ZeroScatter-LoRa: Microcontrollers are RFIDs

Shayan Majumder
School of Eng. & Phys. Sciences
Heriot-Watt University
Edinburgh, Scotland, UK
sm3054@hw.ac.uk

Matthew S. Reynolds
Dept. of Electrical & Computer Eng.
University of Washington
Seattle, WA, USA
msreynol@ece.uw.edu

Stylianos D. Asimonis
Dept. of Electrical & Computer Eng.
University of Patras
Patras, Greece
s.asimonis@upatras.gr

Sandeep Joshi
Dept. of Electrical & Electronics Eng.
Birla Institute of Technology And Science
Pilani, Rajasthan, India
sandeep.joshi@pilani.bits-pilani.ac.in

George Goussetis
School of Eng. & Phys. Sciences
Heriot-Watt University
Edinburgh, Scotland, UK
g.goussetis@hw.ac.uk

Spyridon N. Daskalakis
School of Eng. & Phys. Sciences
Heriot-Watt University
Edinburgh, Scotland, UK
s.daskalakis@hw.ac.uk

***Abstract*—ZeroScatter-LoRa is an all-digital and zero-added-component technique for Long Range (LoRa) backscatter communication using commodity Microcontroller Units (MCUs). Instead of using traditional Radio Frequency (RF) switches for impedance modulation, it utilizes existing digital peripheral pins of ultra-low-power MCUs, such as Inter-IC Sound (I^2S), Serial Peripheral Interface (SPI), or Inter-Integrated Circuit (I^2C), to produce LoRa chirp signals using logic-level changes. We show backward compatibility of ZeroScatter-LoRa with commercial LoRa Wide Area Network (LoRaWAN) gateways in multipath-rich indoor environments with an average power consumption of $9.8\ \mu$A. The results show that the monostatic configuration using Universal Software Radio Peripheral (USRP) in full duplex mode has an achievable range of 2.5 m, and the bistatic configuration using a single-tone generator at a distance of 2 m (transmitter-to-tag) has valid packet reception of more than 20 m (tag-to-receiver). The technique is applicable to billions of existing MCUs using high-speed digital interfaces. The long range that is achieved using MCU pins for backscatter communication also suggests that security risks may be present in existing digital systems if digital I/O lines are not electromagnetically shielded from outside signals.**

***Index Terms*—Backscatter, Chirp Spread Spectrum (CSS), Internet of Things (IoT), Long Range (LoRa) modulation, Radio-Frequency IDentification (RFID), ZeroScatter**

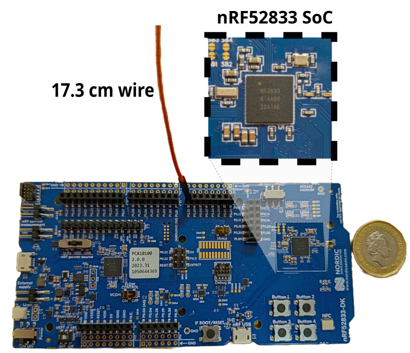


Fig. 1: Photo of the ZeroScatter-LoRa prototype based on the Nordic Semiconductors nRF52833 development kit.

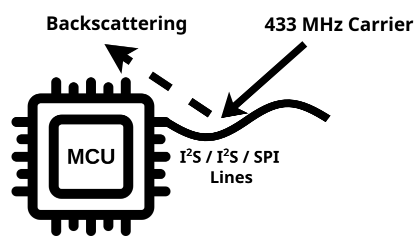


Fig. 2: Schematic of the ZeroScatter-LoRa prototype.

I. Introduction

Harry Stockman's seminal work [1] in 1948 constituted one of the first systematic efforts to develop the theoretical foundations of backscatter communications. This allows devices to communicate wirelessly by reflecting the incoming radio waves, rather than generating their own carrier. Backscatter communications has revolutionized the world of wireless communication since its creation, allowing billions of passive Radio-Frequency Identification (RFID) devices to function without the need for expensive transmission components.

