Demo: Cross-Technology Communication between BLE and Wi-Fi using Commodity Hardware

Alex Bereza*, Ulf Wetzker‡, Carsten Herrmann†, Carlo Alberto Boano‖, Marco Zimmerling*
* Networked Embedded Systems Group, TU Dresden, Germany
‡ Fraunhofer Institute for Integrated Circuits, Division Engineering of Adaptive Systems, Dresden, Germany
† Deutsche Telekom Chair of Communication Networks, TU Dresden, Germany
‖ Institute for Technical Informatics, Graz University of Technology, Austria
alex.bereza@tu-dresden.de ulf.wetzker@eas.iis.fraunhofer.de
carsten.herrmann@tu-dresden.de cboano@tugraz.at marco.zimmerling@tu-dresden.de

Abstract

In this demonstration, we present a prototype of a cross-technology communication (CTC) system that allows a Bluetooth Low Energy (BLE) device to directly send data to a Wi-Fi device using commodity hardware. Towards this goal, we use energy burst patterns to encode information on overlapping channel frequencies. With this demonstration, we prove the feasibility of our holistic CTC approach for popular wireless technologies in the 2.4 GHz ISM band based on off-the-shelf hardware and open-source software.

1 Motivation

Wireless communication technologies have evolved significantly in the past decades. With ever-increasing throughput, wireless supersedes cable-based solutions in many domains. As the success and spreading of wireless technologies continues to grow, however, the radio spectrum gets more and more crowded. In particular, the license-free Industrial, Scientific and Medical (ISM) bands are becoming an increasingly scarce resource due to the proliferation of low-power wireless devices forming the Internet of Things (IoT). This increasing congestion is a serious challenge for wireless systems, as the *radio interference* caused by neighboring devices operating concurrently in the same frequency band leads to an increased packet loss and higher number of packet re-transmissions affecting the latency, throughput, and energy efficiency of the involved networks.

Coordination among co-located wireless networks could help alleviate the interference problem. Different wireless technologies, however, employ different physical layers and bandwidth allocation schemes, and are therefore unable to communicate directly with each other; that is, they cannot interpret signals from another technology. For this reason, a *cross-technology communication (CTC)* scheme that enables low-data-rate communication without the need for dual-radio gateways or additional infrastructure is highly desirable (e.g., to enable cooperative coexistence management).

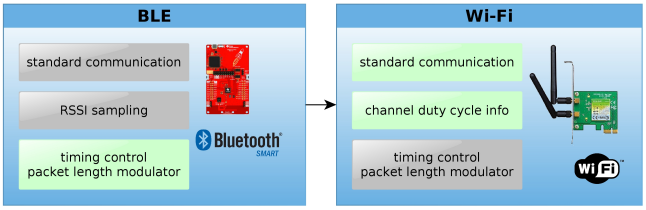

Figure 1. Illustration of our holistic CTC approach with the example of BLE to Wi-Fi communication

2 Design

State-of-the-art CTC schemes, including Esense [2] and FreeBee [3], have several limitations. Esense is restricted to unidirectional communication from Wi-Fi to ZigBee and assumes that the number of different messages is smaller than the alphabet count. FreeBee is a more general, bidirectional approach that takes also BLE into account; however, it requires special hardware, such as FPGA-enabled Wi-Fi development boards. Furthermore, FreeBee's BLE implementation is limited to the three BLE advertisement channels, which prevents generic CTC communication with BLE devices. In both works, robustness is solely achieved by transmitting the same message multiple times and processing it only if it was received more often than a certain threshold.

To address these problems, we introduce a holistic CTC approach for the 2.4 GHz ISM band that is feasible based on commodity hardware and open-source software only. To this end, we use a common transmission scheme among heterogeneous technologies with fundamentally different physical layers by exploiting the typically undesired cross-technology interference. Overlapping channel frequencies of different technologies enable them to sense each other's transmissions if their radio hardware supports channel duty cycle measurements or received signal strength indicator (RSSI) sampling.

International Conference on Embedded Wireless Systems and Networks (EWSN) 2017
20–22 February, Uppsala, Sweden

ISBN: 978-0-9949886-1-4

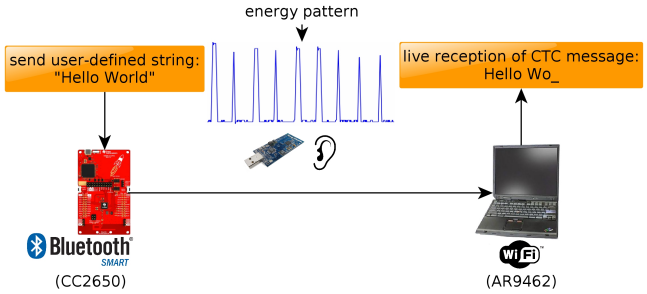

Figure 2. Demonstration setup. A BLE device transmits a user-defined string to a Wi-Fi device. The resulting energy patterns are observed with a passive TelosB sniffer.

