Backscattering Rectifier for Security and Identification in the context of Simultaneous Wireless Information and Power Transfer

Taki Djidjekh, Gaël Loubet, Lamoussa Sanogo, Alassane Sidibé, Guillaume Delai, Daniela Dragomirescu, Alexandru Takacs

Backscattering Rectifier for Security and Identification in the context of Simultaneous Wireless Information and Power Transfer

Taki E. Djidjekh [#$1], Gaël Loubet [#2], Lamoussa Sanogo [#3], Alassane Sidibé [#4], Guillaume Delai [$5], Daniela Dragomirescu [#6], Alexandru Takacs [#7]

[#]LAAS-CNRS, Université de Toulouse, CNRS, UPS, INSA ; 7, Avenue du Colonel Roche, 31400 Toulouse, France.
[$]Ogoxe ; 42, Avenue Gaspard Coriolis, 31100 Toulouse, France.
{[1]taki-eddine.djidjekh, [2]gael.loubet, [3]lamoussa.sanogo, [4]alassane.sidibe, [6]daniela.dragomirescu, [7]alexandru.takacs}@laas.fr,
[5]gdelai@ogoxe.com

***Abstract* — This article presents a proof-of-concept of an innovative security and identification mechanism for Internet of Things applications within the context of Simultaneous Wireless Information and Power Transfer. This easily integrable solution involves modifications only at the RF rectifier level of the wireless Sensing Node, enabling backscattering of the power source wave as a function of a digital private key. The wireless Sensing Node will be able to transmit identification information for a brief period. These details allow the power source system to identify the object and confirm its operational status. This mechanism adds an additional layer of security, independent and complementary of the communication protocol of the wireless Sensing Node.**

Keywords — Backscattering, Internet of Things (IoT), LoRaWAN, Simultaneous Wireless Information and Power Transfer (SWIPT), Wireless Power Transfer (WPT).

I. Introduction

In today's rapidly evolving landscape, the Internet of Things (IoT) has become ubiquitous across diverse sectors, including Structural Health Monitoring (SHM), healthcare monitoring, smart tracking, smart factory, and beyond. This proliferation of wirelessly interconnected devices has revolutionized how to monitor health, optimize industrial processes, and enhance daily life. However, with the increasing reliance on wireless communication within these systems, there emerges a significant vulnerability to cyber threats. The interconnected nature of IoT devices, coupled with their often insufficiently secured communication protocols, presents a challenge in safeguarding against potential attacks [1]. Several IoT protocols have evolved complex Medium Access Control (MAC) layers for authentication and cryptography to mitigate such attacks, as seen in LoRaWAN. However, they remain vulnerable to various cyber-attacks scenarios [2], [3]. Implementing these enhanced security layers into an IoT protocol requires additional computing resources and results in higher power consumption. Furthermore, integrating them into already operational IoT networks adds complexity to the process. In the context of Simultaneous Wireless Information and Power Transfer (SWIPT) and Wireless Power Transfer (WPT) [4], the protocols of IoT systems remain unchanged at the level of information transfer, while the power wave is only utilized for powering the wireless node.

This article presents the integration of a novel mechanism aimed at enhancing the security of IoT applications by using a Backscattering Rectifier (BR) for the WPT link within a network of autonomous wireless nodes in a SWIPT context. The concept was originally presented in a paper for the International Microwave Symposium (IMS) 2024 [5]. Here, we demonstrate the integration of this concept into a battery-less wireless Sensing Node (SN) to showcase its effectiveness.

II. WPT Security and Identification Concept within LoRaWAN Wireless Sensor Network

In a typical SWIPT Wireless Sensor Network (WSN), two different waves are employed to ensure wireless communication and Wireless Power Transfer functions. These WSN consist of multiple battery-free Sensing Nodes (SN) surrounding each Communicating Node (CN), with the CN interconnected in an ad-hoc mesh network.

