Poster: Cross-Technology Communication via Phase Shift Emulation

Jia Zhang, Haotian Jiang, Xiuzhen Guo, Meng Jin and Yuan He
School of Software and BNRist, Tsinghua University
{jia-zhan15, jht15, guoxz16}@mails.tsinghua.edu.cn,
mengj@mail.tsinghua.edu.cn, heyuan@tsinghua.edu.cn

Abstract

Recent works in cross-technology communication (CTC) have achieved high-throughput CTC via physical-layer emulation. Whereas, inherent errors always exist due to imperfect emulation. We notice that the receiver decodes symbols via the phase shift rather than the shape of waveform. Since that a lot of phase sequences satisfy the requirement of phase shift, we can choose an appropriate phase sequence that has less emulation errors to achieve a more reliable CTC. Our method achieves a Packet Reception Ratio(PRR) of 86.2% in our evaluation, which is 2× of WEBee.

1 Introduction

Cross-technology communication (CTC) is a technique that enables devices following different communication standards to communicate with each other directly, which appropriately handles wireless interference and collisions. Existing CTC works can be classified into packet-level CTC and physical-level CTC. Packet-level CTC uses the information of transmitted packets as the information carrier, which results in low throughput. For example, [4] utilizes the transmission timings, [1] utilizes the received signal strength and [6] utilizes the packet length. Physical-level CTC directly emulates the standard waveform with other technologies. [5] changes the WiFi payload to emulate the standard waveform of ZigBee signal. [3] emulates the standard waveform of ZigBee with BLE. [2] uses cross-demapping to realize CTC from ZigBee to BLE. In this way, the physical-level CTC can achieve a high throughput.

Whereas, these methods like WEBee can't emulate the ZigBee signal perfectly due to the hardware restriction. The workflow of WEBee is shown in Figure 1. After the desired ZigBee signal passing the FFT, we find the nearest QAM points to construct the WiFi payload. This process results in intrinsic errors in the emulated signal due to the QAM quantization errors and the cyclic prefix (CP). These errors may lead to the retransmittion of the emulated signal. As a result, the throughput of CTC degrades.

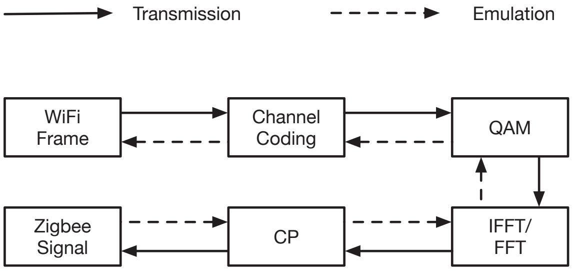

Figure 1. The workflow of WEBee

The predefined QAM points of WiFi are discrete and limited, hence the corresponding QAM points of the desired ZigBee signals after the FFT module can't match the predefined QAM points perfectly. Moreover, only 7 of the 64 subcarriers of WiFi overlapping with ZigBee, which means that only 7 QAM points can be used for the emulation.

Another source of error comes from the cyclic prefix, which is a 0.8us guard interval in every WiFi symbol. The cyclic prefix is copied from the tail of WiFi symbol and pasted into the head of the symbol. The front part of the WiFi symbol is the same with the last part of the symbol due to the cyclic prefix. Whereas, the ZigBee symbol has no such characteristic, hence the CP will result in inevitable errors.

We notice that the decoding of the ZigBee receiver relies on the phase shift between the sampling points rather than the specific shape of the ZigBee waveform, which means different waveforms can be equivalent for the ZigBee receiver as long as their phase shift sequences are the same, hence we can focus on the emulation of the phase shift sequence directly rather than the specific shape of the ZigBee waveform. As is shown in Figure 2, there are numerous phase sequences that can be emulated by selecting the WiFi payload to meet the requirement of the phase shift sequence and the emulated signals have different errors. Therefore, we can choose an appropriate phase sequence with less errors to achieve a more reliable CTC.

