Wang, Shiyue He, Liang Sun, Tao Jiang, and Qian Zhang. Cross-technology communications for heterogeneous iot devices through artificial doppler shifts. *IEEE Transactions on Wireless Communications*, 18(2):796–806, 2018.