Secure Communication with Batteryless Sensors

Naomi Stricker*, Jan Liam Albert†, Md Masoom Rabbani‡, Simon Mayer†, Andres Gomez†
* ETH Zurich, Switzerland, † University of St.Gallen, Switzerland, ‡ KU Leuven, Belgium
nstricker@ethz.ch, mdmasoom.rabbani@kuleuven.be, {janliam.albert, simon.mayer, andres.gomez}@unisg.ch

***Abstract*—Batteryless sensors have recently been proposed as an energy-efficient and cost-effective alternative to battery-powered sensors. By harvesting and immediately consuming ambient energy, it becomes unnecessary to design systems with large energy storages, which significantly increases their form factor, cost, and environmental impact. Many works have focused on designing batteryless systems that sense data, process it, and wirelessly broadcast processed data. Yet wireless security aspects of batteryless applications are only now receiving attention. In this work, we propose a secure communication system based on symmetric key encryption, that enables batteryless sensors to securely broadcast data. Furthermore, we demonstrate this system on a batteryless smartcard in two application scenarios: static sensor deployment for secure data gathering, and mobile device for identification purposes. Our experimental results demonstrate not only the feasibility of secure communication with batteryless devices but also the small overheads of introducing security in wireless beaconing applications.**

***Index Terms*—batteryless systems, data encryption, energy harvesting, secure communication**

I. Introduction

Information gathered by wireless sensing systems is one of the fundamental building blocks of the Internet of Things (IoT). To increase the spatial and temporal granularity of sensed data, these systems must be compatible with long-term deployments in a scalable and affordable manner. This is a difficult challenge since traditional battery-based designs would be restrictive in terms of form factor, cost, reliability, and maintenance. In many IoT use cases, it is desirable that these sensing devices disappear physically, as well as psychologically, motivating the use of thin, deploy-and-forget wireless sensors. Batteryless sensing is a new system design paradigm that, instead of storing large amounts of energy locally, taps into widely-available ambient energy and optimizes away any bulky energy storage elements.

By powering off completely whenever the environment stops providing energy, batteryless devices avoid sleep states that although low-power, when integrated over long-term deployments, represent a significant energy overhead. As soon as environmental energy becomes available again, the fully discharged system can efficiently power up and start sensing within seconds. Batteryless sensors powered by photovoltaics can tap into an abundant energy source found in virtually every human-centered scenario: light. Using light as the primary energy source also has a secondary advantage, this endows users with agency. By just covering the solar cell, or enclosing it in a dark location, the user is certain that the device is completely powered down and incapable of powering up. Only when the user chooses to expose the device to light will the sensor energize and wirelessly transmit data. In certain scenarios, it is not enough to simply transmit raw sensor data over a wireless channel. Additional steps must be taken to secure sensitive data before wirelessly broadcasting.



Fig. 1. The miroCard sensing platform is powered exclusively when exposed to light. A Raspberry Pi Zero receives and prints encrypted BLE beacons. When the photovoltaic cell is obscured, the miroCard fully discharges itself.

There are many security-related aspects to the Internet of Things, each with its own special considerations [1]. In the context of batteryless systems, physical security and memory protection are important elements since devices are typically deployed in physically accessible areas. Many works have focused on hardening batteryless systems, also known as intermittent computers. Researchers have proposed mechanisms that encrypt non-volatile state retention [2] and remote attestation procedures that can detect the presence of malware on the batteryless device during active periods [3]. However, little work has been done in securing the wireless applications executing on batteryless systems. In this work, we introduce secure communication into a batteryless sensing platform with reliability guarantees, an example thereof is shown in Figure 1. Our contributions can be summarized as follows:

- We propose a secure communication scheme between asynchronous batteryless devices and a gateway, using symmetric key encryption.
- We present two batteryless applications transmitting encrypted data over BLE beacons.
- We demonstrate the low overhead of secure communication with an experimental evaluation of real batteryless devices in indoor illuminance conditions.

This work was partly supported by the Swiss National Science Foundation under the NCCR Automation project, grant agreement 51NF40_180545, the GFF-IPF Grant of the University of St.Gallen, and the European Union's Horizon 2020 research and innovation program, grant No. 957218 (*IntellIoT*).