In traditional backscatter systems [2], signal modulation is achieved through impedance modulation circuits that use Radio Frequency (RF) switches, diodes, or transistors to dynamically change the impedance of the connected antennas. Despite the effectiveness of the method, it is also characterized by considerable design complexity that involves impedance matching, impedance modulation circuitry, and the design of the antennas. All these factors increase the cost and complexity of the manufacturing process.

Significant advancements have been made in long range (LoRa) backscatter technology to enable passive communication over a wide area network. For example, the foundational work by Vamsi Talla et al. on LoRa Backscatter [3] showed that this technology can achieve ranges up to 2.8 km with the tag placed 475 m from the carrier source. Similarly, LoRAB [4] utilized ambient Frequency Modulation (FM) broadcast signals to achieve a range of 130 meters. All these works show the potential of LoRa backscatter to achieve long range while maintaining low power consumption.

Parallel efforts have explored RF transmissions from Microcontrollers (MCUs) in the absence of radio hardware. EMLoRa [5] utilizes memory-based electromagnetic radiation and LoRa chirps to achieve transmission distances of hundreds of meters, while LolRa [6] utilizes Inter-IC Sound (I^2S) and Serial Peripheral Interface (SPI) peripherals for transmitting LoRa packets with distances of over 2.5 km using harmonics. However, the use of high-frequency harmonics and high-speed clocking is a limitation in terms of energy efficiency and practicability.

TABLE I: Comparison of ZeroScatter Approaches

Parameter	**ZeroScatter [7]**	**ZeroScatter-BLE [8]**	**ZeroScatter-LoRa (This Work)**
Platform	MCU (PIC12LF1552)	FPGA (iCE40HX1k)	MCU (nRF52833)
Modulation	BPSK	FSK	CSS
Range @ carrier power (dBm)	3 m (monostatic) @ +10 dBm	4 m (bistatic) @ +30 dBm	2.5 m (monostatic), 20 m (bistatic) @ +13.5 dBm (monostatic) @ +10 dBm (bistatic)
Power Consumption	628 µA	Not reported	9.8 µA

University of Washington's seminal work on Zero-Added-Component Backscatter (ZeroScatter) [7] [8] [9] revealed that the current input/output (I/O) pins of commercial Field-Programmable Gate Arrays (FPGAs)/MCUs are able to perform backscatter without the use of external switches. Table I further provides a general comparison of the above approaches in relation to our work.

This work proposes ZeroScatter-LoRa that exploits the use of commonly used digital interfaces like Inter-Integrated Circuit (I^2C), SPI and I^2S, for performing LoRa backscatter. We show that commodity MCUs, available in billions of devices, can be used as RFIDs for wireless communications, while also highlighting the important security implications for digital systems. Figure 1 shows the implemented tag, and Fig. 2 shows the system schematic.

II. Implementation Overview

The Nordic Semiconductor nRF52833 System-on-Chip (SoC) is chosen as the primary processing device due to its ultra-low-power characteristics, such as deep sleep current consumption below 1 µA. Although the nRF52833 includes on-chip RF transceiver functions, these functions are not used in this work. This chip supports an I^2S interface with a variable sampling rate of up to 16 MHz, providing the flexibility to generate chirps with different Spreading Factors (SFs) and Bandwidths (BWs), similar to the approach adopted in LoRAB 2.0 [10] and NoLoRa [11]. A LoRa up-chirp is a linearly frequency-swept signal that sweeps from $f_c - BW/2$ to $f_c + BW/2$ over one symbol period of $2^{SF}/BW$ seconds. This analog waveform is pre-computed offline and quantized to a 1-bit binary sequence, forming a lookup table

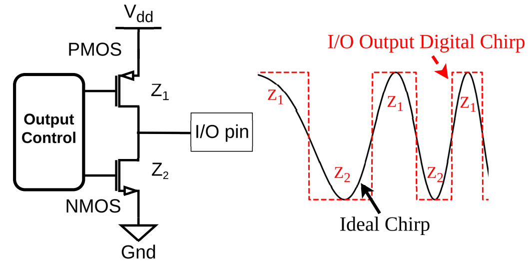
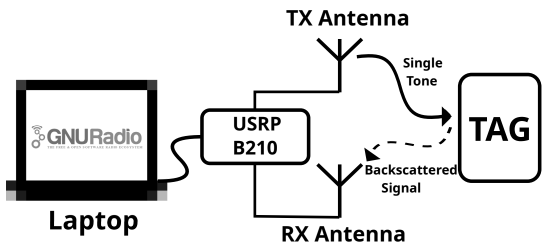


Fig. 3: Typical I/O pin structure for output mode (left) and the resulting modulating digital square-wave control signal sampled from the analog LoRa chirp waveform (right).

