A Fine-grained Modulation Technology for ZigBee Backscatter Communication

Citation for published version:
Xu, Z, Ding, Y & Gong, W 2022, A Fine-grained Modulation Technology for ZigBee Backscatter Communication, in 2022 Microwave Mediterranean Symposium (MMS), 9825557, IEEE, 21st Mediterranean Microwave Symposium 2022, Pizzo Calabro, Italy, 9/05/22. https://doi.org/10.1109/MMS55062.2022.9825557

Digital Object Identifier (DOI):
10.1109/MMS55062.2022.9825557

Link:
Link to publication record in Heriot-Watt Research Portal

Document Version:
Peer reviewed version

Published In:
2022 Microwave Mediterranean Symposium (MMS)

General rights
Copyright for the publications made accessible via Heriot-Watt Research Portal is retained by the author(s) and/or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
Heriot-Watt University has made every reasonable effort to ensure that the content in Heriot-Watt Research Portal complies with UK legislation. If you believe that the public display of this file breaches copyright please contact open.access@hw.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
A Fine-grained Modulation Technology for ZigBee Backscatter Communication

Zhaoyuan Xu  
University of Science and Technology of China  
Hefei, China  
xzyjyx@mail.ustc.edu.cn

Yuan Ding  
Heriot-Watt University  
Edinburgh, United Kingdom, EH14 4AS  
yuan.ding@hw.ac.uk

Wei Gong  
University of Science and Technology of China  
Hefei, China  
weigong@ustc.edu.cn

Abstract—This paper presents the first symbol-level modulation technology for ZigBee backscatter communication. The developed backscatter tag, leveraging ambient ZigBee transmissions as radio frequency (RF) carrier excitation, conveys data by translating an excitation signal into a new ZigBee signal in neighboring ZigBee channels. This avoids the strong interference from the ambient excitation signals. The key enabling technique is a symbol-level codeword translation, which exploits square waves based on the difference between the excitation and tag data. A working prototype was successfully demonstrated to validate the modulation technology, which consists of two parts: an RF frontend circuit and an FPGA-based control circuit. Through extensive experiments and field studies, the evaluation shows that the bit error rates (BERs) can be controlled to be less than 0.1 when the communication distance is within 2 meters.

Index Terms—Backscatter, ZigBee, IoT

I. INTRODUCTION

In recent years, there has been a lot of interest in backscatter communications due to its ultra-low power consumption [1]–[2]. The backscatter tag leverages available over-the-air wireless signals, e.g., Wi-Fi, BLE, ZigBee, LoRa, etc., as radio frequency (RF) carriers over which the data is modulated for information transmission. The elimination of carrier generation and amplification is the key factor that significantly reduces the cost and power consumption of backscatter tags. One of backscatter research branches is to design backscatter tags to interoperate with some commercial wireless networks. For instance, passive-WiFi in [1] modulated 802.11b signals at 1 Mbps with a power consumption of 14.5 $\mu$W; PLoRa in [3] developed a passive LoRa node and its overall power consumption was reduced to just 2.591 $m$W; Interscatter developed in [4] backscattered ambient BLE signals into 802.11b waveforms at 2 Mbps with a power consumption of 28 $\mu$W. With the potential to be power autonomous, backscatter communication technology is one of the enablers to building a smarter world equipped with ubiquitous ultra-low-power Internet-of-Things (IoT) devices.

Codeword translation [5] [6] is a modulation technology that has been widely used in state-of-art (SoA) backscatter systems. Its underlining principle is now explained. When a tag backscatters a bit “1”, it actually translates the excitation codeword into another valid codeword from the same codebook. While when backscattering a bit “0”, it reflects the excitation signal without modification. There need two receivers for signal reception: one for decoding the backscattered signal and the other for decoding the ambient excitation signal. After comparing the outputs of two receivers, the backscattered bit stream can be recovered. The SoA ZigBee backscatter system, FreeRider [6], also took the codeword translation technique. ZigBee transmission is Offset QPSK (OQPSK) modulated that eliminates instantaneous phase flipping (180$^\circ$) between neighboring chips. In its backscatter version in [6], a $\Delta \theta$ (180$^\circ$) phase offset on consecutive $N$ ZigBee symbols ($N = 8$ in practice) was introduced as codeword translation. Since active ZigBee radios embed every 4 bits into one symbol, whereas FreeRider takes N symbols to embed one bit, it inevitably reduces the backscatter throughput by a factor of 4*$N$.

