Effect of Power Conversion Efficiency of the RF Energy Harvester on the Security and Data Rate of the Self-Sustainable IoT Devices

Fariborz Lohrabi Pour, Sook Shin Ha, and Dong Sam Ha
Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA 24061, USA
{fariborzlp,sook,ha}@vt.edu

ABSTRACT

This paper presents a study on the impact of the power conversion efficiency (PCE) of RF energy harvesters on the performance of wireless Internet-of-Things (IoT) devices including the sampling rate and data security. An RF energy harvester to harvest energy from the career frequency of 2.64 GHz is designed and prototyped for measurements. A microcontroller unit (MCU) adopts Tiny Encryption Algorithm (TEA) with a 128-bit key for data encryption. Measurement results indicate that as the amount of energy harvested increases, the maximum sampling rate and the security of the data can also increase. It implies the power conversion efficiency (PCE) impacts on both the data rate and data security of self-powered wireless IoT devices.

CCS CONCEPTS

• **CCS Security and privacyNetwork securityMobile and wireless security → Network security**.

KEYWORDS

IoT, RF energy harvesting, wireless networks, security, low power

ACM Reference Format:
Fariborz Lohrabi Pour, Sook Shin Ha, and Dong Sam Ha. 2023. Effect of Power Conversion Efficiency of the RF Energy Harvester on the Security and Data Rate of the Self-Sustainable IoT Devices. In *European Interdisciplinary Cybersecurity Conference (EICC 2023), June 14–15, 2023, Stavanger, Norway.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3590777.3590796

1 INTRODUCTION

The rapid expansion of the Internet-of-Things (IoT) has been described as a pillar of the fourth industrial revolution for its potential to revolutionize areas ranging from manufacturing and energy production to healthcare and commerce [1, 2]. Following advances in miniaturization and low-power design, the number of interconnected devices has exploded from 0.08 per person in 2003 to a projected 9 devices per person globally by 2025 [3, 9]. This rampant growth in the number of IoT devices and gadgets makes energy availability one of the critical issues impacting the ultimate capacity of IoT networks [10]. Self-powered wireless IoT devices become crucial in the fifth generation (5G) and beyond. RF and mm-wave energy harvesting, as one of the reliable energy sources, has attracted good attention in recent years [6, 7]. Figure 1 shows a block diagram of a self-powered wireless IoT device for sensing. The baseband (BB) processor processes sensed signals, and the transmitter transmits sensed data wirelessly. The energy harvester harvests RF/mm-wave energy from a nearby gateway(s) and powers the device, leading to the elimination of a battery for the device.

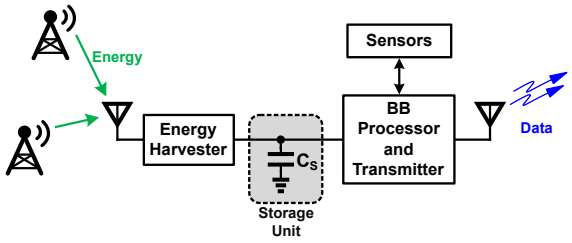

Figure 1: Block diagram of a self-powered wireless IoT device powered by RF energy harvesting.

RF energy harvesters can make wireless IoT devices more vulnerable to security attacks due to additional exposure to RF signals for harvesting. More sophisticated authentication algorithms may be necessary for those devices to protect the safety of the transmitted/received data, but those algorithms increase the power consumption of the devices compared to weakly/in-secured ones [4]. This paper presents the impact of the power conversion efficiency (PCE) of an RF energy harvester on the data rate and the security level of self-powered wireless IoT devices, where the PCE is the ratio of the output power produced by the harvester to the input power at the receiver antenna.

This paper is organized as follows. Section 2 describes our RF energy harvester and its PCE profile. Section 3 presents a self-powered wireless IoT device including the baseband processor and the transmitter. Section 4 shows measurement results such that the maximum sampling rate versus the received input power and the clock frequency of the baseband processor. Section 5 concludes this work.