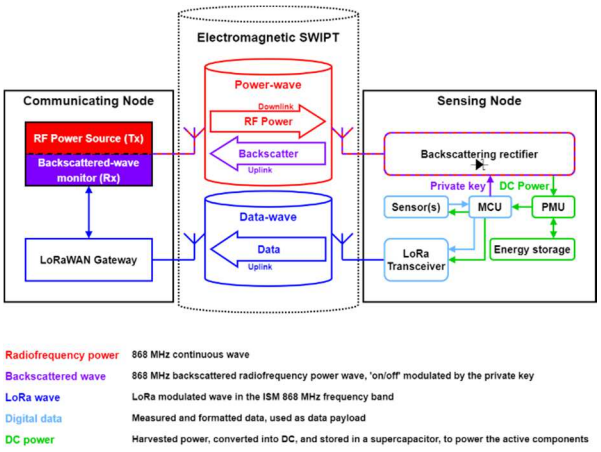

Fig. 1. Architecture of WPT Security and Identification Concept Integrated into LoRaWAN Wireless Sensor Network within a SWIPT context.

As presented in Fig. 1, the SN utilizes LoRaWAN data-waves as an uplink to transmit collected and formatted data to the nearest CN. The CN, particularly the RF power source driven by CN, generates a power-wave as a downlink to wirelessly power the surrounding SN. In this concept, the innovation lies in backscattering and modulating this power-

wave as an additional uplink from the SN, enabling its identification and enhancing the WSN security.

This solution is highly energy-efficient and seamlessly integrates with existing setups. It involves replacing only the standard SN rectifier with a BR, which can be controlled by the SN Microcontroller Unit (MCU). Additionally, the CN requires the addition of a Backscattered-wave monitor. Despite these adjustments, the power consumption of the SN remains virtually unchanged, with only minor software modifications needed to control the backscattering modulation via a private key command. To facilitate reception of the downlink Power-wave and transmission of the Backscattered-wave, as well as the uplink data transmission, two antennas (preferably operating with distinct polarizations) are used.

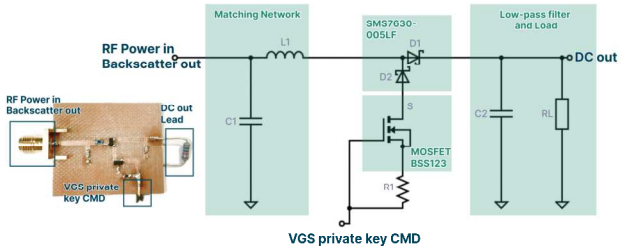

Fig.2. Backscattering Rectifier circuit.

As illustrated in Fig. 2, the proposed Backscattering Rectifier comprises: (i) LC matching network with L = 43 nH (LQW18AN inductor by Murata) and C = 3.3 pF, (ii) a diode pair in a single package (SMS7630-005LF by Skyworks Solutions Inc.), (iii) an N-channel MOSFET (BSS123 by ONSEMI) and (iv) an RC low pass filter (C2 = 100 pF).

The MOSFET operates in a diode-connected state, with a resistor R1 = 4 kΩ placed between the gate and drain. The source is connected to the anode of diode D2, while the drain-gate connection serves for control purposes. By adjusting the voltage applied to the gate (0 V or 3.3 V), the drain-source ON-resistance changes, affecting the flow of current through diode D2 and resistor R1. This manipulation effectively alters the impedance of the circuit, resulting in varying levels of reflection coefficient S_{11} at the input port of the rectifier. The circuit is optimized for energy harvesting when VGS CMD is set to 0 V (OFF) and for backscattering when VGS CMD is set to 3.3 V (ON).

Fig.3. illustrates the integration of the BR into a battery-free LoRaWAN Sensing Node developed beforehand in our laboratory [6] by disabling the existing rectifier. The DC output of BR was directly connected to the Power Management Unit (PMU) of the LoRaWAN SN while one of the General-Purpose Input/Output (GPIO) pins of SN MCU was employed to control the Command Voltage (CMD VGS) of BR MOSFET gate.

