Mimicking GFSK Modulation for WiFi-to-BLE Cross Technology Communication

Chaeyeong Lee, Moonbeom Kim, Sungrae Cho, and Jeongyeup Paek

Department of Computer Science & Engineering, Chung-Ang University, Seoul, Republic of Korea
cxaexeong@cau.ac.kr, mbkim@cau.ac.kr, srcho@uclab.re.kr, jpaek@cau.ac.kr

***Abstract*—In the 2.4 GHz ISM band, mutual interference occurs due to the excessive competition for channel resources among various wireless network technologies that adopt different physical (PHY) and MAC standards. To address this issue, *cross technology communication* (CTC) techniques facilitate direct communication between heterogeneous wireless technologies in the overlapped frequencies. In this paper, we propose a novel method for WiFi-to-BLE CTC that makes a WiFi signal appear like BLE's *Gaussian frequency shift keying* (GFSK) signal. This method has not been attempted in previous PHY-CTC studies. The possibility of the newly suggested approach is demonstrated through the GNURadio simulations.**

***Index Terms*—Cross Technology Communication, WiFi, Bluetooth Low Energy (BLE), OFDM, GFSK**

I. Introduction

Internet of Things (IoT) devices enable diverse applications and services by utilizing various wireless network technologies such as WiFi, Bluetooth Low Energy (BLE), and ZigBee. However, the increase in heterogeneous devices that use different physical (PHY) and MAC layer standards causes performance degradation due to excessive resource competition and mutual interference between them. One simple way to mitigate these problems and enable coexistence among heterogeneous technologies is to use a gateway that is equipped the multiple wireless interfaces. However, due to the overhead caused by packet analysis or task conversion, use of multi-interface gateways is not an efficient solution. On the other hand, *cross technology communication* (CTC) is considered a promising technology that enables direct communication between heterogeneous devices [1]–[5]. CTC is a feasible solution for coexistence, creating a new method for interoperability and data exchange between different wireless devices without the need for a multi-interface gateway.

To communicate seamlessly between heterogeneous devices, overcoming the differences in bandwidth and (de)modulation schemes is an inevitable yet highly challenging task. Specifically, WiFi uses *carrier sense multiple access with collision avoidance* (CSMA/CA) at the MAC layer to prevent collisions while transmitting data using the *orthogonal frequency division multiplexing* (OFDM) modulation at the PHY layer [6]. In the case of BLE, *adaptive frequency hopping* (AFH) is used to avoid interference and congestion by selecting a communication channel based on mutually agreed-upon rules [7]. Furthermore, BLE employs *Gaussian frequency shift keying* (GFSK) to modulate the data in the PHY layer, which enables enhanced signal fine-tuning and helps maintain a high signal-to-noise ratio (SNR). These features of WiFi and BLE make it more difficult and complex to achieve cross-technology communication between them.

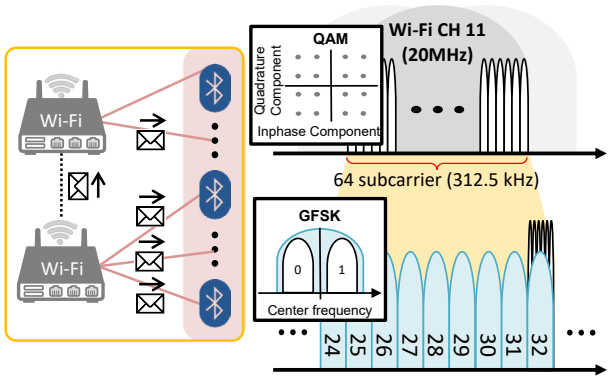


Fig. 1: WiFi to BLE based on *Mimicking GFSK Modulation*.