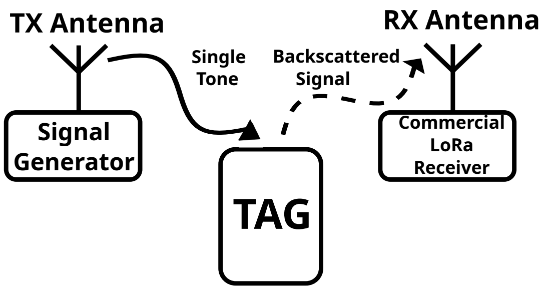
of digital square-wave samples stored in flash memory. The SF and BW together determine both the table length and the required I^2S clock rate, with higher SF values producing longer tables at lower clock frequencies. Despite the coarse 1-bit quantization, the instantaneous frequency trajectory of the chirp is preserved, enabling commercial LoRa receivers to successfully correlate and decode the backscattered signal. During the transmission of the chirps, the data is sent out serially through the I^2S data line, while the Central Processing Unit (CPU) is in a sleep state for most of the time. The Direct Memory Access (DMA) controller transfers the samples of the lookup table to the I^2S peripheral, which significantly contributes to the ultra-low-power characteristics of the device.

Figure 3 (left) shows the typical I/O pin schematic in output mode of an MCU. The sampled digital square-wave of the control signal as shown in the Fig. 3 (right) is directly applied to the I/O pin. In other words, the I/O pin is modulated between two levels, high (PMOS) and low (NMOS). These transistors vary the impedance of the transmission line between the two levels, Z_1 and Z_2. While measuring the exact values of Z_1 and Z_2 is quite challenging with the current evaluation board, we are designing a dedicated board to enable precise impedance characterization. This impedance variation thus generates the baseband modulation required for the backscatter technique. As seen in Fig. 1, a quarter-wavelength matched wire antenna with a length of 17.3 cm (optimal for 433 MHz) is directly connected to the required I/O port which reflects the carrier with the modulated signal.

The 433 MHz ISM band is selected as the carrier frequency due to its lower free-space path loss compared to higher LoRa bands (868 MHz and 915 MHz), favorable indoor multipath propagation, and broad support across commercial LoRaWAN infrastructure. A quarter-wavelength wire monopole is used for its near-resonant impedance at this frequency and its omnidirectional azimuthal radiation pattern, which maximizes coverage without requiring beam alignment. Critically, no impedance matching network is placed between the I/O pin and the antenna. The deliberate mismatch between the pin output impedance and the antenna load is the fundamental mechanism behind the backscatter operation: as the I/O pin alternates between its high (PMOS) and low (NMOS) states, the reflection coefficient at the antenna port is modulated, re-

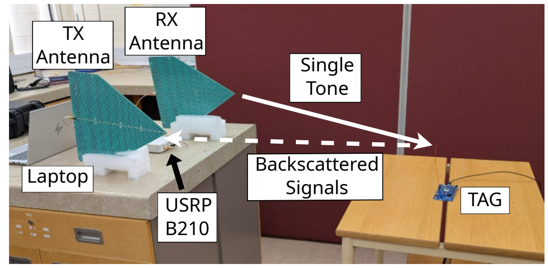


(a)

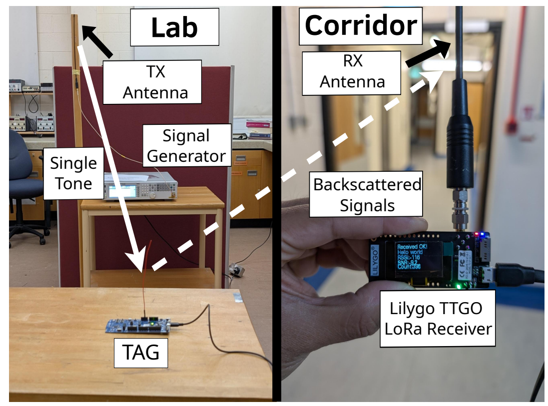


(b)

Fig. 4: Experimental setup block diagrams. (a) Monostatic: USRP B210 transmits and receives. (b) Bistatic: Separated signal generator and LoRa receiver.



