Microprocessors and Microsystems 60 (2018) 24–37

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

Adaptive scheduling to enhance data security and energy efficiency on energy harvesting platform

Claudio Copello, Ning Weng*

Southern Illinois University Carbondale, United States

ARTICLE INFO

Keywords:
Energy management
Radiofrequency identification (RFID tags)
Energy (energy harvesting)
Software (embedded software)

ABSTRACT

Radio-frequency (RF)-based energy harvesting platforms are appealing for always-on applications due to its radio frequency energy harvesting capability. However, the current RF-based energy harvesting capability is limited by many factors including harvesting distance, device constraints, communication, and security. RF-based energy harvesting platforms tend to harvest less energy as the device is further away, and impacts the ability to execute its own applications properly. The limited storage of energy on such platforms will make it even challenging to implement energy-hungry security functions on top of basic functions such as sensing, computing and transmitting. Therefore, by default, a lot of RF-based energy harvesting platforms have no basic security functions implemented, which is not acceptable for security-sensitive applications such as biomedical applications.

In this paper, we propose an adaptive light-weight scheduling mechanism that aims to balance data security and energy efficiency for application on RF-based energy-harvesting platforms. We will then prototype this scheduler on a Wireless Identification and Sensing Platform (WISP) device. The results in this paper will test this scheduling mechanism in action on a WISP device, along with use of a sensor to determine energy impact on the device, a deadline-based mechanism for data distribution, and finally comparing these cases with average voltage and total time.

1. Introduction

RF-based energy harvesting platforms have generated appeal due to its energy harvesting capabilities for wireless applications. The general purpose of these platforms is that these platforms harvest energy wirelessly which allows the platform to execute user defined applications without the use of a battery. While these platforms can be considered more convenient and cost efficient by its embedded and wireless nature, data security and energy efficiency are two important features that are lacking in these platforms. These platforms have been known to allow eavesdropping and signal jamming in the medical field, where some patients have a wireless Implantable Cardioverter Defibrillator (ICD) planted in their heart. The IMDs left unsecured could allow an attacker to intentionally send jolts of electricity [2]. Another example occurs in smartcards and RFID tags, where security protocols may prove difficult to implement without a built-in clock. The lack of time awareness has allowed vulnerabilities such as brute-force attacks that could extract the key of a smartcard [12]. Implementing data security on such platforms also raises the issue of energy efficiency, as complex security algorithms can consume lots of energy and negatively impact the performance of these platforms. Without taking into consideration the amount of energy a platform can harvest, the platform will struggle to perform adequately. These issues demonstrate the need to provide data security and energy efficiency for RF-based energy-harvesting platforms.

RF-based energy harvesting platforms can harvest and store energy for a period of time. Battery-less devices, though, also face a challenge of maintaining energy over time, especially under long distances where a limited supply of energy is available to harvest. Data security on a battery-less device also poses a bigger challenge from energy consumption. Applying encryption to data will require more energy, as well as additional processing power than sending data in plain form. Embedded devices with limited processing capabilities can tend to require much more additional time to process data if the secure method is too complex. When operating a battery-less device under long distances (distances that are not out of range to harvest energy but not close enough to harvest at a decent pace), applying data security can cause such a device to struggle to maintain power and thus require even more time to process.

To overcome the challenges of data security and energy efficiency

* Corresponding author.
E-mail address: nweng@siu.edu (N. Weng).

https://doi.org/10.1016/j.micpro.2018.03.010
Received 26 May 2017; Received in revised form 12 February 2018; Accepted 26 March 2018
Available online 31 March 2018

on a battery-less device, there is a need to design a light-weight scheduler that can adapt the distribution of data based on the amount of energy available on such a device. This light-weight scheduler must be designed with simplicity to avoid waste of energy. The goal of the scheduler is to distribute a given set of data that must be encrypted and transmitted based on the amount of energy the device has harvested. At least two different security methods are required for the scheduler. One that consumes more energy but uses stronger encryption; and another that consumes less energy but uses weaker encryption. Based on the given energy, the scheduler will decide which secure function will be chosen to encrypt the current batch of data and will continue until there is no more data that needs to be transmitted.

For an RF-based energy harvesting platform to allow security, requirements are necessary to ensure the platform is capable of processing data in a secure manner. We assume these devices communicate through an RFID reader, and the device harvests energy from the signal generated by the reader. The data stored on the device is normally generated from the outputs of the sensors or calculated from user-defined functions within the program. Once the data is ready to be transmitted, a simple function is called to transmit the values to the RFID reader, but without any security the reader will receive these values without any encryption. With a limited supply of energy available to harvest and limited space to transmit data, the scheduler proposed earlier will decide which secure function will be used to encrypt the data, and the encrypted data will provide an output that fits the available space to transmit. When the data is transmitted, the output will indicate which secure function was used to encrypt the given set of data. As data is sent in pieces, it is important that the transmitted data also indicate which piece was transmitted to ensure the proper order and integrity of data. For providing identification, RF-based platforms can contain unique identifiers and may be included in the transmitted data.