2 RF ENERGY HARVESTER DESIGN AND PERFORMANCE INVESTIGATION

Figure 2 shows the schematic diagram of an RF energy harvester. The center frequency of the antenna array is tuned at 2.64 GHz to receive the signals from downlink (DL) of the 5G NR n7 band in real-world environments. The half wavelength ($\lambda/2$) antenna array is composed of four (2x2) patch antennas to increase the directivity of the antenna and hence its gain. Since the processor unit requires

EICC 2023, June 14–15, 2023, Stavanger, Norway

ACM ISBN 978-1-4503-9829-9/23/06.
https://doi.org/10.1145/3590777.3590796

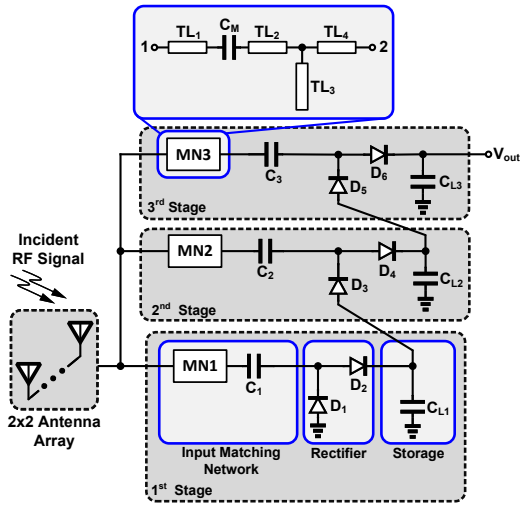

Figure 2: Schematic diagram of the RF energy harvester.

a relatively high supply voltage, three voltage multipliers are cascaded in series to boost the output voltage across the storage unit (e.g. C_s in Figure 1) [7].

The capacitance of the storage unit is determined based on the rate of power dissipation in the baseband (BB) processor and the transmitter. If the available RF power is limited, a passive backscatter-modulated transmitter can be used to decrease the power dissipation of the transmitter [8]. The photograph of the prototyped energy harvester, including the antenna array and the rectifier (rectenna), is shown in Figure 3.

The PCE profile of the energy harvester, i.e., the ratio of the harvested power versus the input power, is also obtained through measurements and shown in Figure 4. The PCE heavily depends on the input power level or the power of the incident RF signal at the receiver. The PCE increases initially as the input power level increases, hits the maximum value of 63% under the input power level of ≈ -2 dBm, and then starts to decrease. Note that the harvested dc output power level increases steadily as the input power level increases.

Figure 5(a) shows the measurement setup to evaluate the performance of the RF energy harvester. The transmitter antenna and the energy harvester are located 1 m apart in an anechoic chamber to minimize interferences in the environment. The measurement results are shown in Figure 5(b). The final voltage of the storage capacitor C_s is 1.2 V under the transmitted power of 10 dBm, and increases to 7.9 V under the transmitted power of 27 dBm. The charging time of a capacitor is obtained as the time taken to rise 10 % of the final voltage to 90 %. The results show that the charging time is 45 sec and equal for all the three different transmitted power levels.

Assuming a wireless IoT device draws the same current from the storage capacitor C_s during the operation, the effective operating time is obtained as follows.

$$\Delta t = \frac{C_s \times (V_c - V_m)}{I_s} \quad (1)$$

where V_c is the C_s voltage, V_m the minimal voltage necessary to operate the device, and I_s the dc current drawn by the device during

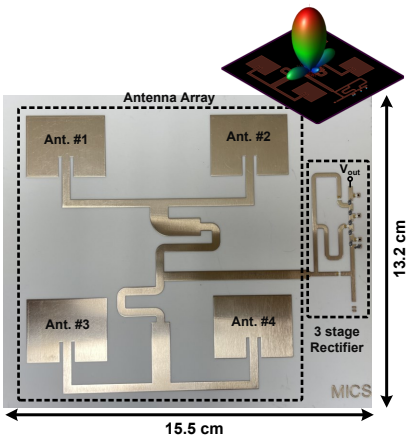

Figure 3: Photograph of the prototyped RF energy harvester and the simulated radiation pattern of the antenna array.

