Poster: Enhanced ZigBee Backscatter Communication using Fine-Grained Chip-Level Modulation

Shixin Wang
University of Science and Technology of China
shixinwang@mail.ustc.edu.cn

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

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

ABSTRACT

Codeword translation is well-known for translating excitation signals into other codewords to provide productive ZigBee backscatter. But the limited throughput of conventional systems using info-rich codewords to transmit a single bit challenge their effectiveness to perform sensor-data transmission. In this paper, we introduce ChipScatter, a novel high-throughput modulation technology that translates excitation codewords into more controllable codewords through fine-grained chip-level modulation. The more controllable categories available, the more bits can be transmitted simultaneously. Evaluation results show that ChipScatter can increase the throughput of productive ZigBee backscatter by up to 8×.

CCS CONCEPTS

• **Networks** → **Sensor networks**; **Network design principles**.

KEYWORDS

Backscatter, ZigBee, Internet of Things

ACM Reference Format:
Shixin Wang, Zhaoyuan Xu, and Wei Gong. 2023. Poster: Enhanced ZigBee Backscatter Communication using Fine-Grained Chip-Level Modulation. In *The 21st Annual International Conference on Mobile Systems, Applications and Services (MobiSys '23), June 18–22, 2023, Helsinki, Finland.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3581791.3597368

1 INTRODUCTION

Ambient backscatter has attracted significant attention in recent years[1][2][3]. It eliminates the need for generating power-expensive RF signals locally and instead modulates tag data over ambient excitations, such as WiFi, ZigBee, Bluetooth, LoRa, etc. This significantly reduces the power consumption of the tags. For example, FreeRider[3] employs codeword translation to converts multiple codewords from ambient excitations into other codewords to provide productive ZigBee backscatter. Multiscatter[2] realizes codeword translation in a single data stream, enabling a single receiver to decode the tag data. Further, SyncScatter[1] focuses on the synchronization problem during tag modulation, which further improves the backscatter reliability. In a word, codeword translation is a key technique that facilitates the advancement of ambient backscatter communication.

Codeword translation works as follows: when a tag needs to send a bit 1, it converts the original codeword in the excitation signal into other codewords from the same codebook, while the excitation signal remains unchanged when sending a bit 0. The receiver decodes the tag data by performing an XOR operation on the excitation and backscattered codeword. Specifically, to modulate bit 1, FreeRider[3] achieves ZigBee backscatter by applying a 180° phase shift to eight consecutive symbols. According to IEEE 802.15.4, every 4 data bits are embedded into 1 symbol, which means that 32 ZigBee data bits are used to transmit 1 bit of tag data during codeword translation. However, this also results in a 32x decrease in backscatter throughput and is a waste of excitation resources.

In this paper, we propose ChipScatter, a novel chip-level modulation technology to enhance the throughput of ZigBee backscatter. **By applying a specific phase shift sequence at the chip-level for each excitation symbol based on the tag data, ChipScatter ensures that the excitation symbol is translated into controllable symbols. This allows for up to 16 controllable categories and up to 4 tag bits within each backscatter symbol.** As a result, the symbols demodulated by the receiver correspond to different tag data, allowing more data to be transmitted in a single transmission.

2 SYSTEM DESIGN AND RESULTS

2.1 ZigBee primer

ZigBee employs offset quadrature phase shift keying (OQPSK) modulation to encode data. As shown in Fig. 1, every 4 data bits are mapped to a single symbol composed of 32 pseudo-noise (PN) chips. These chips are split into two branches: odd-indexed chips modulated onto an in-phase component (I), while even-indexed chips modulated onto a quadrature-phase component (Q). The Q branch incorporates a half-chip delay to reduce peak-to-average power ratio (PARP). After passing through a pulse-shaping filter, a half-sinusoidal signal is generated and transmitted through an RF antenna.

2.2 Fine-grained Chip-level modulation

The idea being explored is whether one chip can be transformed into another through tag modulation. Our simulations on MATLAB show that this is indeed possible. Specifically, by applying a phase modulation of π to the tag, we can transform chip 0 into chip 1, and vice versa. On the other hand, a phase modulation of 0 will keep the chip unchanged. As a symbol consists of 32 chips, we can control the value of the chip by controlling the value of the symbol. This is a fine-grained modulation scheme at the chip level that

*Corresponding author: Wei Gong.

MobiSys '23, June 18–22, 2023, Helsinki, Finland

ACM ISBN 979-8-4007-0110-8/23/06
https://doi.org/10.1145/3581791.3597368

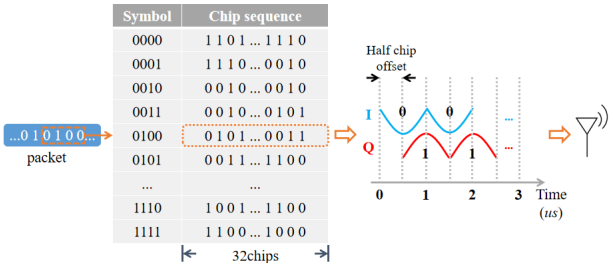


Figure 1: ZigBee signal generation.

we propose, which modulates one symbol into a specific symbol through a tag-specified phase modulation process.

