Cross Technology Communication in Heterogeneous Wireless Networks

Xiuzhen Guo
School of Software and TNLIST, Tsinghua University
guoxz16@mails.tsinghua.edu.cn

Abstract

The proliferation of IoT applications brings the demand of ubiquitous connections among heterogeneous wireless devices. Cross-Technology Communication (CTC) is a significant technique to directly exchange data among heterogeneous devices that follow different standards. We focus on achieving the packet-level CTC and the physical-level CTC between WiFi and ZigBee.

1 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. 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. In recent years, CTC has developed rapidly and there are a lot of CTC techniques. These CTC techniques can be grouped into two categories, packet-level CTCs and physical-level CTCs. Packet-level CTCs exploit free a side-channel as the carrier to convey messages among heterogeneous devices [1, 4, 3]. The side channel typically exists in the following four dimensions: packet energy, packet size, packet interval, and channel state information (CSI). Physical-level CTCs achieve CTC by modifying the payload of the sender to emulate the signal of the receiver [2, 5]. In this way, the receiver can decode the CTC symbols without any modification. In our recent research, we explore and investigate the feasibility of packet-level CTC and physical-level CTC between WiFi and ZigBee.

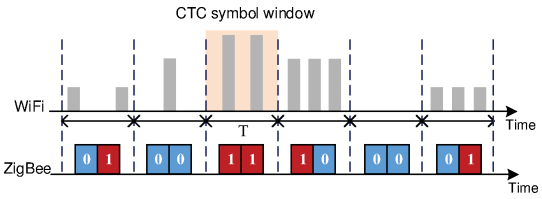


Figure 1. The schematic diagram of amplitude modulation.

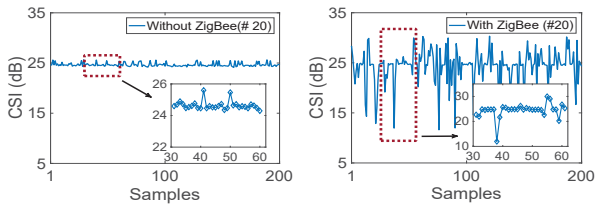
2 Packet-level CTC

In this section, we focus on achieving the packet-level CTC based on the packet energy and the channel state information.

2.1 Packet-level CTC from WiFi to ZigBee Based on Packet Energy

Based on the literature works, we realize that packet energy can be used as a side channel to convey CTC symbols. Previous works control the presence and absence of WiFi packets to convey CTC symbol "1" and "0" respectively. Whereas, it is inefficient if we only use the presence and absence of WiFi packets to encode the CTC symbol. Because there is only two energy levels (one CTC symbol) within a CTC window. The high transmission power of WiFi makes it is possible to increase the number of energy levels to encode multiple CTC symbols within a CTC window.

We propose amplitude modulation that increases the number of energy levels to improve the data rate. We can encode multiple symbols in a receiving window for improving CTC throughput. We take the four energy levels as an example to explain the amplitude modulation. As shown in Figure 1, the sender transmits WiFi packets with three different powers to provide three energy levels, which can be encoded as "01", "10", and "11". The absence of WiFi packets is encoded as "00". The receiver samples the RSSI sequence on the overlapping channel and can detect four different energy levels. In this way, the receiver can decode two CTC symbols within a CTC decoding window. If the number of energy levels is M, the CTC symbols with a CTC window is equal to $log_2 M$.



(a) Without ZigBee packets, subchannel=20

(b) With ZigBee packets, subchannel=20

Figure 2. CSI sequences with/without ZigBee packets.

2.2 Packet-level CTC from ZigBee to WiFi Based on Channel State Information

Compared with Received Signal Strength (RSS), Channel State Information (CSI) is more suitable for the CTC from ZigBee to WiFi. CSI is generally used by WiFi to measure the channel status of each WiFi subcarrier. 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 Figure 2(a) and Figure 2(b), 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. Therefore, we can carefully piggyback ZigBee packets over WiFi packets, without destroying the ongoing WiFi transmissions. The WiFi receiver decodes CTC symbols by the variance of CSI sequence.

In order to use the CSI sequence to enable ZigBee to WiFi CTC, some conditions need to be satisfied: (i) An appropriate subchannel should be selected to make ZigBee and WiFi overlap in the frequency domain. (ii) The ZigBee packet length must be large , which makes ZigBee packets overlap with WiFi packets in the time domain. (iii) An appropriate ZigBee power is needed to make the CSI sequence more distinctive. The sender transmits ZigBee packets satisfied the above conditions and encodes the CTC symbols using presence or absence of ZigBee packets. The receiver receives two sets of information. It decodes the received packet as a regular WiFi packet. It also collects the CSI sequence and uses the SVM classifier to decode the CTC symbol.

3 Physical-level CTC

The efficiency of the packet-level CTC works is bounded due to the limited throughput. First, the duration and interval of the wireless packet is in the range of milliseconds. Embedding CTC symbols into the sparse wireless packets is inefficient. Second, the packet-level CTC fails utilize the bandwidth fully. In this section, we explore the physical-level CTC for achieving high throughput.

3.1 Physical-level CTC from WiFi to ZigBee Based on Digital Emulation

We find that the decoding of the ZigBee receiver doesn't rely on the specific shape of the time-domain waveform. Intrinsically, the ZigBee receiver decodes data based on the binary phase shift between the sampling points. Therefore, in addition to the standard half sine waveform, other types of waveforms can also be decoded as long as these waveforms satisfy the requirement of the binary phase shift sequence. Therefore, different from analog emulation, we propose a novel concept **Digital Emulation** for physical-level CTC. Instead of emulating the standard time-domain waveform of the receiver, we emulate the phase shift directly. There are lots of phase sequences which satisfy the requirement of the phase shift. These phase sequences can be emulated by constructing different payloads of the sender and the emulation errors of these phase sequences are different. Therefore, we have the opportunity to select an appropriate phase sequence with the relatively small emulation errors to achieve a reliable CTC.

3.2 Physical-level CTC from ZigBee to WiFi Based on Cross-Demapping

Physical-level CTC from ZigBee to WiFi can be achieved from two technical insights: (1) Compared to ZigBee's simple encoding and modulation schemes, the rich processing capacity of WiFi offers extra flexibility to process a ZigBee packet. (2) Although not complying with the WiFi standard, a ZigBee packet leaves distinguishable features when passing the WiFi modules. So we reuse several WiFi modules to achieve the physical-level CTC from ZigBee to WiFi.

4 Conclusion

CTC is a significant technique to directly exchange data among heterogeneous devices that follow different standards. In our recent research, we explore and investigate the feasibility of packet-level CTC and physical-level CTC between WiFi and ZigBee.

5 Acknowledgments

I would like to extend my sincere gratitude to my advisor, Dr. Yuan He, for his guidance and encouragement. I am also deeply indebted to all the other predecessors and peers for their help to me.

6 References

[1] X. Guo, Y. He, X. Zheng, L. Yu, and O. Gnawali. Zigfi: Harnessing channel state information for cross-technology communication. In *Proceedings of IEEE INFOCOM*, 2018.

[2] X. Guo, Y. He, X. Zheng, Z. Yu, and Y. Liu. Lego-fi: Transmitter-transparent ctc with cross-demapping. In *Proceedings of IEEE INFOCOM*, 2019.

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

[4] S. M. Kim and T. He. Freebee: Cross-technology communication via free side-channel. In *Proceedings of ACM Mobicom*, 2015.

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