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 front-end 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 μW; PLoRa in [3] developed a passive LoRa node and its overall power consumption was reduced to just 2.591 mW; Interscatter developed in [4] backscattered ambient BLE signals into 802.11b waveforms at 2 Mbps with a power consumption of 28 μW. 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^o) between neighboring chips. In its backscatter version in [6], a $\Delta\theta$ (180^o) 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 ($c_0, c_1, c_2, ..., c_{29}, c_{30}, c_{31}$), which is known as Direct

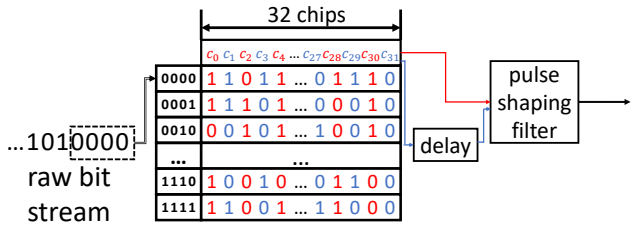


Fig. 1. ZigBee signal generation.

Sequence Spread Spectrum (DSSS). Then, even-indexed chips $(c_0, c_2, ..., c_{28}, c_{30})$ are modulated onto an in-phase component (I) and odd-indexed chips $(c_1, c_3, ..., c_{29}, c_{31})$ 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:

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

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 ϕ_i denote the signal frequency and phase, respectively.

$$\begin{aligned} & I(t) + jQ(t) \\ & = \pm sin(\pi \frac{t}{2T_c} + \frac{m\pi}{2}) \pm j * sin(\pi \frac{t - T_c}{2T_c} + \frac{m\pi}{2}) \\ & = e^{j(\pm\pi \frac{t}{2T_c} + \frac{k\pi}{2})} \\ & = e^{j(2\pi f_i t + \phi_i)} \\ & m \in \{0, 1\}, k \in \{0, 1, 2, 3\}, \\ & f_i \in \{+\frac{1}{4T_c}, -\frac{1}{4T_c}\}, \phi_i \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\} \end{aligned} \quad (2)$$

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

$$S(t) = e^{j2\pi f_c t} * e^{j(2\pi f_i t + \phi_i))} = e^{j(2\pi(f_c + f_i)t + \phi_i)} \quad (3)$$

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 $-2f_0, 0, 2f_0$. ϕ_T denotes the phase of the square waves, which is limited within $\{0, \pi\}$. In order to enable codeword translation, f_T and ϕ_T are determined by the difference between the excitation signal and tag data.

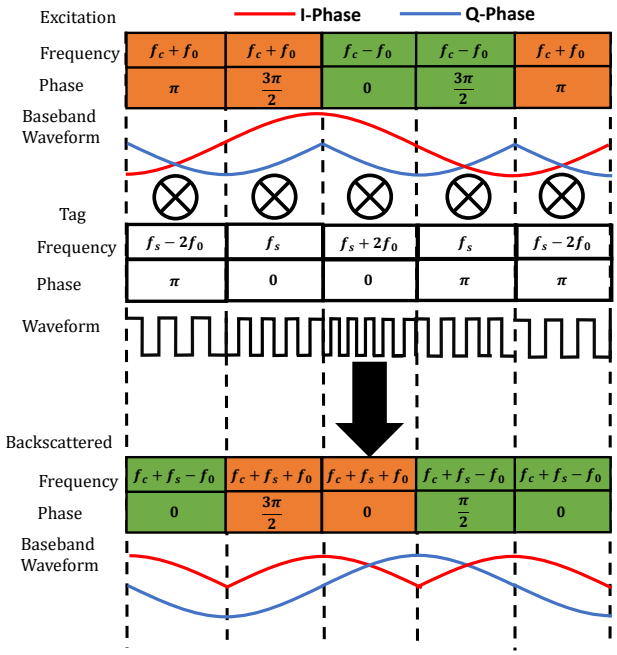


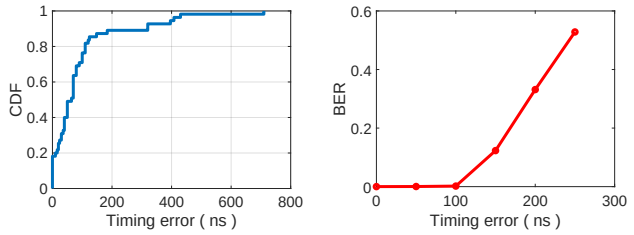
Fig. 2. The symbol-level modulation. The tag modulates excitation ZigBee symbol at basic chip units. The generation of backscattered signals is the multiplication of excitation signals and square waves introduced by the tag.

$$\begin{aligned} & S(t) = e^{j(2\pi(f_c \pm f_0)t + \phi_i)} \quad T(t) = e^{j(2\pi(f_s + f_T)t + \phi_T)} \\ & B(t) = S(t)T(t) \\ & \quad = e^{j(2\pi(f_c \pm f_0)t + \phi_i)} e^{j(2\pi(f_s + f_T)t + \phi_T)} \\ & \quad = e^{j(2\pi(f_c \pm f_0 + f_s)t + (\phi_i + \phi_T))} \end{aligned} \quad (4)$$

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), it can seen that about 70% of envelope detection gives time errors of less than 100 ns, leading to negligible impact on BER performance.