International Conference on Embedded Wireless
Systems and Networks (EWSN) 2019
25–27 February, Beijing, China

ISBN: 978-0-9949886-3-8

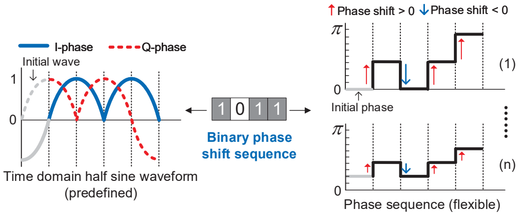
Phase shift > 0
Phase shift < 0
I-phase
Q-phase
Initial wave
1
0
1 0 1 1
Binary phase shift sequence
Time domain half sine waveform (predefined)
π
0
(1)
Initial phase
(n)
Phase sequence (flexible)

Figure 2. The comparison between half sine waveform and phase sequence

2 Design

Our approach to get the appropriate phase sequence can be divided into 3 steps: (i) We generate an initial phase sequence with a greedy algorithm. (ii) We do some optimization to minimize the inevitable errors. (iii) We emulate the phase sequence by selecting the WiFi payload to generate the emulated signal.

In the first step, we choose a square waveform as a basic unit to make sure that the phase shift is stable within a demodulation period. For each ZigBee symbol, we need to choose the initial phase ϕ and the phase shift $\Delta\varphi$ between two consecutive phase to get the phase sequence. We use a greedy algorithm to get the appropriate value of ϕ and $\Delta\varphi$. Therefore, we can generate the phase sequence which can match that of the ZigBee symbol best.

After getting the initial phase sequence, we do some optimization to decrease the inevitable errors. Some inevitable errors in the emulated signal come from the CP in the WiFi, which makes the front part of the WiFi symbol the same with the last part. We can adjust the phase shift $\Delta\varphi$ in some specific segments to make the phase shift of the front part of the emulated symbol more similar to the phase shift of the same part of the ZigBee symbol. Then we use the adjusted phase sequence to get the emulated signal. Moreover, with the emulated signal in the first step, we adjust the phase sequence again to make the emulated result better. We calculate the average of the emulated phase value within every demodulation period as the new phase. Then we use the newly generated phase sequence to get the emulated signal again, and we further use the adjusted phase sequence to get the emulated signal.

The phase sequence represents the waveform we want to emulate. We let the signal pass the FFT module and select the nearest QAM points to generate the emulated signal.

3 Evaluation

We implement our work on USRP N210 and evaluate its performance on the symbol error rate (SER), packet reception ratio (PRR) and goodput. During experiments, the composition of our packet is the same as that of WEBee, hence we can compare their performance fairly. Like WEBee, for each ZigBee channel, we can find the corresponding WiFi center frequency so that the ZigBee channel doesn't overlap with the WiFi pilots and WiFi can communicate with ZigBee directly. Here we set the center frequency of the WiFi channel at 2440MHz and the ZigBee channel at 19. The results are shown in Figure 3. We directly emulate the phase shift rather than the specific shape of the waveform, hence we have less errors in each symbol and get smaller SER. The PRR of our work is 86.1%, which is 2× of WEBee. It means we can detect the preamble, which is necessary for decoding. Both our work and WEBee have the theoretical throughput of the standard ZigBee communication. Whereas, the goodput of our work is around 3× higher than that of WEBee due to the difference in SER and PRR. All these results above show that we can emulate each ZigBee symbol more reliable.

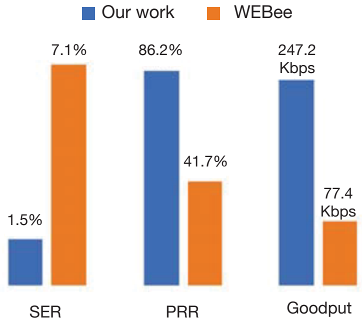

Figure 3. Overall performance comparison

4 Conclusion

In this paper, we propose a new method to achieve physical-layer CTC from WiFi to ZIgBee. We achieve a more reliable CTC via emulating the phase shift sequences corresponding to the standard ZigBee signal rather than the waveform. We evaluate the performance of our work and the results show that we have a 2× improvement in PRR and 3× improvement in goodput comparing to WEBee.

5 Acknowledgments

This work was supported by National Natural Science Foundation of China under grant No.61772306 and No.61472382.

6 References

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

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

[3] W. Jiang, Z. Yin, R. Liu, Z. Li, S. M. Kim, and T. He. Bluebee: a 10,000 x faster cross-technology communication via phy emulation. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*, page 3. ACM, 2017.

[4] S. M. Kim and T. He. Freebee: Cross-technology communication via free side-channel. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, MobiCom '15, pages 317–330, New York, NY, USA, 2015. ACM.

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

[6] Y. Zhang and Q. Li. Howies: A holistic approach to zigbee assisted wifi energy savings in mobile devices. In *INFOCOM, 2013 Proceedings IEEE*, pages 1366–1374. IEEE, 2013.