(a)



(b)

Fig. 5: Experimental setup. (a) Monostatic: USRP B210 with antennas and tag in single room. (b) Bistatic: Signal generator and tag in one room, LoRa receiver in separate room across corridor.

radiating the incident carrier signal encoded with the LoRa chirp.

Experiments are conducted in both monostatic and bistatic configurations (Fig. 4, Fig. 5). In the monostatic setup (Fig. 4a, Fig. 5a), the transmitter and receiver are co-located using a USRP B210 SDR operating in full-duplex mode, with GNU Radio and MATLAB-based LoRa decoders. Ultra-wideband log-periodic antennas (Sevskiy AN220213-01C) cover 370–6000 MHz with 4.5–5 dBi gain and 65–80% efficiency. With TX and RX antennas placed 50 cm apart and oriented toward the tag, the measured inter-antenna isolation (S21/S12) at 433 MHz as shown in Fig. 6, is approximately -63 dB. The TX antenna transmits a 433 MHz CW carrier at $+13.5$ dBm, which is backscattered by the tag and captured by the RX antenna.

In bistatic configuration as shown in Fig. 4b and Fig. 5b, there is spatial separation between the carrier source and receiver. In this configuration, the signal generator is placed at a distance of 2 meters from the tag. It transmits a single-tone CW at 433 MHz with an output power of +10 dBm. The backscattered signals are captured using a commercial LoRa Wide Area Network (LoRaWAN) receiver (LilyGo TTGO LoRa). This receiver, based on Semtech SX1276 chip, has an exceptionally low noise floor of around -140 dBm. The bistatic configuration generally gives longer communication ranges compared to monostatic configurations due to several factors. First, the receiver is placed in a position to receive the strongest signal, not limited to the carrier source. Second, in bistatic configuration, there is less interference between the carrier signal and backscattered signals, which is a major problem in monostatic configurations. Third, in bistatic configurations, both forward and backward links can be independently optimized, which is not possible in monostatic configurations.

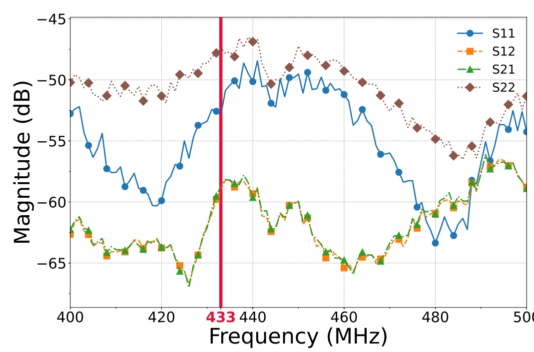


Fig. 6: Measured S-parameters of the two-antenna monostatic setup (400–500 MHz).

III. Power Consumption and Results

The energy efficiency of the proposed system was evaluated by measuring the current consumption of the tag using an nRF Power Profiler II at 1.8 V. With a fixed duty cycle of 1% active transmission time as recommended by official LoRa guidelines [12], the proposed system is able to achieve an average current consumption of 9.8 µA (17.6 µW) irrespective of the SF used, representing approximately 6 times lower

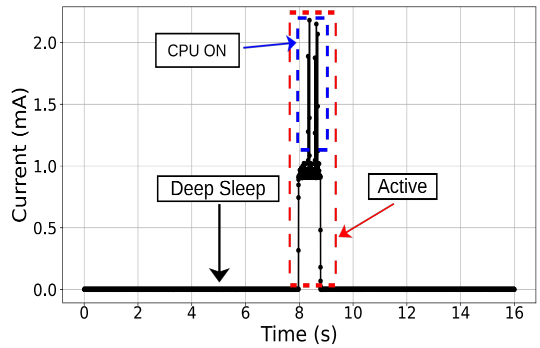


Fig. 7: Current consumption profile showing active transmission and deep sleep periods of the nRF52833 tag measured at 1.8 V.