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

Fig. 3. Synchronization analysis for ZigBee backscatter communication

III. Evaluation

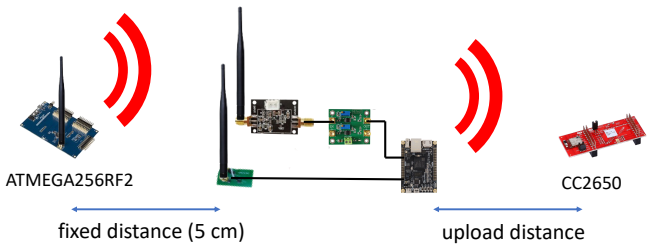
A. Experimental Setup

Our system setup is shown in Fig. 4(a) and Fig.4(ATMEGA256RF2 [13] is used to generate ZigBee excitation signal [14]. TI CC2650 is chosen as the receiver to decode the backscattered ZigBee signals. The distance between the excitation source and the backscatter tag is fixed at 5 cm, with the distance of the uplink, i.e., the link between the tag and the receiver, being varied.

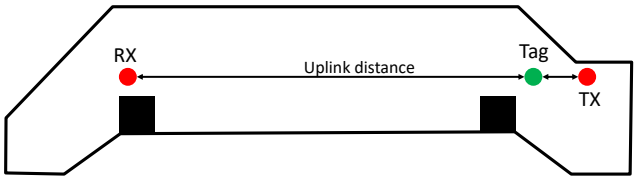
Our backscatter tag consists of two parts: an RF front-end circuit and an FPGA-based control circuit. The RF front-end circuit includes an RF envelope detector and a backscatter modulator. We use AD8313 [15] for envelope detection: an antenna is connected to its input, and its output is connected to a comparator for noise filtering. An FPGA (XILINX ZYNQ 7000) processes the detector output and generates square waves required for RF switch control. We select ADG902 [16] for backscatter signal modulation.

B. BER, RSSI

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

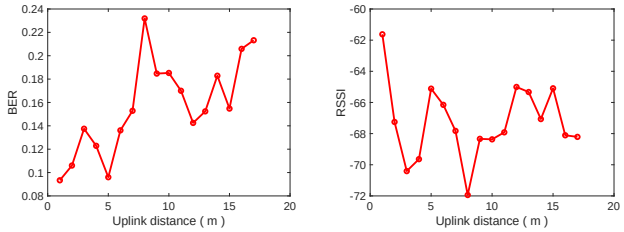


(a) Device connection.



(b) Experimental deployment.

Fig. 4. Experimental setup of the proposed ZigBee backscatter communication.



(a) BER (b) RSSI

Fig. 5. Performance of ZigBee backscatter communication.

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).

IV. Related Work

Backscatter communication is one of the enablers for building an ultra-low-power and ubiquitous IoT world [17] [18] [19] [20]. Researchers have shown that ambient signals (Wi-Fi, ZigBee, LTE, BLE, etc.) can be used for backscatter communication [1] [6] [21] [22] [23]. Further, Many studies are looking into its practical applications [24] [25] [26]. Related works have shown symbol-level backscatter for Wi-Fi communication [27] [28] [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

[1] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R Smith. Passive wi-fi: Bringing low power to wi-fi transmissions. In *Proc. of USENIX NSDI*, 2016.

[2] Xiuzhen Guo, Longfei Shangguan, Yuan He, Jia Zhang, Haotian Jiang, Awais Ahmad Siddiqi, and Yunhao Liu. Aloba: Rethinking on-off keying modulation for ambient lora backscatter. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, SenSys '20, page 192–204, New York, NY, USA, 2020. Association for Computing Machinery.

[3] Yao Peng, Longfei Shangguan, Yue Hu, Yujie Qian, Xianshang Lin, Xiaojiang Chen, Dingyi Fang, and Kyle Jamieson. PLoRa: A passive long-range data network from ambient LoRa transmissions. In *Proc. of ACM SIGCOMM*, 2018.