Viewing the above ZigBee backscatter limitation, here we for the first time propose a novel, fine-grained codeword translation technology for ZigBee backscatter communication. It presents a symbol-level codeword translation for ZigBee backscatter, greatly improving the ZigBee backscatter system throughput. Specifically, the tag utilizes square waves of various frequencies and phases for the transition, which is derived based on the difference between the excitation and tag data to be transferred. To precisely enable codeword translation, the synchronization requirements are evaluated. Besides, in order to avoid excitation signal interference, the backscattered signals are frequency shifted to neighboring ZigBee channels. Through extensive experiments and field studies, we confirm that the bit error ratio (BER) maintains less than 0.1 when the communication distance is kept within 2 meters.

II. SYSTEM OVERVIEW

In this section, we first introduce the generation of ZigBee signals. Then, we present how to introduce a sequence of square waves to complete the codeword translation. This is followed by the evaluation of the synchronization requirements for the symbol-level codeword translation as well as the envelope detector accuracy.

A. ZigBee Primer

The physical layer of ZigBee complies with IEEE 802.15.4 [7]. It adopts OQPSK scheme to modulate information. It supports an over-the-air data rate of 250 kbps at 2.4 GHz ISM band. Its baseband processing procedures are shown in Fig. 1. Every four data bits are mapped into one of the 32-chip PN sequences ($c_0, c_1, c_2, \ldots, c_{29}, c_{30}, c_{31}$), which is known as Direct
Sequence Spread Spectrum (DSSS). Then, even-indexed chips \((c_0, c_2, \ldots, c_{28}, c_{30})\) are modulated onto an in-phase component (I) and odd-indexed chips \((c_1, c_3, \ldots, c_{29}, c_{31})\) are modulated onto a quadrature-phase component (Q). Each branch has a chip rate of 1000 chips/s \((\frac{1}{2T_c}, T_c = 0.5\mu s)\). Branch Q has an extra delay of \(T_c\) to form an offset between I and Q branches. Ultimately, both of the branches pass through a pulse shaping filter, whose expression is shown below:

\[
p(t) = \begin{cases} 
\sin(\frac{\pi t}{T_c}), & t \in [0, 2T_c] \quad \text{input} = 1 \\
-\sin(\frac{\pi t}{T_c}), & t \in [0, 2T_c] \quad \text{input} = 0
\end{cases} \tag{1}
\]

The output of the I and Q combination, see (2), produces a sequence of phase states. \(m\) denotes the state of I/Q branches, which varies every chip units \((T_c)\). \(f_i\) and \(\phi_i\) denote the signal frequency and phase, respectively.

\[
I(t) + jQ(t) = \pm \sin(\frac{\pi t}{T_c} + \frac{m\pi}{2}) \pm j \sin(\frac{\pi t}{T_c} + \frac{(m+1)\pi}{2}) \\
= e^{j(\pm\frac{\pi t}{T_c} + \frac{m\pi}{2}) + j\phi_i} \\
= e^{j(2\pi f_i t + \phi_i)} \\
= e^{j(\frac{1}{4T_c} - \frac{1}{4T_c})}, \quad \phi_i \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}
\]

For simplicity, \(\frac{1}{4T_c}\) is denoted as \(f_0\). The phase change between consecutive chip units is actually limited within \(\{-\frac{\pi}{2}, +\frac{\pi}{2}\}\). The details have been discussed in [8]. These IQ samples are then up-converted to radio frequency, which is mathematically written as

\[
S(t) = e^{j2\pi f_i t + \phi_i} \\
A\ ZigBee\ receiver\ decodes\ information\ by\ measuring\ the\ phase\ changes\ of\ an\ IQ\ sequence.\ This\ is\ achieved\ by\ multiplying\ (or\ correlating)\ the\ measured\ phase\ changes\ with\ the\ phase\ changes\ calculated\ by\ standard\ ZigBee\ symbols\ [9].
\]