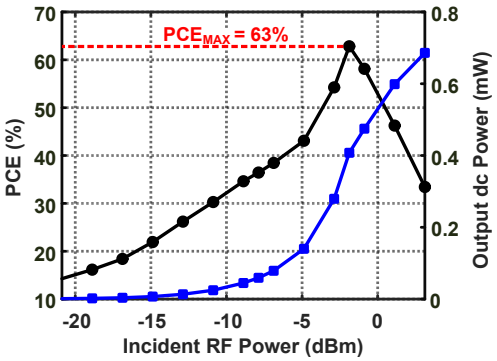

Figure 4: Measured PCE and harvested dc power of the RF energy harvester.

the operation. For example, suppose that the capacitor voltage V_c is 3.95 V for C_s= 2200 μF in Figure 5(b) and the minimum device voltage V_m is 1.2 V. If the device draws a constant dc current of 1 mA, it can operate for about 6 sec. Once the capacitor voltage drops below the minimum supply voltage, the device may go to sleep mode and waits until the capacitor is charged again.

3 BASEBAND PROCESSOR AND TRANSMITTER

Figure 6 shows a simplified schematic diagram of a self-powered wireless IoT device. A quadrature phase shift keying (QPSK) transmitter composed of a ring oscillator, a charge control unit, and a wake-up circuit is responsible for transmitting the encrypted data [5]. A temperature sensor, specifically a negative temperature coefficient (NTC) thermistor, changes its resistance according to the temperature. The MCU (specifically PIC18F45K22 MCU for our prototype) with an embedded analog-to-digital converter (ADC) senses the temperature and encrypts the data. The QPSK transmitter transmits the encrypted data. The energy harvester is connected directly to the MCU, whose minimum supply voltage to operate is 1.2 V.

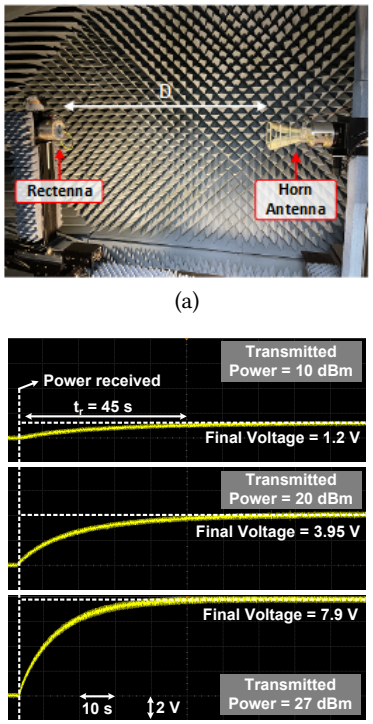

Figure 5: (a) measurement setup for the RF energy harvester, and (b) charging time of the storage capacitor (C_s= 2200 μF) for three different transmitted power levels.

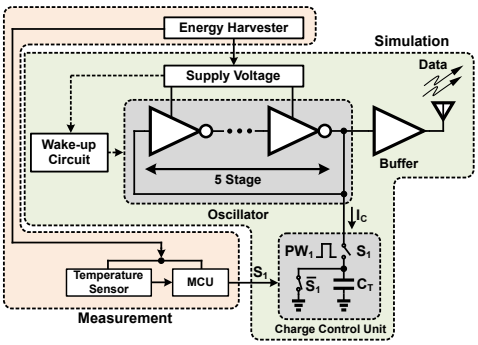

Figure 6: Simplified schematic diagram of a self-powered wireless IoT device.

We adopt Tiny Encryption Algorithm (TEA) [11] for data encryption, as the algorithm provides a reasonable security level, while the encryption process takes a relatively short time compared to most other well-known encryption algorithms.

4 MEASUREMENT RESULTS AND PERFORMANCE EVALUATION

Figure 7(a) shows the block diagram of the measurement setup used for investigating the impact of the PCE on the sampling rate (or data rate) of a self-powered wireless IoT device. The power transmitter provides RF power to the RF energy harvester at the career

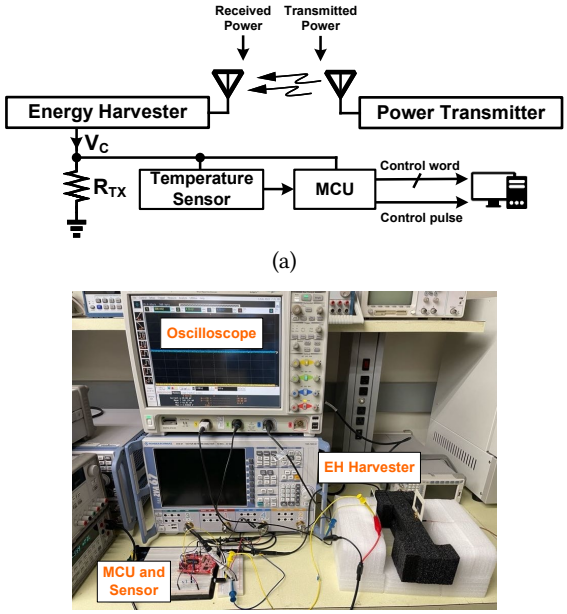

Figure 7: Measurement setup for sampling rates (a) block diagram, (b) photograph.