To realize CTC between the two different technologies, WiFi and BLE, previous studies generally emulated the WiFi packets to be compatible with Bluetooth [1] or relied on symbol transition mapping method [2]. Unlike the approaches attempted in prior work, in this work, we demonstrate the feasibility of *"mimicking GFSK modulation"* on the WiFi transmitter side for WiFi-to-BLE CTC. As shown in Fig. 1, mimicking GFSK enables BLE to receive signals of WiFi through subcarrier manipulation on the WiFi side. To the best of our knowledge, our proposal is the first of its kind, a novel approach that has not been previously attempted in prior research efforts.

The remainder of this paper is organized as follows. We first briefly introduce CTC and summarize prior work in §II. Then, we present the design of our proposal in §III, and demonstrate its possibility in §IV. Finally, we conclude this article in §VI.

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2022R1A4A5034130 & No. 2021R1A2C1008840), and also by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2023-RS-2022-00156353) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation)

II. Background and Motivation

In this section, we briefly overview packet-level and PHY-layer CTC approaches to motivate our work.

A. Packet-Level CTC (Packet-CTC)

In packet-level CTCs, the fundamental mechanism involves periodically detecting the *received signal strength indicator* (RSSI) and *channel state information* (CSI) through the wireless interface. For example, DopplerFi [3] explores how to build a two-way CTC channel between BLE and WiFi using CSI without modifying the MAC-related configurations such as transmission power or time. B2W2 [4] is a communication framework that enables N-way concurrent communication for WiFi to WiFi, BLE to BLE and WiFi to BLE scenarios. B2W2 monitors the changes in signal strength transmitted by BLE devices, and develops a discrete amplitude frequency-shift keying (DAFSK) converter and symbol mapper to overcome the practical challenges of frequency hopping and fixed transmission intervals. In general, these packet-level CTC methods have relatively low throughput, as each packet carries only a few bits of information. For instance, the bit rate of DopplerFi is 290 bps only.

B. Physical-Layer CTC (PHY-CTC)

In order to overcome the low bit rate of packet-level CTC approaches, several physical (PHY) layer CTC approaches have been proposed where it is necessary to overcome the disparities in channel size and modulation techniques. Since different wireless standards employ different (de)modulation techniques, direct interpretation is not possible. Wang *et al.* propose BlueFi [1] which enables the transmission of Bluetooth packets using commercial off-the-shelf WiFi hardware. It includes finding the corresponding WiFi bitstream that generates an IQ waveform sufficiently close to the waveform produced by the Bluetooth transmitter. This process involves iteratively reversing the operations of each block in the transmitter to assess how closely the IQ waveform can be reconstructed from the perspective of the Bluetooth receiver. WiBle [2] suggests *symbol transition mapping* to achieve CTC from WiFi to BLE. Instead of emulating the entire signal expected by the receiver, WiBle leverages the unique signature of WiFi symbols remaining on the BLE receiver to generate the desired BLE phase shifts through WiFi symbol transition mapping. According to their evaluation results, Wible achieves a data rate of 974.3 Kbps which outperforms packet-level CTC based DopplerFi by over 3300x times.

III. Design

Mimicking GFSK modulation begins with the idea that, we can manipulate certain WiFi subcarriers overlapped within the 2 MHz bandwidth of BLE. One WiFi channel overlaps with approximately nine BLE channels, and five to six subcarriers also overlap within each BLE channel. Thus, communication with a single BLE device is achievable using five to six subcarriers. In this paper, we design using GNURadio [8] by manipulating six subcarriers to enable communication with a single BLE device as shown in Fig. 2.

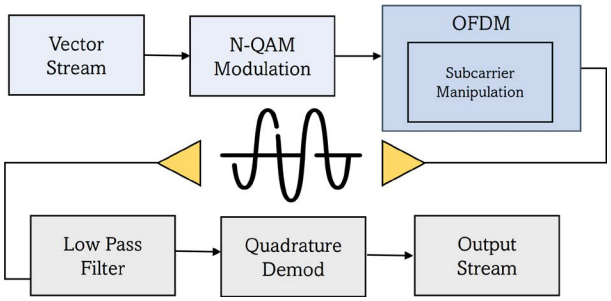


Fig. 2: Diagram of the WiFi-to-BLE on GNURadio.