978-1-6654-6828-2/22/$31.00 ©2022 IEEE

II. Batteryless Sensing

Batteryless sensing systems can efficiently gather data when their surrounding environment provides enough energy. For this to happen, however, several operating parameters must align. A transducer's I-V characteristics vary widely but must be made compatible with the operating conditions of application circuits, which tend to vary little in voltage but largely in current. Furthermore, a small amount of energy storage is necessary to ensure that when the application is active, it can remain active for a minimal amount of time.

In this work, we use a batteryless miroCard [4], which already addresses many of the aforementioned challenges for batteryless system design. Energy input is maximized through power point tracking, while the energy output is simultaneously minimized with feedback-controlled DVFS. An optimized capacitance, whose value is chosen at design time, provides energy guarantees for atomic executions of tasks such as sensing or wireless transmissions. If tasks are energy-bounded, a safe maximum energy consumption can be determined. The miroCard can thus ensure reliable task completion, even if the tasks vary in terms of current and energy consumption.

Batteryless systems activate more often as their environment provides increasing energy. This is achieved by a self-adjusting mechanism that triggers the atomic tasks to adapt the application circuit's average power consumption, $\bar{P}_{\text{application}}$, to the maximum sustainable value. Consequently, the following energy conservation equation holds: $\bar{P}_{\text{harvested}} = \eta \times \bar{P}_{\text{application}}$. Since the harvested power, $P_{\text{harvested}}$, can vary widely, it is important for the application circuit to efficiently operate at different power levels. The overall energy efficiency from the transducer to the application circuitry, η, depends on the DC-DC converters used but can reach up to almost 90% [5].

The miroCard uses inexpensive and long-life SMD ceramic capacitors to buffer small amounts of energy, providing an energy storage size of hundreds of μJ. Compared to a standard CR2032 coin-cell with a nominal energy capacity of 2430 J, the miroCard's capacity is multiple orders of magnitude smaller. Despite the tiny energy budget, this is enough to support a full application cycle with sensing, processing, and transmitting. Since each application execution is executed atomically and independently of each other, non-volatile state retention mechanisms and their security vulnerabilities can be avoided. However, there is still a missing layer of security at the application layer. To be able to securely transmit sensitive data, batteryless sensors must encrypt application data before transmitting them wirelessly.

III. Secure Communication Platform

In this work, we introduce application-level security for batteryless sensors enabling them to transmit sensitive data in encrypted form. This system architecture is present in two prominent application domains, shown in Figure 2, statically deployed sensors, and wearable systems. Our proposed secure communication method consists of a batteryless miroCard and an always-on gateway or WebBluetooth-enabled client. The sample applications consist of reading a sensor, encrypting data, and securely transmitting information via Bluetooth Low Energy (BLE) packets. The receiver then decrypts the data, which can include sensitive sensor data or user-identifying information. This data can then be safely stored in a secure database, or be used for user identification in cloud-based services.

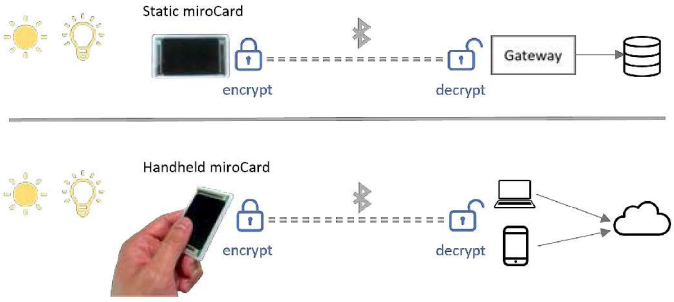


Fig. 2. The miroCard can be used as either a statically deployed sensor that transmits sensitive data securely to a database, or as a handheld mobile device used to securely transmit user identification data for cloud-based services.