B. Symbol-level ZigBee Backscatter Signal Modulation

In this subsection, we present the first symbol-level modulation technology for ZigBee backscatter communication that is illustrated in Fig. 2. It also shifts the backscattered signal to neighboring ZigBee channels, which eliminates excitation signal interference. The expression of ambient ZigBee excitation signals has been shown in (3), whose frequency is limited to \(\{f_c + f_0, f_c - f_0\}\) and phases are chosen from \(\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}\). Here we propose to generate square waves with various frequencies and phases at tags for backscatter codeword translation, as used by some other backscatter works [4] [5]. The backscattered signals \(B(T)\), that can be expressed as a multiplication of excitation signals and generated square waves, are shown in (4). \(S(t)\) denotes the excitation signal and \(T(t)\) is the first harmonic of a square wave. \(f_s + f_T\) is the frequency of the square wave that enables a frequency shift, where \(f_T\) can be chosen from \(-2f_0, 0, 2f_0\). \(\phi_T\) denotes the phase of the square waves, which is limited within \([0, \pi]\). In order to enable codeword translation, \(f_T\) and \(\phi_T\) are determined by the difference between the excitation signal and tag data.

\[
B(t) = S(t)T(t) = e^{j(2\pi(f_s + f_T)t + \phi_T)} \\
= e^{j(2\pi(f_s + f_T)t + \phi + \phi_T)} \tag{4}
\]

C. Synchronization

To enable this symbol-level codeword translation, the system needs to achieve synchronization between the excitation source and the modulation of the backscatter tag. The synchronization instructions and a sequence of phase changes can be
pre-shared with the backscatter tags. There are multiple technologies that achieve this using out-of-band communications [4] [6] [10]. We borrow the idea of achieving synchronization using signal envelope detection. It can extract the signal envelope feature using a suitable control circuit, e.g., an MCU or FPGA. To evaluate the time error using this envelope detection method, we experimentally measured the CCDF of the timing error, which is shown in Fig. 3(a). Next, the system requirement metric for synchronization is evaluated. We used a USRP N210 [11] to emulate a ZigBee backscatter tag. The USRP first captures ZigBee packets at a sampling rate of 10 MSPS, and the codeword translation was implemented with a timing error deliberately added for each sampling point in a controlled manner. These codeword translated ZigBee backscatter signals are transmitted and decoded by a TI CC2650 receiver [12].

The measured BER results versus timing error is plotted in Fig. 3(b). Observing both Fig. 3(a) and (b), we can see that about 70% of envelope detection gives time errors of less than 100 ns, leading to negligible impact on BER performance.

![Fig. 3. Synchronization analysis for ZigBee backscatter communication](image_url)

(a) Timing error of the envelope detector  
(b) BER of different timing errors

We evaluated the impact of the uplink distance on the communication performance of our system. The measurement results are shown in Fig. 5. In Fig. 5(a), we can find that the BER is less than 0.1 when the uplink distance is limited to 2 m. We are able to receive backscattered signals at a maximum uplink distance of 17 m. The received signal strength, as expected, decreases as the uplink distance increases. The measured result is shown in Fig. 5(b).

![Fig. 5. Performance of ZigBee backscatter communication](image_url)

(a) BER  
(b) RSSI

**IV. RELATED WORK**

Backscatter communication is one of the enablers for building a ultra-low-power and ubiquitous IoT world. Researchers have shown that ambient signals (Wi-Fi, ZigBee, LTE, BLE, etc.) can be used for backscatter communication [1] [6] [17] [18]. Related works have shown symbol-level backscatter for Wi-Fi communication [19] [20] [1] [5].

**V. CONCLUSION**

In this paper, we introduced for the first time a symbol-level modulation technology for ZigBee backscatter communication. It utilized various square waves of a few discrete frequencies and phases for the symbol-level ZigBee codeword translation. Besides, we evaluated the synchronization requirements for the translation. Our proof-of-concept experiment has demonstrated the effectiveness of the proposed fine-grained ZigBee codeword translation. The circuit optimization, with regard to complexity and power consumption, will be reported in our future work. We believe our contribution presented in this paper opens the opportunity of ZigBee backscatter communications in more practical applications.

**ACKNOWLEDGEMENT**

Dr Ding’s work was supported by the EPSRC (UK) under Grant EP/V002635/1.
REFERENCES