The BR can operate in two modes simultaneously: (i) the energy harvesting mode, where the BR charges the storage element of the SN via the PMU; and (ii) the backscattering mode, where the BR, driven by a private key provided by the SN, generates a digitally coded backscattered signal. The BR primarily operates in harvesting mode, with brief intervals in backscattering mode.

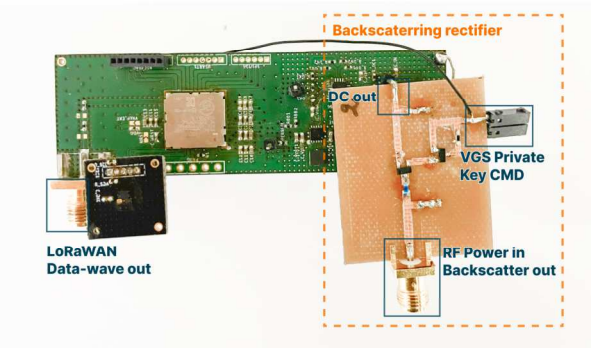

Fig.3. Backscattering Rectifier connected to LoRaWAN autonomous SN.

III. Experimental Results and Proof of Concept

The experiments were conducted in two stages. First, characterizing the performance of the BR. Second, integrating the BR into a LoRaWAN battery-free SN and conducting tests to prove the concept.

A. Characterization of the Backscattering Rectifier

The BR operates within the ISM 868 MHz band and was initially simulated using Advanced Design System (ADS) before being manufactured in our laboratory on standard 2-layer FR4 substrate with a thickness of 0.8 mm. Reflection coefficient measurements, conducted with a Vector Network Analyzer (VNA) (Anritsu MS4647A), show favorable matching conditions for efficient operation within the -20 dBm to -5 dBm input power range.

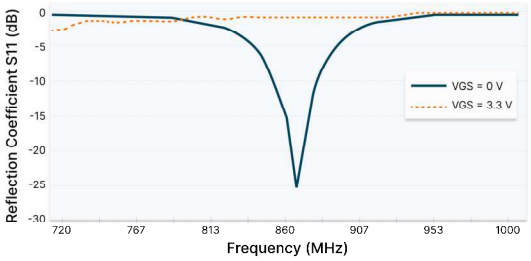

Fig.4. Measured Reflection Coefficient S11 at -10 dBm input power as function of the VGS command signal.

Fig. 4 illustrates the reflection coefficient at -10 dBm input power under two conditions: when VGS = 0 V, indicating the state when the MOSFET is off and the circuit input impedance is matched; and when VGS = 3.3 V, indicating the state when the MOSFET is conducting, altering the circuit impedance and leading to a mismatch.

Next, to conduct efficiency characterization, we utilized an RF signal generator (Anritsu MG3694B) directly connected to the RF input of the BR. The voltage across the load RL = 10 kΩ (representing the input impedance of the PMU) was measured with a high-precision multimeter (Keithley 2000). The experimental data were collected employing a custom automated tool developed in LabVIEW. The results of output voltage and efficiency at 868 MHz, shown in Fig. 5, demonstrate that when VGS=0V, the MOSFET is switched off, causing the diode D2 to float. Consequently, the BR performs RF to DC conversion as a half-wave rectifier, which explains

the low efficiency. Despite this, the BR provides the minimum threshold voltage required by our battery-free LoRaWAN sensor node at the lowest achievable RF input power (-8.5 dBm). Moreover, it achieves a conversion efficiency exceeding 17% across a wide dynamic range of input power.

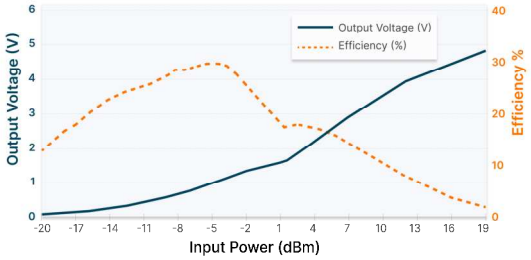

Fig.5. DC output voltage (blue line) and RF-to-DC power conversion efficiency (red dashed line) as function of RF input power with a 10 kΩ load.