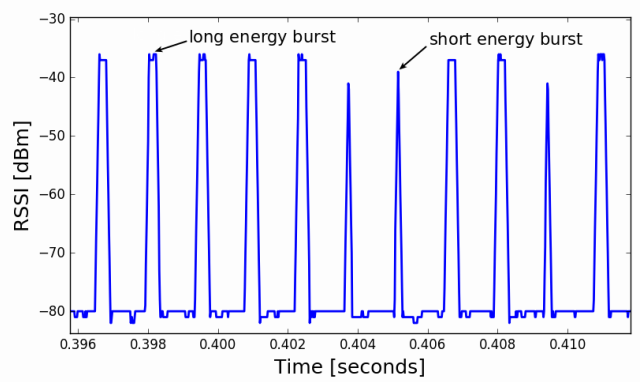

Figure 3. Visualization of CTC energy pattern recorded by a TelosB. Due to averaging effects, the short energy bursts seem to have a lower RSSI level than the long energy busts, and appear as spikes rather than plateaus.

These measurement techniques are needed, for example, to implement CSMA/CA. Like prior work [2, 3], we use them to sense energy bursts caused by transmissions of other technologies. By modulating the duration of energy bursts, we encode information to create a common transmission layer.

Specifically, we design an encoding scheme based on chip sequences with specific auto-correlation and cross-correlation properties. Each CTC packet begins with a start-of-frame sequence to distinguish it from other traffic. For this purpose, we utilize a Barker code of length 13. At zero shift, Barker codes have a high autocorrelation value, while the out-of-phase aperiodic autocorrelation absolute values are less or equal to 1. For payload encoding, we use binary maximum-length sequences to achieve a spreading factor of 8. The sequences are chosen to have low cross-correlation. This way, we add redundancy to each payload bit and provide a basic level of robustness for individual transmissions; re-transmissions can further improve reliability. Furthermore, we provide the first implementation that supports arbitrary BLE channels for CTC transmissions. As a result, our approach is more general than previous works.

Figure 1 depicts the main building blocks of our CTC approach. Every CTC system includes three components: (i) RSSI sampling (BLE) or channel duty cycle information (Wi-Fi) for energy burst detection, (ii) a timing control and packet length modulation block for energy burst transmission, and (iii) support for legacy standard-compliant communication.

3 Demonstration

As a proof of concept, we present our implementation of a CTC system that allows a common BLE transmitter to directly communicate with an off-the-shelf Wi-Fi receiver. To evaluate channel duty cycle information, we empower an off-the-shelf Wi-Fi network interface card to detect the length of distinct energy bursts by modifying its driver running in Linux kernel space. We successfully tested our implementation with the Qualcomm Atheros chipsets AR9462 and AR9287. To send energy bursts, we use the CC2650 [1] BLE platform from TI and an open-source BLE stack [4]. This way, we are able to reliably transmit a bitstream from BLE to Wi-Fi.

We demonstrate the functionality of our proof-of-concept CTC implementation using the setup illustrated in Figure 2. On the BLE side (transmitter), we program the CC2650 to periodically send a user-defined string using BLE data packets to create energy bursts of certain length. Using a TelosB sniffer, we record and visualize the resulting energy pattern (see Figure 3) to illustrate our encoding scheme to the conference attendees and allow for failure analysis.

On the Wi-Fi side (receiver), we load our modified Wi-Fi driver and start our energy burst decoding program. The received energy bursts are immediately decoded, allowing for a live display of the arriving characters on the command line. We also compute and display byte, bit, and chip error rates over a certain time window. Decoding errors due to interference can be analyzed via the recorded energy patterns.

Table 1. Preliminary CTC error rate measurements

	occasional traffic	streaming, browsing
byte error rate	1.5%	48.3%
bit error rate	0.7%	44.6%
chip error rate	2.4%	47.5%

We measured the error rates in two scenarios: (i) on a Wi-Fi channel with only beacons and occasional traffic and (ii) on a Wi-Fi channel used for video streaming and browsing. Our results (see Table 1) show that our design is robust enough to support uncritical applications based on CTC.

With this demonstration, we prove the feasibility of our CTC approach, which we believe will pave the way for many new applications and higher spectrum efficiency.

4 References

[1] Texas Instruments CC2650 SimpleLink multi-standard 2.4 GHz ultra-low power wireless MCU. `http://www.ti.com/product/cc2650` Accessed: Nov 8, 2016.

[2] K. Chebrolu and A. Dhekne. Esense: Communication through energy sensing. In *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2009.

[3] 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)*, 2015.

[4] M. Spörk. IPv6 over Bluetooth Low Energy using Contiki. Master's thesis, Graz University of Technology, Graz, Austria, October 2016.