In this paper, we intend to overcome the constraints of data security and energy efficiency in RF-based energy harvesting platforms by proposing two different schedulers that focus on energy and time, as well as prototyping these schedulers onto an actual platform. Both of these schedulers will distribute a given set of data, encrypt the data, and then transmit. Encryption is based on two security functions, where energy costs are measured. As the energy is measured on the device, the schedulers determine which security function is adequate based on the amount of energy. Prototyping these schedulers onto a platform will then demonstrate the performance and capabilities of how such a platform can handle data security and energy efficiency.

Our paper first proposes an energy-aware scheduler to encrypt and transmit data based on the measured voltage. At a given voltage, the scheduler decides which security function will be used to encrypt the given set of data before transmitting. If the scheduler determines there is not enough voltage to transmit using a more complex function, then the energy efficient method is used. The goal of this scheduler is to minimize power losses and device interruptions.

We also propose a timing aware scheduler to build on the reactive scheduler that perform time deadlines. The goal is to distribute a given set of data based on the voltage, encrypt and determine if the deadline has passed before transmitting. In this scheduler, additional measures are taken for the device to harvest energy by use of a low power mode. The device is given an opportunity to sleep for a moment and harvest more energy before the scheduler continues. These two schedulers are similar, but the timing aware scheduler becomes aware of the time elapsed as data is being distributed. In this scheduler, the goal is to meet the time deadlines of data distribution to where data is received within a timeframe.

Finally, we will prototype these schedulers onto a Wireless Identification and Sensing Platform (WISP) device. The WISP device is considered a wireless, battery-free platform for sensing and computation that is powered and read by a standards complaint Ultra-High Frequency (UHF) RFID reader [1] for a number of embedded low power applications. When running simple applications on the WISP, the WISP first harvests energy and as it executes the given application, a set of numbers is transmitted to the RFID reader for the user to receive. The applications included with the WISP transmit data in an unencrypted manner, and could potentially allow eavesdropping to where the attacker could intercept data. The WISP device will be used to demonstrate our scheduler and security methods in action on an RF-based energy harvesting platform. Our experiments will compare encrypting data using a modern stream cipher (Trivium) and XOR encryption. The Trivium stream cipher is one of the modern stream ciphers currently accepted in the eSTREAM project, where they host a number of accepted stream ciphers for high throughput or embedded applications [3]. XOR encryption is a fallback routine, where this encryption will be used instead when the device determines there is not enough energy to encrypt using Trivium. The user will also receive an indication of which algorithm was used on each output for proper decryption. This paper prototypes an energy-aware scheduler based on the works of Chae et al. [5] that allows the WISP device to send data in the most secure method based on the measured voltage, while investigating energy and timing constraints.

Our proposed system is feasible as cryptography tests [5] were performed on the WISP to demonstrate the capabilities of the platform to provide encryption under energy harvesting constraints. Along with cryptography tests, low power mode features were tested to allow the device to consume less energy. Other influences on distance, RF-based energy harvesting, and device capabilities used in the schedulers were mentioned in the works of Parks and Smith [6], Parks et al. [7], and the microprocessor's datasheet [17]. Aside from the WISP device, we should note that our scheduler can also be prototyped onto other RF-based platforms. Also, the scheduler can implement secure functions other than Trivium and XOR encryption. Nevertheless, there are several specific challenges of prototyping our scheduler such as how WISP can execute modern stream cipher functions, and how these secure functions work when the device is in long ranges, how to distribute sensor data in a secure and energy efficient manner.

The remainder of this paper is designed as follows. Section 2 will discuss constraints related with energy harvesting and security, as well as offering some related work to the experiments done in this paper. Then, Section 3 will demonstrate the energy aware and the timing aware schedulers and its algorithms. Section 4 will prototype these schedulers onto a real RF-based harvesting platform device (WISP). The results of these schedulers will be shown in Section 5. Finally, Section 6 concludes this paper.

2. Background and related work

This section will discuss constraints that are faced with embedded devices in terms of security and energy harvesting. Also, some related work will be discussed to demonstrate similar projects within the scope of this paper. Section 2.1 discusses on certain challenges of energy harvesting on RF-based platforms. Section 2.2 discusses the security functions that will be used in the experiments. Section 2.3 discusses related work.

2.1. Energy harvesting

With a RF-based platform, there are concerns over energy consumption and harvesting when implementing such demanding applications. RF-based platforms must compensate for the limited energy available to harvest and realize the energy consumption used in applications for reliable communication and data integrity. The process in how WISP devices function for instance involves harvesting energy from an RFID reader, such as an Impinj Speedway R1000. Applications for the RFID reader can either involve remote access to the reader, or a program designed by the WISP developers called SLLURP [16]. These two programs will enable the reader to wirelessly send power to such