frequency of 2.64 GHz. We assume that the power dissipation of the RF front end is independent of the sampling rate. (The assumption is justified in the design of the RF front end in [5].) Therefore, the RF front end is replaced with a fixed resistor (R_{TX} = 3.5 $k\Omega$) for the measurement setup. The power dissipation of the RF front end depends on the voltage supplied by the energy harvester. For example, the power dissipation is 411 μW for the supply voltage of 1.2 V. The MCU encrypts the collected data from the temperature sensor with a 128-bit key and 64-bit block size. The control word and the control pulse, originally aimed to control the RF front end, are monitored to verify the operation of the MCU.

Figure 7(b) shows the measurement setup. The power transmitter (not shown) is 1 m from the receiving antenna of the energy harvester, which results in the free space path loss of approximately 40 dB at 2.64 GHz. The transmitted power is swept from 0 dBm to 40 dBm by following a random Poisson pattern, which leads to the received power ranging from -40 dBm to 0 dBm. The MCU power dissipation increases as the sampling rate. If the MCU power dissipation exceeds the power generated by the energy harvester, the output voltage of the harvester decreases until it hits the minimum voltage of 1.2 V. Once the output voltage reaches 1.2 V, the MCU stops the operation, and the output voltage starts to increase. It implies that there is a maximum sampling rate for the MCU to operate for a given input power level received at the antenna of the energy harvester.

We measured the maximum sampling rate for the received power level ranging from -40 dBm to 0 dBm by sweeping the power level of the power transmitter. Figure 8(a) shows measurement results on the maximum sampling rate versus received RF power level of the energy harvester, while the MCU clock frequency is set to 1 MHz.

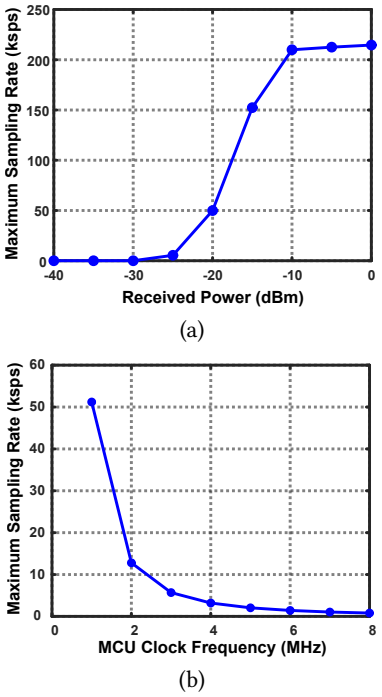

Figure 8: Maximum sampling rate versus (a) received input power level, (b) MCU clock frequency under the received input power of -20 dBm.

When the received RF power is smaller than -30 dBm, the sampling rate is near 0, implying the output voltage of the harvester fails to reach the minimum supply voltage (=1.2 V) required by the MCU. The sampling rate increases as the received power increases, and it hits the maximum value of ≈210 ksps for the received power of -10 dBm. As the harvested power or the output voltage V_c is saturated (as demonstrated in Figure 5(b)) beyond this point and hence the maximum sampling rate. In other words, the PCE of the energy harvester influences the maximum sampling rate or data rate of the IoT device.

The MCU adopts Tiny Encryption Algorithm (TEA) with a 128-bit key for data encryption. To increase the security of sensed data, a more complicated algorithm and/or a longer key is necessary, leading to a heavier computational load and hence requiring a higher clock frequency for the MCU. As the clock frequency of the MCU increases, the power dissipation of the MCU also increases, resulting in decrease of the maximum sampling rate.