A. Encrypting Wireless Data

We propose encrypting application data with a symmetric key algorithm, the Advanced Encryption Standard (AES) [6], which can be effectively executed in software without hardware dependencies. AES is a block cipher, meaning that the plaintext is processed in blocks of equal length (i.e., 128 bits for AES) to obtain the ciphertext. In this process, each block of plaintext is processed through a sequence of steps (i.e., AddRoundKey, SubBytes, ShiftRows, and MixColums). The number of rounds is determined by the key size which can be 128, 192, or 256 bits. To encrypt or decrypt messages with a length greater than the key size with a block cypher, several 'modes of operation' have been proposed. The simplest mode is the Electronic Code Book (ECB). In ECB, the plaintext is split into blocks of equal length and each block is independently encrypted using an algorithm such as AES. Although there are more secure algorithms than ECB, it still shows a number of advantages. For example, the fact that the impact of bit errors is limited to one block makes it easy to deploy in a noise-sensitive environment. In addition, this mode does not require any additional synchronization [7].

B. miroCard Platform

The miroCard is an open-source[1] batteryless sensing platform. It features an organic photovoltaic cell from Epishine with a size of 50 mm×30 mm, an e-peas AEM10941 harvester chip with optimized cold-start, a TI CC2650 MCU, and a Sensirion SHT31 sensor. Developers can execute a wide variety of batteryless applications with atomic energy guarantees by adjusting the equivalent capacitance to the application requirements. As discussed in the previous section, one of the main challenges in batteryless design is to minimize the

[1]https://mirocard.swiss

application's energy requirements, which also minimizes the required capacitance and, consequently, the device's start-up time. In our application, the miroCard senses temperature and humidity, encrypts data, and securely transmits three BLE beacons within a single activation cycle. The payload of each BLE beacon is 21 B long. The first 5 B are a unique preamble, to facilitate the BLE beacon filtering in the receiver, and the subsequent 16 B are the encrypted data. 3 B sensor measurement data and 6 B device UUID are padded to 16 B and then encrypted.

IV. Experimental Evaluation

We experimentally measure the energy requirements of a secure sensing application with the miroCard. The data encryption only contributes a small portion to the overall energy requirement of each application execution. In addition to evaluating the overhead of secure communication, this characterization is important for properly dimensioning the miroCard's energy storage. Furthermore, we evaluate the time the miroCard takes to start up from a fully-off state in an average indoor lighting environment.

Energy Characterization. We use a Rocketlogger [8], a portable measurement device with high accuracy for wide operating ranges, to measure both the sleep current and characterize the application. For the former, the Rocketlogger records the current flowing out of the harvesting chip powering the system. The latter is evaluated by measuring the current flowing out of the capacitor, the supply voltage V_{cc}, and GPIO's to distinguish between different phases within a single application execution. When powered, the miroCard is in a low-power state between activations. In this state, the miroCard consumes on average 4 µA at 2.5 V, excluding the inefficiency of the downconversion. As soon as the internal capacitance reaches the maximum voltage, a trigger activates a single stateless application execution. Figure 3 shows the miroCard's power consumption for a single application activation. Each activation requires on average 207.2 µJ to which sensing the temperature and humidity contributes 67.7 µJ, encrypting the data adds 15.2 µJ and sending three BLE packets requires 51.8 µJ. Data encryption contributes less than 10 % to the energy requirement of each activation. A detailed breakdown of the energy and time per activation across 181 measurements is summarized in Table I.

Start-Up Time. When the miroCard is not exposed to any light, its capacitor voltage drops quickly to a point where even the low-power sleep state cannot be sustained. It then turns completely off, since the small energy storage gets fully depleted. Once light shines on the solar panel again, the system goes through a startup period and charges the capacitance to a voltage above 3.67 V, at which point V_{cc} turns on and the application can execute again. When lighting conditions are highly variable, a reactive and adaptive system with a fast startup is essential for efficient use of ambient energy.

We measure the worst-case time it takes for the miroCard to start up when exposed to a typical indoor environment with an illuminance of 450 lx. The illuminance is determined with a lux meter next to the miroCard's solar panel. A Rocketlogger measures the voltage of the organic solar cell V_{src}, the capacitor voltage V_{cap}, and the supply voltage V_{cc}. The miroCard contains internal capacitors with a total capacitance of 141 µF. Initially, all capacitors are depleted by manually shorting them. This requires the capacitors to be charged from their lowest possible level, thus corresponding to a worst-case startup time. The recorded voltage traces are depicted in Figure 4. Under these conditions, the miroCard's worst-case startup time is only 7.7 s, which enables it to efficiently use and react to varying and unreliable environments.