power consumption (at 0 dBm and 1% duty cycle: 60 µA) compared to the chip's active BLE transmission at similar duty cycle. The fixed duty cycle ensures the proposed system can operate at an efficient level with minimal channel congestion due to simultaneous transmissions of multiple nodes. As seen in Fig. 7, the current consumption of the proposed system is in the range of nA during the deep sleep mode, while the sudden bursts in maximum current consumption are due to the waking up of the CPU to prepare the memory buffers for transmission. The autonomous transmission capability of the proposed system is due to the use of the DMA-controlled I^2S peripheral, allowing the CPU to be in sleep mode during the active transmission period.

The achievable communication range in a backscatter system is governed by the two-way path loss of the link. In the monostatic configuration, the received backscatter power follows a fourth-power range dependence ($\propto R^{-4}$), since the carrier must travel from the reader to the tag and back over the same distance R. In contrast, the bistatic configuration decouples the forward link (carrier source to tag, distance R_1) from the backward link (tag to receiver, distance R_2), yielding a combined path loss proportional to $R_1^{-2}R_2^{-2}$ rather than R^{-4}. When the carrier source is placed close to the tag ($R_1 \ll R_2$), this geometry can achieve significantly longer tag-to-receiver ranges for the same transmit power, directly explaining the order-of-magnitude improvement in range observed between the two configurations.

In the monostatic configuration, the maximum range obtained was 2.5 m indoors using a +13.5 dBm carrier signal at 433 MHz and successful packets were decoded at this distance with a Signal-to-Noise Ratio (SNR) of -2.5 dB. In the packet configuration, SF 8 was used, with 10 kHz BW and 4:8 Coding Rate (CR). The measured range is limited mainly due to the higher noise floor of the USRP software-defined radio device compared to the noise floor of the commercially available LoRa receivers. The full-duplex capability of the USRP B210 device also suffers from self-interference and carrier leakage, which reduces the receiver sensitivity and the range in the monostatic configuration.

In contrast, the bistatic configuration showed improved performance, with the maximum range being greater than 20 m in an indoor environment with a +10 dBm carrier signal at 433 MHz placed 2 m away from the tag. The valid packets were successfully decoded with an SNR of -9.2 dB using the transmission configuration SF 8, 125 kHz BW, and 4:8 CR. The reception was done using the LilyGo TTGO LoRa receiver, which has a significantly better noise floor than the USRP. Notably the bistatic configuration showed robust wall penetration capabilities, with the signals transmitted from inside the laboratory being received in the corridor.

In addition, it was noted that different I/O pins exhibited different backscatter performances. This is mainly due to differences in internal switch configuration and printed circuit board (PCB) trace routing in the MCU development board. Systematic pin selection based on impedance characterization is therefore expected to yield further improvements in backscatter efficiency and achievable range.

IV. Conclusion and Future Work

This paper presents ZeroScatter-LoRa, an all-digital, zero-added-component technique for LoRa backscatter communication that repurposes existing digital peripheral interfaces like I^2S, SPI, and I^2C of commodity MCUs as backscatter radiators. The approach eliminates dedicated RF switches and impedance matching networks, is deployable through firmware-only modifications, and is backward compatible with commercial LoRaWAN infrastructure.

Experimental evaluation in an indoor multipath environment demonstrated an average power consumption of 9.8 µA (17.6 µW) at 1.8 V under a 1% duty cycle which is approximately 6× lower than active BLE transmission at the same duty cycle. The monostatic configuration achieved a range of 2.5 m (SNR of −2.5 dB, +13.5 dBm carrier), while the bistatic configuration extended this to greater than 20 m (SNR of −9.2 dB, +10 dBm carrier with the tag 2 m from the source), including successful wall-penetrating reception across a corridor. These results confirm the viability of ZeroScatter-LoRa as a practical, ultra-low-power RFID-like communication method applicable to the billions of MCUs already deployed worldwide.