To evaluate the backscattering performance of the BR, we utilized an RF signal generator (Anritsu MG3694B) as RF power source, a USB Spectrum Analyzer (Tektronix RSA306B) to receive the Backscattered-wave, and a waveform generator (Keithley 3390) to control the CMD VGS of the BR with a square signal. The experimentation occurred in a wireless environment within an anechoic chamber, employing two patch antennas with +9.2 dBi maximum gain each. One patch served for reception, connected to the spectrum analyzer, while the other connected to the BR. Additionally, the RF power source connected to a +2.5 dBi maximum gain monopole antenna. The distance between the BR antenna and the Power-wave monitoring system (RF power source and spectrum analyzer) antennas was 3.4 meters. All antennas operated with linear polarization. To minimize coupling between the power source and the spectrum analyzer antennas, we aligned the RF power source monopole antenna to ensure its radiation pattern's minimum was directed toward the spectrum analyzer receiving patch antenna. Fig. 6 illustrates the described setup.

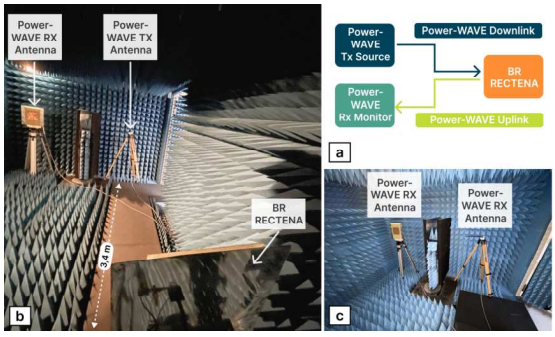

Fig.6. (a) Setup schematic diagram; (b) Photograph of the experimental setup: BR Rectenna (illuminated by Power-wave Tx and controlled by a PVK/waveform generator), the Rx backscattered Power-wave signal is monitored by the Spectrum Analyzer connected to Power-wave Rx antenna; (c) Zoom on Power-wave Tx and Rx antenna positioning.

Several measurements were conducted by varying the waveform generator's square signal frequency at the CMD VGS and the RF power source to test the backscattering dynamic range (difference between high and low state of the backscattered wave). The results demonstrated consistent performance with a stable dynamic range across different frequencies of the VGS CMD signal. Fig. 7 (a) illustrates the backscattered signal received in the spectrum analyzer at 100 kHz VGS CMD signal with a dynamic of 9.5 dB. Additionally, the decrease in dynamic range due to variations in source power did not exceed 1.5 dB, as shown in Fig.7 (b).

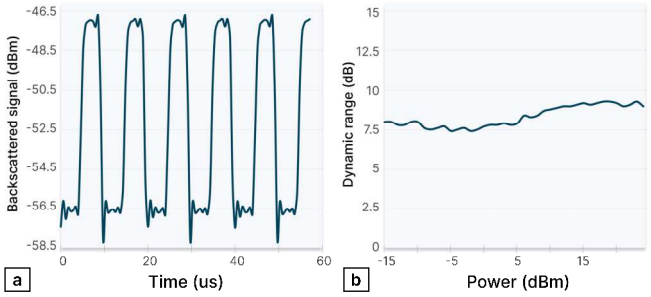

Fig.7. (a) Received backscattered signal displayed on spectrum analyzer for a modulating signal at VGS CMD of 100 kHz; (b) Signal dynamic range as a function of RF source radiated power.

B. Characterization of the Backscattering Rectifier integrated to battery-free LoRaWAN Sensing Node in a real-world environment.