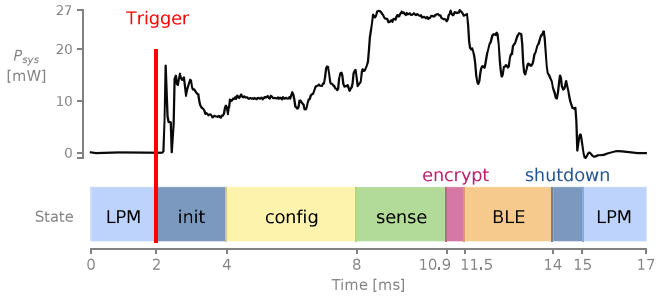


Fig. 3. In each activation, the miroCard senses temperature and humidity and encrypts this data. Three BLE transmissions send the encrypted data in three advertisement channels.

Analysis. Our application-level security is included within a single activation cycle, enabling encrypted communication. This stateless execution by design avoids overheads associated with state retention and also bypasses security weaknesses of state retention mechanisms. Encrypting application data increases execution time by 564 µs, a small fraction of the full sense-process-transmit cycle. The limited overhead and particularly small variance in energy requirement allows the miroCard to contain only a small internal capacitance and thus ensures it starts up quickly. These fast startup times allow efficient use of ambient energy both in static and mobile deployments. One limitation of the miroCard is that it currently supports wireless broadcasting only. Due to the heavily optimized capacitor, an extended reception window to receive data from another device cannot be sustained. As such, all configuration parameters must be known at design time, including the shared key.

TABLE I
Per task evaluation of 181 application executions measured at 2.5 V using a RocketLogger.

Task	E_{mean}	E_{std}	t_{mean}	t_{std}
init	18.525 µJ	0.138 µJ	2.150 ms	0.012 ms
config	45.158 µJ	0.217 µJ	3.965 ms	0.010 ms
sense	67.693 µJ	0.291 µJ	2.741 ms	0.014 ms
encrypt	15.171 µJ	0.192 µJ	0.564 ms	0.007 ms
BLE	51.834 µJ	0.324 µJ	2.698 ms	0.016 ms
shutdown	8.807 µJ	0.210 µJ	0.971 ms	0.031 ms
total	207.188 µJ	0.320 µJ	13.089 ms	0.035 ms

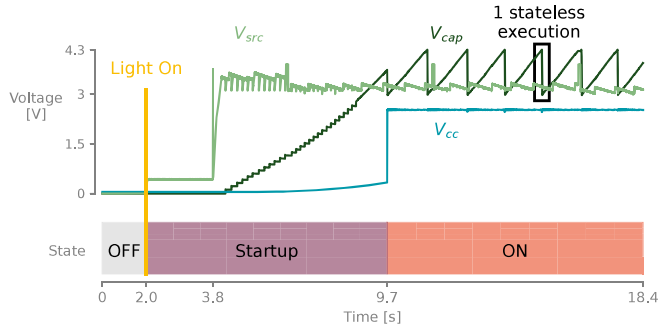


Fig. 4. The secure communication app on the miroCard with C=141 µF can wake up from full discharge within 7.7 s after being exposed to an environment with an illuminance of 450 lx.

V. Related Works

In recent years, batteryless sensors have received increasing interest as a potential solution to the energy bottleneck in IoT sensors. As such, many works have addressed different challenges of designing energy-harvesting systems with very limited energy storage capability. One class of batteryless systems is unable to atomically execute a long processing task. To nonetheless make forward progress, these systems require checkpointing to save the state when they lose energy. A generally applicable lightweight approach for checkpointing was proposed in [9] which requires only little energy to save and restore the state from on-chip non-volatile FRAM memory. Checkpointing systems are typically incompatible with wireless communication, since transmitting packets requires larger energy guarantees.