[4] Bryce Kellogg, Aaron Parks, Shyamnath Gollakota, Joshua R Smith, and David Wetherall. Wi-Fi backscatter: Internet connectivity for RF-powered devices. In *Proc. of ACM SIGCOMM*, 2014.

[5] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. Hitchhike: Practical backscatter using commodity wifi. In *Proc. of ACM SenSys*, 2016.

[6] Pengyu Zhang, Colleen Josephson, Dinesh Bharadia, and Sachin Katti. Freerider: Backscatter communication using commodity radios. In *Proc. of ACM CONEXT*, 2017.

[7] Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low rate wireless personal area networks (wpans). *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, pages 1–320, 2006.

[8] John Notor, Anthony Caviglia, and Gary Levy. Cmos rfic architectures for ieee 802.15. 4 networks. *Cadence Design Systems, Inc*, 41, 2003.

[9] https://www.ti.com/product/CC2420.

[10] Fengyuan Zhu, Yuda Feng, Qianru Li, Xiaohua Tian, and Xinbing Wang. Digiscatter: efficiently prototyping large-scale ofdma backscatter networks. In *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*, pages 42–53, 2020.

[11] https://www.ettus.com/all-products/un210-kit/.

[12] https://www.ti.com/product/CC2650.

[13] https://www.microchip.com/en-us/development-tool/ATMEGA256RFR2-XPRO.

[14] Zhijun Li and Yongrui Chen. Achieving universal low-power wide-area networks on existing wireless devices. In *2019 IEEE 27th International Conference on Network Protocols (ICNP)*, pages 1–11. IEEE, 2019.

[15] Ad8313 datasheet. https://www.analog.com/cn/products/ad8313.html .

[16] Adg902 datasheet. https://www.analog.com/en/products/adg902.html .

[17] Anran Wang, Vikram Iyer, Vamsi Talla, Joshua R. Smith, and Shyamnath Gollakota. FM backscatter: Enabling connected cities and smart fabrics. In *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17)*, pages 243–258, Boston, MA, March 2017. USENIX Association.

[18] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R. Smith, and Shyamnath Gollakota. Lora backscatter: Enabling the vision of ubiquitous connectivity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 1(3), September 2017.

[19] Xin Liu, Zicheng Chi, Wei Wang, Yao Yao, Pei Hao, and Ting Zhu. Verification and redesign of OFDM backscatter. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, pages 939–953. USENIX Association, April 2021.

[20] Vincent Liu, Vamsi Talla, and Shyamnath Gollakota. Enabling instantaneous feedback with full-duplex backscatter. In *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking*, MobiCom '14, page 67–78, New York, NY, USA, 2014. Association for Computing Machinery.

[21] Zicheng Chi, Xin Liu, Wei Wang, Yao Yao, and Ting Zhu. Leveraging ambient lte traffic for ubiquitous passive communication. In *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication*, SIGCOMM '20, page 172–185, New York, NY, USA, 2020. Association for Computing Machinery.

[22] Joshua F. Ensworth and Matthew S. Reynolds. Ble-backscatter: Ultralow-power iot nodes compatible with bluetooth 4.0 low energy (ble) smartphones and tablets. *IEEE Transactions on Microwave Theory and Techniques*, 65(9):3360–3368, 2017.

[23] Mohammad Hossein Mazaheri, Alex Chen, and Omid Abari. Mmtag: A millimeter wave backscatter network. In *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*, SIGCOMM '21, page 463–474, New York, NY, USA, 2021. Association for Computing Machinery.

[24] Lonzhi Yuan, Can Xiong, Si Chen, and Wei Gong. Embracing self-powered wireless wearables for smart healthcare. In *2021 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 1–7, 2021.

[25] Furqan Jameel, Ruifeng Duan, Zheng Chang, Aleksi Liljemark, Tapani Ristaniemi, and Riku Jantti. Applications of backscatter communications for healthcare networks. *IEEE Network*, 33(6):50–57, 2019.

[26] Chenren Xu, Lei Yang, and Pengyu Zhang. Practical backscatter communication systems for battery-free internet of things: A tutorial and survey of recent research. *IEEE Signal Processing Magazine*, 35(5):16–27, 2018.

[27] Manideep Dunna, Miao Meng, Po-Han Wang, Chi Zhang, Patrick Mercier, and Dinesh Bharadia. Syncscatter: Enabling wifi like synchronization and range for wifi backscatter communication. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, pages 923–937. USENIX Association, April 2021.

[28] Bryce Kellogg, Aaron Parks, Shyamnath Gollakota, Joshua R Smith, and David Wetherall. Wi-fi backscatter: Internet connectivity for rf-powered devices. In *Proceedings of the 2014 ACM Conference on SIGCOMM*, pages 607–618, 2014.