In this setup, the battery-free LoRaWAN SN with the BR integrated as illustrated in Fig. 3 was tested in a real-world environment outside the confines of the anechoic chamber, specifically within the manipulation room of the laboratory. The SN utilized two antennas: a +9.2 dBi maximum gain patch antenna (Tx) with horizontal linear polarization for the WPT link at 1.61-meter distance from the backscattering monitor system (Power Source and Spectrum Analyzer), and a monopole antenna (Rx) with a +2.5 dBi gain for the LoRaWAN communication link, featuring vertical linear polarization to minimize coupling. To ensure isolation of the WPT emission and reception, the Power Source and the Spectrum Analyzer were connected to the same +9.2 dBi patch antenna via a RF circulator (Aerotek C11-1FFF). This setup was carried out to allow operation by segregating the power downlink wave from the backscattered wave as illustrated in Fig. 8.

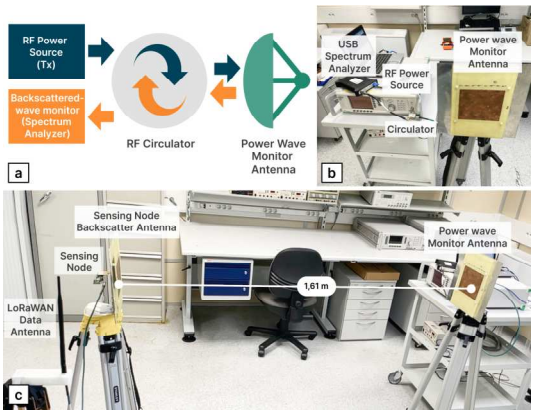

Fig.8 (a) Power wave monitor setup schematic diagram; (b) Photograph of the power wave monitor setup; (c) Photograph of the experimental setup: Sensing Node (illuminated by Power-wave Tx), the Rx Backscattered-wave signal is monitored by the Spectrum Analyzer.

The modifications to the embedded software of the SN were minimal, involving the addition of code to generate a preamble consisting of two bytes and a 128-bit key by toggling the designated GPIO. This process, facilitated by Manchester code/modulation and its ability to simplify synchronization, takes a mere 2 milliseconds, ensuring its execution before the initiation of LoRaWAN communication and the subsequent power-off of the SN. The extra capacity of the SN supercapacitor, dimensioned beforehand to account for component variability and aging, is sufficient to enable the possibility of the execution of the 2 ms code, ensuring seamless operation of the system.

Fig. 9 illustrates the backscattered signal captured by the spectrum analyzer just before the LoRaWAN communication, matching the command private key generated through the MCU's GPIO. The dynamic range of this backscattered signal is only 1 dB above the cross-jamming level (-8 dB). The cross-jamming is caused by: (i) the low isolation of the RF circulator between the Power-wave emission port and the Spectrum Analyzer reception port and (ii) the backscattered fingerprinting of the background of real-environment setup Fig. 8 (c).

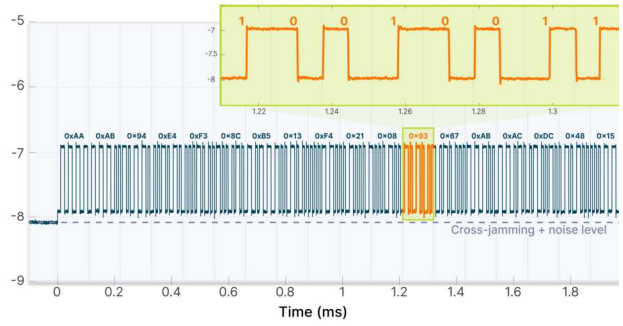

Fig.9 Backscattered signal received (preamble and 128 bits) from the SN just before LoRaWAN communication in real environment with an inset on the received byte 0x93 (Manchester code).