Beyond IoT utility, this work reveals an important and previously understudied security implication: standard digital I/O lines can act as inadvertent sub-GHz backscatter radiators, enabling covert communication channels in systems considered electromagnetically secure. Unlike existing electromagnetic security concerns that target high-frequency harmonics, ZeroScatter-LoRa operates near the fundamental frequency of common digital peripherals, representing a new threat vector that warrants attention from system designers.

Future work will focus on a custom PCB design with integrated solar energy harvesting for battery-free operation, VNA-based impedance characterization of individual I/O pin types, and comprehensive indoor and outdoor range evaluation across varying spreading factors and environmental conditions.

References

[1] H. Stockman, "Communication by Means of Reflected Power," *Proc. IEEE IRE*, vol. 36, no. 10, pp. 1196–1204, Oct. 1948.

[2] R. Torres, R. Correia, N. B. Carvalho, S. Daskalakis, G. Goussetis, Y. Ding, A. Georgiadis, A. Eid, J. Hester, and M. M. Tentzeris, "Backscatter communications," *IEEE Journal of Microwaves*, vol. 1, no. 4, pp. 864–878, 2021.

[3] V. Talla, M. Hessar, B. Kellogg, A. Najafi, J. R. Smith, and S. Gollakota, "LoRa backscatter: Enabling The vision of Ubiquitous Connectivity," in *Proc. ACM Int. joint Conf. on Pervasive and Ubiq. Comp.*, Orlando, Florida, USA, Sep. 2017.

[4] S. N. Daskalakis, A. Georgiadis, M. M. Tentzeris, G. Goussetis, and G. Deligeorgis, "The New Era of Long-Range "Zero-Interception" Ambient Backscattering Systems: 130 m with 130 nA Front-End Consumption," *MDPI Sensors*, vol. 22, no. 11, May 2022.

[5] C. Shen, T. Liu, J. Huang, and R. Tan, "When LoRa Meets EMR: Electromagnetic Covert Channels Can Be Super Resilient," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 1304–1317.

[6] C. Lohr, "LolRa: Transmit LoRa frames without a radio," GitHub, 2025, accessed: Jan. 27, 2026. [Online]. Available: https://github.com/cnlohr/lolra.

[7] A. Dadkhah, J. Rosenthal, and M. S. Reynolds, "ZeroScatter: Zero-Added-Component Backscatter Communication Using Existing Digital I/O Pins," in *2019 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*. IEEE, 2019, pp. 1–3.

[8] S. M. Reyes, C. Fong, J. D. Rosenthal, and M. S. Reynolds, "ZeroScatter BLE: All-Digital, Fully Synthesizable Bluetooth Low Energy (BLE) Backscatter Communication in Verilog RTL for FPGA-Based Devices," in *2024 IEEE International Conference on RFID (RFID)*. IEEE, 2024, pp. 7–10.

[9] J. D. Rosenthal, S. Reyes, and M. S. Reynolds, "An All-Digital, Fully Synthesizable Wireless Analog Voltage Telemetry Sensor Tag Using ZeroScatter Bluetooth Low Energy (BLE) Backscatter," in *2025 IEEE International Conference on RFID Technology and Applications (RFID-TA)*. IEEE, 2025, pp. 1–4.

[10] S. Majumder, C. Lohr, J. Birk, M. M. Tentzeris, G. Goussetis, S. D. Asimonis, and S. Daskalakis, "All-Digital CSS Ambient Backscatter with 17.6 μW Power Consumption and a MISO Receiver," in *IEEE International MTT Symposia 2026: Revolutionizing RF*. IEEE, 2026.

[11] S. Majumder, J. Birk, C. Lohr, G. Goussetis, and S. Daskalakis, "NoLoRa: Ultra-Low-Power LoRa Transmissions Without Active Radios for Battery-Free Devices," in *20th European Conference on Antennas and Propagation 2026*. IEEE, 2026.

[12] LoRa Alliance Technical Committee, "LoRaWAN™ 1.0.3 Regional Parameters," LoRa Alliance, Inc., Tech. Rep. V1.0.3, Jul. 2018.