Figure 8(b) shows measurement results for the maximum sampling rate versus the clock frequency under the received input power of -20 dBm. As expected, the MCU clock frequency increases, the maximum sampling rate decreases steadily. It is noted that to maintain the maximum sampling rate, it is necessary to harvest more energy. The maximum sampling rate is 50 ksps (or ≈100 kbps for QPSK modulation) under the clock frequency of 1 MHz and decreases to < 10 ksps for the clock frequency of 3 MHz. Hence, in order to increase the sampling rate, it is desirable to set a low MCU clock frequency *as long as the MCU can process the necessary encryption*. In summary, a more complicated algorithm and/or a longer key increase the data security, but it reduces the maximum sampling rate, and the PCE of an energy harvester also plays a key role in the aspect.

5 CONCLUSION

This paper presents design of a self-powered wireless IoT device including an RF energy harvester and a transmitter. Our measurement result indicates that as the received input power level increases, the maximum sampling rate of an IoT device increases initially and is saturated beyond a certain power level. To increase the security of the sensed data, a more complicated algorithm and/or a longer key is necessary, leading to a heavier computational load for the MCU and hence more power dissipation. As a high clock frequency of the MCU can provide the capability for high data security, the MCU power dissipation increases to result in decrease of the maximum sampling rate. Our measurement result verifies it. In conclusion, as the amount of harvested energy increases, the maximum sampling rate and the security of the data can also increase, implying the impact of the power conversion efficiency (PCE) on both the sampling rate and data security.

ACKNOWLEDGMENTS

This research was supported in part by the National Science Foundation grant with the award number 2106987.

REFERENCES

[1] Cisco. 2023. What Is Industrial IoT (IIoT)? https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-industrial-iot.html#~q-a
[2] Gizem Erboz. 2017. How To Define Industry 4.0: Main Pillars Of Industry 4.0.
[3] Dave Evans. 2011. The Internet of Things: How the Next Evolution of the Internet is Changing Everything. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
[4] Rabia Khan, Pardeep Kumar, Dushantha Nalin K. Jayakody, and Madhusanka Liyanage. 2020. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Communications Surveys & Tutorials* 22, 1 (2020), 196–248. https://doi.org/10.1109/COMST.2019.2933899
[5] Fariborz Lohrabi Pour and Dong Sam Ha. 2022. An M-PSK Modulated Polar Transmitter Based on a Ring Oscillator with Low Power and Low Design Complexity for IoT Applications. In *2022 IEEE International Symposium on Circuits and Systems (ISCAS)*. 2182–2186. https://doi.org/10.1109/ISCAS48785.2022.9937689
[6] Theodore S. Rappaport, Yunchou Xing, Ojas Kanhere, Shihao Ju, Arjuna Madanayake, Soumyajit Mandal, Ahmed Alkhateeb, and Georgios C. Trichopoulos. 2019. Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond. *IEEE Access* 7 (2019), 78729–78757. https://doi.org/10.1109/ACCESS.2019.2921522
[7] Ryan Reed, Fariborz Lohrabi Pour, and Dong Sam Ha. 2020. An Efficient 2.4 GHz Differential Rectenna for Radio Frequency Energy Harvesting. In *2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS)*. 208–212. https://doi.org/10.1109/MWSCAS48704.2020.9184600
[8] Ryan Reed, Fariborz Lohrabi Pour, and Dong Sam Ha. 2021. An Energy Efficient RF Backscatter Modulator for IoT Applications. In *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*. 1–5. https://doi.org/10.1109/ISCAS51556.2021.9401639
[9] Bardia Safaei, Amir Mahdi Monazzah, Milad Bafroei, and Alireza Ejlali. 2017. Reliability Side-Effects in Internet of Things Application Layer Protocols. https://doi.org/10.1109/ICSRS.2017.8272822
[10] Pietro Tedeschi, Savio Sciancalepore, and Roberto Di Pietro. 2020. Security in Energy Harvesting Networks: A Survey of Current Solutions and Research Challenges. *IEEE Communications Surveys & Tutorials* 22, 4 (2020), 2658–2693. https://doi.org/10.1109/COMST.2020.3017665
[11] David J Wheeler and Roger M Needham. 1995. TEA, a tiny encryption algorithm. In *Fast Software Encryption: Second International Workshop Leuven, Belgium, December 14–16, 1994 Proceedings 2*. Springer, 363–366.