Parameter \ Standard	WiFi	BLE
Center frequency	2.462 GHz	
Bandwidth (subcarrier)	20 MHz (312.5 kHz)	2 MHz
Sampling rate	20 MHz	1 MHz

TABLE I: Summary of Parameter Differences.

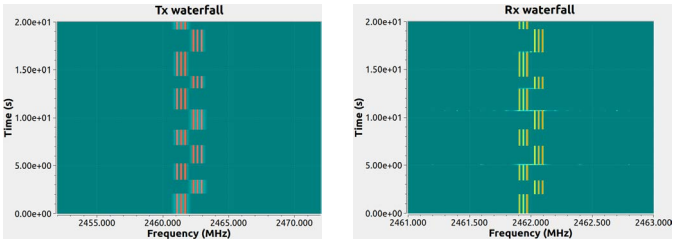
In the transmitter, an additional step involves manipulating subcarriers within the process of generating the conventional OFDM signal. Following the generation of a sample stream from an input vector, symbols are created through QAM modulation. For maintaining the independence and absence of interference between the subcarriers within the given spectrum, the OFDM signal is generated. In the process of OFDM, subcarriers are positioned with the center frequency at multiples of $\pm$312.5 kHz on the desired negative or positive frequency side.

We perform subcarrier manipulation on the transmission side. Additionally, we employ the GFSK demodulation method provided by GNURadio. However, finely adjusting parameter values in accordance with design specifications is a significant work and the outcomes can also be influenced by noise. At the receiver side, a low-pass filter is employed before carrying out GFSK demodulation, effectively restoring the signal. Afterward, GFSK demodulation is performed based on the phase shifts occurring at the point where the amplitude transitions from '0'.

IV. Evaluation

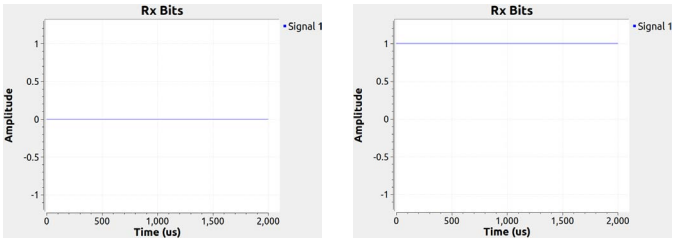
In this section, we first describe the simulation setup, and demonstrate that it is feasible to make a WiFi signal appear like GFSK for WiFi-to-BLE CTC. Subsequently, we assess the viability of the newly proposed approach by comparing the spectrum between the transmitter and receiver sides. Our evaluation employs GNURadio 3.10 in conjunction with Python 3.8. Experimental setup values are presented in Table I.

Fig. 3 and Fig. 4 demonstrate the potential of the approach we have presented. When transmitting 50 bytes of data, the signal at the receiver side varies depending on the positioning of subcarriers (on the negative or positive frequency side). As shown in Fig. 3a, subcarriers transmitted from the negative frequency side are positioned at distances of 2.4610625 GHz,



(a) Tx spectrum **(b)** Rx spectrum

Fig. 3: Spectrum Based on Subcarrier Position.



(a) Rx bits on the negative frequency **(b)** Rx bits on the positive frequency

Fig. 4: Rx bits Based on Subcarrier Position.

2.461375 GHz, and 2.461875 GHz from the center frequency. At this point, it is notable that on the receive side, as evidenced by Fig. 3b, the signals corresponding to lower frequencies are perceptible akin to GFSK-modulated signals (‘0’ bits). It is also evident from Fig. 4a that the signals transmitted by the three subcarriers are received as ‘0’, which is clear.

On the other hand, subcarriers transmitted from the positive frequency side are positioned at distances of 2.4623125 GHz, 2.462625 GHz, and 2.4629505 GHz from the center frequency. These correspond to relatively higher frequencies, hence they are recognized as ‘1’ bits in the GFSK-modulated signals as shown in Fig. 4b. In summary, depending on the frequency side of the signal transmitted by the transmitter, it becomes feasible to detect which binary signal, either ‘0’ bit or ‘1’ bit, has been sent by observing the more prominent frequency representation during GFSK demodulation.