IV. Discussion

The experimental results obtained from the integration of the Backscattering Rectifier into a LoRaWAN battery-free Sensing Node serve as a proof-of-concept in a real environment for the proposed security and identification mechanism. Within the context of Simultaneous Wireless Information and Power Transfer, the provided system showcases seamless hardware integration and minimal software modifications. This underscores the feasibility and practicality of the proposed concept, highlighting its potential to add an innovative layer of supplementary security to battery-free sensing nodes and IoT systems operating in SWIPT context. This approach offers several notable advantages. Firstly, the ease of hardware integration underscores its compatibility with existing IoT infrastructures, minimizing the need for extensive modifications. Additionally, the minimal software adjustments required. Furthermore, by requiring no changes to the Medium Access Control layer, this solution mitigates the risk of introducing compatibility issues or disrupting existing communication protocols. To enhance the dynamic range of the Backscattering Rectifier and decrease the cross-jamming level, employing an RF circulator with higher isolation, utilizing separate antennas with different polarizations (for power wave and backscattered wave) or using the harmonic transponder concept [7]-[8] can be beneficial. Additionally, optimizing the backscattering rectifier to increase efficiency by converting it to a full-wave rectifier may also help cover more SWIPT applications over longer distances.

V. Conclusion

This paper introduces a layer of identification and security that operates independently from specific protocols. This independence ensures compatibility across various IoT communication protocols in a SWIPT context, enhancing versatility and applicability. Importantly, the integration of the Backscattering Rectifier and of the backscattered power wave with LoRaWAN, a widely adopted IoT protocol, underscores its potential for widespread deployment and adoption. The backscattered power wave is a function of physical characteristics of the incoming power wave and of the digital private key provided by LoRaWAN Sensing Node. The successful demonstration of the proposed concept validates its relevance and applicability in real-world IoT scenarios. The obtained experimental results substantiate the effectiveness and feasibility of this new security and identification mechanism. By leveraging SWIPT principles and enabling seamless integration with existing IoT infrastructure, this approach offers a promising avenue for enhancing IoT security without imposing significant hardware or software overheads.

References

[1] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586-602, 1 Oct.-Dec. 2017. doi: 10.1109/TETC.2016.2606384.

[2] S. Loukil, L. C. Fourati, A. Nayyar and C. So-In, "Investigation on Security Risk of LoRaWAN: Compatibility Scenarios," in IEEE Access, vol. 10, pp. 101825-101843, 2022, doi: 10.1109/ACCESS.2022.3208171.

[3] SeungJae Na, DongYeop Hwang, WoonSeob Shin and Ki-Hyung Kim, "Scenario and countermeasure for replay attack using join request messages in LoRaWAN," 2017 International Conference on Information Networking (ICOIN), Da Nang, Vietnam, pp. 718-720, 2017. doi: 10.1109/ICOIN.2017.7899580.

[4] T. D. P. Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas, and J. Li, "Simultaneous wireless information and power transfer (SWIPT): Recent advances and future challenges," IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 264–302, 1st Quart., 2018. doi: 10.1109/COMST.2017.2783901.

[5] T. E. Djidjekh, L. Sanogo, G. Loubet, A. Sidibé, D. Dragomirescu, A. Takacs, "A New Security and Identification Concept for SWIPT Systems in IoT Applications," 2024 IEEE/MTT-S International Microwave Symposium (IMS), 2024. to be published.

[6] G. Loubet, A. Sidibe, P. Herail, A. Takacs, and D. Dragomirescu, "Autonomous Industrial IoT for Civil Engineering Structural Health Monitoring," IEEE Internet of Things Journal, vol. 11, no. 5, pp. 8921-8944, 2024. doi: 10.1109/JIOT.2023.3321958.

[7] X. Gu, R. Khazaka and K. Wu, "Single-Ended Reconfigurable Wireless Power Harvesting and Harmonic Backscattering," 2023 IEEE Wireless Power Technology Conference and Expo (WPTCE), San Diego, CA, USA, pp. 1-4, 2023.

[8] V. Palazzi, L. Roselli, M. M. Tentzeris, P. Mezzanotte, and F. Alimenti, "Energy-Efficient Harmonic Transponder Based on On-Off Keying Modulation for Both Identification and Sensing," Sensors, vol. 22, no. 2, p. 620, Jan. 2022.