Table 1: Tag bits-to-phase mapping

Tag bits	Phase										
0000	0	0	0	0	0	...	0	0	0	0	0
0001	0	0	π	π	0	...	0	π	π	0	0
0010	π	π	π	π	0	...	π	π	π	0	0
0011	π	π	π	π	π	...	π	π	0	π	π
...	...										
1100	π	π	0	π	π	...	π	π	0	0	0
1101	π	0	π	π	π	...	0	0	π	π	π
1110	0	π	0	0	π	...	0	0	0	π	0
1111	0	0	0	π	0	...	π	0	π	π	0

For instance, if we want to modulate symbol 0 into symbol 1, we can achieve this through the tag's phasing process. Since their first chip has a value of 1 and a phase difference of 0, we only need to set the tag's phase modulation to 0. The second chip also has the same value and phase difference, so we still set the phase modulation to 0. However, the value of the third chip is different, with a phase difference of π. Therefore, we need to set the tag's phase modulation to π. We can repeat this process for the remaining chips, thereby modulating symbol 0 into symbol 1. Thence, based on this approach, we can create a modulation table, as shown in Table 1, which we can use to modulate symbol 0 into other specified symbols.

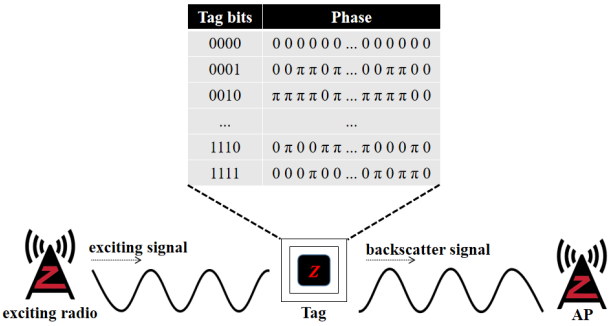
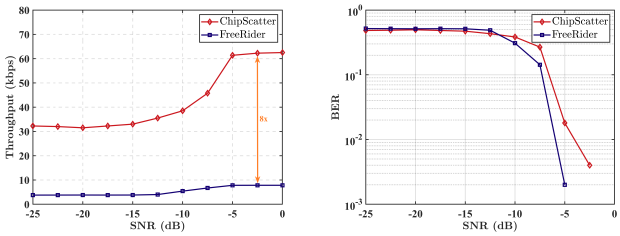


Figure 2: System overview.

Our system uses ZigBee's 16 available symbols to transmit tag data that consists of multiple bits. Fig. 2 provides an overview of the system. The exciting radio sends a known sequence of all 0s, which the tag modulates into one of the 16 symbols using phase modulation. Specifically, the tag performs modulation with reference to Table 1 and selects an appropriate modulation process according to the data to be sent (e.g., 0001). The tag then generates a backscatter signal by modulating the received signal accordingly (e.g., 0, 0, π, π, 0, π, 0, 0, ...). When the backscatter signal reaches the receiver, the corresponding symbol is decoded, allowing the receiver to determine the tag data being sent (in this case, 0001).

2.3 Evaluations

We compared our system's throughput and bit error rate (BER) with FreeRider. In order to tradeoff throughput and BER, we used four symbols to transmit four bits of tag data. **The results obtained, as shown in Fig. 3a, our system achieved a significant 8× increase in throughput over FreeRider, peaking at 60 kbps.** The BER, as shown in Fig. 3b, remained lower than 1.8% when the signal-to-noise ratio (SNR) exceeded -5. The results show that the BER of our system is slightly higher than that of FreeRider. The reason behind this is that our system requires a more refined modulation process to achieve the specified symbol compared to FreeRider. Nevertheless, the difference in BER is not significant and remains within an acceptable range.



(a) Throughput **(b) BER**

Figure 3: Throughput, BER performance under different SNR.

3 CONCLUSION

We introduced ChipScatter, a high-throughput ZigBee backscatter system. Specifically, ChipScatter delivers an 8× improvement in throughput while maintaining a similar bit error rate with FreeRider. This breakthrough technology opens up new opportunities for ZigBee backscatter applications.

4 ACKNOWLEDGEMENT

We thank the anonymous reviewer for the helpful comments. This work was supported by NSFC Grant No. 61932017 and 61971390.

REFERENCES

[1] M. Dunna, M. Meng, P. Wang, C. Zhang, P. Mercier, and D. Bharadia. 2021. SyncScatter: Enabling WiFi like synchronization and range for WiFi backscatter Communication. In *Proc. of USENIX NSDI.*
[2] W. Gong, L. Yuan, Q. Wang, and J. Zhao. 2020. Multiprotocol backscatter for personal IoT sensors. In *Proc. of ACM CONEXT.*
[3] P. Zhang, C. Josephson, D. Bharadia, and S. Katti. 2017. Freerider: Backscatter communication using commodity radios. In *Proc. of ACM CONEXT.*