Starting with Bluetooth 5.0, the standard introduces a new modulation scheme with 2 Msym/s in the supported PHY layers, allowing BLE to transmit data using a 2 MHz bandwidth [9]. On the other hand, the OFDM data rate can be calculated using the following formula.

$$\frac{\textit{Data subcarriers} \times \textit{Modulation} \times \textit{Coding} \times \textit{Spatial streams}}{\textit{Symbol Interval Time}}$$

With 48 data subcarriers used according to the IEEE 802.11g standard, the data rate can reach a maximum of 54 Mbps. Under the assumption that all conditions are the same, theoretically, each subcarrier would have a data rate of 1.125 Mbps. In this paper, specific subcarriers were manipulated by combining both positive and negative frequencies to demonstrate the feasibility of mimicking GFSK for WiFi-to-BLE CTC. A total of six subcarriers were used under this configuration, resulting in a data rate of 6.75 Mbps. Therefore, we have shown the ability to communicate with a single BLE channel by selectively utilizing six subcarriers.

V. Discussion

In this paper, *Mimicking GFSK Modulation* experimented in an ideal environment devoid of noise. However, there remain several challenges ahead of us to make the idea practical. Adding noise to the OFDM signal intended for transmission results in signal interference, disrupting the uniform flow of the signal. When WiFi’s amplitude is sufficiently increased, however, small levels of noise may be disregarded. As far as we know, the amplitude representation provided by GNU-Radio shows numerical values without units, so comparing it with actual WiFi signals based only on conjecture would be ambiguous. Therefore, we plan to construct a simulation that includes precise parameter values and close real-world conditions to facilitate a more comprehensive and accurate assessment.

VI. Conclusion

Tremendous effort on the development of cross technology communication are underway in academia. By leveraging the functional capabilities of diverse wireless technologies within overlapping frequencies, CTC holds limitless potential due to its direct communication foundation. In this paper, we proposed a novel approach to *Mimicking GFSK Modulation* for WiFi-to-BLE CTC, which is the first of its kind to the best of our knowledge, and investigated its possibility through GNURadio simulations.

In subsequent research endeavors, we intend to utilize SDR devices such as USRP in real-world environments to conduct research and advance its development.

References

[1] H.-W. Cho and K. G. Shin, “BlueFi: bluetooth over WiFi,” in *Proceedings of the ACM SIGCOMM Conference*, 2021, pp. 475–487.

[2] L. Li, Y. Chen, and Z. Li, “WiBle: Physical-layer cross-technology communication with symbol transition mapping,” in *18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2021, pp. 1–9.

[3] W. Wang, S. He, L. Sun, T. Jiang, and Q. Zhang, “Cross-technology communications for heterogeneous IoT devices through artificial doppler shifts,” *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 796–806, 2018.

[4] Z. Chi, Y. Li, H. Sun, Y. Yao, Z. Lu, and T. Zhu, “B2W2: N-way concurrent communication for iot devices,” in *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, 2016, pp. 245–258.

[5] Y. Chen, M. Li, P. Chen, and S. Xia, “Survey of cross-technology communication for IoT heterogeneous devices,” *IET Communications*, vol. 13, no. 12, pp. 1709–1720, 2019.

[6] I. C. Society, “IEEE Std 802.11-2016 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 2016.

[7] M. Woolley, “Bluetooth Core Specification Version 5.2,” *Bluetooth SIG*, 2020.

[8] “GNURadio,” [last accessed on August 2023]. [Online]. Available: https://www.gnuradio.org/

[9] J. Yin, Z. Yang, H. Cao, T. Liu, Z. Zhou, and C. Wu, “A survey on Bluetooth 5.0 and mesh: New milestones of IoT,” *ACM Transactions on Sensor Networks (TOSN)*, vol. 15, no. 3, pp. 1–29, 2019.