A second class of batteryless sensors can perform larger tasks within a single activation, thus avoiding the need for interrupting, saving, and restoring the state of computation. The authors of [10] propose an energy storage system that can be dynamically configured to have different energy guarantees depending on the application requirements. An asynchronous BLE beaconing system was proposed in [11] that can efficiently operate in various lighting conditions and transmit both current and historical sensor data from an off-chip non-volatile data buffer. Synchronous communication requires systems to be powered for sufficiently long or wake up at specified times, both of which are at odds with batteryless systems. In [12], this challenge is addressed by enabling synchronous device-to-device communication for batteryless systems. The proposed FLYNC method relies on disturbances in lighting systems caused by powerlines. When batteryless systems are exposed to the same lighting environment, their synchronization is greatly simplified. Visible light was also leveraged for synchronization in [13]. In combination with a backscatter radio, their approach enables batteryless systems to exchange energy status and communication scheduling information.

In the security domain, several vulnerabilities of batteryless systems have been researched. A lightweight remote attestation method proposed in [3] for intermittent systems detects malware while the system is active. It furthermore, provides probabilistic software guarantees while the system is off. For the class of batteryless systems that rely on checkpointing, [2] propose to encrypt the checkpoints. The thus increased overhead is reduced by optimizing when to perform checkpointing. An atomic approach for secure checkpointing is also proposed in [14]. The method associates each checkpoint with a fingerprinting power-on state and also cryptographically chains it to the previous checkpoint. Security weaknesses related to checkpointing are not relevant for batteryless systems that perform an entire application execution with each activation.

VI. Conclusions

In this work, we propose a secure communication scheme that enables light-powered batteryless sensors to asynchronously transmit sensitive information to a gateway. Secure communication is achieved using the AES symmetric encryption algorithm with pre-shared keys and implemented using a software library on a batteryless sensing platform. We implement two batteryless applications with atomic energy guarantees, one for sensitive data gathering and another for user identification, both of which rely on secure data exchange. Our experimental results show a worst-case start-up time of only 7.7 s at 450 lx, with a small execution time overhead incurred by the data encryption.

References

[1] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Security in energy harvesting networks: a survey of current solutions and research challenges," *IEEE Communications Surveys & Tutorials*, 2020.

[2] Z. Ghodsi, S. Garg, and R. Karri, "Optimal checkpointing for secure intermittently-powered iot devices," in *Proc. of ICCAD*, IEEE, 2017.

[3] M. M. Rabbani, E. Dushku, J. Vliegen, A. Braeken, N. Dragoni, and N. Mentens, "Reserve: Remote attestation of intermittent iot devices," in *Proc. of SenSys'21*, ACM, 2021.

[4] A. Gomez, "On-demand communication with the batteryless mirocard: demo abstract," in *Proc. of SenSys'20*, 2020.

[5] A. Gomez, L. Sigrist, M. Magno, L. Benini, and L. Thiele, "Dynamic energy burst scaling for transiently powered systems," in *Proc. DATE Conf.*, IEEE, 2016.

[6] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography, Springer, 2002.

[7] D. Bujari and E. Aribas, "Comparative analysis of block cipher modes of operation," in *International Advanced Researches & Engineering Congress*, 2017.

[8] L. Sigrist *et al.*, "Measurement and validation of energy harvesting iot devices," in *Proc. of DATE*, IEEE, 2017.

[9] H. Jayakumar *et al.*, "Quickrecall: A hw/sw approach for computing across power cycles in transiently powered computers," *JETC*, 2015.

[10] A. Colin, E. Ruppel, and B. Lucia, "A reconfigurable energy storage architecture for energy-harvesting devices," in *Proc. ASPLOS Conf.*, ACM, 2018.

[11] L. Sigrist, R. Ahmed, A. Gomez, and L. Thiele, "Harvesting-aware optimal communication scheme for infrastructure-less sensing," *ACM Transactions on Internet of Things*, 2020.

[12] K. Geissdoerfer and M. Zimmerling, "Bootstrapping battery-free wireless networks: Efficient neighbor discovery and synchronization in the face of intermittency," in *Proc. USENIX NSDI Symp.*, 2021.

[13] A. Torrisi, K. S. Yıldırım, and D. Brunelli, "Autonomous energy status sharing and synchronization for batteryless sensor networks," in *Proc. SenSys'21*, ACM, 2021.

[14] A. S. Krishnan, C. Suslowicz, D. Dinu, and P. Schaumont, "Secure intermittent computing protocol: Protecting state across power loss," in *Proc. of DATE*, IEEE, 2019.